

Державний університет телекомунікацій

Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М.

Мережі бездротового широкосмугового доступу

Навчальний посібник

Київ 2015

УДК 621.396.2
П217

Рецензенти:

Романюк В.А. доктор техн. наук,
Військовий інститут телекомунікацій та інформатизації НТУУ «КПІ»
Гряник М.В., доктор техн. наук
технічний директор компанії Freenet

Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. **Мережі бездротового широкосмугового доступу.**
Навчальний посібник. – К.: ДУТ, 2015. – 196 с.

В навчальному посібнику розглянуті принципи побудови логічної і фізичної структури бездротових мереж передачі інформації, включаючи персональні мережі стандартів Bluetooth, IEEE 802.15.3 (3a), локальних бездротових мереж стандартів IEEE 802.11, регіональних мереж широкосмугового фіксованого та мобільного радіодоступу сімейства стандартів IEEE 802.16-2004 та IEEE 802.16e-2005.

Видання призначено для студентів, які навчаються за напрямом „Радіотехніка”. Він також буде дуже корисний для аспірантів, інженерів та наукових співробітників, які спеціалізуються у застосуванні, проектуванні та дослідженні систем та комплексів радіозв'язку та їх елементів.

УДК 621.396.2
П217

@ Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. 2015

Зміст

Вступ.....	5
Розділ 1. Стан та перспективи розвитку систем та мереж бездротового доступу.....	7
1.1 Класифікація мереж бездротового доступу.....	7
1.2 Стан і перспективи розвитку бездротових телекомунікаційних технологій.	11
1.2.1 Ринкові аспекти.....	11
1.2.2 Технологічні аспекти.....	13
Розділ 2. Сучасні технології побудови комп'ютерних мереж.....	29
2.1 Принципи побудови сучасних комп'ютерних мереж.....	29
2.1.1 Концепції та термінологія.....	29
2.1.2 Рівні ієрархії телекомунікаційних протоколів.....	33
2.1.3 Обладнання комп'ютерних мереж.....	44
2.2 Сучасні та перспективні мережні технології.....	56
2.2.1 Технології побудови локальних мереж.....	56
2.2.2 Технології побудови глобальних мереж.....	70
2.3 Канали зв'язку в сучасних комп'ютерних мережах.....	94
2.3.1 Сучасний стан розвитку каналів передавання даних.....	94
2.3.2 Характеристики каналів зв'язку в комп'ютерних мережах.....	96
2.3.3 Технології побудови каналів зв'язку на основі СКС для комп'ютерних мереж.....	106
Розділ 3. Бездротові локальні мережі стандартів IEEE 802.11.....	109
3.1 Основні принципи побудови та функціонування мереж IEEE 802.11.....	111
3.2 MAC-рівень стандарту IEEE 802.11.....	113
3.3 Фізичний рівень стандарту IEEE 802.11b.....	117
3.4 Особливості стандарту IEEE 802.11a.....	123
3.5. Характеристики базового обладнання мереж Wi-Fi.....	127
Розділ 4. Персональні бездротові мережі.....	136
4.1 Технічні аспекти побудови і функціонування мереж персонального зв'язку технології Bluetooth.....	136
4.1.1 Стандарти Bluetooth і Home RF.....	136
4.1.2 Архітектура і логічна структура мереж Bluetooth.....	137
4.1.3 Структура пристроїв Bluetooth.....	142
4.1. 4 Типи антен для мереж Bluetooth.....	144
4.2 Високошвидкісні персональні мережі стандарту IEEE 802.15.3(3a)..	147
4.2.1 Специфікація IEEE 802.15.3.....	147
4.2.2 Надшвидкісні персональні мережі IEEE 802.15.3a.....	149
4.3 Низькошвидкісні мережі стандарту IEEE 802.15.4 (ZigBee).....	153

Розділ 5. Мережі широкосмугового бездротового доступу сімейства стандартів IEEE 802.16 (WiMAX).....	157
5.1 Структура та особливості стандарту IEEE 802.16-2004.....	157
5.1.1 Загальні аспекти.....	157
5.1.2 Фізичний рівень стандарту IEEE 802.16-2004.....	158
5.1.3 MAC-рівень стандарту IEEE 802.16-2004.....	166
5.1.4 Керування з'єднаннями в мережах фіксованого доступу IEEE 802.16.....	169
5.1.5 Mesh-мережі.....	170
5.1.6 Формат заголовку MAC-рівня.....	174
5.2 Мережі WiMAX мобільного доступу IEEE 802.16e.....	184
5.2.1. Загальний огляд.....	184
5.2.2. Базова мережна модель для мобільних систем зв'язку.....	185
5.2.3. Визначення дальності на основі OFDMA.....	192
5.2.4. Попередня аутентифікація.....	196
5.2.5. Механізм керування потужністю.....	197
5.2.6. Шифрування відновлень CID.....	198
5.2.7. Порядок розподілу IP-адрес.....	199
5.2.8. Формування кадру OFDMA.....	199
5.3 Ринок мережевого та абонентського обладнання стандарту IEEE 802.16 в Україні та країнах СНД.....	202
Література.....	209

ВСТУП

З недавніх пір людина і комп'ютер стали просто нерозлучні. Спочатку комп'ютери були кожний по собі, потім їх об'єднали в локальну мережу, потім - у глобальну. Об'єднання окремо вартих комп'ютерів у групи дозволило досягти небачених висот як у технологічному плані, так і у свідомості людини. Існують різні типи й способи побудови комп'ютерних мереж. Однак в останні роки усе перспективніше стають мережі, побудовані за допомогою радіотехнологій, що дозволяють придбати максимальну мобільність і незалежність.

В даний час очевидно, що бездротові мережі практично знаходяться поза конкуренцією по оперативності розгортання, мобільності, ціні і широті можливих додатків, у багатьох випадках будучи єдиним економічно виправданим рішенням.

Для України в якій велика територія поєднується з відносно невисокою щільністю населення, бездротові рішення мають особливе значення, оскільки дозволяють економічно і оперативно створювати вітчизняну телекомунікаційну інфраструктуру на обширних територіях.

У зв'язку з цим вельми актуально є видання книги, де б в систематизованому вигляді були відображені стан і тенденції розвитку технологій радіодоступу. В даний час, не дивлячись на достатньо велику кількість літератури по телекомунікаційним системам і мережам в Україні, видань присвячених питанням особливостям побудови і функціонування сучасних і перспективних технологій радіодоступу явно не достатньо. Даний навчальний посібник покликаний заповнити цю прогалину.

В ньому розглянуті бездротові мережі стандартів Bluetooth, IEEE 802.15.3 (3a), локальних бездротових мереж стандартів IEEE 802.11, регіональних мереж широкосмугового доступу стандартів IEEE 802.16-2004 та IEEE 802.16e-2005.

Автори даного посібника являються відомими фахівцями в галузі проектування і упровадження бездротових мереж передачі інформації. В основу даного видання покладені отримані ними теоретичні результати і досвід створення локальних і регіональних широкосмугових бездротових мереж. Особливу цінність представляють матеріали, що відображають досвід впровадження та технічної експлуатації широкосмугових систем IEEE 802.16-2004 в країнах Прибалтики, Казахстану та Росії вітчизняними фахівцями ТОВ «НТУ Сервіс».

Незважаючи на те, що за останні роки ситуація з виданням вітчизняної літератури по новим інформаційно-комунікаційним радіотехнологіям трохи покращилася й були видані навчальні посібники [90, 97-100, 107,108], вона все-таки залишає бажати кращого. Зокрема, гостро відчувається недолік методично пророблених видань, тому що в багатьох навчальних посібниках або занадто коротко й недостатньо

глибоко зачіпається досліджуване питання, або вони являють собою конспект технічної документації.

Книга становить інтерес для організацій, фірм і фахівців, що розробляють і експлуатують сучасні бездротові системи доступу, або професійно займаються технічним обслуговуванням та експлуатацією систем радіозв'язку. Вона може бути служити навчальним і довідковим посібником для студентів радіотелекомунікаційних факультетів ВНЗів і слухачів центрів підвищення кваліфікації.

На закінчення хотілося б подякувати всіх спеціалістів компанії «НТУ Сервіс», добродійним впливом яких ця книга здійснилася. І особлива вдячність генеральному директору компанії «НТУ Сервіс» Літвінову Ю.М., який брав активну участь при обговоренні розділів 4-6 і докторам технічних наук Грянику М.В. і Романюку В.А. за підтримку й коштовні ради при написанні книги.

РОЗДІЛ 1 СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ ТА МЕРЕЖ БЕЗДРОТОВОГО ДОСТУПУ

1.1 Класифікація мереж бездротового доступу

Мережі бездротового доступу призначені для бездротового доступу абонентів до стаціонарних мереж, які засновані на інфраструктурі оптоволоконних або кабельних мереж.

Класифікацію мереж бездротового доступу можна провести за наступними критеріями:

- За масштабом охопленої території.
- За видом зв'язків абонентів у мережі.
- За використовуваною технологією.
- За швидкістю переданої інформації.
- За діапазоном використовуваних частот.
- За економічними показниками.

За **масштабом охопленої території** мережі бездротового доступу поділяються на:

- Мережі персонального зв'язку (Personal Area Network - PAN). Площа, охоплена такою мережею, не перевищує декількох квадратних метрів (дальність зв'язку - до 10 - 15 метрів). За допомогою таких мереж здійснюється підключення до кабельної або бездротової локальної мережі, а також приєднання різноманітних периферійних пристроїв до системних блоків комп'ютерів.
- Локальні бездротові мережі (Wireless Local Area Network - WLAN) забезпечують зв'язок на відстані до кількох сотень метрів і служать для об'єднання в мережі груп комп'ютерів в офісах і підключення їх до мереж більшого масштабу, наприклад, до мережі Інтернет.
- Мережі міського або районного масштабу (Wireless Metropolitan Area Network - WMAN) дозволяють охоплювати абонентів у радіусі кілька кілометрів або десятків кілометрів від базових станцій мережі.

За **видом зв'язку** мережі бездротового доступу поділяються на:

- Мережі виду «крапка - багатокрапка», коли зв'язок всіх абонентів зі стаціонарною мережею й абонентів один з одним здійснюється через центральну «крапку доступу» або «базову станцію». Схема такої мережі виглядає у вигляді зірки.
- Мережі із прямим або опосередкованим з'єднанням абонентів між собою, іноді називані мережами Ad Hoc. Зв'язок зі стаціонарними мережами може здійснюватися як безпосередньо кожним абонентом (при наявності

радіовидимости), так і через один або декілька абонентів, безпосередньо з'єднаних з такими мережами. При цьому використовується взаємна ретрансляція сигналів абонентами, тобто зв'язок здійснюватися декількома передачами від абонента до абонента. У таких мережах реалізуються мережні протоколи, що включають у собі механізми самоорганізації мереж.

У мережах радіодоступу використовуються різні технології фізичного (сигнального) рівня. Їхньою загальною рисою є використання широкосмугових сигналів, тобто сигналів, смуга частот яких в ефірі істотно перевищує смугу частот переданого інформаційного сигналу. Такий вид сигналів пов'язаний з отриманою К. Шенноном формулою швидкості передачі по каналу зв'язку, у якій показано, що ця швидкість пропорційна займаній сигналом смугою частот.

У наш час використовується три основних способи розширення смуги частот радіосигналу - за допомогою скачкової зміни частоти сигналу (англ. Frequency Hop Spread Signal - FHSS); за допомогою зміни фази одночастотного сигналу відповідно до коду полоснорасширяющей послідовності (Direct Sequence Spread Spectrum - DSSS) і шляхом застосування безлічі сигналів на ортогональних (незалежних) несучих (Orthogonal Frequency Digital Multiplexing - OFDM). Останнім часом розширюється застосування в мережах радіодоступу надширокосмугових сигналів (Ultra Wide Band - UWB), заснованих на генерації коротких імпульсів без несучих частот.

Всі прийняті до впровадження й розроблювальні технології стандартизовані або стандартизуються для сумісності устаткування різних виробників. Найменування стандартів пов'язані з організаціями або асоціаціями організацій, якими вони були розроблені.

Найпоширенішими технологіями фізичного (сигнального) рівня є наступні:

Технологія **Bluetooth** (стандарт Міжнародного Інституту електричних і електронних інженерів **IEEE 802.15.1**) призначена для персональних мереж, тобто мереж у межах однієї або декількох кімнат будинків [73,74]. Фізично типовий Bluetooth пристрій являє собою радіоприймач і радіопередавач, що працюють на частотах 2400-2483,5 МГц. Ці частоти обрані не випадково, вони є відкритими й вільними від усякого ліцензування в більшості країн світу (Україна не входить у їхнє число).

Використовувані частоти визначають можливості Bluetooth по передачі даних. Ширина каналу для Bluetooth пристроїв становить 723,2 кбіт/с в асинхронному режимі (втім, навіть у цьому режимі все-таки залишається

до 57,6 кбіт/с для одночасної передачі у зворотному напрямку), або 433,9 кбіт/с у повністю синхронному режимі. Якщо не передаються дані, то через Bluetooth з'єднання можна передавати до 3 аудіоканалів. Кожний з аудіоканалів підтримує по 64 кбіт/с синхронному аудіоканалі в кожному напрямку. Крім цього, можлива й комбінована передача даних і голосу.

Головною особливістю Bluetooth є те, що різні Bluetooth пристрої з'єднуються один з одним автоматично, як тільки вони з'являються в межах досяжності.

Стандарт **IEEE 802.11b**, відомий також як Wi-Fi (wireless fidelity) або бездротова локальна мережа (WLAN), був прийнятий в 1999 р.[27-47, 75-82]. У якості базової радіотехнології в ньому використовується метод DSSS з 11-розрядними послідовностями Баркера. Завдяки високій швидкості передачі даних (до 11 Мбіт/с), практично еквівалентній пропускній здатності звичайних провідних ЛС Ethernet, а також орієнтації на "освоєний" діапазон 2,4 ГГц, цей стандарт завоював найбільшу популярність у виробників устаткування для бездротових мереж.

Мережі цього стандарту побудовані за принципом «крапка - багатокрапка», тобто є базові станції (Hot Spot), підключені до кабельних мереж, і, що розташовуються навколо них абонентські станції (стаціонарні й переносні комп'ютери).

Крім стандарту 802.11b застосовуються стандарти **802.11a** і **802.11g** [58]. Перший зі стандартів використовує OFDM у діапазоні 5 ГГц, другий - є комбінацією стандартів 802.11b і 802.11a і адаптований для роботи в діапазоні 2,4 ГГц. У цьому стандарті можливий зв'язок за технологією 802.11b (швидкість до 11 Мбіт/с) і 802.11a (швидкість до 54 Мбіт/с).

Стандарт **802.16** відомий як WiMax [1-13, 48-67, 83-89]. Він забезпечує обмін даними зі швидкістю до 54 Мбіт/с на відстані до 50 км від базових станцій, тобто ставиться до регіональних або муніципальних масштабів. У ньому використовується технологія OFDM. У режимі OFDM передбачена одночасна передача на 256 піднесучих, що дозволяє, за рахунок збільшення приблизно в таку ж кількість разів, тривалості елементарного символу, одночасно приймати прямий і відбитий від перешкод сигнали або взагалі працювати тільки по відбитих сигналах поза межами прямої видимості. Режим OFDMA передбачає роботу на 2048 піднесучих у режимі відразу з декількома абонентами, OFDM. При стандартній кількості піднесучих - 256, забезпечується одночасна робота з 8 абонентами.

Передбачено режими тимчасового й частотного дуплекса. Вид модуляції й кодування можуть змінюватися адаптивно від пакета до пакета індивідуально для кожного абонента, що дозволяє збільшити реальну

пропускну здатність приблизно вдвічі в порівнянні з неадаптивними системами. Передбачена рандомізація, завадостійке кодування й три методи модуляції: QPSK, 16QAM і 64QAM. Максимальна швидкість передачі, передбачена в стандарті - 134,4 Мбіт/с при смузі 28 МГц і модуляції 64 QAM. Система призначена для роботи в різних ділянках діапазону частот 2-11 ГГц.

Технологія використання **надширокосмугових сигналів UWB** (стандарт IEEE 802.15.4a) заснована на передачі безлічі закодованих імпульсів не гармонійної форми дуже малої потужності (0,05 мВт) і малої тривалості в широкому діапазоні частот (від 3,1 до 10,6 ГГц). Передача даних на відстань до 5 метрів (персональні мережі) здійснюється зі швидкістю від 400 до 500 Мбіт/с. Зв'язок на більші відстані обмежена випромінюваною потужністю відповідно до вимог адміністрацій зв'язку багатьох країн, що побоюються перешкод від таких сигналів традиційним системам радіозв'язку [30-41, 90-94].

За допомогою UWB-технології можна створювати спеціальні мережі, у яких трохи надширокосмугових пристроїв зможуть підтримувати зв'язок між будь-якими вузлами. Короткі сигнали UWB порівняно стійкі до багатопрменевого загасання, що виникає при відбитті хвилі від стін, стелі, будинків, транспортних засобів. Високошвидкісні UWB-пристрої добре підходять для роботи з відеопотоками й додатками, що вимагають швидкого пересилання даних. Низкошвидкісне UWB обладнання може застосовуватися для відстеження місця розташування на місцевості власників бездротових пристроїв і різних об'єктів.

Економічна оцінка застосування мереж радіодоступу зв'язана з вартістю устаткування, що, у свою чергу, пов'язана з масовістю виробленого устаткування. Зазначені вище системи радіодоступу є найпоширенішими й, отже, оптимальні з економічної точки зору.

1.2 Стан і перспективи розвитку бездротових телекомунікаційних технологій

1.2.1 Ринкові аспекти

На сьогодні інтерес багатьох до бездротового доступу визначається вступом телекомунікацій у новий етап свого технологічного розвитку й відповідною трансформацією бізнес-середовища галузі. Перехід до інформаційного суспільства супроводжується конвергенцією мереж, глобалізацією й персоналізацією телекомунікаційних послуг.

Все виразніше стає тенденція переходу користувачів від споживання й поширення інформації через канали загального використання до створення індивідуального інформаційного середовища й власного потоку контенту. У держсекторі вона проявляється в створенні “електронних урядів”, розвитку телемедицини й теленавчання. У бізнесі підтверджується широким використанням корпоративних мереж. Для населення центром одержання основної інформації, спілкування й розваги усе більше стає Інтернет.

«Розсмакувавши» нові можливості інфокомунікаційних технологій (ІКТ), споживачі вже висунули тезу “все, завжди й усюди”. Точніше, першими його висунули провідні світові виробники обладнання зв'язку. Для них технології роздільної передачі голосу й даних переходять у клас повсякденної рутини, і практично все нове обладнання, яке пропонують вендери, реалізує комплексні інтегровані рішення на основі пакетних технологій.

Влада голосових послуг фіксованої телефонії, як і можливість росту операторів на традиційних ринках, скорочуються. Освоюючи ІР-рішення, найбільші світові оператори переорієнтуються з послуг голосового зв'язку на надання користувачам доступу до всіх видів трафіку й контенту по одному каналу, сподіваючись за рахунок залучення ІКТ-послуг високої якості підвищити своє ARPU. Більшість переконана, що основним генератором зростання доходів стануть мультимедійні послуги мультисервісних ІР-мереж, особливо відеопослуги (поширення телерадіопрограм, відео на вимогу, надання мобільного ТВ-контенту й т.п.). А експерти прогнозують практично рівні внески в доходи галузі від голосових послуг, доступу в Інтернет і відеопослуг уже в близькому майбутньому.

Передача різних видів цифрової інформації поступово нівелює технологічні особливості компаній різних сегментів ринку й приводить до росту конкуренції між операторами. Телефонні компанії починають конкурувати з кабельними, оператори КТБ – надавати послуги телефонії й доступу в Інтернет, Інтернет-провайдери (наприклад, Google) - надавати відео- і голосові послуги, а оператори бездротових мереж опановують весь спектр послуг фіксованого зв'язку.

Одночасно стають помітними й тенденції консолідації операторів, що раніше працювали в різних сегментах ринку, а також поглинання вендерами виробників нішевих продуктів і рішень. Наприклад, 2 грудня 2005 р. компанія Alcatel, яка являється основним постачальником обладнання для швидкісного доступу (за даними компанії Dell'Oro, у середині 2005 р. Alcatel контролювала 32,3 % його ринку, а Huawei - 13,2 %), оголосила про придбання 25 % акцій 2Wire - розробника широкосмугових домашніх мережних рішень - для того, щоб розширити підтримку послуг Triple Play і прискорити їх розповсюдження.

У світі наростає й попит на рішення широкосмугового доступу (ШД). Розширення проникнення ШД дає будь-якій країні серйозний шанс для посилення свого потенціалу. У розвинених країнах він уже став одним з наріжних каменів побудови інформаційного суспільства, і уряди вкладають гроші в державні програми по його проникненню "у кожний будинок". І це зовсім не альтруїзм, вони сподіваються й навіть упевнені у величезній віддачі. Наприклад, за оцінками провідного американського економіста Роберта Э. Литана, тільки в сфері охорони здоров'я розвиток ШД, а на його основі телемедицини, заощадять США 927 млрд. дол., а у випадку прискореного проникнення швидкісних каналів обміну інформацією - ще півтриліона доларів. Хоча ці цифри й мають потребу в уточненні, проте зрозуміло, що загальний ефект від повсюдного проникнення ШД буде величезний.

Всі ці фактори зробили високошвидкісні мережі зв'язку й широкосмуговий доступ в Інтернет секторами світових телекомунікацій, які найшвидше розвиваються.

За оцінками фахівців, світова абонентська база ШД подвоюється щорічно й уже в першій половині 2005 р. значно перевищила 100 млн. користувачів. У лідерах тут Китай, де, за даними Міністерства інформатики, уже 53 млн. абонентів широкосмугового зв'язку, а в розрахунку на родину (домогосподарство), попереду всіх - Корея й Сінгапур. У Європі, де багато країн прийняли державні програми підключення до ШД організацій і домогосподарств, аналітична компанія Research and Markets нарахувала 47 млн. Користувачів ШД. Серед лідерів по впровадженню ШД - Бельгія, Нідерланди, Данія й Швеція, а по темпах росту попереду Великобританія й Франція.

Поряд з основними світовими технологіями ШД — мережами кабельного телебачення й DSL-каналами, останнім часом посилюється проникнення волоконно-оптичних і бездротових рішень. Експерти очікують, що в США в 2007 р. ринок бездротового широкосмугового доступу (БШД) досягне 5 млрд. дол.

Підвищена увага до ефірних видів доступу концентрується навколо послуг стандартів 3G, Wi-Fi і, особливо, WiMAX. Корпорація Intel домоглася того, що технологія Centrino для мобільних ПК стала однією з швидко впроваджуваних у світовій історії комп'ютерів.

Критики Wi-Fi вважають, що ця технологія по функціональності серйозно уступає не лише локальним мережам, але й EV-DO і WiMAX, а орієнтація на людей з низьким доходом підштовхує територіальні мережі загального доступу до фінансового краху, як це трапилося в Орландо (США). Там муніципальні влади відмовилися платити 1800 дол. на місяць за підтримку Wi-Fi, оскільки з 1,8 млн. жителів мережею користувалося не більше 27 чоловік у день.

Виробники вважають, що задовольнити практично будь-які потреби в доступі операторів швидкісних широкосмугових мереж і забезпечити високошвидкісний доступ в Інтернет скрізь, де відсутні кабельні й провідні мережі, може WiMAX. Проте до масового впровадження цієї технології ще необхідно забезпечити сумісність пристроїв і обладнання різних виробників, гармонізувати частотні діапазони для цього стандарту, хотілося б мати й побільше позитивних прикладів його застосування.

На початку грудня 2005р. IEEE схвалила дванадцятку редакцію стандарту мобільного WiMAX (802.16e-2005). Новий стандарт дозволяє підтримувати зв'язок між нерухомою станцією й мобільним пристроєм, що перебуває в русі.

1.2.2 Технологічні аспекти

У світлі проведеного аналізу ринкових загальних тенденцій розвитку бездротових мереж сімейство існуючих технологічних рішень по бездротовим телекомунікаційним мережам, які поєднані стандартами, виглядає сьогодні так (рис. 1.1):

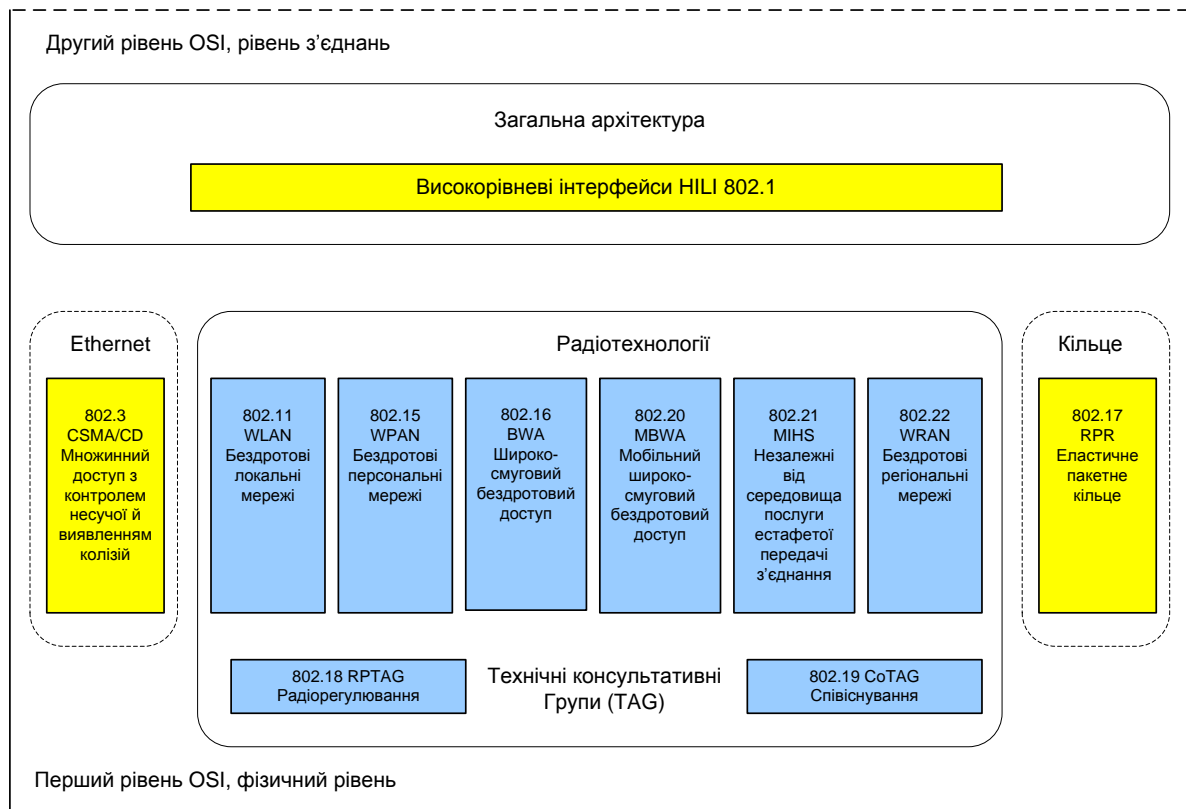


Рис 1.1 Огляд проектної групи IEEE P802, Комітету по стандартам для локальних і міських мереж

Як видно із рис. 1.1 радіотехнології переважають (синій блок):

- 802.11 - бездротові локальні мережі (Wireless Local Area Network, WLAN);
- 802.15 - бездротові персональні мережі (Wireless Personal Area Network, WPAN);
- 802.16 - бездротовий широкосмуговий доступ (Broadband Wireless Access, BWA);
- 802.18 - техніко-консультативна група по радіорегулюванню (Radio Regulatory Technical Advisory Group, RRTAG);
- 802.19 - техніко-консультативна група по співіснуванню (Coexistence Technical Advisory Group, CTAG);
- 802.20 - мобільний широкосмуговий бездротової доступ (Mobile Broadband Wireless Access, MBWA);
- 802.21 - незалежні від середовища послуги естафетної передачі з'єднання (Media Independent Handover Services, MINS);
- 802.22 - регіональні бездротові мережі - використання телевізійних частотних діапазонів для передачі даних (Wireless Regional Area Network, WRAN).

В області радіомереж акцент зміщується на сегмент локальних і міських мереж. У локальних мережах справжній фурор зробив стандарт 802.11n, де визначаються радіомережі із продуктивністю 100 Мбіт/с. У

міських мережах основна увага приділяється мобільним додаткам. Недавно затверджений стандарт 802.16e здатний вплинути на спосіб життя сучасної людини: у майбутньому доступ до Internet стане можливий звідусіль, у тому числі в поїздах і автомобілях, що рухаються з високою швидкістю.

Необхідною умовою для цього є досягнення результатів, на які націлена група 802.21 (незалежні від середовища послуги естафетної передачі з'єднання). Мова йде про передачу з'єднання не тільки між двома радіомережами одного типу, але й між радіомережами, побудованими на основі різних технологій.

Досить цікава також діяльність групи 802.22 (регіональні бездротові мережі). Цифровізація наземного телебачення (DVB-T) веде до звільнення частотних діапазонів, внаслідок чого виникає природне бажання використати їх у майбутньому для передачі даних.

Бездротові локальні мережі

У сфері бездротового зв'язку, як і колись, домінуюче положення займає група 802.11 (рис. 1.2), де недавно був підготовлений стандарт 802.11e для підтримки якості послуг (Quality of Service, QoS). Через швидке заповнення частотних діапазонів у не ліцензованих смугах 2,4 і 5,6 ГГц галузь потребує найшвидшої появи цих функцій, оскільки вони у край необхідні для надання якісних послуг, наприклад для передачі голосу по IP (Voice over IP, VoIP) по бездротових мережах.

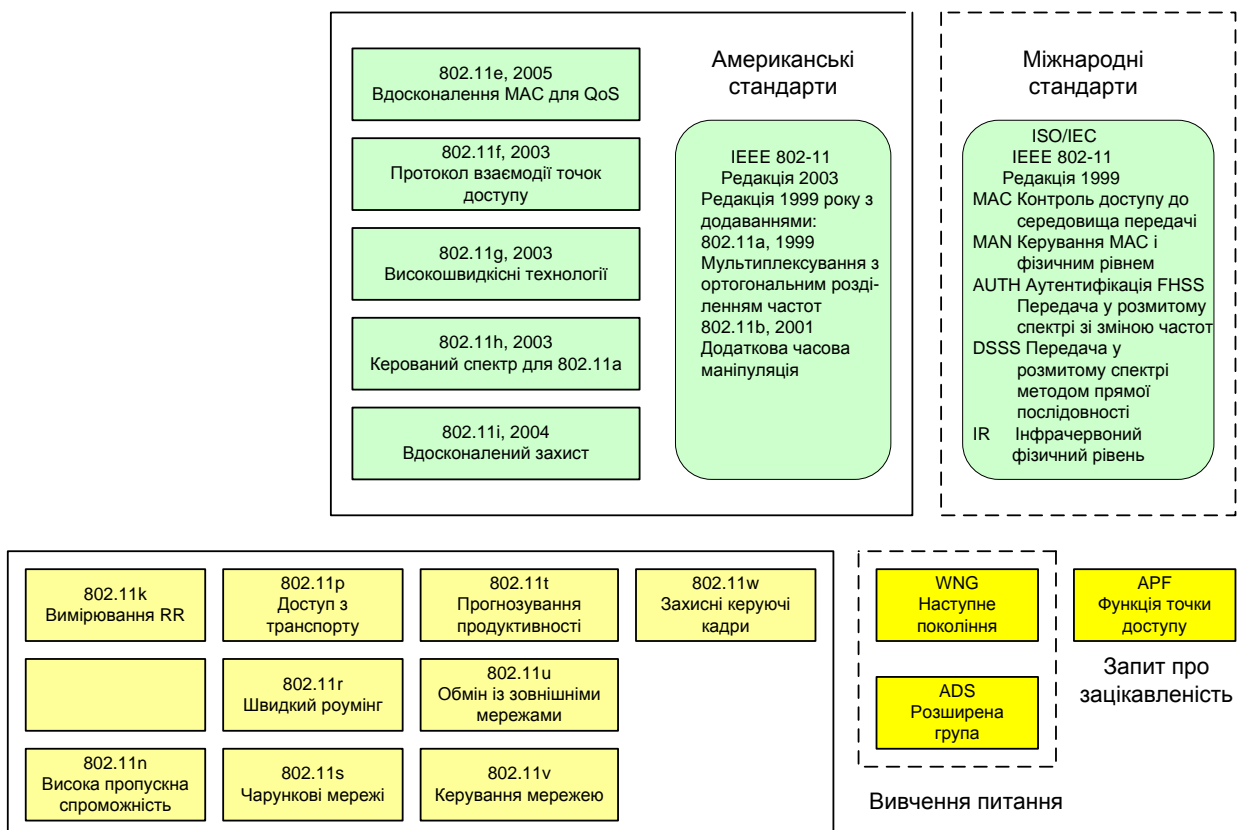


Рис 1.2 Стандарти і проекти 802.11 (бездротові локальні мережі)

Найгарячішою темою в області бездротових мереж є технологія передачі даних зі швидкістю 100 Мбіт/с (802.11n). Хоча сьогодні численні виробники й пропонують інтерфейси з відповідною функціональністю, але мова, на жаль, іде про рішення, що не відповідають стандартам. Тим часом двом досі непримиренним таборам MIMO у Комітеті по стандартизації (TGn Sync і WWISE) удалося все-таки досягти компромісу. Прийнята спільно пропозиція нарешті задасть напрямок для подальшої роботи. А виходить, є надія, що відповідний стандарт все-таки з'явиться - однак поки не ясно, чи відбудеться це цього року.

Нових стандартів можна чекати й від робочих груп 802.11u і 802.11w. Перед обома поставлені конкретні завдання, і зараз іде підготовка перших проектів. Група 802.11u (Wireless Interworking with External Networks) розробляє рішення по спільній роботі із зовнішніми мережами стандарту 802, наприклад UMTS. 802.11v (Wireless Network Management) визначає функції мережного керування для бездротових мереж. Крім того, в області керування група 802.11w (Protection of Management Frames) займається захистом керуючих з'єднань.

З 802.11 тісно співробітничає група 802.15 (Wireless Personal Area Networks), відповідальна за стандарт Bluetooth. Її ціль - розширення, а також звуження смуги пропускання. Останнє необхідно для того, щоб зменшити споживання енергії й тим самим підвищити час роботи пристроїв (приміром, датчиків). У процесі підготовки перебувають відповідні розширення й поліпшення стандарту 802.15.4 (Zigbee).

Бездротові міські мережі

Поряд з 802.11 у бездротовій області найбільшу активність проявляє група 802.16 (широкосмуговий бездротовий доступ) (див. рис. 1.3).

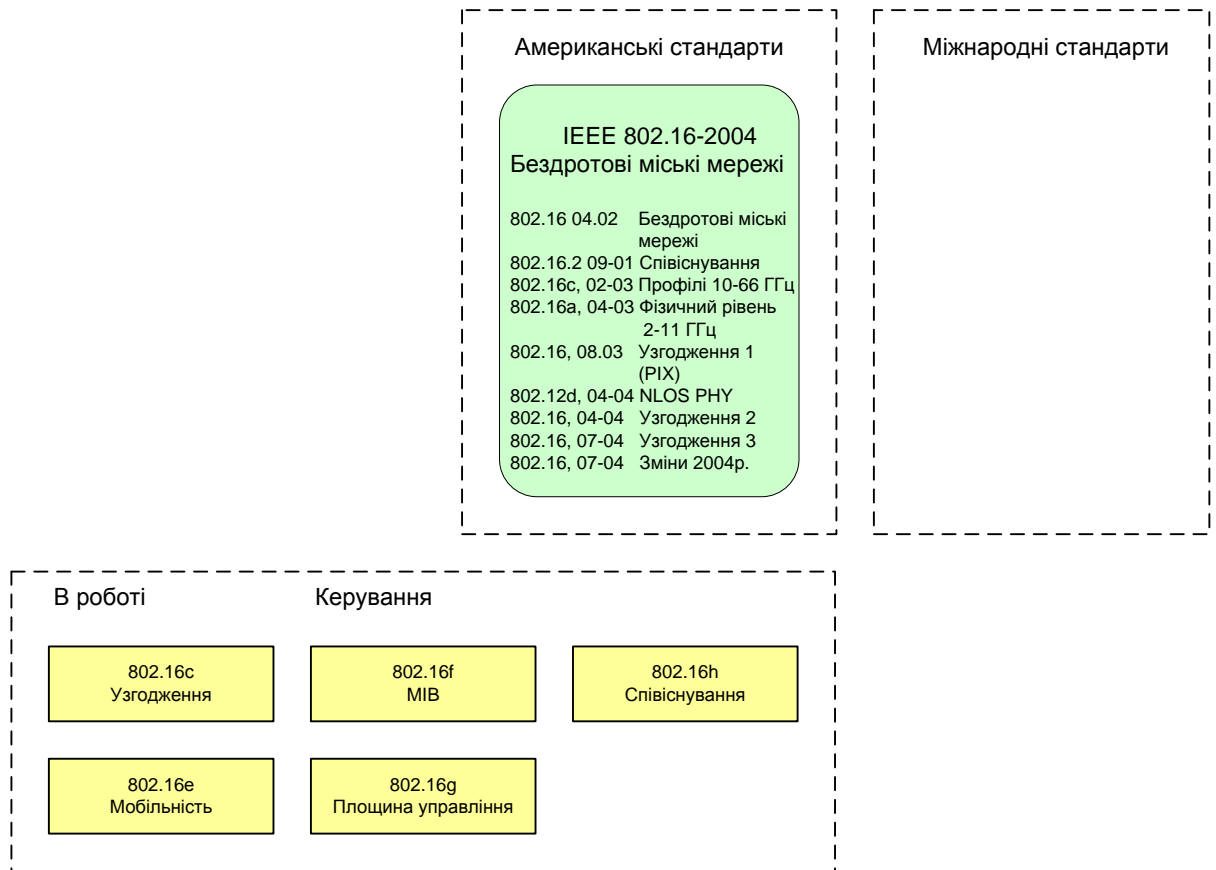


Рис 1.3 Стандарти та діяльність групи 802.16 (WiMAX)

Робоча група IEEE 802.16 була створена в 1999 р., а через два роки з'явився WiMAX-форум, утворений фірмами Nokia, Harris Corp., Ensemble і Crossspan. До середини 2005 р. форум об'єднав уже 230 учасників.

Стандарт IEEE 802.16 був схвалений у грудні 2001 р. і став першим стандартом в області WMAN, що реалізує топологію «точка-багатоточка». Спочатку він був орієнтований на частотний діапазон від 10 до 66 ГГц і передбачав наявність прямої видимості (LOS - Line of Sight), проте це було істотним недоліком у міських умовах. Прикладом такої системи є мережа радіодоступу компанії Ensemble, яка вже багато років використовується в Ризі (Латвія). За своїм характером це скоріше мережа LMSC, що працює в діапазоні 10 ГГц і забезпечує широкосмуговий радіодоступ у масштабах міста.

Першим закінченим стандартом можна вважати стандарт IEEE 802.16а, схвалений у січні 2003 р., який вмістив у себе відчутну кількість нових функцій. Насамперед понизився частотний діапазон і, як наслідок, він передбачав роботу поза прямою видимістю із множинними перевідбиттям, тобто в режимі багатопроменевого поширення й інтерференції сигналу (NLOS, Near або Non Line of Sight).

У липні 2004 р. був схвалений стандарт IEEE 802.16REVd, основна відмінність якого полягає у підтримці фіксованого офісного або

домашнього кінцевого термінального обладнання з технологією NLOS, що враховує у моделі радіоканалу наступні фактори:

- три типи кліматичних зон зі своїми умовами загасання при поширенні сигналу А, В і С;
- доплер-ефект, що виникає в середовищі поширення;
- фактор затримки, що виникає на прийомному кінці при поширенні сигналу;
- К-фактор, зв'язаний зі статистикою фіксованих або змінних рівнів сигналу;
- зменшення коефіцієнту підсилення антени в умовах каналів з перевідбиттям сигналу.

Крім того, ефективна робота в таких умовах забезпечується завдяки підтримці додаткових функцій боротьби із множинними перевідбиттями. Крім методів підвищення ефективності радіоканалів, які широко застосовуються (адаптивної модуляції (фазоманіпуляційного сигналу QAM_{xx}) - Adaptive modulation; застосування кодування для корекції помилок (Error correction); керування потужністю передавачів (Power control) використовуються спеціальні методи боротьби з інтерференційними перешкодами:

- технологія ортогонального частотного кодування OFDM;
- підканали (Sub-Channelisation);
- антени з гостро направленою діаграмою Directional antennas;
- поділ прийомних і передавальних антен (Transmit and receive diversity).

Прикладами реалізації таких систем є:

- CD 3000 компанії Granger TC у партнерстві з L3 Communication, що використовує технологію MIMO й OFDM, що підтримує на фізичному рівні 12 адаптивних режимів модуляції, що в 10 разів ефективніше, ніж 3G системи, а на MAC рівні забезпечує розширений ARQ, QoS і CoS, CBR і CIR, і здатна забезпечити зв'язок з об'єктами, що рухаються зі швидкістю до 30 миль/год;
- BreezeMAX компанії Alvarion, що відповідає вимогам IEEE 802.16 і ETSI HiperMAN, що використовує OFDM-256 у смузі до 14 МГц (партнерство з Alcatel і Intel);
- WiMAX Ecosystem компанії Fujitsu, що використовує OFDM- 256 у смузі до 20 МГц;
- SkyMAX компанії Siemens, що використовує OFDM-256 у смузі 14 МГц із можливістю розширення до OFDM-1024 і має розвинені механізми QoS (L2 IEEE 802.1p, L3 IPv4 DSCP і ToS) і Co (UGS, nrt-PS, rt-PS, BE).

Необхідно підкреслити, що в CD 3000 застосовується метод боротьби з інтерференційними перешкодами, який поки що не стандартизований в WiMAX, але досить ефективний для досягнення максимальних розмірів зони радіопокриття. Ефект досягається за рахунок використання просторового розходження інтерференційної картини і

декількох просторово рознесених антен на прийом і передачу (MIMO - Multiple Input Multiple Output), що дозволяє, за рахунок мажоритарного прийому істотно підвищити відношення сигнал/шум. Максимальний розмір стільника й невелика смуга робочих частот вигідно відрізняють цю систему від інших претендентів на реалізацію національних програм впровадження стандарту WiMAX.

У районах з високою потребою в пропускній здатності базової станції й значною абонентською щільністю більш ефективна система SkyMAX.

У грудні 2005 року Робоча група IEEE 802.16, що займається розробкою стандартів для міських мереж широкосмугового бездротового доступу (ШБД), оголосила про прийняття виправлень до стандарту 802.16-2004, що раніше пропонувалися в проектах IEEE 802.16e і 802.16f (виправлена версія стандарту IEEE 802.16-2004). У стандарті IEEE 802.16e робоча смуга частот розширена до 256 несучих (OFDM-256) для нарощування пропускної здатності й акцент зроблений на мобільність кінцевого користувача. Таким чином, стандарт був розповсюджений і на обладнання для мобільних мереж ШБД. У цей час Комітет по стандартам Інституту IEEE приступив до об'єднання документів, що описують стандарт 802.16-2004 і схвалені виправлення до нього.

Наприкінці січня 2006 року представники WiMax Forum повідомили про першу сертифікацію продуктів WiMax, що підтримують цю технологію. Це сумісні між собою готові вироби й досвідчені зразки обладнання для фіксованих мереж WiMax, що відповідають вимогам стандартів IEEE 802.16-2004 і European Telecommunications Standards Institute HiperMAN. Готові до застосування операторами зв'язку базові станції PacketMax 5000 і RedMax AN-100U представлені компаніями Aperto Networks і Redline Communications. Досвідчені зразки базової станції SQN2010 і пристроїв для кінцевих користувачів miniMax, створені відповідно компаніями Sequans Communications і Wavesat Inc., призначені для виробників мережного обладнання. Всі продукти працюють у частотному діапазоні 3,5 ГГц. Сертифікація 2,5-гігабітних пристроїв очікується пізніше.

З матеріалів Другої Всеросійської науково-практичної конференції, організованої консорціумом WiMAX Forum у грудні 2006 року при сприянні ряду учасників цієї організації, впливає що, у цей час ведеться активна робота, метою якої є включення WiMAX до складу стандартів IMT-2000 Міжнародного союзу електрозв'язку. Зараз в IMT-2000 входить п'ять технологій. Планується, що WiMAX стане шостий у цьому списку й одержить назву "IP-OFDMA". У рамках IMT розвивається проект IMT-Advanced, де вже фігурують швидкості доступу на рівні 1 Гбіт/с для стаціонарних абонентів й 100 Мбіт/с для мобільних пристроїв. Для реалізації відповідності із цими вимогами в рамках 802.16 планується почати роботу над проектом, що одержав умовну назву 802.16m. Одним з основних вимог до 802.16m стане підтримка встаткування стандарту

802.16e-2005. Зокрема, абонентські пристрої 802.16e-2005 повинні працювати з базовими станціями 802.16m, а базові станції стандарту 802.16e-2005 - мати можливість працювати в складі мережі 802.16m.

Якщо останній проект є справою досить віддаленого майбутнього, то над 802.16j (Multihop Relay) робота вже почалася з організації в травні 2006 року спеціальної робочої групи. Завдання проекту полягає в створенні ретрансляторів для збільшення зони покриття WiMAX-мереж. На даний момент робоча група розробила сценарії застосування нової технології, а також почала прийом технічних пропозицій. Як впливає з матеріалів виступів фахівців на конференції, технологія Multihop Relay може застосовуватися для подолання перешкод, поліпшення покриття усередині будинків, швидкого розгортання мереж у місцях надзвичайних ситуацій або проведення масових заходів, а також забезпечення зв'язку для пасажирів об'єктів, що рухаються (поїздів, автобусів, кораблів). З інших проектів, над якими ведеться робота в рамках стандарту IEEE 802.16, на конференції відзначені стандарти 802.16h й 802.16g. Перший з них присвячений побудові мереж у неліцензюваних діапазонах (наприклад, у США таким є діапазон 5,8 ГГц) - основним завданням у цьому випадку є створення механізмів з дозволу конфліктів. Другий присвячений проблемам керування мережею й зараз перебуває в стадії набору голосів для твердження.

Сертифікація мобільних пристроїв повинна початися на початку цього року, а перші сертифікаційні пристрої з'являться на ринку до середини 2007 року. Спочатку будуть сертифікуватися системи, що працюють у діапазоні 2,3 й 3,5 ГГц, а сертифікація систем 2,5 ГГц, у яких передбачено застосування адаптивних антенних систем, почнеться трохи пізніше - у середині 2007 року.

Після того як в 2004 р. був затверджений необхідний режим роботи в умовах відсутності прямої видимості (non Line of Sight, nLoS), все стало обернутися навколо аспекту мобільності (802.16e).

Виробники пристроїв стандарту 802.16 (базових станцій і обладнання для встановлення у клієнта) продемонстрували можливість взаємодії своїх пристроїв на форумі WiMAX, а цього року можна розраховувати на появу комерційних мереж стандарту 802.16 і в Європі. Далекий Схід пішов уже набагато далі: там під гаслом WiBro (Wireless Broadband - бездротовий широкопasmовий доступ) іде широкомасштабне розгортання технології 802.16.

Проте центральна тема – мобільність - розвивається не настільки гладко, як хотілося б, оскільки цим аспектом розпочала займатися й група 802.20 (мобільний широкопasmовий бездротовий доступ). Відповідно до уставу IEEE, робочу групу 802.20 не слідувало створювати зовсім, з огляду на те, що вже існувала 802.16e, яка до того ж встигла представити практично готовий стандарт, у той час як 802.20 лише починає роботу над своїм. Є підозра, що група 802.20 закінчить так само, як і група 802.12, яка так і не довела справу до кінця.

Ще одна проблема дублювання виникла у відносинах між групами 802.16 і 802.22 (бездротові регіональні мережі) - обидві у великій мірі зацікавлені у використанні потенціалу телевізійних частотних діапазонів, що звільняються. Однак варто враховувати, що на телевізійних каналах працюють і інші пристрої, наприклад бездротові мікрофони. Їх функціонуванню не повинне заважати обладнання, що знову з'являється. Останнє означає, що для використання цих каналів технологію 802.16 необхідно помітно розширити. Як рішення проблеми група 802.16, чого доброго, залишить телевізійний частотний діапазон групі 802.22, що застосовує технологію, сумісну з 802.16.

Варто також згадати про фурор, який зроблено в IEEE 802 німецькими фахівцями: за назвою WIGWAM (Wireless Gigabit with Advanced Multimedia Support - бездротова гігабітна передача з розширеною підтримкою мульти-медіа) була представлена гігабітна технологія, що в 2010 р. може стати новою сходинкою у розвитку бездротових технологій.

Європейський інститут телекомунікаційних стандартів ETSI і робоча група BRAN (Broadband Radio Access Networks) розробляють стандарт HIPERMAN, спрямований на:

- технологічне зближення Європи й США в області систем бездротової передачі даних;
- ліквідацію роздробленості на ринку мобільного зв'язку, обумовленою несумісністю стандартів;
- забезпечення взаємодії з IEEE 802.11.

В основу HIPERMAN на фізичному рівні покладений стандарт IEEE 802.16-2004. Деякі розходження спостерігаються на каналному (MAC) і мережному рівнях. Основну увагу ETSI приділяє типам додатків і якості послуг.

Робоча група IEEE 802.20 Mobile Broadband Wireless Access (MBWA), затверджена в грудні 2002 р., зосереджена на наданні послуг мобільним користувачам Інтернету, що рухається зі швидкістю до 250 км/ч. Перші зразки обладнання очікуються не раніше 2007 р.

Не чекаючи прийняття стандарту, оператори України, Європи, Америки, Росії й Азії впроваджують pre-WiMAX системи. Найбільші оператори таких систем - AT&T, Sprint Canada, T-Mobile.

Мережі стандарту WiMAX, безумовно, досить швидко вийдуть на ринок і створять конкуренцію іншим рішенням проблеми надання широкопasmового доступу, еквівалентного технології xDSL. Впровадження забезпечить швидке розгортання на досить великих територіях, що особливо актуально для місць із нерозвиненою мережною інфраструктурою (наприклад, нові заміські райони, історичні центри міст і т.п.).

Впровадження технології WiMAX в Україні істотно полегшить реалізацію проектів «Телефонізація й інтернетизація села», «Інтернет - у кожену школу» і т.д., дозволить гнучко й ефективно забезпечувати квартирний і комерційний сектори широкопasmовим доступом. Однак

відсутність чіткого стандарту, низька сумісність і відносно висока, у порівнянні з технологією xDSL, вартість обладнання стримують її розвиток. Крім того, частотний діапазон 2-11 ГГц є в Україні ліцензованим і відносно щільно зайнятим операторами мереж радіодоступу інших технологій. Тому системи WiMAX, що володіють максимальною гнучкістю й адаптивністю в частотно-територіальному плануванні, безумовно, виявляться головними претендентами на модернізацію існуючих систем радіодоступу.

Скільки вже було проведено дискусій в останні роки щодо розвитку технологій цифрового телебачення й пов'язані з ним питання про майбутнє мереж третього покоління й здавалося, що триумф мереж третього покоління (3G) от-от наступить, однак, поширення технологій бездротових мереж знову ставить їхнє майбутнє під сумнівом. Вся справа в тому, що повсюдне настання цифрової телефонії (VoIP), уже здатної використати, наприклад, Wi-Fi, а в перспективі - і WiMAX, що може стати доступною вже через рік-два, ставить під питання доцільність високої плати за ефірний час і «стільникові мегабайти». Не випадково росте інтерес і до такої технології, як UMA (Unlicensed Mobile Access), покликаної забезпечити бездротовий зв'язок, задіявши не ліцензовані частотні діапазони - у цьому випадку, 2,4 ГГц і технологію Wi-Fi. Philips, що продемонструвала референс-дизайн платформи UMA, також створила економічний і дуже компактний модуль Wi-Fi, втім, успіхів на цьому поприщі досягла не тільки Philips. Крім Wi-Fi в UMA, у принципі, можна також використати Bluetooth і навіть DECT, втім, до інтеграції останньої в мобільні телефони проявляють інтерес лише одиничні виробники й у вигляді досить специфічних рішень. Таким чином, Wi-Fi-мережі вже поступово наступають на 3G, а що ж буде потім, із приходом WiMAX?

Не можна списувати з рахунків і Bluetooth - чутки, що витали в повітрі про те, що Bluetooth у майбутньому об'єднається з UWB (технологіями ультраширококуткового зв'язку) і Wireless USB, виявилися правдою. Bluetooth SIG (Special Interest Group) навіть розробила відповідну «дорожню карту», щоправда, з одним застереженням - фізичний рівень UWB повинен бути один, а не два, які до того ж один з одним несумісні. Мова йде про застарілий вже конфлікт між прихильниками двох різних підходів до реалізації UWB — з використанням усього спектру (DS-UWB) і з розбиттям на піддіапазони (MBOA-UWB). Якщо останні (на чолі прихильників MBOA-UWB стоїть Intel), наприклад, «продавили» свої специфікації в якості базових для Wireless USB, то перші (за DS-UWB радіє група компаній на чолі з Freescale) уже навіть випустили адаптер для ПК, що підтримує як Bluetooth, так і DS-UWB. У тому випадку, якщо на озброєння галузі буде прийнятий один конкретний варіант фізичного рівня UWB, Bluetooth, що уже зараз можна використати в UMA, в 2007 року буде здатний забезпечити пропускну здатність порядку 480 Мбіт/с.

Можливо, що з появою технологій наступного, четвертого покоління (4G), ситуація зміниться на користь стільникових мереж - все-таки головна їхня перевага та, що більшу площу покриття не перевершила ніяка інша технологія. Компанія NTT DoCoMo, вже не раз дивувавши світ здібностями стандартів четвертого покоління (4G), провела чергові польові випробування, у ході яких була досягнута пропускна здатність, що дозволяє завантажити диск формату DVD менш ніж за хвилину. Пропускна здатність нового стандарту така, що при русі в межах міста на автомобілі зі швидкістю 20 км/год становить 100 Мбіт/сек, чого досить для перегляду потокового відео High-Definition (32 потоки відеоданих). Якщо ж абонент стоїть на місці, то швидкість обміну даними збільшується до 1 Гбіт/с. На сьогоднішній день мережі третього покоління (3G) DoCoMo надають швидкість завантаження даних 384 Кбіт/сек і швидкість відправлення 129 Кбіт/сек (цей показник характерний і для інших мереж, створених за технологією W-CDMA). Таким чином, приріст у пропускній спроможності мереж четвертого покоління в порівнянні з мережами третього покоління складе як мінімум 260 разів! Для того щоб досягти таких показників, був застосований метод кодування VSF-Spread OFDM (Variable-Spreading-Factor Spread Orthogonal Frequency Division Multiplexing), у якому потік даних передається одночасно в декількох частотних діапазонах. Крім того, застосовується підхід MIMO (multiple-input-multiple-output), який, до речі, використовується у бездротових мережах 802.11n. Метод MIMO передбачає передачу даних по різних маршрутах мережі - наприклад, передача даних на один мобільний термінал може вестися відразу із двох базових станцій (БС), за умови, звичайно, невеликої відстані відносно одна одної й абонента.

В Samsung вважають, що майбутнє саме за мобільною передачею даних і послугами в мережах 4G, які повністю засновані на протоколі IP. Компанія має намір просувати продукти й рішення WiMAX на світовий ринок і брати участь у міжнародній сертифікації Mobile WiMAX, що почнеться в 2007 р. У нинішньому році планується випуск устаткування WiBro і для інших частот (2,5, 3,5, 5 ГГц). Як повідомили в компанії, переговори про створення досвідчених зон подібних мереж у Росії вже йдуть, однак про конкретні проекти говорити поки рано. Тим часом у Москві діє дослідницький центр Samsung, де розробляється ПО, у тому числі й для мереж WiBro. Сьогодні вся інфраструктура доступу в таких мережах, включаючи термінальні пристрої, будується на обладнанні Samsung, проте у компанії стверджують, що з початком сертифікації на відповідність стандарту 802.16e проблем сумісності між обладнанням Mobile WiMAX від інших постачальників і WiBro не виникне. WiBro у стані забезпечувати обмін даними (до 30 Мбіт/с) на швидкості понад 90 км/год.

Компанія Samsung Electronics представила в жовтні 2006 року на виставці "Инфоком-2006" у Москві працюючу систему ширококутового

бездротового доступу (ШБД) стандарту IEEE 802.16e-2005, вірніше його модифікації, відомої за назвою WiBro.

За словами фахівців Samsung по системах і мережах зв'язку, термін WiBro скоріше застосуємо до назви мережі, уже розгорнутої в Кореї, а сама система повністю відповідає вимогам стандарту IEEE 802.16e-2005 і претендує в майбутньому на проходження сертифікації консорціуму WiMAX Forum.

Виробник позиціює свою систему ШБД як закінчене рішення, що включає в себе інфраструктурне встаткування, власну систему керування, деякі елементи IMS-платформи, а також абонентські пристрої. Основним функціональним компонентом цієї системи є базова станція (БС), що випускає в трьох варіантах: RAS (Radio Access Station) Standard - для районів із щільною забудовою, U-RAS Mini - для зон з низькою щільністю абонентів (сільські райони, шосе й т.п.), а також U-RAS HS - для застосування усередині будинків і споруджень (є можливість застосування розподілених антен).

Виробник випускає встаткування для діапазонів 2,3, 2,5 й 3,5 ГГц. Ширина радіоканалу в даний момент становить 8,75 й 10 МГц, готується до випуску встаткування із шириною каналу 5 й 7 МГц, а для БС RAS Standard - ще й 20 МГц. Пікова пропускна здатність БС RAS Standard, представленої на виставці "Инфоком-2006", становить 20 Мбіт/с на сектор (БС складається із трьох секторів). Роботою декількох БС управляє центр комутації ACR (Access Control Router). У даний момент випускається два види ACR - ACR Standard, здатний управляти більше 150 БС й ACR Mini (75 БС).

Як вище відзначалася, порівняно молода (на тлі мереж мобільного зв'язку третього покоління, які почали створюватися в 2000 році) технологія WiMAX досить швидко здобула собі популярність завдяки високій спектральній ефективності (кількості біт даних на одиницю частоти несучої). Вона навіть розглядалася деякими як потенційний кандидат в основу технологій мобільного зв'язку четвертого покоління. Однак, поки більшість промисловців настроєна скептично.

Так, навіть лобісти WiMAX, на чолі яких традиційно виступає корпорація Intel, визнали в ході щорічних зборів асоціації WCA (Wireless Communications Association), що ринкова частка WiMAX, швидше за все, буде невеликий, тому що більша частина ринку залишиться за LTE (Long Term Evolution) - сімейством технологій, що є розвитком стандарту GSM. До того ж, WiMAX як і раніше перебуває на старті: зараз уже існують 122 комерційні WCDMA-мережі в 55 країнах, що нараховують близько 70 млн. абонентів. По даним Bechtel Communications, про підтримку 802.16e (мобільного варіанта WiMAX) поки не оголосив ще жоден оператор.

Нарешті, є ще одна компанія -- Qualcomm, що заявила про плани демонстрації технології, яка забезпечує пропускну здатність 10 Мбіт/с і кращу спектральну ефективність, чим WiMAX. І Qualcomm не самотня у своєму прагненні знайти альтернативу WiMAX - аналогічні роботи

ведуться в Китаї й, можливо, що пілотний варіант широкопasmової мобільної мережі може бути запущений в експлуатацію до початку Літніх Олімпійських ігор у Пекіні в 2008 році.

Китайська альтернатива WiMAX побудована на базі технологій SCDMA (синхронно-кодового поділу каналів), також використовуваної в 450 МГц стандарті мобільного зв'язку TD-SCDMA, і зветься **McWiLL** (Multicarrier Wireless internet Local Loop). Повідомляється, що вже ведуться тестові випробування в декількох китайських містах, у числі яких — Гуанчжоу й Киндао. У тестові випробування вживають спроби передачі даних, потокового аудіо й відео. McWiLL сполучає традиційне для SCDMA використання вузькосmових голосових каналів і широкопasmову передачу даних. В McWiLL також використовується адаптивна модуляція CS-OFDMA, динамічний розподіл каналів, ФАР.

Стверджується, що при використанні 5 МГц каналів у діапазоні 1,8 ГГц, одна базова станція здатна забезпечити пропускну здатність до 15 Мбіт/с (що в п'ять разів менше теоретичного максимуму для WiMAX) на дистанціях від 1 до 3 км (у міських умовах). В 400 МГц діапазоні дальність зв'язку досягне від 20 до 60 км (у сільській місцевості), пропускну здатність буде, природно, набагато нижче. Клієнтський термінал, що задіє 1 МГц субканали, здатний одержувати дані зі швидкістю до 1 Мбіт/с і відправляти зі швидкістю 500 Кбіт/с, рухаючись зі швидкістю до 120 км/ч. Компанія Xipei, що розробляє технологію бездротового зв'язку, зараз готує до випуску кілька прототипів, серед яких вузли доступу, PCMCIA-плати й модулі для КПК. Також компанія розробляє прототип 3G/McWiLL-телефони.

Сьогодні над технологіями мобільного зв'язку четвертого покоління активно працюють не тільки в Японії, Кореї, Китаї, але й у Тайвані. За повідомленнями глави TW4G (Taiwan 4G), у країні буде розроблений тайваньський варіант 4G на основі бездротових мереж IEEE 802.16e (WiMAX). Для цього TW4G у співробітництві з Тайваньським науково-дослідним інститутом (ITRI, Industrial Technology Research Institute) веде роботи над стандартом, у якому використовуються IEEE 802.16e й 802.16j (MMR, Mobile Multi-hop Relay). Якщо ці роботи увінчаються успіхом, TW4G внесе свої пропозиції для стандартизації як міжнародний стандарт. Як й у багатьох інших бездротових технологіях, в TW4G використовується мультиплексування по ортогональним несучим (OFDM). Відомо також, що в розробці технології беру участь китайська ZTE, Samsung й Intel, а також члени альянсу MMR, у яких входять Motorola й Fujitsu UK. Для Intel, так, втім, і для Motorola, розробки тайваньців, мабуть, становлять найбільший інтерес, адже вже в найближчі роки на ринках Європи й, можливо, деяких країн Азіатсько-Тихоокеанського регіону очікується конкуренція технології передачі даних HSDPA у мережах мобільного зв'язку з бездротовими мережами IEEE 802.16e.

Відомо також, що японці усе тісніше співробітничать із китайцями в області 4G: порівняно недавно NTT DoCoMo створила науково-

дослідний центр для спільної роботи з китайськими компаніями, а на роботи в цьому напрямку китайський уряд уже виділило 18,7 млн. доларів і планує виділити ще 24,9 млн. Тестування південнокорейського варіанта 4G, побудованого на 802.20 з використанням OFDM почнеться в 2007 році.

Бездротові сенсорні мережі

Сьогодні концепції NGN і широкосмугового доступу забезпечують надання повного спектру послуг, які поєднують мовні послуги, передачу даних і доступ в Інтернет, цифрове мультимедіамовлення й інтерактивні аудіовідеопослуги. Виникає питання: «Що ж далі?» Які тенденції розвитку телекомунікацій? Наступний етап розвитку телекомунікаційної інфраструктури очікується в результаті створення так званих сенсорних мереж. Середовище, що реалізує прозорий доступ до будь-якого сенсору (датчику або контролеру датчиків), а також віддалене керування виконавчими механізмами, запропоновано називати BcN (Broadband convergence Network). Охват нею більше 10% населення країни можна вважати ознакою побудови і-суспільства (від англ. ubiquitous – скрізь проникаючий).

Тенденції даного напрямку розвитку чітко простежуються. У наш побут міцно ввійшли поняття:

- «розумний будинок», що поєднує автоматизовані комплекси керування системами життєзабезпечення будинків (WLAN/WiMAX);
- «бортовий комп'ютер» літака, автомобіля й т.д., що обробляє й аналізує показники датчиків (наприклад, остання модель BMW 7 серії поєднує на своєму борті близько 256 спеціалізованих комп'ютерів - контролерів) (WPAN/WiMAX);
- дистанційні системи відеоспостереження за транспортними потоками й виявлення ситуацій, що загрожують охороні правопорядку в рамках антитерористичних програм і концепцій «безпечне місто»;
- дистанційні системи спостереження за життєдіяльністю живих організмів, що дозволяють не тільки аналізувати міграції тварин, але й контролювати ключові параметри стану здоров'я хронічних хворих (хвороби серця, діабет і т.д.), яким може раптово знадобитися термінова медична допомога (WBAN/WPAN/WiMAX).

Остання тенденція є ключовою у розвитку мобільних мереж, тому що сенсорні мережі в сполученні з мережами мобільної передачі даних надають нову якість - мобільність дистанційної діагностики й чіткість позиціонування об'єкта, який обслуговується. Улітку 2005 року в Південній Кореї була проведена демонстрація прототипу бездротової сенсорної мережі (Wireless Sensor Networks - WSN), яка була розташована на людині й вирішувала наступні завдання:

- контроль індивідуальних таємниць, тобто динамічна біопараметрія (свого роду електронний паспорт на основі Badge Type

Computer);

- контроль медичних показників (аналіз пульсу по алгоритмах східної пульсодіагностики й т.п.);
- контроль напрямку руху;
- контроль доступу в приміщення, до комп'ютера й т.д.

Очевидно, що в силу масовості найбільш бурхливий розвиток сенсорних мереж варто очікувати в області бездротових технологій, які дозволяють розгорнути сенсорні мережі (мережні органи почуттів) на землі, у повітрі, над і під водою, у будинках і на живих організмах. Перспективи впровадження сенсорних мереж і масштабність їх використання в життєдіяльності людини й техніці дають підставу припускати появу значного по обсязі синтетичного трафіку, що змінює загальну структуру трафіку при переході до u-України.

Сучасні бездротові мережі повинні забезпечувати високу безпеку й низьку вартість і обладнання, і послуг, а також задовольняти новій парадигмі:

- відрізнитися високою масштабністю;
- бути реконфігурованими й адаптованими;
- застосовувати із кінця в кінець мережі пакетної комутації (протокол IP);
- прозоро (завжди, скрізь і в будь-яких умовах) надавати послуги мобільної передачі даних, незалежно від територіальної приналежності оператора й типу доступу бездротового середовища, що використовуються.
- Прозорість надання послуг може бути досягнута гармонізацією наступних рішень:
 - прозорість протоколу IP;
 - типи адресації (кожний термінал та/або користувач повинен мати унікальну адресу незалежно від поточного місця розташування й точки приєднання);
 - узгодження протоколів на всіх рівнях мережної моделі, насамперед на рівні сигналізації;
 - керування мобільністю (mobility management) як глобальна функція для автоматичного роумінгу й визначення відповідності між мережною адресою, що динамічно змінюється (точкою поточного приєднання) і статичним ім'ям терміналу;
 - керування місцезнаходженням (location management), що вирішує завдання: адресації, спостереження за місцезнаходженням, частоти відновлення службової інформації, персональної мікро- і макромобільності;
 - керування хендовером, що забезпечує ініціювання усередині- і міжсистемного хендовера, а також маршрутизацію сесії/з'єднання; керування сесією/з'єднанням (session management), що забезпечує безперервність сесії/з'єднання; керування ресурсами (resource management), що забезпечує: ініціацію хендоверу (у який

момент часу й при яких умовах); якість обслуговування; визначення й пророкування руху; м'який (що дозволяє терміналу одержувати дані від двох і більше точок доступу) або твердий (що вабить за собою високі втрати й погрозу переривання послуги)хендовер; згладжування частогохендоверу, необхідне при знаходженні терміналу на границі точок доступу;

- бездротовий інтерфейс - взаємодія між різними бездротовими інтерфейсами на різних рівнях.

Гармонізація, у свою чергу, забезпечується реалізацією концепції ABC (Always Best Connected), що дозволяє користувачеві багатогодового терміналу, при використанні деякої послуги, самостійно або довіряючи ПО терміналу вибирати мережу доступу (з відповідним QoS). Крім того, користувач повинен мати можливість у будь-який момент змінити своє рішення, якщо в ході сеансу з'явиться більше кращий варіант.

При такій кількості найрізноманітніших технологій для повсякденного користування в них можна легко заплутатися. В таблиці 1.1 зрівнюються важливі параметри вже існуючих і очікуваних радіотехнологій.

Табл. 1.1. Характеристики бездротових мереж

		UMTS	802.11в	802.11а	802.11g	802.16	802.16e	802.2	802.11n	HSxPA	WGWAM
Максимальна швидкість передачі даних	Мбіт/с	2	11	54	54	70	24	4	100	10	1000
Частотні діапазони	ГГц	1,8-2,1	2,4	5	2,4	2-66	2-6	<3,5	2,4	1,8-2,1	5-60
Ліцензовані діапазони		так	ні	ні	ні	так	Так	так	ні	так	так
Діапазон	км	0,5	0,1	0,05	0,1	70	1,5	1	0,1	0,5	50
Ширина каналу	МГц	5	20	20	20	1,5-20	1,5-20	1,25-5	2*20	5-10	n*20
Спектральна ефективність	біт/с	<0,5	0,6	2,7	2,7	5	5	3,2	5	5	5
Мобільність	км/год	н/д	н/д	н/д	н/д	н/д	250	250	н/д	н/д	600
Модуляція		QPSK	DSSS	OFDM	OFDM	OFDM	OFDM	OFDM	OFDM	CDMA	OFDMA
Безпека			WEP	WEP	WEP	3CES/ AES	3DES/ AES				
Якість послуг		так	ні	ні	ні	так	так	так	ні	так	так
Стандарт		2000	1999	1999	2003	2004	>=2005	>=2006	>=2006	>=2007	>=2010

До того ж в табл. 1.1 відбиті й технічні проблеми, з якими доводиться боротися UMTS: у порівнянні із сучасними технологіями так звана спектральна ефективність виявляється менше однієї десятої. Наступне покоління UMTS - високошвидкісний пакетний доступ (High Speed Packet Access, HSxPA) - відстає від рівня наступних розробок. У сучасних методах (обмежений) ефір використовується набагато ефективніше,

ніж в UMTS. Техніка вже в стані запропонувати 5 біт на 1 Гц. Як показують, в стандарті 802.11n і WIGWAM, більше висока швидкість передачі даних досягається не подальшим ущільненням - тобто більше розумним кодуванням, а збільшенням числа каналів, які використовуються.

Дечого вдалося досягти й у плані збільшення радіусу дії: якщо для методу 802.11 (а також UMTS) типовий радіус комірки становить 100 м, то в 802.16 розмір комірки сягає до 1,5 км. При цьому необхідно враховувати, що широкої смуги пропускання (пікових значень швидкості передачі даних) можна досягти лише при ідеальних умовах, тобто у випадку мінімальної відстані. Інакше кажучи, при більших відстанях пропусканна здатність помітно падає.

Проте важлива відмінність між технологіями 802.11 і 802.16 полягає в тім, що 802.11 використовується в локальних мережах, а 802.16 - у міських. 802.16 пропонує прекрасні функції забезпечення безпеки і якості послуг, завдяки яким провайдер може надати гарантовані мережні послуги.

РОЗДІЛ 2

СУЧАСНІ ТЕХНОЛОГІЇ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Принципи побудови сучасних комп'ютерних мереж

2.1.1 Концепції та термінологія

Ідею обміну інформацією між комп'ютерами розпочали втілювати у власні розробки майже від початку своєї діяльності усі провідні виробники комп'ютерів. Для цього кожен виробник створював спеціалізовані засоби, які згодом, завдяки діяльності спеціалістів різних країн, перетворилися на стандартизовані компоненти комп'ютерних мереж (рис.2.1).

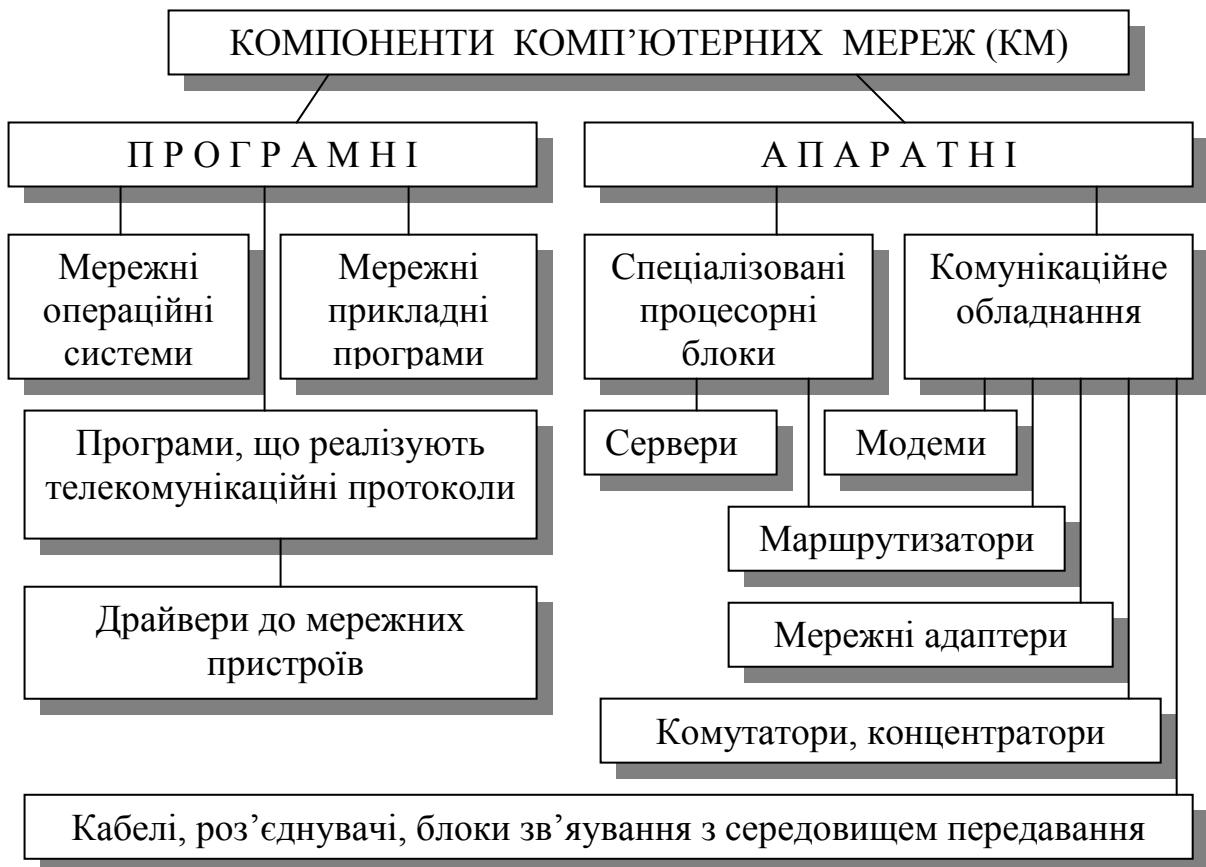


Рис. 2.1. Класифікація основних компонентів комп'ютерних мереж

Цю діяльність на початку очолював Міжнародний консультативний комітет з телефонії та телеграфії (МККТТ), а після перетворень, що відбулися у 1993 році, її очолює Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU), що є спеціалізованим органом Організації Об'єднаних Націй. Розробкою міжнародних стандартів для

комп'ютерних мереж займається сектор стандартизації телекомунікації ІТУ (ITU Telecommunication Standardization Sector, ІТУ-Т).

Результатом цієї діяльності є можливість об'єднання мереж від різних виробників. Яскравим прикладом такого об'єднання є мережа Інтернет.

Перелік найбільш відомих розробників стандартів КМ та їх основних розробок надано у додатку (див.дод.1).

У загальному вигляді КМ являють собою сукупність комп'ютерів, що з'єднані за допомогою комунікаційного обладнання.

Метою створення КМ є надання кожному користувачеві потенційної можливості користування ресурсами усіх комп'ютерів, що підключені до мережі [1].

Варіанти з'єднання комп'ютерів можуть відрізнятися за топологією.

Термін **топологія** (*topology*) означає конфігурацію мережі у цілому.

Найбільш поширені топології КМ – шинна, кільцева та зіркоподібна (рис.2.2).

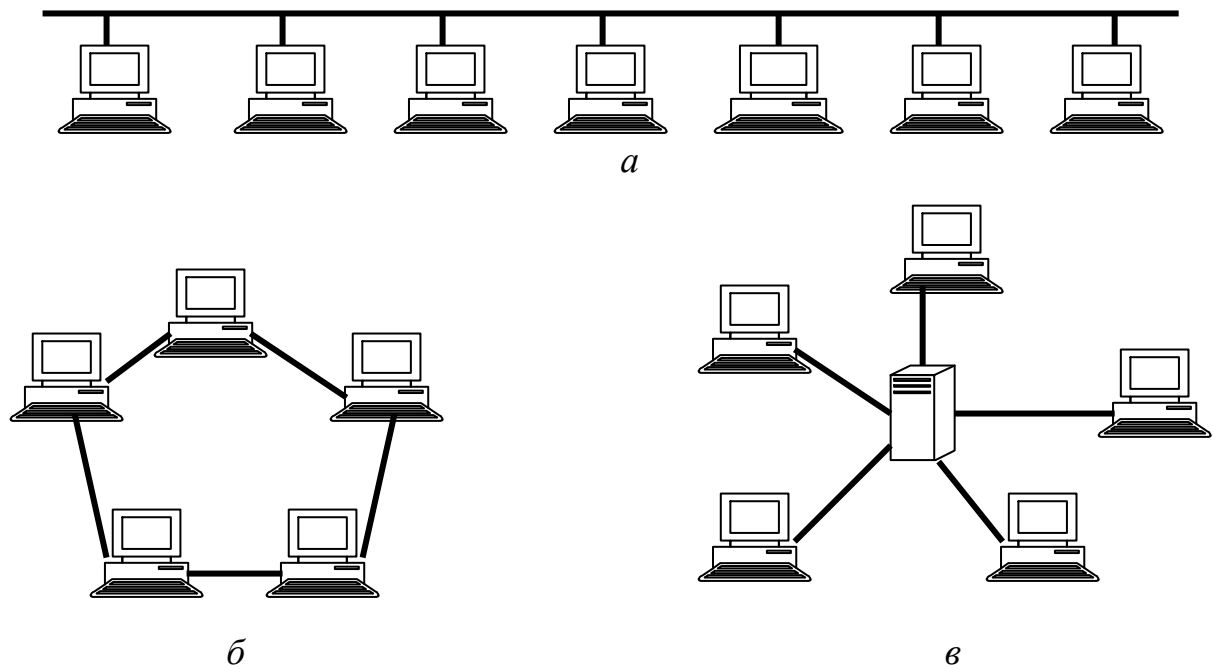


Рис. 2.2. Основні варіанти топології КМ:

a – шина; *b* – кільце; *v* – зірка.

Ці найпростіші варіанти топологій відповідають окремим або не поєднаним між собою мережам. З урахуванням міжмережних зв'язків

топологія може бути як завгодно складною сумішшю найпростіших варіантів. На рис.2.3 схематично зображено деревоподібну та повнозв'язну топології.

У математичному понятті топологія являє собою граф, вершинами якого є комп'ютери, а ребрами – зв'язки між ними. Комп'ютер, що підключений до мережі називають вузлом, станцією або хостом (host).

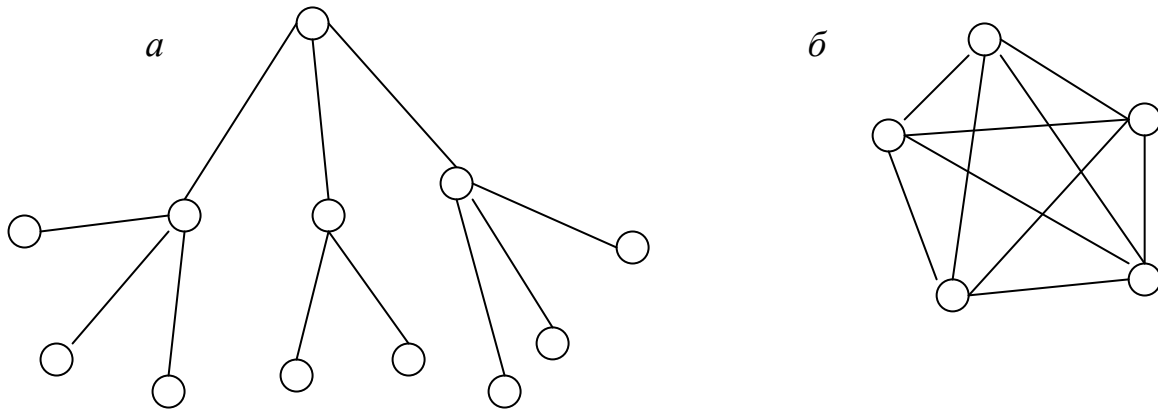


Рис. 2.3. Топології мереж:

a – деревоподібна; *б* – повнозв'язна.

У понятті топології КМ не враховується територіальне розміщення вузлів (що суттєво відрізняє це поняття від розуміння топології в інших системах), а враховуються тільки логічні зв'язки між комп'ютерами [2].

Крім поняття топології КМ, існує поняття топології фізичних зв'язків між мережними пристроями. Ці пристрої можуть являти собою комутаційне обладнання, що не підпадає під поняття вузла мережі, бо вузлами мережі вважають тільки такі системи, які опрацьовують, приймають та/або передають пакети інформації. Цей момент буде розглянуто детальніше на прикладі мережі Ethernet у підрозділі 3.1.

Термінологія у галузі КМ ще остаточно не визначилась. Наведемо означення, які ми будемо використовувати в подальшому.

Реальна система – це сукупність комп'ютера (або кількох комп'ютерів), програмного забезпечення, периферійного обладнання, терміналів та персоналу, яка опрацьовує інформацію та може бути повністю автономною.

Автономна система – це реальна система, що не приєднана до мережі.

Відкрита система – це система, що відповідає стандартам побудови відкритих систем та може бути приєднана до мережі.

Комунікаційна система – це відкрита система, яка забезпечує обмін даними між абонентськими системами у відкритій інформаційній системі.

Реальна остаточна система – це реальна система, яка виконує у мережі функції станції даних, тобто є джерелом та/або споживачем інформації.

Абонентська система – це реальна відкрита система, яка є постачальником та/або споживачем ресурсів мережі, забезпечує доступ до них користувачів і керує взаємозв'язком відкритих систем.

Ініціаторами та учасниками обміну інформацією в абонентських системах є прикладні процеси.

Прикладний процес – це процес у реальній остаточній системі, який опрацьовує інформацію для визначених потреб.

Прикладами прикладних процесів можна вважати дії користувача за терміналом у одній остаточній системі та програму доступу до бази даних у другій остаточній системі. Зв'язок між прикладними процесами цих систем забезпечується за допомогою середовища передавання даних.

Середовище передавання даних – це сукупність комунікаційного обладнання та програм, що реалізують телекомунікаційні протоколи, яка забезпечує процес передавання даних між остаточними системами.

Структуру середовища зв'язку відкритих систем визначає стандарт 7498 ISO. За цим стандартом середовище зв'язку розподіляють на сім рівнів ієрархії. На кожному рівні використовують поняття об'єкта рівня.

Протокол – це стандартизовані правила обміну інформацією між об'єктами однакового рівня ієрархії різних відкритих систем.

Інтерфейс – це сукупність засобів обміну інформацією між об'єктами сусідніх рівнів ієрархії однієї системи.

Стек протоколів – це достатній набір протоколів для здійснення взаємодії вузлів мережі.

Архітектура комп'ютерної мережі – це узагальнююче поняття, що об'єднує топологію, стек протоколів, інтерфейси та комунікаційне обладнання комп'ютерної мережі.

Масштаб комп'ютерної мережі – це поняття, що пов'язане з територіальним розміщенням вузлів мережі.

За масштабом КМ розподіляють на локальні (*Local Area Network, LAN*) та глобальні (*Wide Area Network, WAN*).

Локальні комп'ютерні мережі (ЛКМ або ЛМ) територіально обмежені. Вони забезпечують зв'язок у межах будинку або групи будинків, що розташовані близько один від одного.

Глобальні мережі (ГМ) територіально не обмежені. Їх поділяють на дві категорії: магістральні мережі (*Backbone*), що забезпечують зв'язок між віддаленими потужними вузлами різних міст, країн, континентів, та мережі доступу (*Access network*), які забезпечують зв'язок між віддаленою невеликою локальною мережею або окремим комп'ютером з центральною мережею.

Проміжне місце за масштабом між локальними та глобальними мережами займають **регіональні мережі** (*Metropolitan Area Network, MAN*), що обслуговують територію великого міста, та **кампусні мережі** (від англ. *campus* – університетське містечко).

Діаметр мережі – відстань між найвіддаленішими вузлами. Для локальних мереж з кабельними з'єднаннями цю відстань вимірюють по довжині кабелю.

Трафік – характеристика процесу передавання інформації, що для КМ визначають як кількість переданих даних за проміжки часу.

2.1.2 Рівні ієрархії телекомунікаційних протоколів

Модель взаємодії відкритих систем (*Open System Interconnection, OSI*) була розроблена Міжнародною організацією зі стандартизації на початку 80-х років. Середовище передавання даних за цією моделлю розподіляється на сім рівнів (стандарт 7498 ISO). Кожен рівень виконує конкретний набір завдань. Межі між рівнями обрано так, щоб обмін інформацією був мінімальним. Функції кожного рівня локалізовані таким чином, щоб заміна одного рівня не спричиняла заміну інших.

Користуючись поняттям об'єкта рівня, можна сказати, що протоколи кожного рівня це є мова спілкування об'єктів одного рівня різних відкритих систем. Необхідною умовою такого спілкування є дотримання стандартів синтаксису та семантики цієї мови. Повний набір протоколів (стек протоколів) повинен забезпечити спілкування об'єктів на усіх рівнях від верхнього до нижнього. Існують десятки стандартизованих стеків протоколів різних за призначенням і можливостями, про які піде мова у цьому підрозділі. Кожен із цих стеків має свої особливості. При цьому рівні ієрархії телекомунікаційних протоколів у багатьох стеках не завжди

точно відповідають рівням моделі OSI. Так буває, що один рівень ієрархії стеку протоколів відповідає двом-трьом рівням моделі OSI. Буває навпаки, що одному рівню моделі OSI відповідають декілька рівнів ієрархії стеку телекомунікаційних протоколів. У цьому випадку рівні ієрархії протоколів називають підрівнями, а рівнем називають сукупність цих підрівнів.

У таблиці 2.1 надано перелік рівнів моделі OSI.

Таблиця 2.1

Стандартні рівні моделі взаємодії відкритих систем

Номер та назва рівня за стандартом	Назва рівня українською мовою	Назва рівня у російських джерелах	Функціональне призначення Рівня
7 Application layer	Прикладний	Прикладной	Взаємодія прикладних процесів
6 Presentation layer	Відображення	Представительный	Перетворення даних (кодів, форматів)
5 Session layer	Сеансовий	Сеансовый	Керування Діалогом
4 Transport layer	Транспортний	Транспортный	Встановлення наскрізного прозорого сполучення
3 Network layer	Мережний	Сетевой	Вибір маршруту та доставка Пакетів
2 Data Link layer	Канальний	Канальный	Передавання даних між сусідніми вузлами
1 Physical layer	Фізичний	Физический	Зв'язування з фізичним середовищем

Слід звернути увагу на розрізнення таких понять як прикладний процес і прикладний рівень. На рис. 2.4 показано взаємодію прикладних процесів двох віддалених відкритих систем. Прикладний рівень являє

собою ту частину середовища передавання даних, яка має інтерфейс з прикладним процесом. Прикладні процеси віддалених систем використовують середовище передавання даних для спілкування між собою. Середовищем передавання даних для цих процесів є сукупність об'єктів усіх семи рівнів у системах клієнта і сервера, а також фізичні середовища (лінії зв'язку) і усі, що зображені на рис.2.4, об'єкти маршрутизатора. Маршрутизатор – це пристрій, що забезпечує з'єднання фізичних середовищ різних первинних мереж. Кількість маршрутизаторів на шляху передавання інформації між системами клієнта і сервера може досягати кількох десятків. В межах однієї мережі зв'язок здійснюється без маршрутизаторів.



Рис. 2.4. Взаємодія прикладних процесів двох реальних остаточних систем (клієнта і сервера) за стандартом 7498 ISO

Для успішного зв'язку необхідно, щоб протоколи рівнів 7к, 6к, 5к та 4к відповідно співпадали з протоколами рівнів 7с, 6с, 5с та 4с, протоколи мережного рівня (3к, 3м та 3с) мають бути однаковими або сумісними протягом усього шляху передавання інформації у мережі. Протоколи

канального та фізичного рівнів можуть відрізнятися від сполучення до сполучення, але для кожного сполучення вони повинні співпадати. У нашому випадку повинні відповідно співпадати протоколи рівнів 2к та 1к з протоколами рівнів 2мк та 1мк, а також 2мс та 1мс з 2с та 1с.

Така модель взаємодії відкритих систем була створена для того, щоб майбутні розробники телекомунікаційних протоколів спирались на неї як на стандарт. Проте сучасні реально існуючі мережі не відповідають у повній мірі цьому стандарту. Стек протоколів, який було розроблено відповідно до моделі OSI, практично не знайшов свого місця у реальних мережах. Фактично стандарт 7498 ISO у повній мірі не було впроваджено.

Розглянемо стеки, що найбільш часто використовуються у сучасних мережах, та звернемо увагу на спільні риси цих стеків зі стандартом.

Найбільшого поширення набув стек протоколів TCP/IP, який було розроблено у 1969 році (за 14 років до появи стандарту 7498 ISO). Цей стек покладено в основу мережі Інтернет. Порівняємо функції протоколів стеку TCP/IP зі стандартом (рис. 2.5).

Рівні моделі OSI	Рівні стеку TCP/IP
Прикладний	Прикладний
Відображення	
Сеансовий	
Транспортний	Транспортний
Мережний	Міжмережний
Канальний	Мережного інтерфейсу (Канальний)
Фізичний	

Рис. 2.5. Відповідність ієрархічних рівнів моделі OSI (за стандартом 7498 ISO) та стеку протоколів TCP/IP

У стеку TCP/IP виділяють чотири ієрархічні рівні, які функціонально відповідають семи рівням моделі OSI. Функції трьох верхніх рівнів моделі OSI об'єднані у одному прикладному рівні стеку TCP/IP та функції двох нижніх рівнів моделі об'єднані у одному рівні мережного інтерфейсу, який також називають канальним рівнем.

Схема взаємодії прикладних процесів з використанням протокольного стеку TCP/IP (рис.2.6) практично не відрізняється від схеми взаємодії за стандартом 7498 ISO, що зображена на рис.2.4.

Усі вимоги щодо сумісності протоколів, які виконують одні й ті самі функції, однакові у обох схемах.

На прикладі обміну інформацією між об'єктами усіх рівнів протокольного стеку TCP/IP, ознайомимось далі зі загальними принципами побудови стеків телекомунікаційних протоколів комп'ютерних мереж.

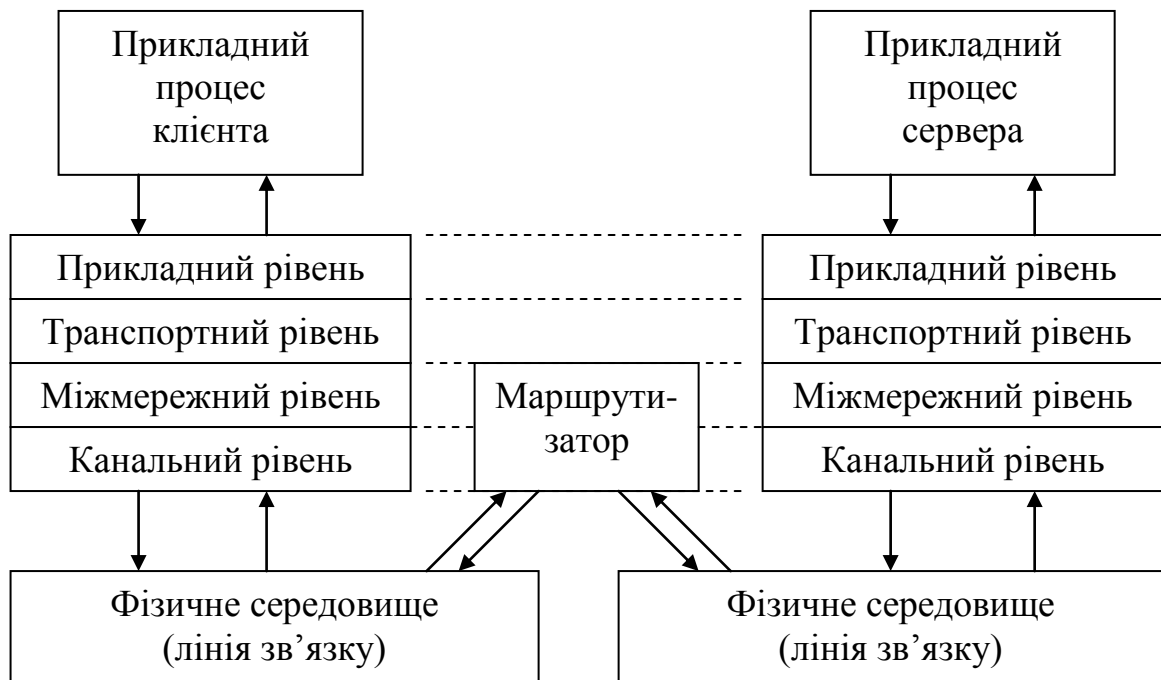


Рис. 2.6. Взаємодія прикладних процесів у мережі з використанням стеку протоколів TCP/IP

Розглянемо послідовність дій, що виконуються на кожному рівні протокольного стеку TCP/IP, у реальній остаточній системі під час передачі повідомлення (рис.2.7). Прикладний процес у цьому випадку є відправником інформації. Перед тим як потрапити у лінію зв'язку, повідомлення доповнюється заголовками від кожного ієрархічного рівня, а на канальному рівні доповнюється ще й кінцівкою. До лінії зв'язку повідомлення потрапляє у вигляді пакета або серії пакетів канального рівня, що зветься кадрами (*frame*). Усі рівні, крім канального, реалізовані у вигляді програмного забезпечення. Канальний рівень потребує апаратних засобів для з'єднання з фізичною лінією зв'язку.

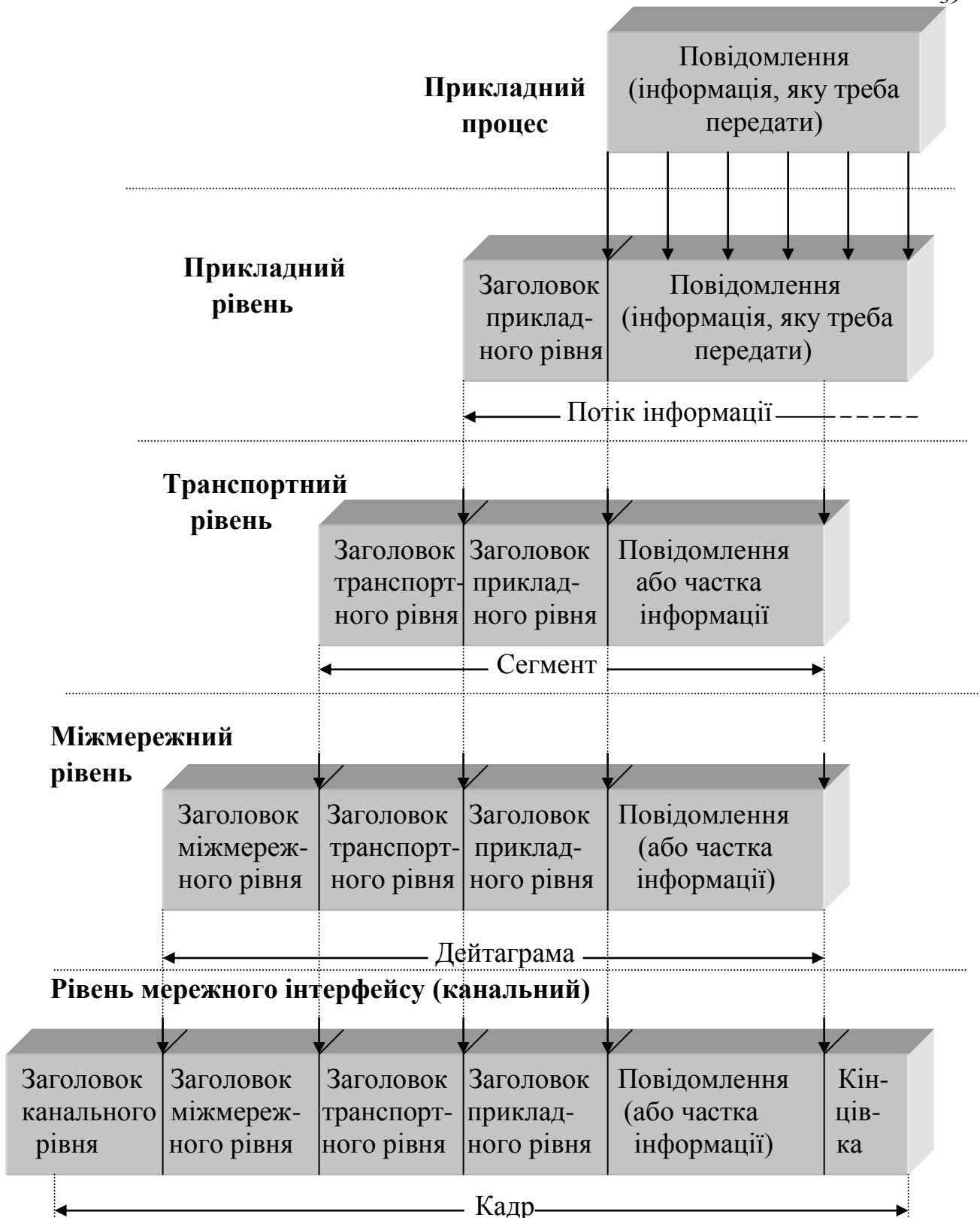


Рис. 2.7. Послідовність формування пакетів на ієрархічних рівнях стеку протоколів TCP/IP

На прикладному рівні (*application layer*) існує декілька протоколів, що забезпечують доступ до мережі різноманітним прикладним процесам. У кожному з протоколів передбачено декілька варіантів повідомлень.

Довжина повідомлень практично не обмежується. У деяких протоколах передбачена можливість перетворення даних (кодів, форматів).

Після приєднання заголовка на прикладному рівні утворюється так званий потік інформації, який передається на транспортний рівень.

На транспортному рівні (*transport layer*) існує два базових протоколи TCP (*Transmission Control Protocol*) та UDP (*User Datagram Protocol*). Головний протокол цього рівня TCP. Він забезпечує керування процесом передавання даних. Розглянемо детальніше процедури, які виконуються при цьому.

Спочатку виконується процедура встановлення з'єднання, яка полягає в обміні спеціальними інформаційними пакетами. Цей обмін здійснюється між об'єктами транспортного рівня систем відправника та одержувача інформації. Тільки після успішного обміну цими пакетами розпочинається процес передавання даних.

Далі потік інформації, що надходить з прикладного рівня, формується в інформаційні пакети. Довжина пакетів обмежена. Її максимальне значення задають під час інсталяції програмного забезпечення і вибирають в залежності від типу мережного обладнання. Так, для мереж сім'ї Ethernet ця довжина становить 1500 байт. Коротенькі повідомлення можуть розміщуватись в одному пакеті, а довгий потік інформації буде поділено на частки максимально допустимої довжини.

Під час сеансу передавання даних між об'єктами транспортного рівня систем відправника та одержувача інформації існує зворотний зв'язок. Після успішного прийняття кожного пакета на транспортному рівні одержувача формується відповідь, яка передається на транспортний рівень відправника. Ця відповідь зветься квитанцією або підтвердженням. У разі затримки підтвердження той самий пакет може відправлятися повторно протягом встановленого інтервалу часу, після якого передавання даних буде припинено.

Після успішного завершення процесу передавання даних виконується процедура роз'єднання, яка нагадує процедуру з'єднання, бо також являє собою обмін спеціальними пакетами між об'єктами транспортного рівня систем відправника та одержувача інформації. Закінчення цієї процедури свідчить про те, що потік інформації безпомилково передано на прикладний рівень системи одержувача.

Протокол UDP призначений для термінової передачі коротеньких повідомлень без встановлення з'єднання та без підтверджень. При цьому

пакет, що складається з повідомлення та заголовка UDP, називають так само, як пакет міжмережного рівня дейтаграмою, а не сегментом, як пакети з TCP заголовком.

На міжмережному рівні (*internet layer*) відбувається доставка пакетів між об'єктами транспортного рівня систем відправника та одержувача інформації. Головна функція, яка виконується на цьому рівні, полягає у виборі найкращого маршруту доставки пакетів. Кожен пакет проходить свій шлях незалежно від інших. При цьому гарантії, що пакет дійде до адресата, немає. Можливі порушення порядку надходження пакетів, а також розмноження їх.

Головний протокол міжмережного рівня зветься IP (*Internet Protocol*). Пакети, що формуються відповідно до цього протоколу, зветься дейтаграмами або данограмами. Вони складаються з пакетів транспортного рівня (сегментів) та заголовків міжмережного рівня.

Крім протоколу IP, на міжмережному рівні є протоколи, які забезпечують виконання операцій пошуку маршруту для доставки пакетів та знаходження адрес сусідніх маршрутизаторів.

На рівні мережного інтерфейсу (*network interface layer*) відбувається доставка пакетів між об'єктами міжмережного рівня, що належать одній мережі на фізичному рівні моделі OSI. Пакети цього рівня складаються з пакетів міжмережного рівня, заголовків канального рівня та кінцівок у вигляді контрольної суми.

У стеку протоколів TCP/IP, якщо перевірка контрольної суми кадру дає негативний результат, кадр відкидають.

Розподіл найбільш відомих протоколів стеку TCP/IP за ієрархічними рівнями показано на рис.2.8. Призначення цих протоколів полягає у наступному.

HTTP (Hypertext Transfer Protocol) – протокол для передавання Web-сторінок (гіпертексту).

FTP (File Transfer Protocol) – протокол для передавання файлів.

SMTP (Simple Mail Transfer Protocol) – протокол для передавання повідомлень електронною поштою.

Telnet – протокол для емуляції терміналу віддаленого комп'ютера.

DNS (Domain Name System) – доменна система імен, яка призначена для перетворення символьних імен мережних ресурсів у цифрові адреси серверів, де розміщено ці ресурси.

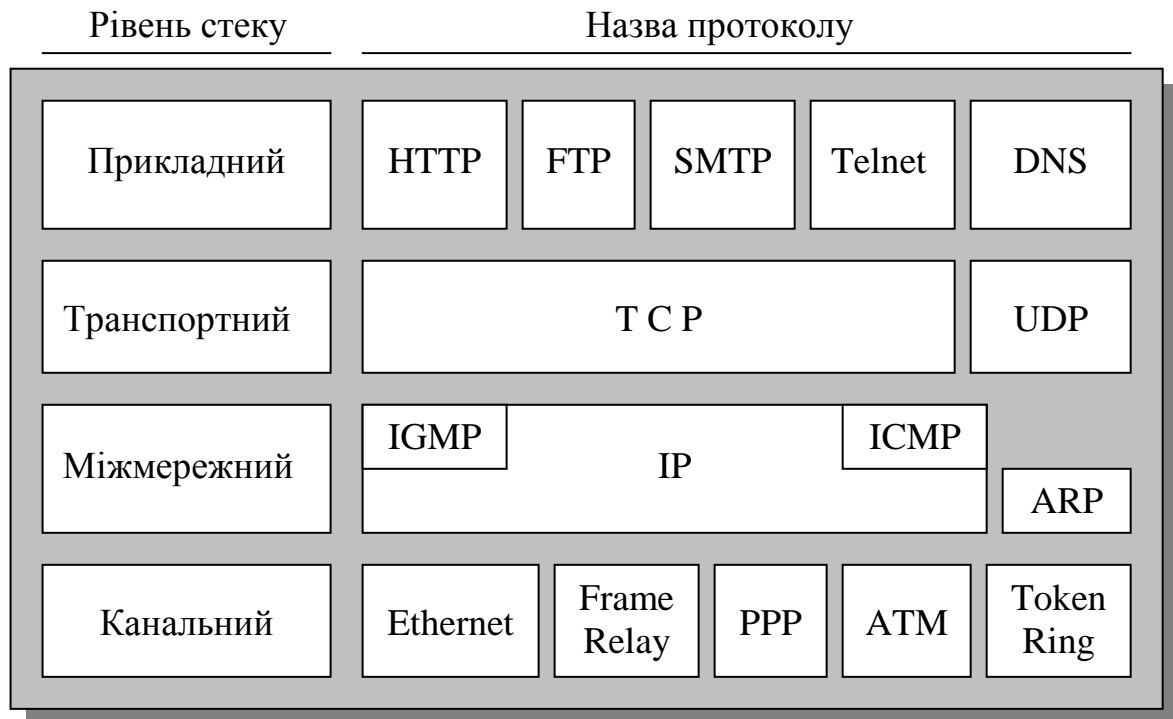


Рис. 2.8. Протоколи стеку TCP/IP

TCP (Transmission Control Protocol) – протокол, що забезпечує надійне логічне з’єднання тип “один до одного” та гарантує вірність передавання даних.

UDP (User Datagram Protocol) – протокол, що забезпечує можливість передавання широкомовних повідомлень без гарантії їх отримання споживачами інформації.

IP (Internet Protocol) – протокол, що забезпечує переміщення пакетів між мережами, але не гарантує доставку пакетів за адресою одержувача.

IGMP (Internet Group Management Protocol) – протокол, що забезпечує широкомовність для груп користувачів, які мають єдину групову адресу (multicast). Ця адресація призначена для економічного розповсюдження інформації у великих корпоративних мережах. Зараз такою технологією користуються в межах експерименту.

ICMP (Internet Control Message Protocol) – протокол для обміну службовою інформацією між маршрутизаторами (про виявлення помилок та аварійні ситуації), а також для перевірки працездатності мережі.

Пакети IGMP та ICMP протоколів доповнюються IP-заголовком та циркулюють між об’єктами міжмережного рівня, чим пояснюється їх особливе місце на рис.2.8.

ARP (Address Resolution Protocol) – протокол для визначення фізичної адреси інтерфейсу. Ця адреса необхідна для формування заголовка пакета канального рівня (кадру). Пакети ARP протоколу не доповнюються IP-заголовком міжмережного рівня, а одразу пакуються в кадри (пакети канального рівня), бо вони циркулюють тільки в межах однієї мережі.

Ethernet – найбільш розповсюджена технологія побудови каналів зв'язку у локальних мережах.

Frame Relay – найбільш розповсюджена технологія побудови каналів зв'язку для глобальних мереж.

PPP (Point-to-Point Protocol) – протокол, що широко застосовують для побудови каналу зв'язку між двома віддаленими вузлами, що з'єднані між собою фізичною лінією зв'язку.

ATM (Asynchronous Transfer Mode) – нова універсальна технологія побудови каналів зв'язку для глобальних і локальних мереж, що забезпечує гарантовану якість і терміновість передавання даних. За цією технологією створюють нові швидкісні магістральні мережі для передавання даних в Україні. Високі ціни на обладнання стримують процес розширення застосування технології ATM.

Важливою перевагою стеку TCP/IP є можливість утворення вузлів-маршрутизаторів, які одночасно приєднані до різних мереж. Це дозволяє переносити інформацію між мережами різного типу та створювати альтернативні шляхи доставки інформаційних пакетів. Якщо трапляється аварія на одному з шляхів, пакет автоматично буде направлений на інший шлях. Отже, робота мережі не припиняється під час аварій на окремих вузлах, а також під час приєднання нових вузлів.

Розглянемо структуру ще одного з широко розповсюджених стеків, що має назву NetBIOS/SMB. Цей стек протоколів з'явився у 1984 році для побудови локальних мереж на IBM-сумісних комп'ютерах, він увійшов до складу всіх версій операційної системи Windows. У цьому стеку не передбачено жодного протоколу на мережному рівні, що не дає змоги створення маршрутизаторів для об'єднання різних мереж (рис.2.9).

Стек NetBIOS/SMB дозволяє створювати тільки локальні мережі.

Рівні моделі OSI Рівні стеку NetBIOS/SMB

Прикладний	SMB
Відображення	
Сеансовий	
Транспортний	NetBIOS
Мережний	Канальний
Канальний	
Фізичний	

Рис. 2.9. Відповідність рівнів моделі OSI та стеку протоколів NetBIOS/SMB

На каналному рівні стеку NetBIOS/SMB використовують ті самі протоколи та технології, що й для стеку TCP/IP.

SMB (Server Message Block) – протокол, що забезпечує прикладному процесу доступ до файлів та принтерів інших комп'ютерів.

NetBIOS (Network Basic Input/Output System) – протокол, що доповнює базову систему (BIOS) персональних комп'ютерів типу IBM PC функціями для роботи у мережі.

Порівнюючи між собою можливості двох стеків NetBIOS/SMB та TCP/IP, бачимо, що кожен з них займає своє особливе місце за призначенням. Стек NetBIOS/SMB дозволяє легко створювати невеликі мережі, а ті ускладнення, які пов'язані з використанням стеку TCP/IP, виправдовуються можливістю утворення міжмережних зв'язків та підключення до всесвітньої мережі Інтернет.

2.1.3 Обладнання комп'ютерних мереж

У цьому розділі ми розглянемо технічні засоби, які необхідні для підключення комп'ютера до існуючої мережі, а також для створення власної локальної мережі.

Перше приєднання до мережі найчастіше починається з придбання модему та підключення його до комп'ютера і телефонної лінії. Цей доступ до мережі зветься на англійській мові “dial-up access”. Таке приєднання

вже не задовольняє багатьох користувачів, які бажають підвищення швидкості обміну інформацією. Прогнозують, що у найближчі роки модеми відійдуть у минуле, бо замість звичайного телефону будуть побудовані високошвидкісні канали для доступу до інформаційних мереж. Проте зараз модемний зв'язок застосовують ще досить широко.

Слово модем є скорочення від слів модулятор та демодулятор, а модуляція – це зміна параметрів фізичного процесу у лінії зв'язку під впливом процесу, що надходить з джерела інформації.

Модеми бувають внутрішні (які приєднують до шини в середині процесорного блока) та зовнішні (які приєднують до послідовного порту). Внутрішні модеми мають вигляд окремої плати (карти), що займає роз'єднувач розширення комп'ютера, а зовнішні модеми мають свій корпус з окремим блоком живлення та займають роз'єднувач СОМ-порту.

Найбільш розповсюджені модеми це ті, що приєднують до звичайної телефонної лінії разом з телефонним апаратом. У таких модемах, крім можливості автоматичного набору номера для встановлення з'єднання, можуть бути передбачені додаткові сервісні можливості.

Факс-модеми можуть приймати та передавати факс-повідомлення.

Звукові модеми можуть записувати та відтворювати мовні повідомлення.

SVD-модеми (Simultaneous Voice and Data) можуть одночасно передавати дані та мовлення.

У нових модемах стандартів V.90 та V.92 уведено функції Call Waiting та Modem on hold, що дають змогу перервати сеанс зв'язку з сервером, якщо надійшов телефонний виклик. Після закінчення розмови можна продовжити перерваний сеанс зв'язку. Ці функції не можуть бути реалізовані без підтримки з боку цифрової АТС.

Кожен з сучасних модемів має спеціальний режим для керування робочими характеристиками. У цьому режимі модем сприймає команди від СОМ-порту комп'ютера. Коди команд відповідають стандарту, що був розроблений фірмою Hayes на початку 80-х років. Модеми через це називають Hayes-сумісними. Майже всі команди починаються з комбінації двох латинських літер АТ (Attention – Увага!). Наведемо приклади деяких команд:

ATZ – встановлення початкових значень параметрів модему;

ATDT# – тональне набирання телефонного номера;

ATDP# – імпульсне набирання телефонного номера;

AT&F – встановлення параметрів модему, що закладені виробником;
 AT&W – запам'ятовування поточних значень параметрів модему.

Увімкнувши модем, його треба спочатку налаштувати. Для цього треба ввести послідовність команд ініціалізації, яка залежатиме від конкретних умов використання модему.

Швидкість передавання даних регламентує такий ряд стандартів:

V.21 – 300 біт/с;

V.22 – 1200 біт/с;

V.22 bis – 2400 біт/с;

V.32 – 4800 та 9600 біт/с;

V.32 bis – 14400 біт/с;

V.34 – 28800 біт/с;

V.34+ – 33600 біт/с;

V.90 – 56 Кбіт/с в напрямку від сервера до клієнта та 33600 біт/с в напрямку від клієнта до сервера;

V.92 – 56 Кбіт/с в напрямку від сервера до клієнта та 48 Кбіт/с в напрямку від клієнта до сервера.

Цей ряд стандартів розроблявся протягом десятків років. Перші модеми мали меншу швидкість передавання та не були адаптивними. Починаючи з стандарту V.34 (прийнятого у 1994 році), розпочався період виробництва адаптивних модемів. Ці модеми під час передавання даних можуть змінювати швидкість залежно від характеристик каналу зв'язку. На початку сеансу швидкість становить 300 біт/с (стандарт V.21), що забезпечує максимальну надійність передавання даних. Далі починається процес тестування лінії зв'язку з метою вибору оптимальної швидкості передавання.

У наступних стандартах розширювали можливості режимів адаптації, та підвищували максимальну швидкість передавання даних.

Швидкість передавання у модемах стандартів V.90 (1998 р.) та V.92 (2000 р.) збільшена до 56 Кбіт/с внаслідок вилучення етапу аналого-цифрового перетворення сигналу на шляху від сервера до клієнта. Таке можливо тільки у випадку, коли на всьому шляху передавання пакетів АТС будуть тільки цифровими.

Купляючи новий модем для підключення до телефонної лінії, можна не турбуватись про якість передавання даних. Всі сучасні модеми адаптивні і мають сумісність зі старими модемами. Краще придбати модем на більшу швидкість. Він може підтримувати зв'язок з усіма модемами

меншої швидкості. Якість передавання даних залежить в першу чергу не від вибору модему, а від якості телефонного каналу. Найвищу якість забезпечують цифрові АТС. Досвід показує, що легше встановлюється зв'язок між модемами одного типу.

Крім модемів для телефонних ліній, існують модеми для швидкісного передавання прямим кабелем (Limited Distance Modem, або Short Range Modem). Ці модеми дозволяють досягти швидкостей, що дорівнюють одиницям або десяткам Мбіт/с, але довжина та якість проводу значно впливають на характеристики передавання даних. За допомогою таких модемів можна створювати різні варіанти цифрових абонентських ліній (Digital Subscriber Line, DSL), тому ці модеми ще називають DSL-модемами.

Підключення до мережі Інтернет за допомогою DSL дозволяє досягти значно більшої ефективності в роботі у порівнянні з телефонним модемом. Витрати на створення прямого кабельного підключення до найближчого вузла мережі Інтернет повністю виправдовують себе якщо підключається група з десяти або більше користувачів, що об'єднані у локальну мережу. При цьому кожен користувач має можливість значно скоротити витрати часу на приймання та передавання інформації.

Широкий спектр технологій DSL потребує ретельного дослідження характеристик кабельної лінії для визначення можливостей ефективного використання тієї чи іншої технології. Приблизну оцінку швидкості передавання даних можна отримати вимірявши активний опір мідної пари. Для цього на одному кінці лінії проводи з'єднують між собою, а на другому – підключають вимірювальний прилад. Якщо опір не перевищує 800 Ом, можна отримати швидкість передавання 1,5-2,0 Мбіт/с. Якщо опір дорівнює 1500 Ом, то швидкість не перевищуватиме 0,6 Мбіт/с.

Сьогодні відомі декілька технологій DSL.

- ADSL (Asymmetric DSL) використовує асиметричні потоки інформації. Швидкість передавання від сервера до користувача 1,5–6,0 Мбіт/с, а від користувача до сервера 64–640 Кбіт/с.
- HDSL (High bit rate DSL) використовує симетричні потоки в обох напрямках зі швидкістю 1,5–2,0 Мбіт/с. Потребує 4 проводи (дві пари).
- VDSL (Very high bit rate DSL) забезпечує підвищену швидкість до 51 Мбіт/с, але відстань передавання зменшена до 100–300 м.

- SDSL (Single line Symmetric DSL) використовує симетричні потоки зі швидкістю 384 Кбіт/с.
- RADSL (Rate Adaptive DSL) використовує адаптацію швидкості передавання в інтервалі 0,6–7,0 Мбіт/с для одного потоку, та 128–1000 Кбіт/с – для другого.

Швидкісний канал не раціонально створювати тільки для одного користувача. Для ефективного використання можливостей швидкісного каналу пропонується об'єднання 10–20 користувачів у локальну мережу (рис.2.10).

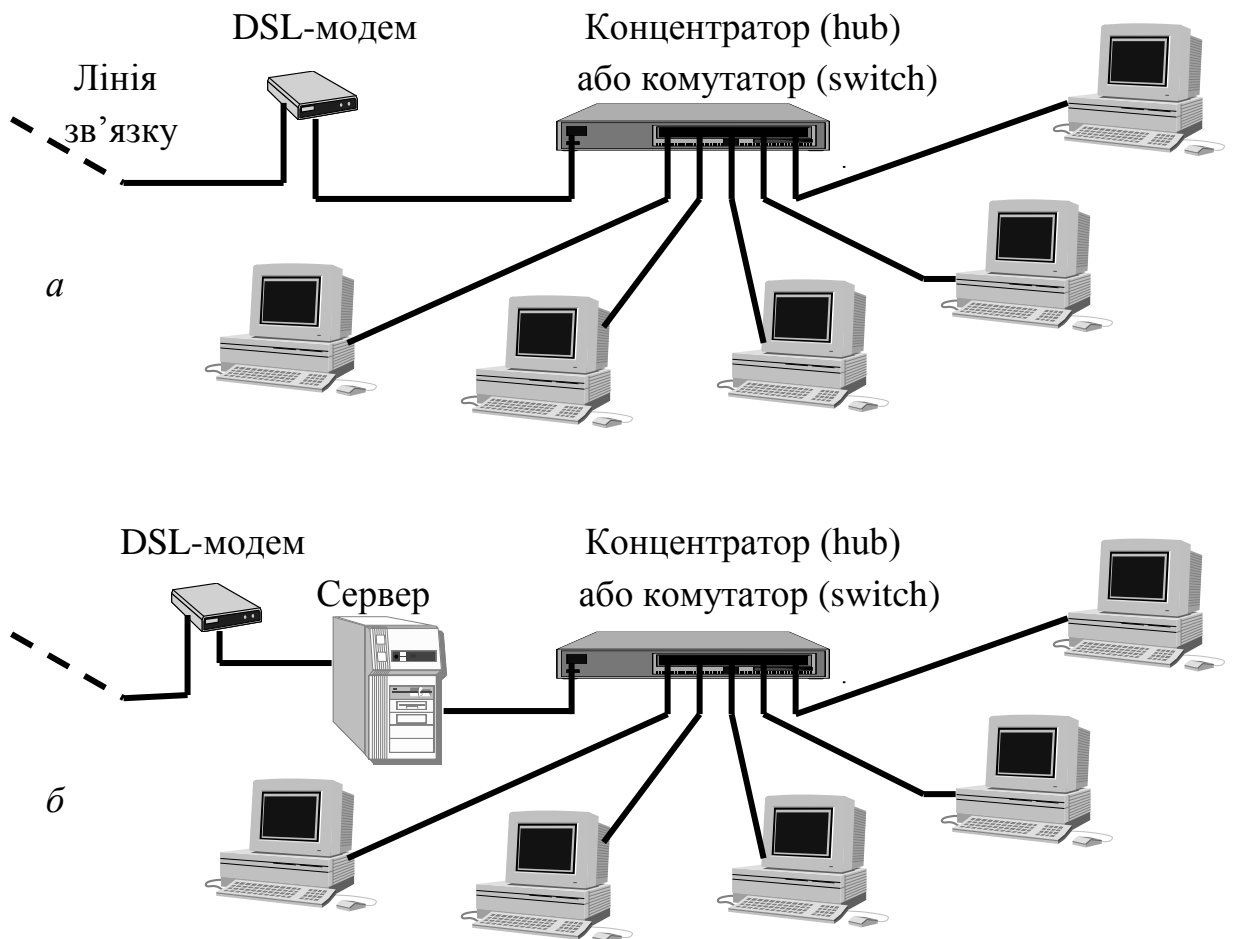


Рис. 2.10. Схема підключення локальної мережі до каналу зв'язку:
а – безпосередньо; *б* – через сервер.

Розглянемо варіанти вибору обладнання для побудови локальних мереж, що зображені на рис.2.10.

У сучасних умовах найдоцільніше створювати локальні мережі на основі комутаторів або концентраторів, що належать до сім'ї Ethernet-

технологій. Технології цієї сім'ї відрізняються одна від одної швидкістю передавання інформації та типом кабелю. Межове значення швидкості передавання може бути 10 Мбіт/с, 100 Мбіт/с (Fast Ethernet) або 1000 Мбіт/с (Gigabit Ethernet). Кабелі можуть бути коаксіальні (не рекомендовані у нових розробках через ненадійність), скручена пара (найбільш розповсюджені) та волоконно-оптичні (використовують мало через високу ціну обладнання).

У кожному комп'ютері, що приєднується до мережі, встановлюється мережний адаптер, який безпосередньо приєднується до внутрішньої шини комп'ютера. Такі адаптери ще називають мережними картами від американської назви NIC (Network Interface Card). В цих адаптерах реалізовані функції фізичного та каналного рівнів моделі OSI.

Вибираючи адаптер, треба звернути увагу на такі характеристики:

- Розрядність (16, 32, 64) та тип шини (EISA, PCI, PCI-X, MCA) комп'ютера.
- Тип роз'єднувача (або роз'єднувачів) для підключення кабелю.

Роз'єднувачі бувають такі:

RJ-45 – для скрученої пари (чотири пари);

BNC – для тонкого коаксіального кабелю;

AUI – для товстого коаксіального кабелю;

MIC, ST, SC – для волоконно-оптичного кабелю.

Центральною частиною сучасних адаптерів є мікропроцесори, які опрацьовують інформаційні пакети каналного та фізичного рівнів. Оперативна пам'ять адаптера відображається на адресний простір комп'ютера. У цю пам'ять записують інформацію перед передаванням та після приймання. Її можна одночасно читати і записувати з боків адаптера та комп'ютера. Таке рішення дозволяє розвантажити процесор комп'ютера від виконання зайвих процедур під час обміну інформацією через мережу.

Слід звернути особливу увагу на алгоритмічні можливості адаптерів. Є адаптери, що призначені для встановлення у потужні сервери. У таких адаптерах закладені можливості оптимізації обміну інформаційними потоками з множиною комп'ютерів. Ці функції не потрібні у випадку, коли адаптер буде встановлюватись у комп'ютер кінцевого користувача, а ціна за непотрібні можливості може бути досить значною.

Сучасні адаптери у момент підключення розпочинають автоматичний пошук найкращого режиму роботи за допомогою обміну спеціальними пакетами. Для цього використовують спеціалізовані

протоколи, що доробляються з появою кожної нової властивості адаптерів. Такі протоколи утворюють підрівні канального та фізичного рівнів стандартної моделі OSI (рис. 2.11).



Рис. 2.11. Підрівні канального та фізичного рівнів протоколів технології

Fast Ethernet

Тип кабелю вибирають виходячи з можливостей розміщення комутаційного обладнання та відстані між комп'ютерами, віддаючи перевагу скрученій парі. Характеристики, які слід враховувати під час вибору типу кабелю надані у таблиці 2.2.

Сучасне комутаційне обладнання дозволяє поєднувати в одній мережі різні типи кабелю, а також різні швидкості передавання. Наприклад, обираючи скручену пару як найбільш вигідний тип кабелю для підключення комп'ютерів, що віддалені не більш як на 100 метрів, інші

комп'ютери, що віддалені більше ніж на 100 метрів, можуть бути підключені коаксіальним або волоконно-оптичним кабелем. Для такого поєднання виробники мережного обладнання встановлюють роз'єднувачі різного типу на одному концентраторі або комутаторі.

Таблиця 2.2

Характеристики кабелю для побудови локальних мереж

Тип кабелю	Швидкість передавання, Мбіт/с	Максимальна довжина відрізка, м	Вартість	Надійність
Скручена пара категорії 3 або 5	100	100	Низька	Висока
Скручена пара категорії 5, 6 або 7	1000	100	Середня	Висока
Багатомодовий волоконно-оптичний	1000	550	Висока	Висока
Одномодовий волоконно-оптичний	10000	5000	Висока	Висока
Твинаксіальний	1000	25	Середня	Висока
Тонкий коаксіальний	10	185	Низька	Низька
Товстий коаксіальний	10	500	Висока	Низька

У позначенні обладнання, що підтримує декілька варіантів швидкості передавання даних, пишуть 10/100 або 10/100/1000, що означає автоматичний вибір найбільшої з можливих швидкості передавання для кожного з'єднання. Мережні адаптери також можуть підтримувати декілька варіантів швидкості передавання. На одному адаптері можуть бути встановлені роз'єднувачі різних типів, але одночасно до адаптера має бути підключений тільки один кабель.

Вибираючи концентратор (hub) або комутатор (switch) для приєднання комп'ютерів до мережі, слід віддавати перевагу комутаторам з наступних причин.

- Комутатори позбавляють локальну мережу від втрати пакетів через накладання одного пакета на другий. Така аварійна ситуація називається колізією. Вона виникає тоді, коли моменти початку передавання даних від різних комп'ютерів співпадають або близькі один до одного. Колізії майже не впливають на працездатність мережі, якщо реальна швидкість передавання даних значно менша від максимальної. Загроза втрати працездатності локальних мереж, що побудовані на базі концентраторів, стає значною, коли сумарна швидкість передавання перевищує половину від максимальної.
- Комутатори аналізують адреси пакетів і відправляють кожен пакет за адресою до конкретного комп'ютера. У концентраторах адреси не перевіряються, і пакети відправляються одночасно на всі комп'ютери локальної мережі. Це дозволяє користувачам локальної мережі приймати та аналізувати чужі пакети, що утворює загрозу конфіденційності.
- Комутатор дозволяє одночасно підтримувати зв'язок між декількома парами комп'ютерів локальної мережі на максимальній швидкості, що принципово неможливо у мережах, що побудовані на базі концентраторів.
- У великих локальних мережах неможливо приєднати усі комп'ютери до одного концентратора або комутатора, тому виникає потреба у з'єднанні декількох концентраторів або комутаторів між собою та рознесенням їх на певну відстань (рис.2.12). При цьому кількість з'єднань концентраторів обмежується таким чином, щоб пакети на шляху від відправника до одержувача проходили не більш ніж чотири концентратори. Для комутаторів такого обмеження немає, а залишається тільки єдине обмеження на загальну кількість комп'ютерів у локальній мережі. Ця кількість для мереж, що побудовані з використанням технологій сім'ї Ethernet, не може перевищувати 1024.

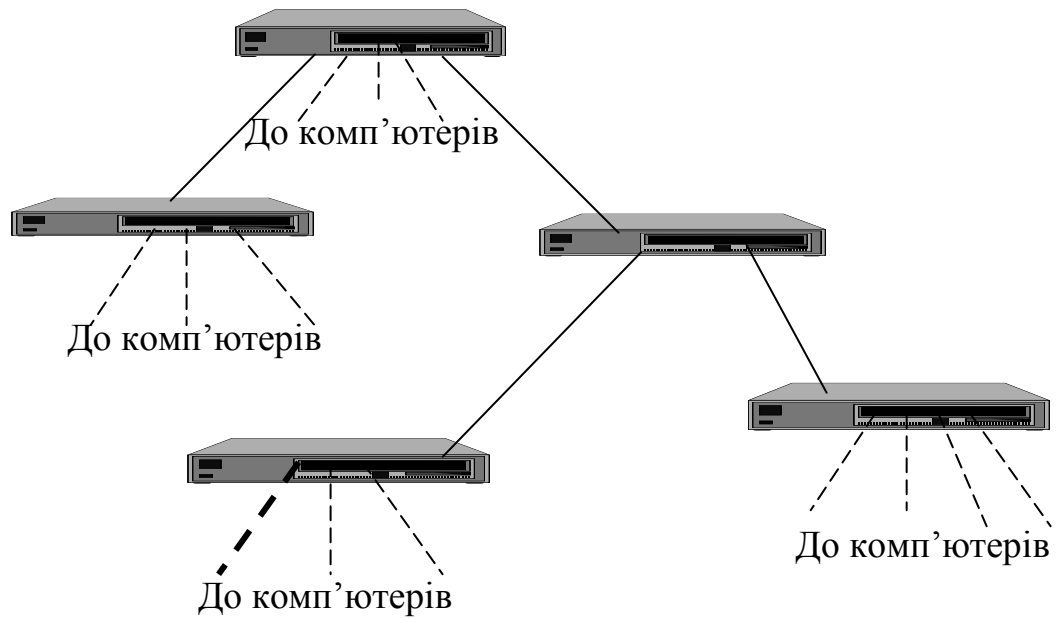


Рис. 2.12. Древоподібна топологія з'єднань концентраторів або комутаторів локальної мережі

Характеристики концентраторів та комутаторів, що користуються найбільшим попитом, наведено у таблиці 2.3.

Таблиця 2.3

Основні параметри типового активного комунікаційного обладнання локальних мереж на базі Ethernet-технологій

Назва обладнання	Кількість портів	Швидкість, Мбіт/с	Тип кабелю	Примітка
Концентратор (Hub)	4 або 8	10	Скручена пара	
	1	10	Тонкий коаксіальний	*
Концентратор	8	100	Скручена пара	
Концентратор	16 або 32	10	Скручена пара	
	1	10	Тонкий коаксіальний	*
	1	10	Товстий коаксіальний	*
Комутатор (Switch)	4, 5, 8, 16 або 24	10/100	Скручена пара	
	1 або 2	1000	Волоконно-оптичний або скручена пара	*

Примітка. Наявність портів, що описані у рядках з приміткою (*), не розповсюджується на усі моделі концентраторів або комутаторів.

Великий вибір комутаторів та концентраторів, що існує на сучасному ринку, дозволяє побудувати найрізноманітніші варіанти з'єднань.

Конфігурація з'єднань повинна бути деревоподібною. Ні в якому разі не допускається дублювання зв'язків або кільця.

Варіанти підключення комп'ютерів до концентратора або комутатора за допомогою кабелю типу скручена пара (UTP, Unshielded Twisted Pair) зображені на рис.2.13.

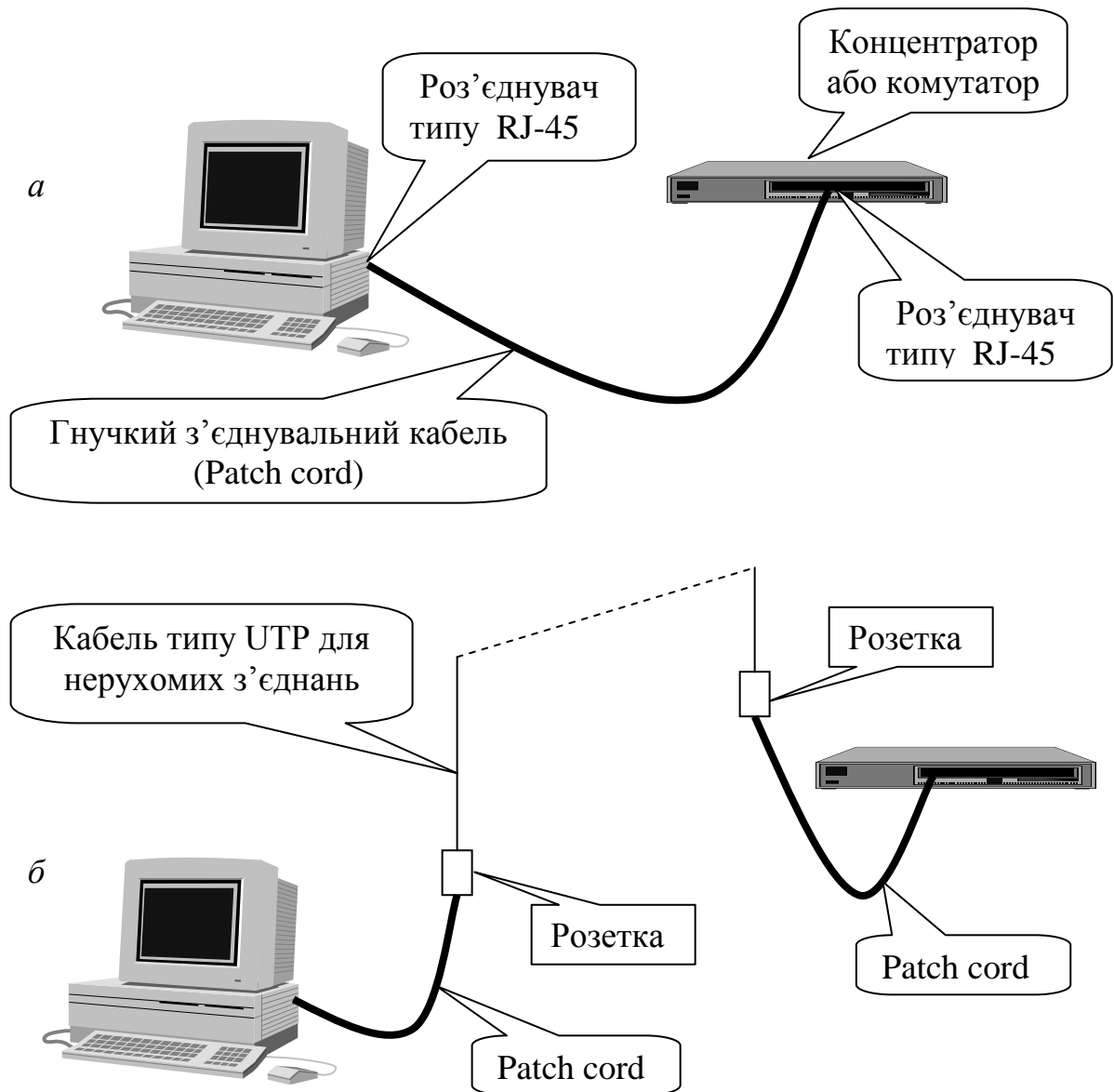


Рис. 2.13. Приєднання комп'ютера до концентратора або комутатора:

а – на малій відстані (у межах кімнати); **б** – на значній відстані (до 100 м)

Стандартні варіанти розміщення кінців скручених пар у роз'єднувачах типу RJ-45 показано у додатку 2.

Якщо відстань від комутатора або концентратора перевищує 100 метрів, то замість скрученої пари можна використовувати тонкий коаксіальний кабель (до 185 м) або товстий коаксіальний кабель (до 500 м). У випадках, коли відстань перевищує 500 метрів, можна прокладати волоконно-оптичний кабель або утворити з'єднання за допомогою телефонної пари з DSL-модемами, що мають у комплекті роз'єднувач до порту Ethernet. Останній варіант обмежує швидкість обміну інформацією з комп'ютером, що підключений до мережі за допомогою DSL-модемів.

Ділянка мережі, де для з'єднання обрано тонкий коаксіальний кабель, зображена на рис. 2.14.

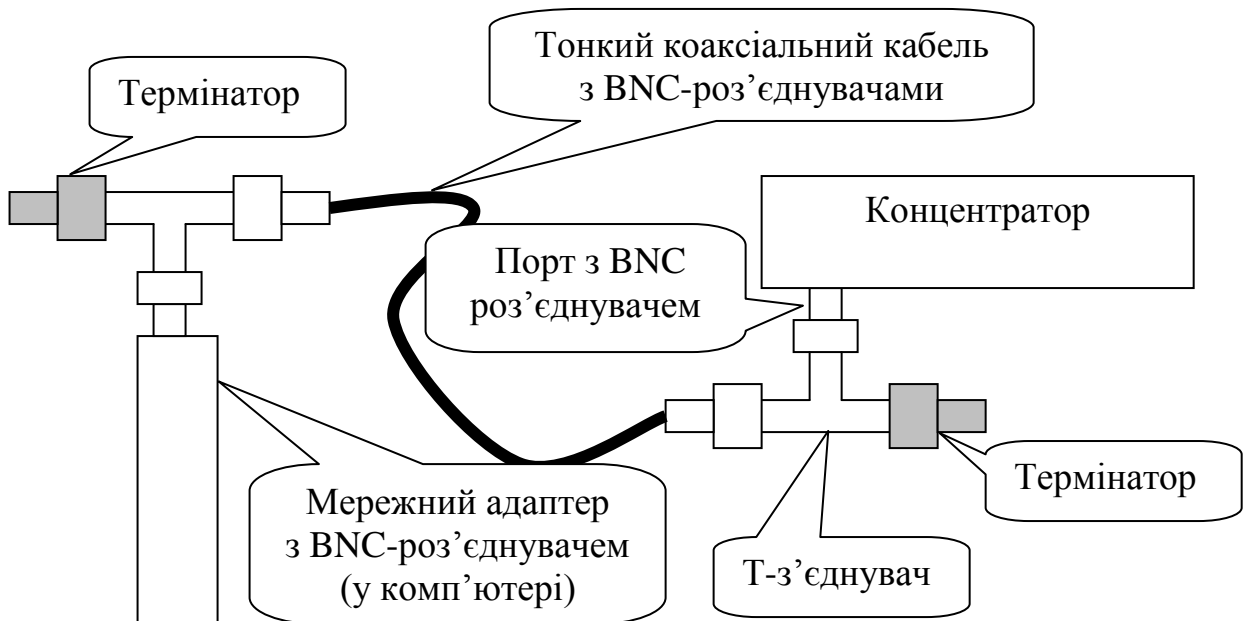


Рис. 2.14. Приєднання комп'ютера до концентратора за допомогою тонкого коаксіального кабелю

Для переходу від скрученої пари на волоконно-оптичний кабель можна використовувати конвертери – комутатори, що мають тільки два роз'єднувачі різного типу. Широкий асортимент конвертерів дозволяє реалізувати усі можливі варіанти з'єднань різнотипних кабелів.

2.2 Сучасні та перспективні мережні технології

2.2.1 Технології побудови локальних мереж

Поняття мережної технології, згадуючи, що слово технологія походить від грецьких слів τέχνη (майстерність) та λόγος (слово або наука), можна розглядати як сукупність знань про те, як створити комп'ютерну мережу. Іноді поняття мережної технології розглядають у більш широкому плані, включаючи до нього не тільки знання, але й повний набір програмних та апаратних засобів, з яких може бути побудована комп'ютерна мережа [2].

У цьому розділі ми розглянемо найважливіші особливості побудови локальних комп'ютерних мереж (ЛКМ).

Розпочнемо з каналного рівня, бо саме він пов'язаний з придбанням тих чи інших технічних засобів та прокладанням кабелів, що потребує найбільших витрат часу і коштів у процесі створення мереж.

Дві різні топології було покладено у конкуруючі між собою ще з 80-х років розробки двох, багато в чому протилежних, технологій каналного рівня ЛКМ.

Першою з них є шинна топологія з невпорядкованим груповим методом доступу до спільного середовища передавання CSMA/CD (Carrier Sense Multiply Access with Collision Detection), при якому неминучі колізії (цей метод вперше застосували ще у 1968 році на радіоканалі в мережі Aloha у Гавайському університеті). Все це й було покладено в основу технології Ethernet, розробкою якої займалися три відомі фірми DEC, Intel та Xerox.

Кільцева топологія з маркерним (впорядкованим) методом доступу була покладена в основу другої технології Token Ring. Розробка цієї технології була завершена у 1984 році відомою компанією IBM. У той час компанії IBM належало близько 90% світового обсягу виробництва обчислювальної техніки.

Недовіра до технології Ethernet була зрозумілою, бо наявність колізій відштовхувала майбутніх користувачів ЛКМ та примушувала віддавати перевагу технології Token Ring, у якій колізії неможливі. Але з часом ця точка зору змінилась, і зараз технологія Ethernet є домінуючою. Майже всі ЛКМ, яких в світі нараховується близько 10 мільйонів, побудовані на основі технології Ethernet. Чому ж так сталося?

Маркерний метод доступу, який було використано у технології Token Ring, позбавляє від колізій, бо дозвіл на передавання надається за допомогою маркера. Маркер – це спеціальний пакет, який передається між вузлами доки не потрапить на вузол, що має повідомлення для відправки.

Розглянемо випадок, коли на вузлі №1 є пакет з повідомленням, що слід відправити на вузол №3 (рис. 2.15).

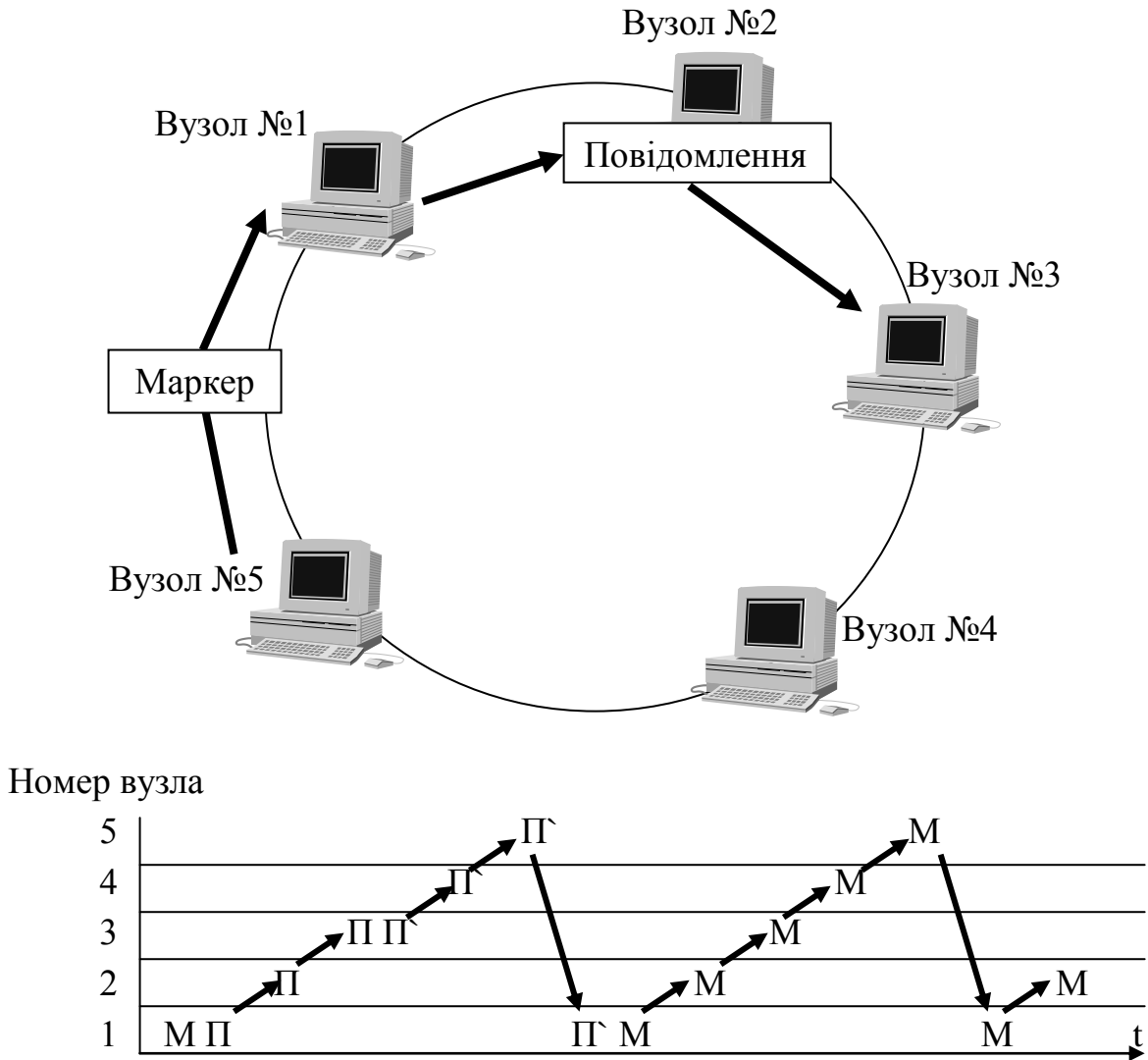


Рис.2.15. Принцип маркерного доступу

Дочекавшись маркера М (початок діаграми на рис.2.15), вузол №1 передає замість маркера пакет П з повідомленням. У заголовку пакета містяться адреси відправника та одержувача, тому вузол №2 не перехоплює пакет, а відсилає його далі по колу на вузол №3. Вузол №3, отримавши повідомлення на свою адресу, відправляє далі по колу копію

пакета П з прапорцем про отримання П'. Пакет П' по колу повинен дійти до вузла №1, де його зміст порівнюється з повідомленням, що було відправлено. У разі позитивного результату порівняння вузол №1 відправляє маркер М, який до цього часу був затриманий. Після цього рух маркера по колу відновлюється до появи наступного повідомлення.

Цей алгоритм тільки на перший погляд здається простим, бо ми не розглядали ситуації, які необхідно враховувати в реальних умовах. Ось деякі з них.

- Комп'ютери у мережі можуть вимикатись і вмикатись коли завгодно.
- Завада може знищити маркер і треба буде його відновлювати.
- Маркер під час відновлення може подвоїтись.
- Слід передбачити можливість підключення до мережі нових комп'ютерів.
- Пакет з повідомленням відправлено у той час, коли комп'ютер одержувача вимкнено.

Через наявність подібних ситуацій мережі Token Ring виявляються складнішими в експлуатації та адмініструванні у порівнянні з мережами Ethernet.

Головний недолік мережі Ethernet (наявність колізій) виявився не таким вже й серйозним у порівнянні з її перевагами.

Колізії не призводять до серйозних наслідків в умовах значного (у два-три рази) перевищення перепускної здатності каналу над середньою швидкістю передавання інформації. Це співвідношення у локальних мережах легко забезпечити, бо протяжність цих каналів у більшості не перевищує десятків метрів. Крім того, мережі Ethernet дешевше створювати і значно легше адмініструвати.

Маркерний метод доступу знайшов своє втілення у технології FDDI (Fiber Distributed Data Interface), у якій було збережено алгоритми та структуру пакетів технології Token Ring. Технологія FDDI (стандарт 1988 року) стала першою технологією ЛКМ на волоконно-оптичному кабелі. Швидкість передавання було підвищено до 100 Мбіт/с, а максимальну довжину кільця збільшено до 200 км. Вона була розрахована на великі за масштабом локальні мережі, у яких відстань між сусідніми вузлами може досягати 2 км. У цей час перепускна здатність каналів у мережах Ethernet була 10 Мбіт/с.

На початку 90-х років 10-мегабітний Ethernet ще задовольняв користувачів, бо співвідношення швидкодії комп'ютерних шин ISA або EISA до швидкості передавання було задовільним, а запас перепускної здатності був достатнім, щоб колізії не спричиняли серйозних проблем. Але з появою шини PSI (133 Мбайт/с) почали виникати проблеми через колізії. Ці проблеми було знято з впровадженням 100-мегабітної технології Fast Ethernet (стандарт 1995 року), а далі було стандартизовано технології Gigabit Ethernet (у 1998 році) та 10Gigabit Ethernet (у 2002 році).

Стрімкий розвиток технологій сім'ї Ethernet не обмежився підвищенням швидкості. У середині 90-х років для з'єднання комп'ютерів у мережах Ethernet почали застосовувати комутатори, що позбавило ці мережі від зловісних колізій, а наприкінці 1993 року було впроваджено дуплексну технологію Ethernet, яка усунула обмеження на відстань передавання. Таким чином, технологія Ethernet фактично перетворилась на універсальну технологію канального рівня мереж довільного масштабу.

Ознайомимось детальніше з цією лідируючою технологією.

Усі вузли мережі Ethernet підключені до спільного середовища передавання сигналів і мають право у будь-який момент часу розпочинати передачу, при умові що не прослуховується чужий сигнал. Через таку неупорядкованість може виникнути ситуація, коли кілька вузлів одночасно або з невеликою розбіжністю у часі розпочнуть передавання. Цього не можна уникнути за допомогою прослуховування, бо через відстань між вузлами відправлений сигнал можна відчутти лише через деякий час. Тому було використано алгоритм, який дозволяє зберігати цілісність інформації під час колізій.

Вузол-передавач продовжує прослуховування сигналів разом з передаванням. При відсутності колізії сигнал, що прослуховується, повинен співпадати з тим, що передається. У разі виявлення розбіжності припиняється передавання пакета, і замість нього передається спеціальний сигнал (jam-послідовність), який відрізняється від інформаційних пакетів і повідомляє усі вузли мережі про перехід у режим затримання початку передавання на випадковий проміжок часу. Після цього усі вузли, що мають розпочати передавання або вже розпочали передавання, повинні витримати паузу тривалістю у m інтервалів довжиною 512 проміжків між бітами, де m – ціле число, що вибирають з рівною ймовірністю у діапазоні $[0, 2^N]$, де N – номер спроби передавання даного пакета, але не більше за

- 802.2 – Logical Link Control, LLC – управління логікою передавання даних;
- 802.3 – Ethernet з методом доступу CSMA/CD.

Усе сучасне обладнання для побудови мереж Ethernet дозволяє формувати та автоматично відрізнити всі чотири варіанти кадрів (див. рис.2.16). Під позначкою кожного поля кадру наведено довжину у байтах.

DA – Destination Address – адреса одержувача.

SA – Source Address – адреса відправника.

L – Length – довжина поля даних у байтах.

Data – поле даних.

FCS – Frame Check Sequence – контрольна сума).

Ці поля однакові для всіх варіантів кадру, крім Ethernet DIX, що має ще й другу назву Ethernet II. Замість поля L у цьому кадрі міститься поле T – Type або Ether Type, що призначене для кодування типу протоколу, пакет якого розміщено у полі Data. Наприклад, для стеку TCP/IP це може бути пакет IP або ARP. Значення кодів у полі T обрано більшими за 1500, щоб легко було відрізнити кадр Ethernet DIX від усіх інших, де на цьому місці знаходиться поле L, у якому число не може бути більшим за 1500. Для протоколу IP значення T дорівнює 2048, а для ARP – 2054.

У кадрі Row 802.3, що використовувався компанією Novell у старих розробках, немає відомості про те, який пакет знаходиться у полі Data, бо там міг бути тільки пакет протоколу IPX. Це ситуація нетипова. Заголовок пакета кожного протоколу, крім протоколів верхнього рівня, повинен мати відомості про тип пакета, що вкладено. Ці відомості необхідні для виклику тої чи іншої програми обробки вкладеного пакета. У нових розробках компанії Novell використовується кадр 802.3/LLC.

Заголовок LLC, що розміщено у кадрі 802.3/LLC, дозволяє не тільки звертатись до різних програм в залежності від типу вкладеного пакета, але й керувати логікою роботи протоколу Ethernet. Він вміщує такі поля:

DSAP – Destination Service Access Point – код точки доступу до служби одержувача, що визначає ту чи іншу програму обробки пакета;

SSAP – Source Service Access Point – код точки доступу до служби відправника;

C – Control – управління, що має три варіанти структури, які зображено на рис. 2.17.

Для нунумерованих кадрів (Unnumbered)

1	1	M	P/F	M
1	1	2	1	3

Для керуючих кадрів (Supervisory)

1	0	S	–	N (R)
1	1	2	5	7

Для інформаційних кадрів (Information)

0	N (S)	P/F	N (R)
1	7	1	7

Рис.2.17. Варіанти структури поля управління

Під позначенням (або змістом) кожної ділянки поля надано кількість бітів, а інформація у них може бути занесена така:

M – тип команди;

S – службова інформація;

P/F – ознака того, що потрібна відповідь на команду;

N(S) – номер кадру, що відправлений;

N(R) – номер кадру, що очікується.

Якщо повідомлення займає більше ніж 128 кадрів, нумерація продовжується за циклом.

Заголовок SNAP (SubNetwork Access Protocol – протокол доступу до підмереж) складається з двох полів:

OUI – Organizationally Unique Identifier – код фірми, що контролює значення поля T;

T – має те саме значення, як у кадрі Ethernet DIX.

Управління логікою передавання LLC полягає у можливості вибору одного з трьох наступних режимів:

LLC1 – без встановлення з'єднання та без підтвердження;

LLC2 – із встановленням з'єднання та з підтвердженням;

LLC3 – без встановлення з'єднання, але з підтвердженням.

Різні режими управління логікою передавання потрібні для того, щоб забезпечити можливість роботи з усіма стандартизованими стеками телекомунікаційних протоколів.

У сучасних комп'ютерах з операційною системою Windows найлегше встановити стек протоколів NetBEUI, розроблений фірмами Microsoft та IBM, який надає зручні можливості для роботи у локальній мережі. Цей стек використовує режим LLC2, що гарантує вірність передавання інформації на канальному рівні.

Для роботи в мережі Інтернет треба встановити стек TCP/IP, який на канальному рівні може використовувати те саме обладнання Ethernet, що й стек NetBEUI. Обидва стеки можуть працювати одночасно на одному Ethernet обладнанні. Виявлення та виправлення помилок передавання у стеку TCP/IP виконує протокол транспортного рівня TCP, тому на канальному рівні використовується режим LLC1, що забезпечує найвищу швидкість через відсутність витрат часу на встановлення з'єднання та підтвердження. При цьому у всіх бітах байта С, крім двох перших встановлюються нулі.

Процедура встановлення з'єднання являє собою обмін службовими пакетами між відправником та одержувачем перед початком передавання інформації для впевненості у наявності зв'язку.

Після перевірки кожного пакета за контрольною сумою одержувач відправляє спеціальне повідомлення (підтвердження) про прийняття чергового пакета. Тільки після прийняття підтвердження відправник може бути впевненим про нормальне завершення процесу передавання пакета. До того часу поки не будуть прийняті підтвердження, відправник не приймає рішення про завершення передавання повідомлення, а продовжує через деякий час повторно передавати пакети, на які не отримано підтверджень.

Головною частиною заголовка MAC (Media Access Control – керування доступом до середовища) є адреси одержувача (DA) та відправника (SA) пакета. Ці адреси називають фізичними або апаратними, а найчастіше – MAC-адресами. Незважаючи на велику кількість фірм, що виробляють обладнання мереж Ethernet, не може бути двох виробів з однаковими апаратними адресами. Про це піклується комітет 802 IEEE, що визначає кожному виробникові унікальний ідентифікатор організації OUI (Organizationally Unique Identifier). Адреса кожного мережного адаптера, або іншого пристрою, що може відправляти та приймати кадри Ethernet, у

трьох старших байтах містить OUI, а у трьох правих (молодших) байтах номер виробу від організації виробника. Перші два біти OUI завжди 00.

Для визначення MAC-адреси адаптера на комп'ютері з операційною системою Windows можна скористатись командою `ipconfig /all`, результат якої можна побачити на екрані у режимі MS DOS (рис.2.18).

```

Windows 2000 IP Configuration
    Host Name . . . . . : stud1
    Primary DNS Suffix . . . . . : kit.knuba.edu.ua
    Node Type . . . . . : Hybrid
    IP Routing Enabled . . . . . : No
    WINS Proxy Enabled . . . . . : No
    DNS Suffix Search List . . . . . : kit.knuba.edu.ua
                                        knuba.edu.ua

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . : kit.knuba.edu.ua
    Description . . . . . : Realtek RTL8139 (A) PCI
    Physical Address . . . . . : 00-20-4D-40-30-A2
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address . . . . . : 10.3.61.13
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.3.61.250
    DHCP Server . . . . . : 10.3.61.233
    DNS Server . . . . . : 10.3.61.233
    Lease Obtained . . . . . : 8 грудня 2003 р. 14:03:59
    Lease Expires . . . . . : 8 грудня 2003 р. 18:03:59
  
```

Рис.2.18. Результат дії команди `ipconfig /all`

Цей результат замість висвітлення на екрані можна занести у файл типу Text DOS, якщо команду доповнити параметром: `> ім'я файла`.

Цю саму інформацію у деяких операційних системах сім'ї Windows можна одержати за допомогою команди `winipcfg /all`.

Значення MAC-адреси `00-20-4D-40-30-A2` бачимо у рядку `Physical Address`. У операційній системі FreeBSD ця адреса була б записана у формі `00:20:4d:40:30:a2`.

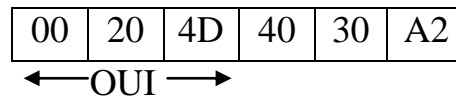
Бачимо, що у старшому (лівому) байті два перші біти мають нульове значення. Це означає, що три лівих байти `00-20-4D` являють собою OUI, а три правих `40-30-A2` – номер виробу від організації-виробника.

Для групових (multicast) та широкомовних (broadcast) адрес старший біт першого байта повинен мати значення 1.

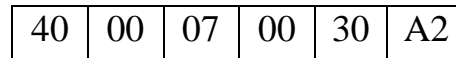
Для індивідуальних адрес обмеженого використання (наприклад, для експериментів), старші два біти першого байта повинні мати значення 01.

Приклади різних варіантів MAC-адрес зображено на рис.2.19.

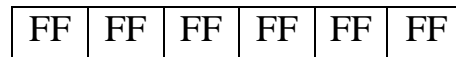
Індивідуальна адреса, що містить OUI від комітету 802 IEEE



Індивідуальна адреса, що не містить OUI (для локальних дій)



Широкомовна адреса пакета, що призначений усім вузлам мережі



Адреса пакета, що призначений групі вузлів,
які спеціально запрограмовані на прийняття пакетів з цією адресою

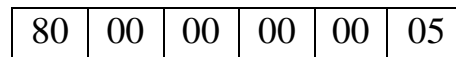


Рис.2.19. Структура байтів різних варіантів MAC-адрес

Адреса відправника може бути тільки індивідуальною, а адреса одержувача може бути як індивідуальною, так і широкомовною або груповою.

Розглянемо процедури перетворення послідовності байтів у сигнали, які призначені для передавання на фізичному рівні у мережах сім'ї технологій Ethernet. Метод такого перетворення залежить від типу середовища та номінальної швидкості передавання даних.

Сучасне обладнання мереж Ethernet автоматично вибирає найбільш ефективний режим одразу після підключення. Це стосується адаптерів, концентраторів та комутаторів найбільш розповсюдженої технології Fast Ethernet. Такі адаптери можуть підтримувати 5 режимів роботи:

- 10Base-T – по двох скручених парах категорії 3;
- 10Base-T full-duplex – по двох скручених парах категорії 3;
- 100Base-TX – по двох скручених парах категорії 5;
- 100Base-T4 – по чотирьох скручених парах категорії 3;
- 100Base-TX full-duplex – по двох скручених парах категорії 5.

Вибір того чи іншого режиму здійснюється шляхом спеціальних переговорів (Auto-negotiation), що автоматично підтримуються між пристроями каналного рівня мережі. Сценарій цих переговорів побудовано таким чином, щоб нові пристрої, які мають більшу кількість режимів, мали б можливість налагодити зв'язок зі старим обладнанням мереж Ethernet.

Для передавання послідовності бітів у канал зв'язку можуть використовуватись різні варіанти імпульсного кодування. Кілька таких варіантів зображено на рис.2.20.

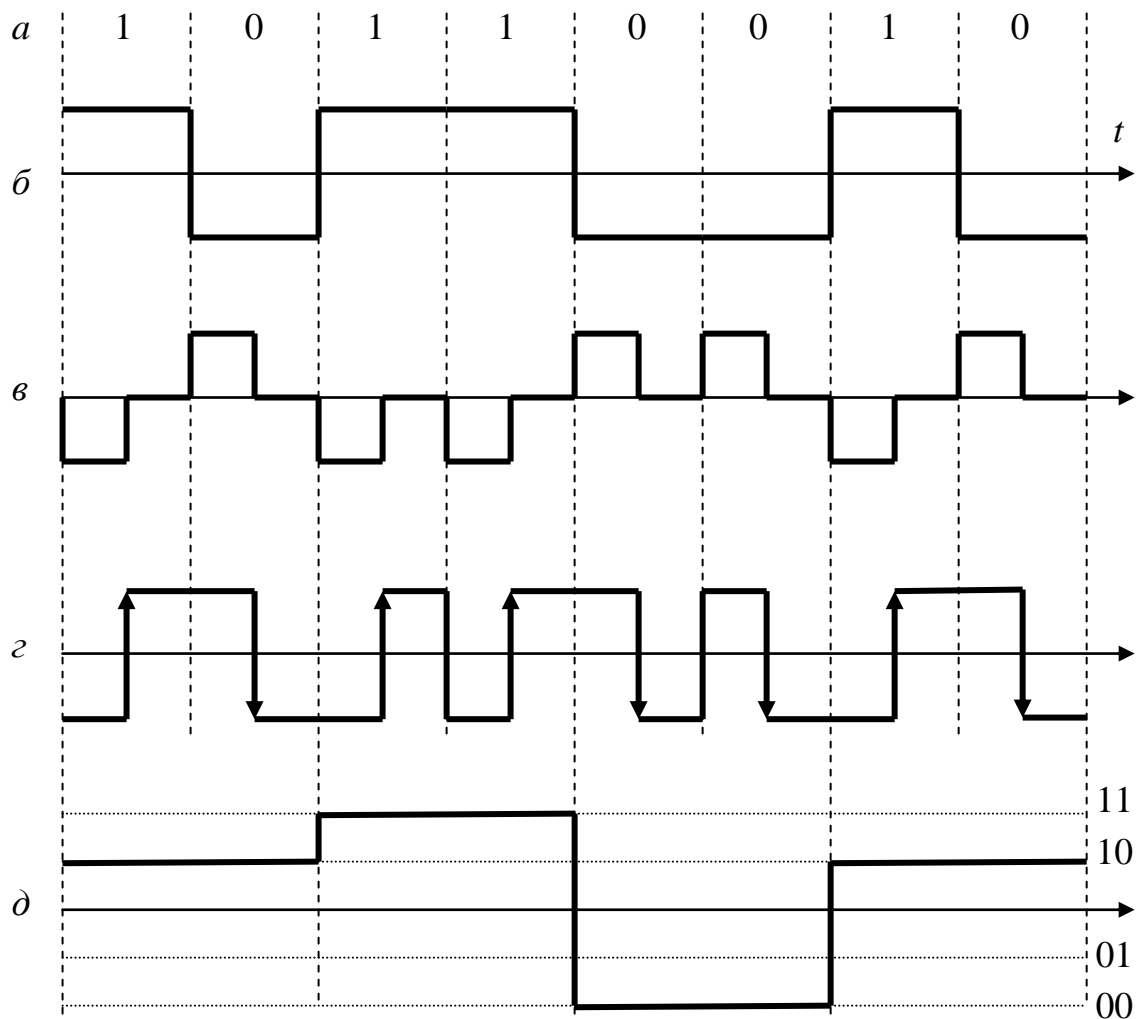


Рис.2.20. Методи кодування у каналах зв'язку:

a – вхідна послідовність бітів; *б* – код NRZ (Non Return to Zero);

в – код RZ (Return to Zero); *г* – Манчестерський код; *д* – код PAM5

Розглянемо особливості кожного з цих методів кодування.

У найпростішому методі, що зветься NRZ (без повернення до нуля), використовують два рівні потенціалу (електричної напруги або інтенсивності світлового променя). Верхній рівень означає 1, а нижній – 0. Недоліком цього методу є труднощі у синхронізації, що виникають під час передавання довгих послідовностей нулів або одиниць. Синхронізація у мережі Ethernet вирішується за допомогою таймера, який починає відлік часу після прийняття преамбули.

Тривалість передавання кожного біта на швидкості 10 Мбіт/с становить 0,1 мкс, а у кадрі може налічуватись до 12 тисяч інформаційних бітів. Протягом цього часу таймер повинен визначати оптимальні моменти для оцінювання значення кожного сигналу. Щоб забезпечити необхідну точність визначення таких моментів треба коригувати частоту таймера. Для цього використовують зміну потенціалу. Дані про відхилення фактичного моменту зміни потенціалу від того, що був визначений за таймером, є інформацією для коригування. Відсутність зміни потенціалу під час передавання довгої послідовності нулів або одиниць не дозволяє коригувати частоту таймера, що може призвести до втрати точності синхронізації. У цьому й полягає недолік методу NRZ.

У коді RZ першу половину бітового інтервалу займає імпульс, що несе інформацію (негативний імпульс означає 1, а позитивний – 0), а другу половину – нульовий потенціал. Перевагою такого методу кодування є простота синхронізації, але при цьому спектр сигналу буде удвічі ширший, ніж для коду NRZ, що пояснюється у додатку 5.

Манчестерський код, що довгий час був єдиним кодом фізичного рівня для мереж Ethernet, відрізняється найпростішою процедурою синхронізації, бо зміна потенціалу обов'язково відбувається на кожному бітовому інтервалі. Напрямок цієї зміни (у середині бітового інтервалу), що зображено стрілками на рис. 2.20 з, обрано за інформаційну ознаку. Зміна з нижнього на верхній рівень означає 1, а з верхнього на нижній – 0. У цьому коді використовується два рівні потенціалу, що забезпечує більшу завадостійкість при однаковій максимальній потужності сигналу, ніж у коді RZ.

Сучасні потреби у підвищенні швидкості передавання даних та нові можливості створення точних таймерів примусили розробляти мережні технології з більш продуктивним використанням смуги частот каналу, ніж у системах з манчестерським кодом. Звичайно, нове обладнання підтримує роботу у манчестерському коді для налагодження зв'язку із застарілими засобами, а також для автоматичного узгодження режиму роботи за технологією NWay Auto-Negotiation, що була запропонована компанією National Semiconductor у 1994 році.

У технології Fast Ethernet для передавання інформації зі швидкістю 100 Мбіт/с використовують код 4В/5В, який полягає в тому, що кожен 4 біти вихідного коду замінюють на комбінацію з 5 бітів, користуючись таблицями відповідності (рис. 2.21).

4 біти	5 бітів	4 біти	5 бітів	4 біти	5 бітів	4 біти	5 бітів
0000	11110	0100	01010	1000	10010	1100	11010
0001	01001	0101	01011	1001	10011	1101	11011
0010	10100	0110	01110	1010	10110	1110	11100
0011	10101	0111	01111	1011	10111	1111	11101

Рис.2.21. Відповідність 4 і 5 бітових послідовностей для коду 4В/5В

Після такого перекодування виключається можливість появи довгих послідовностей нулів або одиниць, що дозволяє використовувати код NRZ. При цьому для забезпечення швидкості передавання інформації 100 Мбіт/с необхідно передавати біти зі швидкістю 125 Мбіт/с, що не призводить до суттєвого розширення спектра сигналу і може бути забезпечено на кабелі типу скрученої пари категорії 5.

У технології Gigabit Ethernet для передавання інформації із швидкістю 1000 Мбіт/с використовують код PAM5, у якому кожним двом бітам відповідає один з п'яти рівнів потенціалу. При цьому тривалість імпульсів вибрано 8 нс (такою ж як в технології Fast Ethernet). Це дозволяє досягти швидкість у 250 Мбіт/с на кожній парі категорії 5. На чотирьох скручених парах, що використовують одночасно, максимальна швидкість дорівнює 1000 Мбіт/с.

У сучасних мережах Ethernet можуть взаємодіяти декілька різношвидкісних технологій. Для забезпечення одночасної роботи цих технологій не обов'язково втручатись адміністратору. Розглянемо як це відбувається за допомогою технології NWay Auto-Negotiation.

Партнерами операції узгодження режимів роботи є порти адаптерів, комутаторів та концентраторів. Кожен партнер повідомляє іншому про технологію, яку він підтримує, надсилаючи імпульсні послідовності у манчестерському коді з періодом 16,8 мс. Найстаріше обладнання, що підтримує тільки один режим 10Base-T, надсилає лише один імпульс NLP (Normal Link Pulse), що свідчить про його працездатність. Обладнання Fast Ethernet та Gigabit Ethernet надсилають інформаційне слово LCW (Link Code Word), структура якого наведена у таблиці 2.4.

Таблиця 2.4

Призначення полів інформаційного слова LCW

Найменування поля	Кількість бітів	Призначення Поля
Селектор	5	Код базової технології
Технологічні можливості	8	Код режиму роботи
RF (Remote Fault)	1	Прапорець, що повідомляє про помилку
Ask	1	Прапорець підтвердження
NP (Next Page)	1	Прапорець наявності додаткової інформації (продовження)

Технологія узгодження передбачає розширення у разі появи нових базових технологій та режимів роботи.

Процедура узгодження полягає у виборі найбільш пріоритетного з можливих режимів роботи. Пріоритети обрано таким чином, щоб режимам з більшою швидкістю передавання відповідали вищі пріоритети.

Найбільші пріоритети надані дуплексним режимам. Це такі режими, що разом з появою комутаторів, фактично призвели до революційних змін у технології Ethernet. Розглянемо детальніше ці зміни.

Основою створення технології Ethernet було спільне середовище передавання з неминучістю колізій. На початку цим середовищем був радіоканал (ефір). У перекладі з англійської Ether означає ефір, а net є скороченням від Network – мережа. Далі було впроваджено коаксіальний кабель, що виконував функції ефіру, залишаючись спільним середовищем. Поява концентраторів полегшила обслуговування мережі, але не позбавила від спільного середовища з колізіями. Все це примушувало враховувати суворі обмеження на максимальну відстань між вузлами мережі та кількість підсилувачів або концентраторів на шляху проходження сигналу. А розробникам нових мережних технологій треба було враховувати вимоги до мінімальної довжини кадру.

Дуплексний Ethernet являє собою два окремі фізичні середовища передавання між двома пунктами. При цьому одночасний початок передавання з двох пунктів не призведе до колізії, бо кожному з напрямків передавання надається окреме середовище. Ніяких обмежень на відстань, що пов'язані з можливістю колізій, у дуплексному режимі не існує.

Комутатор, хоч і нагадує за зовнішніми ознаками концентратор, але він виконує розподіл середовища передавання на окремі сегменти. Кожен порт комутатора, що відповідає своєму сегменту мережі, має окремий процесор з блоком пам'яті на декілька кадрів. Сигнали від вузлів мережі потрапляють не у спільне середовище, а у пам'ять свого сегмента. Зрозуміло, що колізії при цьому неможливі.

Головний процесор комутатора, що забезпечує обмін інформацією між сегментами, має високу швидкодію. Він запам'ятовує фізичні адреси кожного вузла та пересилає пакети між сегментами з врахуванням адрес одержувачів. Якщо адреса невідома, пакет надсилається на всі вузли. Поступово таблиця адрес у комутаторі доповнюється, бо у кожному пакеті, що потрапляє на який завгодно порт комутатора, є фізична адреса відправника. Ця адреса запам'ятовується разом з номером порту, з якого надійшов цей пакет. Різні порти комутатора можуть приймати та передавати пакети з різною швидкістю, бо швидкість, з якою було прийнято пакет на одному з портів, не залежить від швидкості, з якою цей пакет буде передано з другого порту.

Крім каналного рівня, для забезпечення роботи локальної мережі необхідно на кожному комп'ютері встановити програмне забезпечення одного або декількох стеків протоколів верхніх рівнів. Їх конкретний вибір залежить від потреб користувача, типу комп'ютера та операційної системи. Канальний адаптер та інше обладнання мережі Ethernet забезпечує незалежну роботу для довільної кількості стандартних стеків протоколів верхнього рівня.

Головним обмеженням технологій локальних мереж є неможливість перевищити максимальну кількість вузлів. Для технології Ethernet ця кількість становить 1024. Подолання цього обмеження є задачею рівня міжмережних зв'язків або мережного рівня.

2.2.2 Технології побудови глобальних мереж

Створення мереж глобального масштабу ставить на перший план задачу подолання двох головних обмежень, що існують у технологіях локальних мереж, а саме: обмежень на кількість вузлів та на відстань передавання. Крім цього, важливо забезпечити можливість об'єднувати у єдину мережу різноманітні комп'ютери та локальні мережі, що побудовані на обладнанні від різних виробників. Все це у наш час забезпечує комплекс

мережних технологій, що називають Internet-технологіями. Основою цього комплексу можна вважати стек протоколів TCP/IP, який було розроблено у період з 1975 до 1979 року за ініціативою Міністерства оборони США для мережі ARPAnet (Advanced Research Project Agency network). Ця мережа, що у той час об'єднувала кілька десятків комп'ютерів крупних навчальних та наукових закладів США, зараз визнана початком всесвітньої мережі Інтернет. З 1983 року мережу ARPAnet було повністю переведено на стек TCP/IP, після чого розпочався швидкий розвиток цієї мережі. Назва Інтернет з'явилась у 1989 році як похідна від назви протоколу IP.

Широке розповсюдження стеку TCP/IP та створення на його основі мережі Інтернет пояснюється гнучкістю системи адресації та економним використанням каналних ресурсів.

Розглянемо особливості системи адресації стеку TCP/IP, у складі якої прийнято виділяти три типи адрес.

- Апаратні адреси, що використовуються у пакетах каналного рівня, наприклад MAC-адреси для мереж сім'ї Ethernet.
- IP-адреси, що посідають головне місце у процесі доставки пакетів.
- Символьні адреси, які називають доменними іменами. Цими адресами ми зазвичай користуємось для доступу до ресурсів у мережі Інтернет.

З апаратними адресами ми ознайомились у попередньому підрозділі 3.1 на прикладі технології Ethernet (MAC-адреси). Взагалі, тип апаратних адрес залежить від того, яке обладнання використовується на каналному рівні цієї чи іншої мережі, бо стек TCP/IP забезпечує взаємодію з усіма стандартними засобами каналного рівня. У деяких випадках, коли маршрутизатори зв'язані між собою окремим каналом, апаратних адрес може не бути.

IP-адреси являють собою адресну частину IP-пакетів. Ці пакети призначені для доставки інформації у мережах зі складною структурою. Мережі, де використовують IP-пакети називають IP-мережами.

Усі вузли IP-мережі розподіляють на такі дві категорії.

- Host (хост) – вузол, що відсилає та приймає інформацію у вигляді IP-пакетів.
- Router (маршрутизатор) – вузол, що пересилає IP-пакети з однієї мережі в іншу.

Структуру мережі такого типу зображено на рис.2.22.

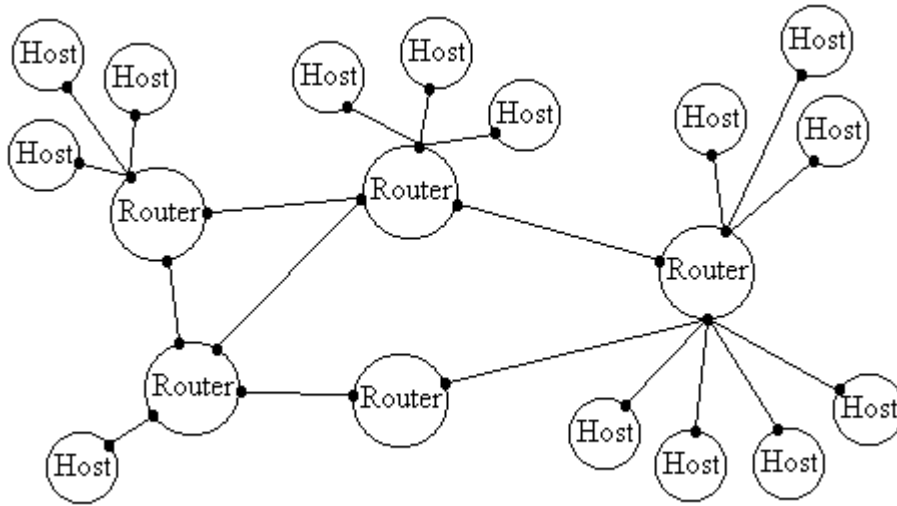


Рис.2.22. Варіант логічної структури IP-мережі

Маршрутизатори мають декілька з'єднань (не менше двох), що відрізняє їх від хостів. Фізично один комп'ютер може одночасно бути маршрутизатором та хостом, але за логічною структурою це будуть два різні вузли. Кожному із з'єднань, що позначені на рис.2.22 чорними крапками, надається своя унікальна IP-адреса.

Довжина IP-адреси становить 32 біти (4 байти). Записують IP-адреси у вигляді чотирьох десяткових чисел від 0 до 255, відокремлених крапками, наприклад 180.38.0.214. Кожне число відповідає байту.

Загальна кількість IP-адрес не може перевищити 4,3 млрд. Вважають, що цієї кількості буде недостатньо для мережі всесвітнього масштабу і прогнозують в період між 2005-2010 роками перехід на шосту версію протоколу IP (IPv6), де довжину IP-адрес збільшено до 128 бітів.

Виникнення дефіциту IP-адрес, скоріш за все, можна пояснити не їх обмеженою кількістю, а невпорядкованістю системи розподілу адрес між користувачами, що мало місце на початку формування адресного простору мережі Інтернет. Справа в тому, що у розподілі IP-адрес не враховувалось територіальне розміщення мереж. Доцільно було б скористатись досвідом міжнародної телефонії, де на початку номера розміщені цифри, що означають код держави, далі – код міста, а останні цифри визначають номер конкретного абонента. Але через те, що Інтернет деякий період розповсюджувався стихійно, розподіл адрес провадився без урахування перспективи розвитку.

У структурі 32-бітної IP-адреси виділяють дві логічні частини. Ліва (старша) частина означає адресу мережі, а права (молодша) – адресу вузла у цій мережі. Спочатку було запропоновано визначати розмір лівої та правої частин за допомогою класів А, В, С, D та Е (рис.2.23).

	Адреса мережі	
Клас А	0 8 бітів	Адреса вузла (24 біти)
Клас В	10 Адреса мережі (16 бітів)	Адреса вузла (16 бітів)
Клас С	110 Адреса мережі (24 біти)	Адреса вузла
Клас D	1110	28 бітів для групових адрес
Клас Е	11110	Цей клас зарезервовано для експериментів

Рис.2.23. Класи IP-адрес за документом RFC 791

Як бачимо з рис.2.23, завдяки розподілу на класи, легко визначити довжину лівої та правої частин адреси в залежності від значення бітів на початку адреси. Але вже в кінці 80-х років почали відчуватись серйозні недоліки цієї системи. Так, клас А, що запланований на дуже великі мережі з кількістю вузлів до 16 777 214, був не затребуваний, а клас С, у якому кількість вузлів не може перевищувати 254 (адреси вузлів з нулів та з одиниць заборонені), утворює проблеми з маршрутизацією через велику кількість мережних адрес. У класі С загальна кількість адрес мереж перевищує два мільйони, а маршрутизатор, щоб визначити маршрут для кожного пакета, повинен перебрати всі можливі варіанти цих адрес. Проблеми з маршрутизацією почали утворюватись у 1992 році, коли число мереж було близько 30000. Фактично тільки клас В, у якому кількість адрес для мереж становить 16384, а для вузлів – 65534, задовольняв усі вимоги, але був швидко вичерпаний.

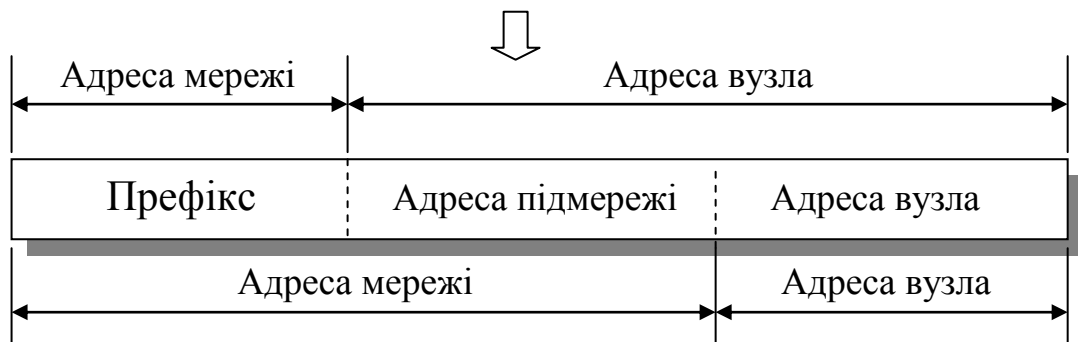
Для подолання кризової ситуації з призначенням IP-адрес винайшли засоби CIDR (Classless Inter-Domain Routing – безкласова міждоменна маршрутизація) та VLSM (Variable Length Subnet Masks – маски підмереж змінної довжини), де маска означає кількість бітів у лівій частині. Ці засоби дозволяють розподіляти адреси незалежно від класів А, В та С.

Метод CIDR дозволив організації IANA (Internet Assigned Numbers Authority), яка має абсолютну владу по розподілу адрес у мережі Інтернет, виділяти блоки IP-адрес без класових обмежень.

Для позначення блоків IP-адрес зараз використовують такий запис 206.16.0.0/16, де число 16 означає розмір у бітах лівої частини IP-адреси. Цю частину ще називають префіксом. Усі біти правої частини адреси у цьому записі заповнюють нулями.

Метод VLSM дозволяє провайдерам послуг Інтернет, що отримали у власне розпорядження великий блок IP-адрес, розподіляти адреси між своїми підмережами також без класових обмежень. У структурі IP-адреси тепер можна виділити групу бітів у середній частині, що означають адресу підмережі (рис.2.24).

З точки зору IANA (зовнішня маршрутизація)



З точки зору провайдер (внутрішня маршрутизація)

Рис.2.24. Структура IP-адреси з урахуванням створення підмереж

Така структура IP-адреси нагадує міжнародний номер телефону, де префікс відповідає коду держави, адреса підмережі – коду міста, а решта – номеру телефону абонента. Проблему з маршрутизацією було вирішено шляхом раціонального розподілу на зовнішню і внутрішні (автономні) системи визначення маршрутів (рис. 2.25).

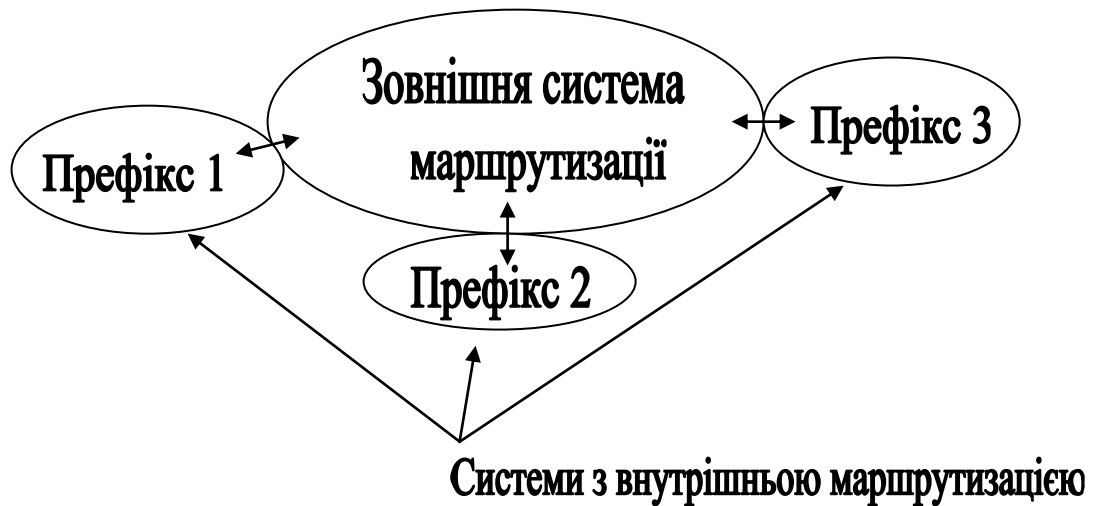


Рис.2.25. Розподіл маршрутизації на автономні системи

Як бачимо з рисунка, для маршрутизаторів зовнішньої системи, що орієнтуються на префікси, у даному випадку існують тільки три мережі. А у системах із внутрішньою маршрутизацією усі пакети з чужим префіксом одразу відсилають у зовнішню систему. Такий розподіл позбавляє від необхідності на кожному маршрутизаторі тримати весь список мережних адрес. Розмір цього списку обмежується внутрішніми та суміжними мережами своєї системи.

На основі цього розподілу виникло поняття автономної системи, яке визначено документом RFC 1930 у 1996 році.

Автономна система – група з одного або з декількох префіксів IP-адрес для однієї або декількох, що з'єднані між собою, мереж, які мають єдину та чітко визначену політику маршрутизації.

Фактично під це поняття підпадають як системи з внутрішньою маршрутизацією, так і зовнішня система. Крім того, не виключається можливість встановлення додаткових зв'язків між будь-якими автономними системами. Але чим більше таких зв'язків, тим складніше маршрутизація, а відповідно – збільшення часу обробки кожного пакета, що зменшує продуктивність системи передавання. У виборі оптимальної кількості зв'язків та встановленні обмежень на їх використання і полягає політика маршрутизації кожної автономної системи. Зараз усі автономні системи мережі Інтернет мають офіційний статус та реєстраційний номер.

Адреси класу D (див. рис.2.23) призначаються групам вузлів мережі Інтернет. Пакет з такою адресою доставляють на всі вузли конкретної групи. Для цього у кожний маршрутизатор, що може зустрітись на шляху

пакета, вводять інформацію про напрямки передавання по кожній груповій адресі. Адреси цього класу не знайшли широкого використання.

Важливим аргументом за відсутність дефіциту в кількості IP-адрес є можливість необмеженого використання внутрішніх адрес для всіх комп'ютерів, що працюють у мережі Інтернет як клієнти. Адреси, що зарезервовані ICANN (Internet Corporation for Assigned Names and Numbers) для використання у внутрішніх мережах, наведено у таблиці 2.5.

Таблиця 2.5

IP-адреси, що зарезервовані ICANN, для внутрішніх мереж

Клас	Діапазон IP-адрес	Кількість адрес
A	10.0.0.0 – 10.255.255.255	16 772 216
B	172.16.0.0 – 172.31.255.255	1 048 576
C	192.168.0.0 – 192.168.255.255	65 536

Ці адреси не використовуються у загальній частині мережі Інтернет. Ними можна забезпечити будь-яку кількість внутрішніх мереж, бо одні й ті самі адреси можна використовувати у різних мережах, також можна у кожній внутрішній мережі створювати свої додаткові внутрішні мережі. При цьому усі вузли цих мереж можуть мати доступ до мережі Інтернет за допомогою технології NAT (Network Address Translation – трансляції мережних адрес) або NAPT (Network Address Port Translation – трансляції мережних адрес портів).

Фактично, адреси у загальній частині мережі Інтернет (такі адреси прийнято називати реальними IP-адресами) потрібні тільки для серверів та маршрутизаторів, до яких необхідно забезпечити загальний доступ. Усі інші вузли мережі Інтернет можуть не мати реальних адрес. Докладніше технологію NAT буде розглянуто у наступному параграфі 4.3.

Існують IP-адреси для спеціального використання, що називають особливими IP-адресами. Перелік цих адрес наведено у таблиці 2.6.

Таблиця 2.6

IP-адреси, що зарезервовані для спеціального використання

Адреса у двійковому вигляді	Призначення
000000 ... 000000 (усі 32 нулі)	Пакет адресований на вузол, де цей пакет був сформований
0000.....0000<адреса вузла> (нулі замість адреси мережі)	Пакет адресований вузлу своєї ж мережі
1111111 ... 111111111 (усі 32 одиниці)	Пакет адресований усім вузлам своєї мережі
<адреса мережі>0000 ... 0000 (нулі замість адреси вузла)	Таку адресу зарезервовано для позначення мереж в цілому і не рекомендовано використовувати як адресу конкретного вузла
<адреса мережі>1111 ... 1111 (одиниці замість адреси вузла)	Пакет адресований усім вузлам мережі, що визначена адресою

Крім цього, зарезервовано діапазон адрес 127.0.0.0 – 127.255.255.255, з яких використовують тільки одну адресу 127.0.0.1 для тестування працездатності програмного забезпечення стеку протоколів TCP/IP на своєму комп'ютері за допомогою команди ping.

Якщо ввести команду ping 127.0.0.1 на комп'ютері, де встановлено стек протоколів TCP/IP, отримаємо відповідь про нормальну доставку пакетів, хоч цей комп'ютер може бути і не підключеним до мережі.

Доступ до необхідного ресурсу у мережі Інтернет не в кожному випадку можна отримати за допомогою IP-адреси. Часто буває, що сервер, на якому знаходяться декілька різних ресурсів, має тільки одну реальну IP-адресу. Трапляються випадки коли один ресурс знаходиться на декількох серверах з різними IP-адресами. Тобто IP-адреси буває недостатньо для визначення місця знаходження потрібного ресурсу. При цьому виникає необхідність у використанні символьних адрес, які ще називають доменними іменами. Крім того, символьними адресами зручніше користуватись, ніж числовими, бо їх легше запам'ятовувати.

Система доменних імен DNS (Domain Name System) виникла як розвиток системного файла hosts.txt ще з мережі ARPAnet, у якому знаходилась таблиця відповідності IP-адрес до символьних імен. Головна задача системи DNS – це знаходження IP-адреси сервера, на якому

розміщено ресурс, що має задане доменне ім'я. Через величезну кількість доменних імен стало неможливим зберігати ці імена у одному файлі.

Першу версію DNS було створено ще у 1983 році, а роботи з її вдосконалення тривають.

До складу сучасної системи DNS відносять три основні компоненти.

- Розподілена база доменних імен (DNS database).
- Сервери імен (name server).
- Клієнтські програми визначення IP-адрес (name re-solver).

Простір доменних імен нагадує деревоподібну файлову структуру (рис. 2.26).

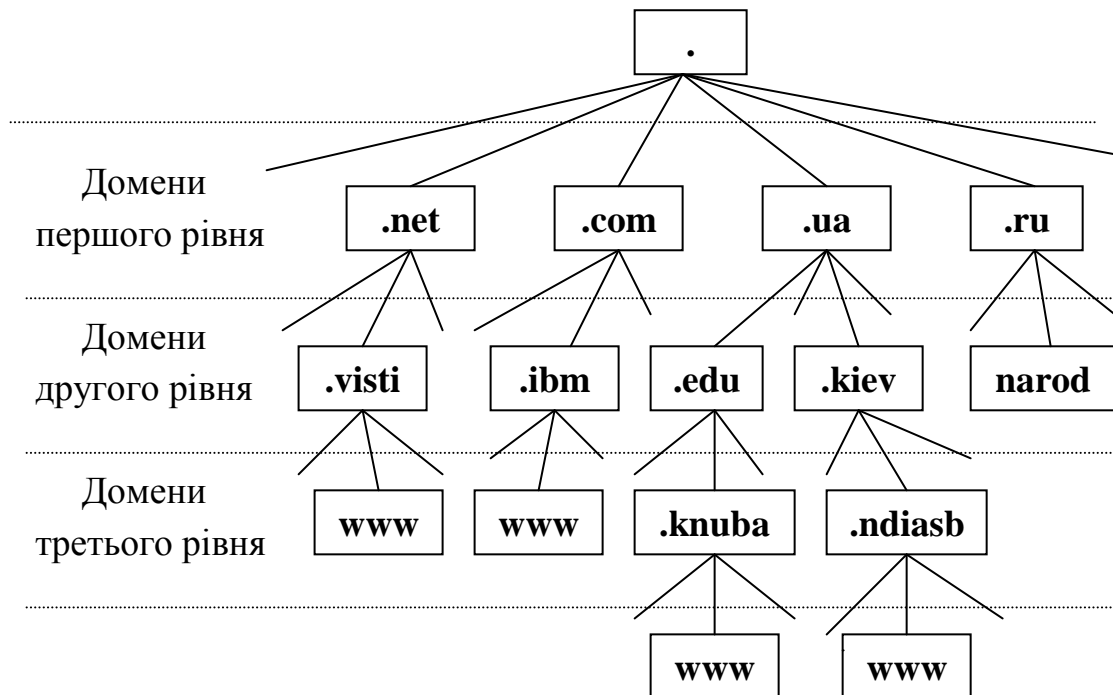


Рис.2.26. Фрагмент структури простору доменних імен

Корінь цього дерева позначений символом “.” (крапка). Цей символ повинен стояти у кінці кожного доменного імені, але у форматі інтерфейсу користувача його не ставлять. У записах, що знаходяться в базі даних, відсутність цієї крапки є грубою помилкою.

Зміст бази даних DNS коригується вручну у текстових файлах, після чого за допомогою програми з цих файлів формуються рядки бази даних, що мають назву resources records (записи про ресурси). Ця база має такі шість полів:

NAME – ім'я ресурсу (255 байт).

TYPE – тип ресурсу.

CLASS – клас ресурсу.

TTL – час зберігання запису про ресурс у пам’яті користувачів.

RDLLENGTH – довжина поля даних (число до 65535).

RDATA – дані (до 65535 байт).

Зразок текстового файлу для коригування записів у базі даних DNS зображено на рис. 2.27.

```

$TTL 86400
dim.kiev.ua. IN SOA ns2.ndiasb.kiev.ua. adm.ndiasb.kiev.ua. (
    200304121;serial number
    28800 ;refresh period
    1800 ;retry refresh this often
    604800 ;expiration period
    86400 ;minimum TTL
)

    IN NS ns2.ndiasb.kiev.ua.
    IN NS ns2.elvisti.kiev.ua.

    IN MX 5 smtp.ndiasb.kiev.ua.
    IN MX 10 smtp2.visti.net.
    IN A 195.64.255.162

www IN A 195.64.255.162
ftp IN A 195.64.255.162

```

Рис.2.27. Текстовий файл, що відповідає одній з зон бази даних DNS

У першому рядку цього файлу задано значення TTL в секундах.

У другому рядку знаходиться початок запису типу SOA (Start of Authority). З цього запису починається зона домену, ім’я якого стоїть на початку рядка (у полі NAME).

Параметр IN означає клас ресурсу (він відповідає полю CLASS). В нашому прикладі використовується тільки один клас IN (Internet).

Запис типу SOA у полі RDATA має сім параметрів, що відділяються один від одного пропусками. Перший параметр означає ім’я головного (primary) сервера DNS, на якому знаходиться ця зона. Другий – адреса електронної пошти особи, що відповідає за DNS-сервер. Для відправлення листів до цієї особи слід замінити першу крапку у адресі на символ @. У кінці рядка стоїть ліва дужка, що свідчить про наявність продовження запису у наступних рядках до появи правої дужки. Наступні 5 числових параметрів можна було б написати у одному рядку без дужок. Вони

записані у окремих рядках тільки для зручності читання. Значення числових параметрів ми розглянемо трохи нижче, а зараз звернемо увагу на крапки з комою. Вони означають кінець рядка. Кінцеві символи, включаючи крапку з комою, не заносяться у базу даних DNS.

Далі у рядках наведено записи наступних трьох типів.

NS – ім'я DNS серверу. Кількість таких записів дорівнює кількості серверів (головного та допоміжних), у яких розміщено цю зону DNS.

MX – ім'я сервера, на який слід відправляти електронну пошту. У цих записах числа 5 та 10 означають пріоритети. Числа вибирають які завгодно, але враховують, що меншому числу відповідає вищий пріоритет.

A – IP-адреса вузла, де знаходиться ресурс, ім'я якого вказано у полі NAME.

В усіх цих записах пропуски на початку рядку означають, що поле NAME буде скопійоване із запису SOA. Текст на початку рядка, що не закінчується крапкою, буде доповнено крапкою та копією поля NAME з запису SOA. Для останніх двох рядків поля NAME будуть виглядати, як `www.dim.kiev.ua.` та `ftp.dim.kiev.ua.` відповідно.

Сервери DNS відносно джерела інформації бувають:

- головними або первинними (Primary Name Server), у яких базу даних заповнюють та коригують вручну;
- допоміжними або вторинними (Secondary Name Server), у яких база даних регулярно копіюється з головного сервера;
- кешуючі (Cache only Server), що зберігають кешовану інформацію.

Головний та допоміжний сервери DNS повинні розміщуватись у різних мережах. Необхідно, щоб існував хоч один допоміжний сервер. Сервер може бути одночасно головним для одних зон та допоміжним для інших.

Функціонування системи DNS у разі сучасної версії програмного забезпечення BIND v.4.9 має такий вигляд.

Допоміжні сервери поновлюють свої дані від головного сервера згідно числових параметрів запису SOA (див. рис. 2.27).

Перший числовий параметр, що має назву `serial number`, являє собою довільне число, яке слід змінювати під час коригування зони DNS.

Другий числовий параметр являє собою період запитів (у секундах) від допоміжного сервера до головного. Копіювання даних відбувається тільки у тому разі, коли виявляється заміна параметру `serial number`.

Третій числовий параметр являє собою період повторень запитів у разі невдалої спроби встановлення зв'язку (у секундах).

Четвертий числовий параметр обмежує період невдалих спроб до моменту їх остаточного припинення.

Останній числовий параметр обмежує знизу значення TTL.

Розглянемо процедуру визначення IP-адреси за допомогою DNS.

Клієнтська програма робить запит до DNS-сервера, що обслуговує мережу клієнта. Якщо у кеші сервера є відповідь на запит клієнта, він одразу відповідає. Інакше, сервер починає процедуру опитування інших серверів, починаючи з корінного. Адреса корінного серверу завжди відома.

За алгоритмом роботи сервери DNS можуть бути рекурсивними або ітеративними (не рекурсивними). Рекурсивними називають такі сервери, які можуть формувати запити до інших серверів з метою здобуття остаточної відповіді про IP-адресу ресурсу. Ітеративні сервери не формують запити до інших серверів, а дають не повну відповідь у вигляді IP-адреси наступного сервера, до якого слід звертатись за відповіддю.

Корінні сервери завжди ітеративні. Вони надають відповідь у вигляді списку IP-адрес DNS серверів, які обслуговують домен першого рівня. Наприклад, якщо у запиті задано ім'я `www.dim.kiev.ua`, то у відповіді будуть адреси серверів домену `ua`, до яких слід звертатись із цим самим запитом.

Після одержання такої відповіді перший сервер, який є рекурсивним, формує черговий запит за IP-адресами, що отримані у списку.

Так буде продовжуватись доти, поки не прийде остаточна відповідь у вигляді IP-адреси або відмови. Цю відповідь сервер відправляє клієнту, а той використовує її під час формування заголовків IP-пакетів, структуру яких наведено у таблиці 2.7.

Таблиця 2.7

Структура заголовка IP-пакета

Найменування даних	Кількість біт даних	Значення даних, або приклади заповнення
Номер версії	4	0100 для IPv4 (версія 4 протоколу IP)
Довжина заголовка у 32-бітних словах	4	від 0101 до 1111 (від 20 байт основної частини заголовка до 60 байт)
TOS Тип сервісу (Type Of Service)	3	Пріоритет від 000 до 111 (111 – вищий)
	1	1 – мінімізувати затримку передавання
	1	1 – максимізувати перепускню здатність
	1	1 – максимізувати надійність
	1	1 – мінімізувати вартість передавання
	1	1111 – максимізувати безпечність
Загальна довжина пакета у байтах	16	Для мереж сім'ї Ethernet 1500 байт. Не може бути більше ніж 65535 байт
Ідентифікатор для фрагментації	16	Всі фрагменти одного пакета мають однакове значення цього ідентифікатора
Зарезервований біт	1	Завжди нульовий
Прапорець DF	1	1 – заборона фрагментації пакета
Прапорець MF	1	1 – цей фрагмент не останній
Зміщення	13	Кількість байт від початку поля даних
Час існування TTL (Time To Live)	8	Кількість вузлів, що може пройти пакет до моменту його знищення
Тип протоколу верхнього рівня	8	1 – ICMP, 6 – TCP, 17 – UDP
Контрольна сума заголовка	16	Цю суму перераховують на кожному вузлі після зменшення TTL
IP-адреса відправника пакета	32	
IP-адреса одержувача пакета	32	
Додаткові дані, яких може не бути (IP OPTIONS)	1	1 – слід копіювати у всіх фрагментах
	2	Клас додаткових даних (0 або 2)
	5	Номер варіанта додаткових даних
Довжина варіанта додаткових даних	8	Кількість байтів у варіанті додаткових даних
Доповнення даних кожного варіанта до 32-бітного слова	0 або 16	

Значення першого байта додаткових даних наведено у таблиці 2.8.

Таблиця 2.8

Варіанти додаткових даних IP-пакета

Номер варіанта	Клас даних	Біт-ознака копіювання	Призначення варіанта додаткових даних
0	0	0	Кінець додаткових даних
1	0	0	Нічого не робити
2	0	1	Таємно
3	0	1	Обов'язково пройти IP-адреси за списком
4	2	0	Скласти список відліків часу по вузлах
5	0	1	Цілком таємно
7	0	0	Скласти список IP-адрес на маршруті
9	0	1	Пройти тільки по IP-адресам, що у списку

Додатковими даними зручно користуватись для тестування мережі. Для цього можна скористатись командою `ping`, у параметрах якої задають необхідний варіант.

Призначення протоколу IP полягає у доставці пакетів за адресою до одержувача. Точний маршрут пакета можна вказати за допомогою додаткових даних IP-заголовка (варіант номер 9), але для цього на боці відправника треба знати IP-адреси усіх маршрутизаторів, які знаходяться на шляху передавання пакета. Це у більшості випадків неможливо, бо структура мереж часто змінюється. Варіант номер 9 використовують для тестування мереж, а у інших випадках маршрут IP-пакетів визначають автомати, що закладені у маршрутизаторах.

Процедуру визначення маршруту передавання пакетів називають **маршрутизацією (routing)**.

Існує велика множина алгоритмів маршрутизації. У найпростіших випадках такі алгоритми реалізують за допомогою програмних модулів, що інтегровані у мережному програмному забезпеченні. Для вузлів мереж великої потужності функції маршрутизації виконують спеціальні процесорні блоки. Загально визнаним лідером у виробництві таких блоків є фірма CISCO.

Усі сучасні алгоритми маршрутизації побудовані на базі маршрутних таблиць (таблиць маршрутизації), на які не існує загального стандарту.

Таблицю маршрутизації (routing table) у системі Windows можна переглянути за допомогою команди `route print` (рис.2.28).

```

C:\>route print

Активные маршруты:

Сетевой адрес          Маска          Адрес шлюза      Интерфейс      Метрика
0.0.0.0                0.0.0.0       172.16.23.250   172.16.22.1    1
127.0.0.0             255.0.0.0     127.0.0.1      127.0.0.1      1
172.16.16.0           255.255.240.0 172.16.22.1    172.16.22.1    1
172.16.22.1           255.255.255.255 127.0.0.1      127.0.0.1      1
172.16.255.255       255.255.255.255 172.16.22.1    172.16.22.1    1
224.0.0.0             224.0.0.0     172.16.22.1    172.16.22.1    1
255.255.255.255     255.255.255.255 172.16.22.1    172.16.22.1    1

```

Рис.2.28. Результат виконання команди route print

З цієї таблиці розпочинається пошук фізичних адрес (MAC-адрес), що необхідні для формування кадрів, у які вкладаються IP-пакети.

Процес знаходження фізичних адрес базується на використанні спеціального протоколу ARP (Address Resolution Protocol), який забезпечує пошук фізичної адреси, що відповідає IP-адресі інтерфейсу (табл.2.9).

Таблиця 2.9

Структура ARP-пакета у мережі Ethernet зі стеком TCP/IP

Найменування даних	Кількість біт даних	Значення даних
Код технології канального рівня	16	1 для Ethernet
Код протоколу мережного рівня	16	2048 для протоколу IP
Довжина фізичної адреси	8	6 (байт у MAC-адресі)
Довжина мережної адреси	8	4 (байти у IP-адресі)
Код операції ARP (запит/відповідь)	16	1- запит, 2 – відповідь
MAC-адреса відправника пакета ARP	48	
IP-адреса відправника пакета ARP	32	
MAC-адреса одержувача пакета ARP	48	Нулі у запиті
IP-адреса одержувача пакета ARP	32	

Розглянемо алгоритм пошуку маршруту та формування Ethernet-кадру, у який буде вкладено (інкапсульовано) IP-пакет, на прикладі цієї

мережі, для якої віддруковано таблицю маршрутизації (див. рис. 2.28). Схему фрагмента цієї мережі зображено на рис. 2.29.

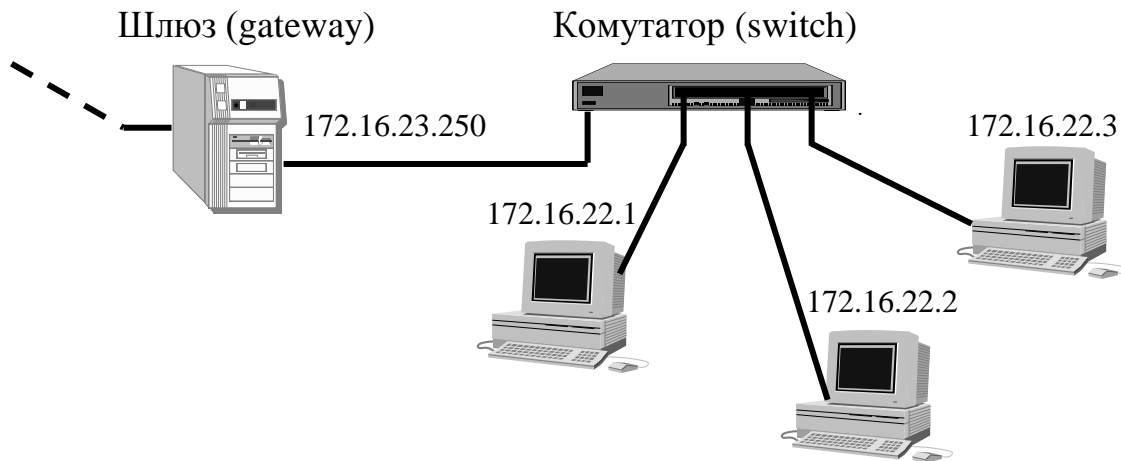


Рис. 2.29. Схема мережі для пояснення алгоритму маршрутизації

Припустимо, що ми працюємо в цій мережі, знаходячись за комп'ютером з IP-адресою 172.16.22.1. Всі IP-пакети, що відправляються з нашого комп'ютера матимуть адресу відправника 172.16.22.1, а IP-адреси одержувачів у цих пакетах будуть залежати від того, з яким комп'ютером ми будемо встановлювати зв'язок.

За допомогою аналізу IP-адреси одержувача відрізняють пакети прямої доставки (direct delivery), що адресовані до комп'ютерів нашої локальної мережі (адреси 172.16.22.2 та 172.16.22.3), та пакети непрямої доставки (indirect delivery), що адресовані до комп'ютерів поза межами нашої локальної мережі і доставлятимуться через шлюз (шлюз – це одна з назв маршрутизатора, що з'єднує дві мережі).

Для пакетів прямої доставки у ARP-запитах на місце IP-адреси одержувача пакета ARP (див. таблицю 4.6) ставлять адресу кінцевого одержувача інформації, а для пакетів непрямої доставки на цьому місці ставлять адресу шлюзу.

Розглянемо детально процес аналізу IP-адрес, який виконується з використанням таблиць маршрутизації (див. рис. 2.28).

Якою б довгою не була таблиця маршрутизації (на деяких вузлах у цих таблицях нараховуються сотні тисяч рядків), пошук маршруту для

кожної адреси потребує обчислень з участю всіх без винятку рядків таблиці. Алгоритм цих обчислень полягає у наступному.

Між IP-адресою одержувача і маскою виконують побітову операцію AND окремо для кожного рядку маршрутної таблиці. Маска являє собою 32-бітне слово, у якому біти, що відповідають адресі мережі, дорівнюють одиниці, а біти, що відповідають адресі вузла, дорівнюють нулю. Цю операцію називають накладанням маски на IP-адресу для виявлення адреси мережі. Результат виконання операції у кожному рядку порівнюють з мережною адресою. Якщо результат порівняння виявляється позитивним, цей рядок помічають, як один з можливих маршрутів.

Легко з'ясувати, що для першого рядку таблиці, у якому маска і мережна адреса мають значення 0.0.0.0, результат порівняння буде завжди позитивним. Маршрут за цим рядком вибирається тільки тоді, коли в усіх інших рядках не виявилось позитивних результатів порівняння.

Другий рядок таблиці відповідає зарезервованій адресі 127.0.0.1, яка використовується для перевірки працездатності програмного забезпечення стеку TCP/IP на комп'ютері, що може бути і не приєднаним до мережі.

Третій рядок таблиці призначений для виявлення IP-пакетів прямої доставки (адресовані в межах своєї локальної мережі).

Четвертий рядок таблиці розрахований на випадок, коли пакет буде відправлено на адресу свого комп'ютера. Цей пакет переправляють на адресу 127.0.0.1, що забезпечує доставку в межах свого комп'ютера.

Особливими за принципом формування пакетів є три останні рядки таблиці. Так передостанній рядок призначений для виявлення пакетів з груповими адресами. Два інші з цих рядків відповідають ширококомовним IP-адресам. Вони потребують у Ethernet заголовках використовувати ширококомовні MAC-адреси. У останньому рядку таблиці виявляються пакети так званої обмеженої ширококомовної розсилки (в межах своєї локальної мережі), а у п'ятому рядку таблиці виявляють пакети ширококомовної розсилки в межах мережі з адресою 172.16.0.0 (мережа класу B).

У більш складних випадках, коли маршрутизатор об'єднує декілька мереж, може бути помічено декілька рядків у таблиці маршрутизації, що відповідають можливим напрямкам передавання пакета. У цьому разі перевагу віддають рядку з меншим значенням метрики, яка являє собою умовну відстань до одержувача пакета. У нашій таблиці (див. рис. 2.28) метрика всіх маршрутів дорівнює одиниці, бо не існує таких IP-адрес, для

яких було б помічено декілька рядків у цій таблиці, тобто метрика в нашому випадку не впливає на вибір маршруту. У разі, коли метрики у помічених рядках співпадають, пакет відправляють за одним з можливих маршрутів, користуючись генератором випадкових чисел.

Крім вибору маршруту, кожен маршрутизатор виконує такі дії.

- Перевірку вірності змісту кожного поля у заголовку IP-пакета для знищення пакетів, що мають хоч одне пошкодження.
- Зменшення на одиницю значення TTL або знищення пакетів, у яких TTL=0.
- Фрагментацію пакета у випадку, коли довжина пакета більше, ніж розмір буфера у наступному маршрутизаторі. Якщо є необхідність у фрагментації, але встановлено прапорець DF, що забороняє фрагментацію, пакет знищується.
- Знищення пакетів, що не можуть бути передані одержувачу через відсутність необхідного маршруту або з інших причин.
- Формування спеціальних повідомлень для відправника про знищення пакетів за допомогою протоколу ICMP (Internet Control Message Protocol - протокол діагностичних повідомлень мережі).
- Опрацювання додаткових даних у заголовку IP-пакета.
- Формування IP-пакета з новою контрольною сумою заголовка.
- Відправка пакета за маршрутом з використанням технології або протоколу канального рівня.
- У разі необхідності маршрутизатор може бути налаштований для захисту інформаційних ресурсів за допомогою знищення пакетів, що мають не дозволені значення IP-адреси відправника або одержувача. У маршрутизаторах можуть виконуватись і більш складні перевірки пакетів за типом протоколів верхніх рівнів або за типом сервісів. Детальніше питання захисту інформаційних ресурсів ми розглянемо у наступному параграфі 4.3.

Повідомлення, що надсилаються у разі знищення IP-пакетів з метою інформування відправника інформації про аварійні ситуації, формуються у вигляді пакета ICMP, який вкладається у IP-пакет. Тобто протокол ICMP використовує протокол IP для передавання своїх пакетів. Протоколи IP та ICMP є протоколами міжмережного рівня.

Структура пакета ICMP, зображена у таблиці 2.10.

Таблиця 2.10

Структура пакета ICMP

Найменування даних	Кількість біт даних	Значення даних
Тип повідомлення (Type)	8	2 – одержувач недосяжний; 3 – заборона передавання через перевантаження маршруту; 4 – направлення на інший маршрут; 8 та 0 – луна-відповідь та луна-запит; 11 – визначений час вичерпано; 12 – помилковий параметр; 13 та 14 – запит та відповідь значення часу (у мілісекундах за Гринвічем)
Код повідомлення (Code)	8	В залежності від типу повідомлення уточнює причину знищення пакета
Контрольна сума	16	
Додаткові дані	32	Можуть доповнювати код повідомлення або не використовуються
Додаткові дані змінної довжини		Найчастіше це IP-заголовок та 8 байт з поля даних пакета, що був знищений

Значення кодів для повідомлень типу 3 наведено у таблиці 2.11.

Таблиця 2.11

Значення кодів повідомлень ICMP у випадку Type=3

Код	Значення повідомлення
0	Мережа недосяжна
1	Вузол недосяжний
2	Протокол верхнього рівня не має підтримки
3	Порт недосяжний
4	Необхідна фрагментація, але є ознака заборони
5	Хибний маршрут від відправника
6	Невідома адреса мережі
7	Невідома адреса вузла
8	Вузол ізольовано
9	Адміністративна заборона доступу до мережі
10	Адміністративна заборона доступу до вузла
11	Мережа недосяжна для даного типу сервісу
12	Вузол недосяжний для даного типу сервісу

Повідомлення типу 4 згідно RFC 1812 відправляти не треба.

Для повідомлень типу 5 у додаткових даних розміщено IP-адресу маршрутизатора. Значення кодів для повідомлень типу 5 наведено у таблиці 2.12.

Таблиця 2.12

Значення кодів повідомлень ICMP у випадку Type=5

Код	Значення повідомлення
0	Направлення пакета у мережу
1	Направлення пакета на вузол
2	Направлення пакета у мережу за типом сервісу
3	Направлення пакета на вузол за типом сервісу

Для повідомлень типу 11 значення кодів повідомлень наведено у таблиці 2.13.

Таблиця 2.13

Значення кодів повідомлень ICMP у випадку Type=11

Код	Значення повідомлення
0	Вичерпано час існування пакета
1	Вичерпано час збирання фрагментів

Для повідомлень типу 12 значення кодів повідомлень наведено у таблиці 4.11.

Таблиця 4.11

Значення кодів повідомлень ICMP у випадку Type=12

Код	Значення повідомлення
0	У додаткових даних зазначено номер хибного байта
1	Відсутній необхідний варіант додаткових даних у IP-заголовку (це може бути варіант 2 – таємно або 5 – цілком таємно)
2	Хибне значення довжини пакета

Для повідомлень типу 8 та 0 у додаткових даних розміщуються ідентифікатор (перші 16 біт) та номер повідомлення (останні 16 біт).

Значення ідентифікатора однакове для кожної пари запит-відповідь, а номер повідомлення (починається з нуля) у відповіді збільшується на 1.

Не у всіх аварійних випадках з передаванням IP-пакетів відправляють повідомлення ICMP. Маршрутизатори не формують ICMP-

повідомлення про знищення широкомовних та багатоадресних IP-пакетів, фрагментів IP-пакетів, крім першого, та про знищення пакетів з повідомленнями ICMP.

Серед існуючих маршрутизаторів можна виділити такі три категорії.

- Найпростіші маршрутизатори, що виконують обмежену кількість функцій. Вони аналізують IP-пакети та обирають маршрут, але не підтримують автоматичний обмін інформацією про маршрути з іншими маршрутизаторами. Коригування таблиці маршрутів при цьому повністю покладено на персонал.
- Маршрутизатори, що підтримують протоколи обміну інформацією про маршрути з іншими маршрутизаторами та обчислюють найкращі маршрути після кожної зміни у таблиці, але не забезпечують високу якість функціонування за такими показниками як швидкодія та мінімізація використання мережних ресурсів.
- Високоякісні маршрутизатори, які швидко адаптуються до змін у мережі та ощадливо використовують мережні ресурси.

Протоколи маршрутизації, що являють собою правила автоматичного обміну інформацією між маршрутизаторами, прийнято розподіляти на два типи. Це протоколи внутрішнього шлюзу IGP (Interior Gateway Protocol), що використовують в межах автономних систем, та зовнішнього шлюзу EGP (Exterior Gateway Protocol), що використовують між автономними системами.

Найбільш відомим протоколом внутрішнього шлюзу є RIP (Routing Information Protocol). Цей протокол вперше було застосовано у мережі ARPAnet ще у 1969 році. За цим протоколом перевага віддається маршруту, що пролягає через меншу кількість маршрутизаторів. Маршрутна інформація у таблицях поновлюється автоматично через кожні 30 секунд за допомогою широкомовних повідомлень. Протокол RIP використовують у невеликих мережах, де кількість маршрутів не перевищує кілька десятків.

Для великих мереж було розроблено протоколи RIP2 (RFC 1723) та OSPF (Open Shortest Path First, RFC 2178), де врахована можливість побудови підмереж і зменшено обсяг обміну маршрутною інформацією між маршрутизаторами. Широкого розповсюдження серед провайдерів Internet набули протоколи IGRP (Internet Gateway Routing Protocol) та EIGRP (Enhanced Internet Gateway Routing Protocol), що розроблені та

розповсюджуються фірмою Cisco як програмне забезпечення до своїх маршрутизаторів. Ця фірма є світовим лідером на ринку маршрутизаторів.

Для маршрутизації між автономними системами використовують протокол BGP (Border Gateway Protocol). На відміну від внутрішньої маршрутизації, граничні маршрутизатори передають у інші системи тільки ту інформацію, яку дозволяє адміністратор, враховуючи економічні, юридичні та інші обставини, що зветься політикою маршрутизації.

Важливу роль у стеку TCP/IP відіграє протокол транспортного рівня TCP. Функції цього протоколу полягають у наступному.

- Перевірка зв'язку та встановлення з'єднання між відправником та одержувачем інформації. У разі невдалої спроби з'єднання на верхній рівень видається сигнал про аварійну ситуацію.
- Вибір оптимальної швидкості передавання пакетів із врахуванням можливостей одержувача інформації та каналу зв'язку.
- Перевірка вірності передавання кожного пакета за допомогою контрольної суми. При цьому хибні пакети знищуються, а вірні пакети підтверджуються відправленням сигналів-квитанцій. У разі затримки квитанції пакети передають повторно. Може трапитись, що через цю затримку деякі пакети надійдуть по кілька разів.
- Контроль послідовності надходження байтів до одержувача інформації. Для цього на боці відправника даних здійснюють нумерацію байтів, а на боці одержувача перевіряють номери байтів від пакета до пакета. Порушення послідовності байтів виправляють, впорядковуючи послідовність пакетів. Зайві пакети відкидають.
- Припинення передавання та розірвання з'єднання у разі затримки пакетів на час, що перевищує визначений тайм-аут. При цьому верхні рівні відправника та одержувача інформації сповіщають про аварію.
- Розірвання з'єднання у разі завершення передавання усієї необхідної інформації. При цьому на верхні рівні відправника та одержувача інформації надаються сигнали про нормальне закінчення процесу передавання.

Структуру заголовка, який додається на транспортному рівні стеку TCP/IP, наведено у таблиці 2.14.

Таблиця 2.14

Структура TCP-заголовка

Найменування даних	Довжина у бітах	Значення даних, або приклади заповнення
Порт відправника (Source port)	16	Номер з'єднання формується автоматично
Порт одержувача (Destined port)	16	Номер означає протокол прикладного рівня (23 – TELNET, 25 – SMTP, 80 – HTTP, 110 – POP3, 21 – FTP)
Номер байта даних, що передається першим у пакеті	32	За початок відліку беруть випадкове число
Номер байта даних, що очікується	32	Цей номер може залишатись незмінним у разі відсутності інформації, крім сигналів-квитанцій (підтверджень)
Кількість 32-бітних слів у TCP-заголовку	6	5 або 6
Не використовують	4	Завжди нульові
URG (Urgent), що означає терміновість	1	1 – є термінові дані 0 – немає термінових даних
ACK (Acknowledge) – підтвердження	1	1 – пакет прийнято без помилок 0 – це початковий пакет сеансу зв'язку
PSH (Push) – виштовхування	1	1 – дані слід передати одержувачу не очікуючи наступний пакет
RST (Reset) – відмова	1	1 – аварійне припинення зв'язку
SYN (Sync) – синхронізація	1	1 – у перших двох пакетах сеансу зв'язку
FIN (Final) – кінець	1	1 – у завершальних трьох пакетах
Розмір вікна	16	Кількість вільних байт у буфері
Контрольна сума	16	Сумуються усі дані сегменту та частина заголовку IP (псевдо заголовок)
Кількість термінових байт у пакеті	16	
MSS (Max segment size) – максимальний розмір сегмента	16	Максимальна кількість байт у сегменті (передають тільки на початку сеансу)
Доповнення до 32-бітного слова	16	Використовують тільки до даних про максимальний розмір сегмента

Початок TCP-заголовка займають номери портів, що являють собою доповнення до IP-адрес, відповідно відправника та одержувача пакета.

Терміном порт у комп'ютерній лексиці часто називають ті чи інші фізичні або логічні точки доступу.

Для доставки пакета до комп'ютера достатньо знати IP-адресу, але у одному комп'ютері можуть одночасно підтримуватись у активному стані багато процесів зв'язку і необхідно визначати до якого з цих процесів належить кожний пакет. Коли для одного сайту ми відкриваємо кілька вікон, то пакети до кожного вікна мають абсолютно однакові IP-адреси, але протокол TCP надає їм різні номери портів, що й дозволяє відрізнити ці пакети.

На рис.2.30 відображено значення даних у TCP-заголовках для трьох початкових пакетів сеансу зв'язку.

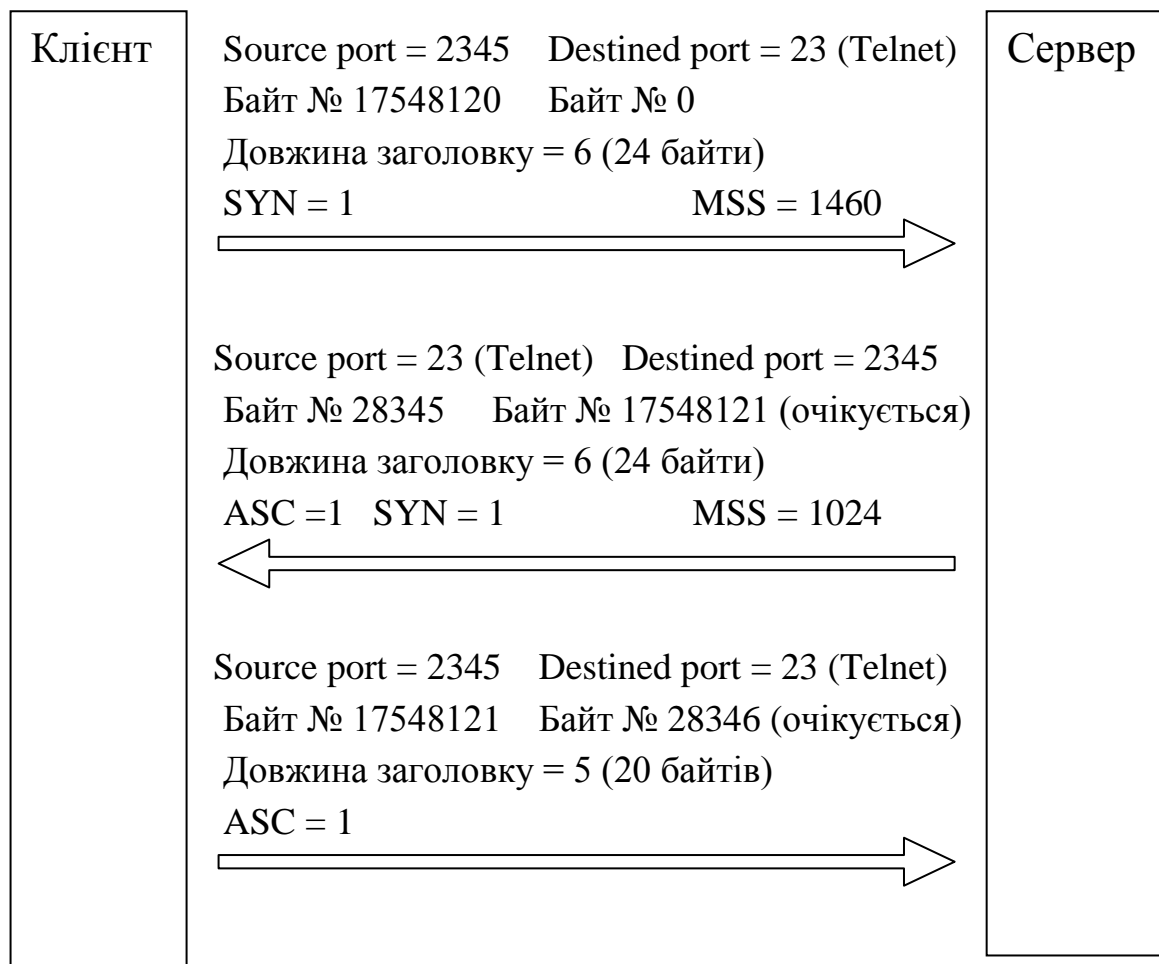


Рис. 2.30. Процедура встановлення з'єднання за протоколом TCP

Після успішного обміну першими трьома пакетами, що називають процедурою встановлення з'єднання, розпочинається обмін даними. У нашому випадку, коли протоколом верхнього рівня є Telnet, з боку клієнта

у пакетах даних відправлятимуться команди з клавіатури, а у відповідях від сервера надходять дані для відображення на екрані терміналу. Цей режим обміну даними широко розповсюджений у роботі адміністраторів вузлів мережі Internet.

Крім протоколу TCP на транспортному рівні стеку TCP/IP є протокол UDP, структуру заголовка якого надано у таблиці 2.15.

Таблиця 2.15

Структура UDP-заголовка

Найменування даних	Довжина у бітах	Значення даних, або приклади заповнення
Порт відправника (Source port)	16	Номер з'єднання формується автоматично
Порт одержувача (Destined port)	16	Номер означає протокол прикладного рівня (123 – NTP, 161 – SNMP)
Довжина пакету	16	Кількість байт даних та UDP-заголовку
Контрольна сума (може не формуватись, а замінитись нулями)	16	Сумуються дані і UDP-заголовок пакету та частина заголовку IP (псевдо заголовок)

Протокол UDP не забезпечує надійності передавання інформації, але його необхідність обумовлена можливістю передавання широкомовних та термінових повідомлень.

Розглянуті у цьому підрозділі протоколи являють собою основу стеку TCP/IP, без якого важко уявити собі сучасну комп'ютерну мережу.

2.3 КАНАЛИ ЗВ'ЯЗКУ В СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

2.3.1 Сучасний стан розвитку каналів передавання даних

Високі темпи зростання потужності комп'ютерів стимулювали розвиток технологій міжкомп'ютерного зв'язку. Різноманіття існуючих мережних технологій та забезпеченість каналами для передавання даних привели до того, що сьогодні вже стала фактом можливість об'єднання

всіх комп'ютерів світу у єдину мережу. За останні 10 років максимальна швидкість передавання даних у локальних мережах сім'ї Ethernet-технологій збільшилась у 1000 разів, що перевищує темпи зростання швидкодії шин персональних комп'ютерів (ПК). Порівняння цих темпів по роках наведено у таблиці 2.16.

Таблиця 2.16

Швидкість передавання даних у локальних мережах сім'ї Ethernet-технологій та швидкодія шин ПК на той самий час

Назва стандарту мережі	Рік прийняття стандарту	Максимальна швидкість, Мбіт/с	Тип шини ПК	Швидкодія шини ПК, Мбіт/с
10Base-T	1991	10	EISA	256
100Base-T	1995	100	PCI	1064
1000Base-T	1998	1000	PCI-X	8528
10GBase-SX	2002	10000	PCI Express	20000

Для нормальної взаємодії комп'ютера з каналом локальної мережі має витримуватись співвідношення швидкодії шини комп'ютера до швидкості передавання даних приблизно 10:1, бо інакше може трапитись так зване захоплення шини процесом передавання і робота комп'ютера на деякий час буде заблокована. Таким чином, аналізуючи дані, що наведені у таблиці 3.1, бачимо, що в останні роки виникло деяке випередження у швидкості з боку засобів передавання даних відносно до шини ПК.

Зараз можна констатувати той факт, що подальший розвиток технологій передавання даних та побудови каналів комп'ютерних мереж у наш час фактично не стимулюється через відсутність відповідного зростання обсягів даних, які треба передавати. Не слід забувати, що кінцевим споживачем інформації є людина, яка не може сприймати інформації більше, ніж дозволяють її природні можливості.

Наявність резерву перепускної здатності існуючих каналів для передавання даних та перевищення пропозицій у послугах інформаційного транспорту над попитом свідчать про те, що на сьогоднішній день людство не має такого обсягу інформації для передавання, щоб суттєво завантажити існуючі канали.

2.3.2 Характеристики каналів зв'язку в комп'ютерних мережах

Канали передавання даних являють собою підмножину каналів зв'язку, яка використовується для передавання інформації до комп'ютерів або між комп'ютерами. У загальному розумінні канал зв'язку являє собою сукупність фізичного середовища передавання сигналів та апаратури для утворення каналу.

Сигнал – це фізичний процес, який використовують для передавання інформації. Найчастіше цей процес являє собою електричний, оптичний або електромагнітний імпульс.

Розглянемо основні характеристики, за якими класифікують канали зв'язку. Ці характеристики можна розподілити на такі три групи.

- Характеристики фізичного середовища передавання сигналів (вид фізичного середовища та його властивості щодо перетворення сигналів).
- Характеристики апаратури для утворення каналу, до яких віднесемо методи формування сигналів (методи модуляції та кодування), принцип синхронізації, методи комутації та розділення каналів по напрямках передавання.
- Кількісні та якісні характеристики, за якими визначають можливості передавання даних, а саме: перепускна здатність, швидкість, надійність, затримка, завадостійкість та вартість.

За видом фізичного середовища канали можуть бути кабельні, радіо, проводові, оптичні та акустичні. У свою чергу, кабельні канали розділяють за типом та конструкцією кабелю.

Найбільш розповсюджені кабелі у вигляді скрученої пари, коаксіальні та волоконно-оптичні. Кабелі можуть бути екранованими, що мають металеву оболонку (екрануючу), яка захищає від впливу зовнішніх електромагнітних полів, а також зменшує енергію, що випромінюється з кабелю у зовнішнє середовище. Усі кабелі мають захисну пластикову оболонку, яка захищає середовище передавання сигналів від механічних пошкоджень під час прокладання та від шкідливого впливу зовнішніх факторів (вологи, сонячних променів, агресивних атмосферних домішок).

Коаксіальний кабель має в середині мідну жилу, яка знаходиться під шаром ізоляції, та металеву оболонку навколо неї (рис. 2.31).

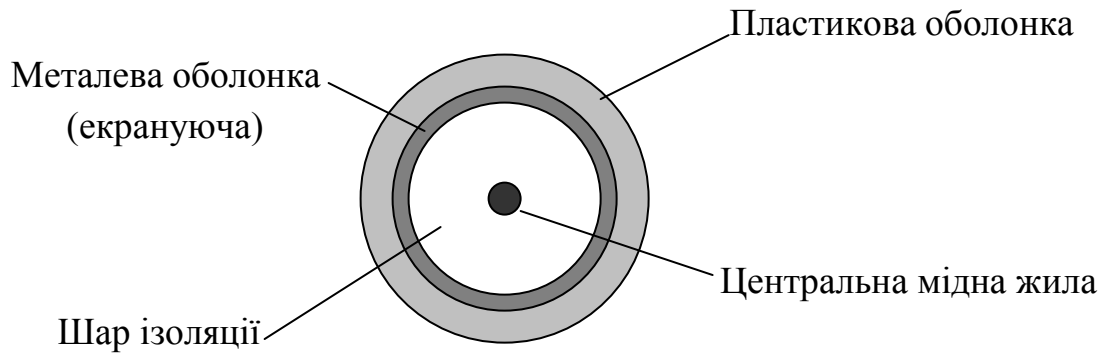


Рис. 2.31. Структура коаксіального кабелю

Зовнішній діаметр товстого коаксіального кабелю становить 12,5 мм, а тонкого коаксіального кабелю – 6,25 мм.

Волоконно-оптичні кабелі бувають одномодовими та багатомодовими.

Мода – це електромагнітна хвиля, яка має певну просторову структуру.

У центральній частині усіх типів волоконно-оптичних кабелів знаходиться скляне волокно, по якому поширюється світловий промінь. Це скляне волокно оточене скляною оболонкою, яка має менший показник заломлення, ніж волокно, тому світловий промінь віддзеркалюючись від оболонки, повертається у центральне волокно, де продовжує свій рух далі.

У одномодовому кабелі (Single Mode Fiber, SMF) центральне волокно має діаметр від 5 до 10 мкм, що сумірно з довжиною хвилі світла, яка може бути 1,3 або 1,55 мкм. Саме цим значенням довжини хвилі відповідають максимальні значення коефіцієнта передавання світлових сигналів крізь оптичне волокно. Малий діаметр волокна сприяє руху світла вздовж волокна і зменшує ймовірність віддзеркалювання від оболонки. Тому одномодовий кабель має у десятки і навіть у сотні разів кращі показники якості передавання світлових сигналів, ніж багатомодовий кабель. Проте вартість лазерних випромінювачів та фотоприймачів, які необхідні, щоб утворити та сприйняти з необхідною точністю тоненький світловий промінь поки що залишається високою. Найбільш ефективним місцем застосування одномодового кабелю є канали далекого зв'язку. Сучасні системи на одномодовому волокні працюють зі швидкостями більш ніж 1 Тбіт/с на відстань понад 3000 км без підсилювачів.

Багатомодовий кабель (Multi Mode Fiber, MMF) має більший діаметр світловода (50 мкм або 62,5 мкм), що дозволяє використовувати

випромінювачі на світлових діодах замість лазерних. Це зменшує витрати на обладнання каналів зв'язку, але швидкість і відстань передавання при цьому також зменшуються відповідно до сотень Мбіт/с і десятків кілометрів.

Щороку збільшується асортимент волоконно-оптичних кабелів. Ці кабелі виготовляють з різною кількістю жил (рис. 2.32) від одиниць до десятків.

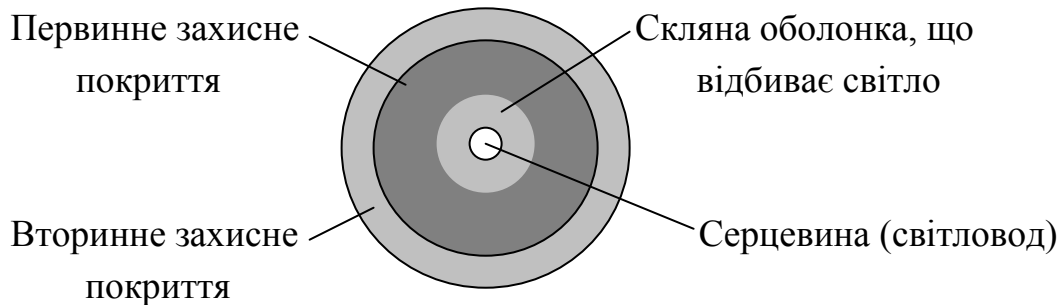


Рис. 2.32. Структура жили волоконно-оптичного кабелю

У позначенні кабелю крім кількості жил прийнято вказувати сукупність діаметрів серцевини та оболонки (у мікрометрах), наприклад, 9,5/125 або 50/125.

Волоконно-оптичні кабелі забезпечують стійкий зв'язок в умовах сильних електромагнітних завад, гарантують захист від прослуховування та відповідають найсуворішим екологічним вимогам. Недоліком цих кабелів є мала механічна стійкість та висока вартість налагоджування з'єднань.

Для побудови каналів зв'язку у локальних мережах найдоцільніше використовувати кабель типу неекранованої скрученої пари (Unshielded Twisted Pair(UTP)). Такий кабель є найдешевшим і найпоширенішим фізичним середовищем передавання інформації у локальних мережах.

Крім неекранованої скрученої пари, використовують екрановану та обгорнуту фольгою скручену пару (Shielded Twisting Pair(STP)) та (Foiled Twisting Pair(FTP)) відповідно. У загальному вигляді скручена пара – це вісім ізольованих мідних провідників, що скручені попарно у спільній захисній оболонці (рис. 2.33).

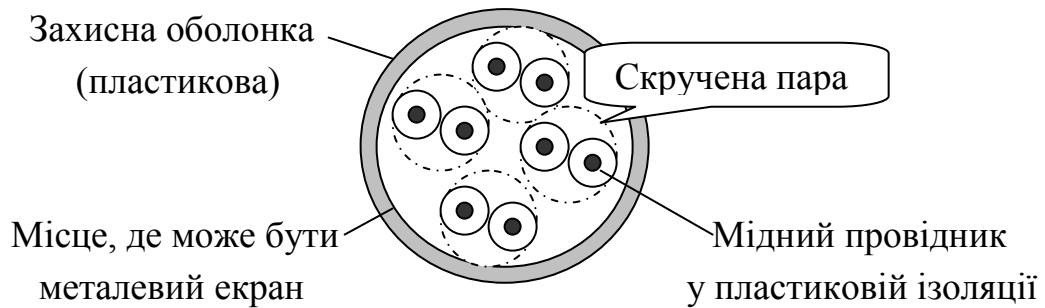


Рис. 2.33. Структура кабелю типу скручена пара

За технічними характеристиками кабелі поділяють на категорії (або класи), які наведено у таблиці 2.17.

Таблиця 2.17

Основні технічні параметри кабелів

Категорія кабелю	Частота, МГц	Швидкість, Мбіт/с
1	<1	до 0,02
2	1	1
3	16	16
4	20	20
5	100	100
5+, 5E	100	155
6	250	1000
7	600	

Незважаючи на труднощі, що пов'язані з прокладанням кабелів, саме на кабельні канали припадає переважна більшість (близько 90%) від загального обсягу передавання даних. Цей факт можна пояснити тим, що кабельні канали дозволяють забезпечити найвищу швидкість, надійність та захищеність процесу передавання.

Останніми роками зазнав бурхливого розвитку напрям передавання даних з використанням радіоканалів. Це обумовлено поширенням мобільних телефонів та кишенькових комп'ютерів.

З кожним роком все тісніше стає в діапазонах радіочастот, бо потреби у мобільному зв'язку зростають, а ефірні ресурси мають природне

обмеження. Серйозною проблемою стає розподіл можливостей ефіру між користувачами.

Найбільш популярною мережною технологією, що використовує ефірні ресурси, є технологія VSAT (Very Small Aperture Terminal). Ця технологія базується на використанні геостаціонарних супутників, що розміщені над екватором на висоті близько 36 тис.км. За ціною такий зв'язок сумірний з кабельним, але затримка сигналів становить близько 0,3 с через велику відстань, що необхідно перетинати сигналам.

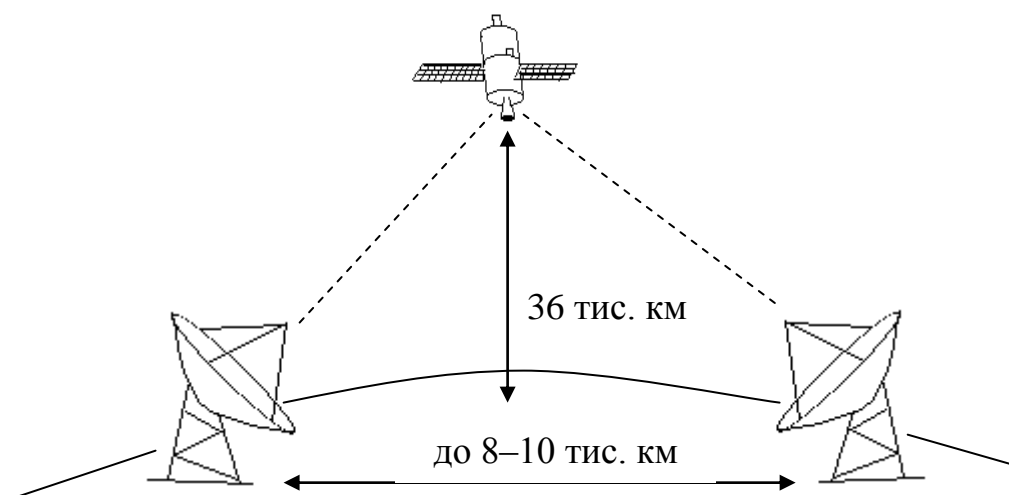


Рис. 2.34. Проходження сигналів через геостаціонарний супутник

Час проходження сигналів визначають через відстань, знаючи, що їх швидкість у всіх випадках близька до швидкості світла (300000 км/с).

Для телефонного зв'язку затримка сигналу, що має місце у системах з геостаціонарним супутником, перевищує норму, тому створюють супутникові системи на менших висотах. Чим менша висота орбіт супутників, тим більшу кількість супутників треба використовувати для забезпечення нормальної зони покриття. Системи, що базуються на низькоорбітальних супутниках (Low Earth Orbit (LEO)), налічують десятки або сотні супутників на висоті до 3000 км. Так система Iridium використовує 66 супутників, а системи, що розробляє корпорація Teledesic, налічують до 840 супутників.

Останнім часом почали з'являться системи, що використовують радіозв'язок для побудови мереж у межах будинку. Перша на Україні така мережа з'явилась у 2003 році у готельному комплексі Президент-готелю "Київський", де кожен клієнт, який має мобільний ПК з підтримкою

технології Intel Centrino, може приєднатись до локальної мережі та мати можливість користуватись E-mail. Мережа побудована на базі обладнання Cisco Aironet 340 Series. Швидкість передавання даних близько 10 Мбіт/с на відстань до 100 м.

Мобільний доступ до мережі Інтернет забезпечує послуга GPRS (General Packet Radio Service), що надає змогу передавання даних у мережах стандарту GSM (Global System for Mobile Communication) зі швидкістю до 107,3 Кбіт/с. Зараз на порозі новий стандарт UMTS (Universal Mobile Telephone Service) зі швидкістю до 2 Мбіт/с[6].

Проводові канали відходять у минуле. Ми ще іноді бачимо залишки неізольованих мідних і сталевих дротів, що натягнуті рядами, на дерев'яних опорах вздовж залізниць. Ці канали зв'язку після електрифікації залізниць втратили якість через вплив потужних завад від електровозів.

Останнім часом у містах західної Європи набуває розвитку впровадження оптичних каналів зв'язку з лазерними випромінювачами. Ця технологія має назву FSO (Free Space Optics). Її переваги полягають у тому, що за короткий час (від кількох днів до місяця) можна створювати канали зі швидкістю передавання даних 100 Мбіт/с – 2,5 Гбіт/с на відстань до 5 км не використовуючи ефірні регламентовані частоти. Останнє звільняє від необхідності отримання дозволу на установку обладнання. Недоліком такої технології є вплив атмосферних явищ (сильного снігу або граду) на якість зв'язку [8].

У лабораторних умовах дослідниками систем FSO отримано швидкість передавання даних 160 Гбіт/с. Відстань передавання у деяких системах перевищує 10 км. Апаратура може бути розташована у закритому приміщенні, бо промінь лазера добре проникає крізь віконне скло. Постачальники апаратури FSO гарантують надійність зв'язку 99,9 %, а у випадках, коли відстань не перевищує 1 км, надійність зростає до 99,99 %.

Акустичні канали використовують на військових об'єктах для передавання сигналів у водному середовищі з використанням ультразвуку.

Важливими характеристиками фізичного середовища передавання сигналів є амплітудно-частотна та фазово-частотна характеристики (АЧХ) та (ФЧХ). Ці характеристики в ідеальному випадку мають вигляд, що зображений на рис. 2.35.

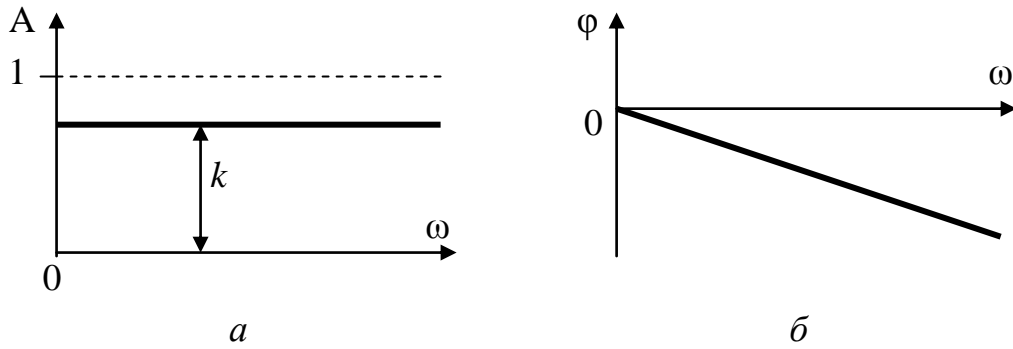


Рис.2.35. Ідеальні варіанти АЧХ (а) та ФЧХ (б) фізичного середовища:
 А – амплітуда (на вході в середовище дорівнює одиниці); φ – фаза; ω – частота;
 k – коефіцієнт ослаблення ($0 < k < 1$).

При умові ідеальних характеристик форма сигналів, що проходять крізь середовище передавання, залишається незмінною. У ідеальному середовищі сигнали можуть тільки ослаблюватись та затримуватись. Ослаблення залежить від значення k , а затримка – від нахилу ФЧХ. На вході у середовище ФЧХ співпадає з віссю частоти ω , а затримка сигналу на виході з середовища пропорційна тангенсу кута нахилу ФЧХ.

У реальних середовищах передавання не буває ідеальних АЧХ та ФЧХ. Для них введено поняття смуги частот перепускання. Це той діапазон частот, у якому слід вибирати значення робочих частот для формування сигналів. Вважають, що у цьому діапазоні АЧХ та ФЧХ у певній мірі наближені до ідеальних. Форма сигналів, що проходять крізь реальне середовище передавання, завжди змінюється. Ці зміни можна з достатньою точністю визначити за допомогою математичних методів, вимірявши АЧХ та ФЧХ.

Зміну форми сигналів, що відбувається у середовищі передавання через відхилення АЧХ та ФЧХ від ідеальних, називають спотворенням.

Крім спотворень форми, які можуть бути визначені математичними методами, у каналах зв'язку мають місце ще й випадкові явища, що називаються завадами.

Завади розподіляють на дві категорії:

- адитивні – це випадкові процеси, що додаються до сигналів;
- мультиплікативні – це випадкові зміни коефіцієнта ослаблення k .

Завади являють собою випадкові процеси, параметри яких описують за допомогою методів теорії ймовірностей.

Апаратуру для утворення каналів зв'язку класифікують за методами, які використовують для перетворення повідомлень, що надходять з джерела інформації, у сигнали – фізичні процеси, які розповсюджуються у фізичному середовищі (рис. 2.36).

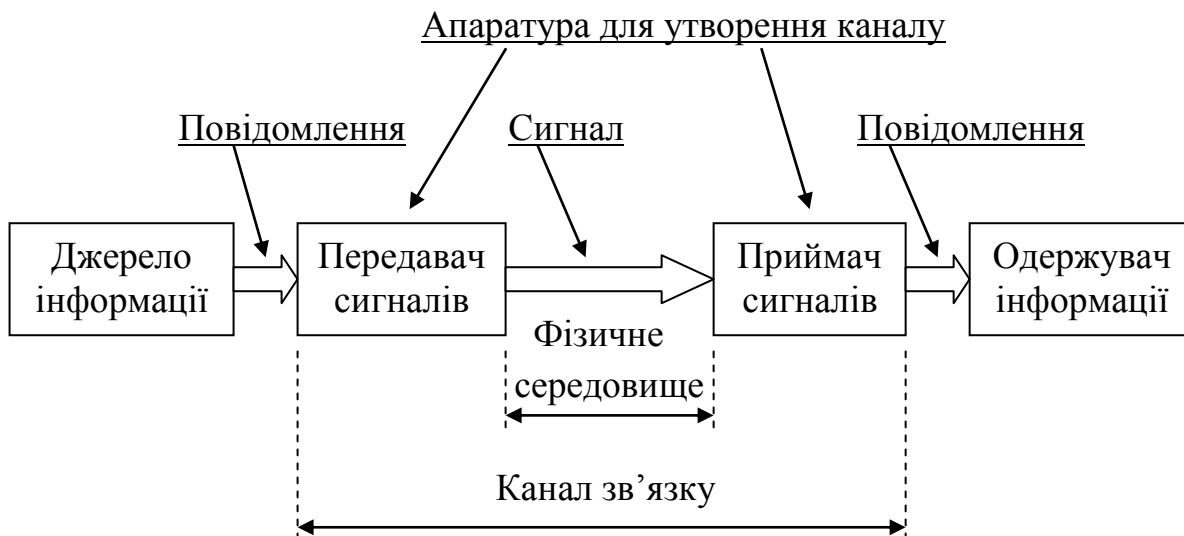


Рис.2.36. Схема найпростішої системи передавання інформації

У зображеній на рис.2.36 найпростішій системі інформація передається в одному напрямку та через єдине середовище. У реальному випадку, коли відбувається обмін інформацією між процесами у віддалених комп'ютерах, може бути багато послідовних етапів перетворення та передавання повідомлень через різні фізичні середовища.

Процес перетворення повідомлень у сигнали прийнято розподіляти на два основні етапи. Перший етап називають кодуванням, а другий – модуляцією. Етапи перетворення сигналів у повідомлення на стороні одержувача називають демодуляцією та декодуванням.

Кодування може складатись з декількох окремих процедур. Метою цих процедур може бути:

- зменшення збитковості повідомлень (“стиснення інформації”);
- забезпечення конфіденційності;
- підвищення завадостійкості за рахунок внесення збиткової інформації, наприклад контрольних сум, що дозволяє виявити можливі помилки у переданих даних.

Метою етапу модуляції є перетворення закодованих повідомлень у фізичні процеси, що здатні до передавання у фізичному середовищі.

Музичний термін модуляція, що означає перехід з однієї тональності в іншу, у зв'язківців використовується як поняття зміни параметрів коливань високої частоти-носія під впливом процесу, що несе інформацію.

Більшість середовищ, що використовуються для передавання сигналів, мають працювати в обмеженому діапазоні частот. Ці обмеження можуть накладатись природними властивостями середовища або дозволом на користування середовищем.

Частота-носії у математичному вигляді є синусоїдою $A \cdot \sin(\omega t + \varphi)$, де параметри A , ω та φ являють собою відповідно амплітуду, частоту та фазу. Зміна цих параметрів відповідає поняттям амплітудної, частотної та фазової модуляції. У модемах для телефонних ліній зв'язку на швидкостях від 9600 біт/с до 48 Кбіт/с використовують амплітудно-фазову модуляцію з придушенням частоти носія.

У цифрових системах передавання з імпульсними носіями інформації модуляцію називають амплітудно-імпульсною, частотно-імпульсною, фазово-імпульсною, широтно-імпульсною та імпульсно-ковою. Останній метод означає, що кожному значенню параметра процесу, який несе інформацію, відповідає кодова послідовність імпульсів. При цьому бачимо зближення понять кодування і модуляції, які у цифрових системах іноді вживають як синоніми.

За принципом синхронізації системи розподіляють на синхронні та асинхронні. У синхронних системах існує канал синхронізації, що надає змогу точного визначення моментів надходження сигналів до приймача. У асинхронних системах моменти надходження сигналів невідомі.

За напрямками передавання системи розподіляють так:

- **симплексні**, де інформація передається тільки у одному напрямку;
- **дуплексні**, де інформація може передаватись одночасно у прямому та зворотному напрямках;
- **напівдуплексні**, де інформація може передаватись у прямому та зворотному напрямках, але не одночасно.

За методом комутації розглядають такі три типи систем.

- **Системи з комутацією каналів**, у яких канал надається абонентам у повне користування на сеанс зв'язку. Тільки після закінчення сеансу канал вважають вільним і можуть надавати його іншим абонентам.

- **Системи з комутацією повідомлень**, у яких канал надається на час передавання повідомлення. Кожне повідомлення доповнюють заголовком, у якому знаходиться адреса одержувача повідомлення.
- **Системи з комутацією пакетів**, у яких повідомлення розділяють на фрагменти обмеженої довжини, що називають пакетами. Кожен такий фрагмент доповнюють заголовком з адресою одержувача та службовою інформацією, яка забезпечує можливість відтворити повідомлення після прийняття усіх фрагментів. Цей метод комутації найбільш розповсюджений у комп'ютерних мережах. Він забезпечує найкращі умови спільного користування каналами зв'язку.

За допомогою апаратних засобів фізичне середовище зв'язку може бути розподілене на певну кількість незалежних каналів. Цей розподіл у телефонії прийнято називати ущільненням. Методи ущільнення бувають такі:

- **частотне**, при якому кожному каналу виділяють окрему смугу частот;
- **часове**, при якому кожному каналу виділяють фіксовані інтервали часу;
- **компенсацією луни**, що дозволяє одночасне передавання сигналів у прямому та зворотному напрямках в єдиному середовищі;
- **кодове**, що співпадає за принципом з методом комутації пакетів.

Недоліки перших двох методів ущільнення полягають у тому, що за кожним каналом жорстко закріплено частину фізичного ресурсу, і немає можливості гнучкого розподілу сумарного ресурсу залежно від потреб користувачів під час передавання інформації. Кодове ущільнення знімає цей недолік, що є важливою перевагою для систем передавання даних, де протягом сеансу зв'язку може суттєво змінюватись інтенсивність потоків інформації.

Для оцінки можливостей каналів зв'язку незалежно від типу фізичного середовища та методів їх побудови використовують наступний ряд характеристик.

- **Перепускна здатність** – це максимальне значення швидкості передавання даних у каналі зв'язку, яку можна було б досягти теоретично при умові вибору найкращих (можливо реально не існуючих) методів кодування та модуляції. Формули для обчислення перепускної здатності надано у додатку 3.

- **Максимальна швидкість передавання даних** – це найбільша швидкість, яку можна досягти в умовах існуючих апаратних та технологічних обмежень конкретної системи.
- **Надійність** – це здатність системи нормально працювати при умові можливості тимчасової або повної втрати працездатності. Оцінюють надійність за допомогою параметрів що базуються на результатах статистичних досліджень. До таких параметрів у першу чергу слід віднести середню тривалість безвідмовної роботи та ймовірність безвідмовної роботи. Останній використовується для систем, у яких можлива короточасна втрата працездатності, що ліквідується сама по собі.
- **Затримка** – це проміжок часу від початку передавання сигналу до моменту надходження сигналу на вхід приймача. Цей параметр обумовлений швидкістю розповсюдження сигналів у фізичному середовищі і залежить від довжини шляху, який проходять сигнали. У практичних розрахунках цю швидкість вважають рівною швидкості світла у вакуумі.
- **Завадостійкість** – це властивість зберігати вірність передавання інформації в умовах дії завад. Для оцінки завадостійкості прийнято користуватись значенням ймовірності помилки у передаванні біта або байта.
- **Вартість передавання даних** залежить від витрат на створення та обслуговування власного каналу або від цінової політики власника каналів. Існує декілька варіантів плати за користування каналами зв'язку. Канали можна брати в оренду. При цьому сплачується щомісячна орендна плата за тарифом, що встановлює власник (на Україні це “Укртелеком”). Можлива угода про щомісячну плату за обсяг переданих та/або прийнятих даних з урахуванням обмежень на максимальну швидкість передавання. Можливе надання каналу з обмеженням максимальної швидкості без урахування обсягу переданих даних. У каналах що побудовані за технологією Frame Relay плата береться залежно від гарантованої швидкості передавання даних. Найбільш складною є система оплати послуг за технологією АТМ (Asynchronous Transfer Mode), де враховується багато параметрів, що гарантують користувачеві необхідну якість зв'язку.

2.3.3 Технології побудови каналів зв'язку на основі СКС для комп'ютерних мереж

Останнім часом спостерігається стрімке поновлення технологій побудови каналів зв'язку. Цей процес тісно пов'язаний із загальним розвитком інформаційних технологій та поширенням комп'ютерних мереж. Головною характерною рисою цього процесу є поступове наближення до єдиної форми зберігання та передавання інформації у цифровому вигляді.

На початку впровадження комп'ютерних мереж для передавання даних між комп'ютерами використовували аналогові телефонні канали, а зараз, навпаки, для телефонії використовують канали мережі Інтернет. І цей процес з кожним роком поглиблюється. Цифровий зв'язок поступово витіснює аналоговий в сучасних системах телефонії та телебачення.

Зміни відбуваються в мережах усіх масштабів від локальних мереж у межах будинків до глобальних мереж у межах земної кулі.

У проєктах нових будинків вже закладають структуровані кабельні системи, що призначені виконувати функції універсального середовища для передавання інформації. Ця універсалізація позбавляє від необхідності окремого прокладання телефонної, охоронної, пожежної, телевізійної та інших інформаційних мереж, включаючи локальні комп'ютерні мережі та доступ до Інтернет. Збитковість, що закладається у ці системи, призначена гарантувати протягом наступних 10–15 років відсутність необхідності у прокладанні додаткових кабелів для передавання інформації. Згідно зі стандартом ISO/IEC 11801 структурована кабельна система (SCS, Structured Cabling System) має такі складові частини (рис.2.37):

- CD (Campus Distributor) розподільник на групу будинків (кампусний);
- магістраль, що об'єднує групу будинків (до 1500 м);
- BD (Building Distributor) розподільник будинку;
- магістральний кабель будинку (до 500 м);
- FD (Floor Distributor) розподільник поверху;
- горизонтальний кабель (до 90 м);
- пункт переходу з одного типу кабелю на інший (необов'язково);
- TO (Telecommunication Outlet) телекомунікаційний роз'єднувач.

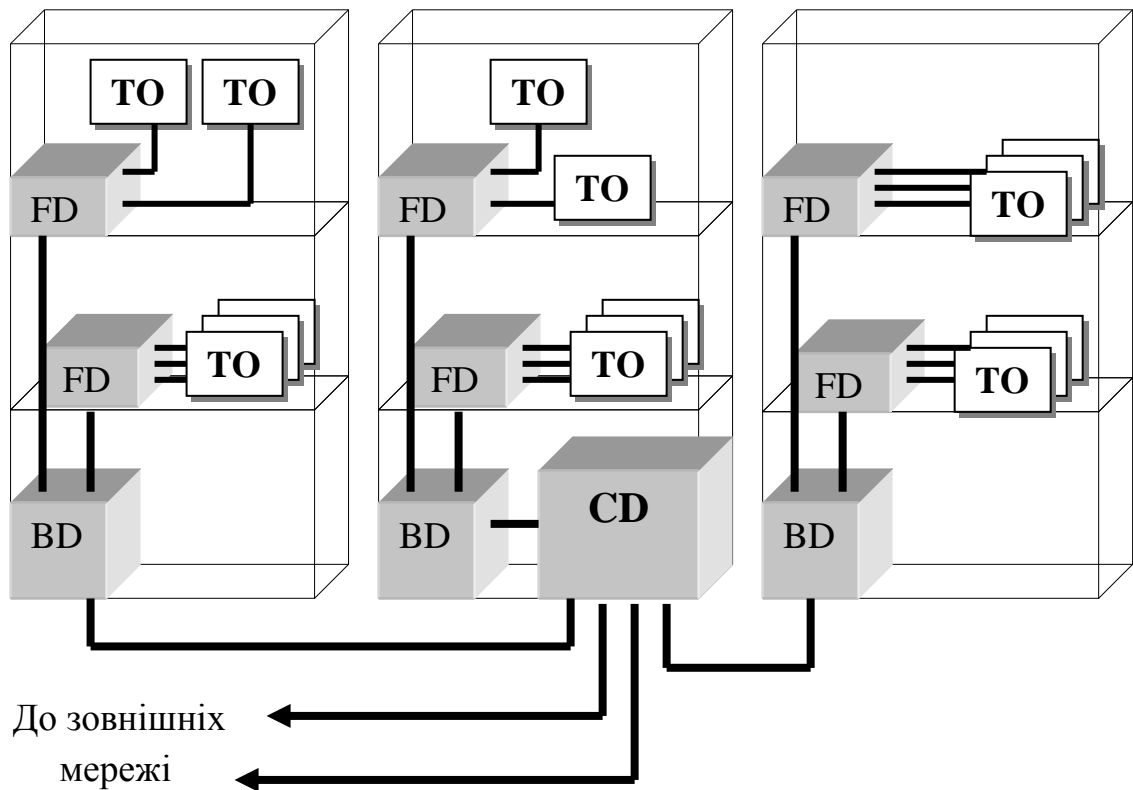


Рис.2.37. Схема структурованої кабельної системи

Стандартом встановлено, що кабелі повинні мати категорію від п'ятої до сьомої. Це може бути скручена пара або волоконно-оптичний. Не увійшов у стандарт коаксіальний кабель. На кожні 1000 м² виробничої площі повинен бути хоча б один FD. Якщо на поверсі мало користувачів, то можна використовувати FD сусіднього поверху. На кожні 10 м² площі встановлюють два ТО. Також по два ТО встановлюють на кожну робочу ділянку. Кожний ТО являє собою розетку роз'єднувача типу RJ-45, до якої комутаційним шнуром може бути приєднаний комп'ютер або інший пристрій.

Фактично SCS являє собою комп'ютерну мережу, у якій на каналному рівні можуть застосовуватись технології Fast Ethernet, Gigabit Ethernet та ін. Для забезпечення одночасного передавання по каналах цієї мережі різноманітної інформації може використовуватись стек протоколів TCP/IP. Як бачимо, у цій системі для підключення телефону, телебачення

та інших пристроїв використовують універсальний канал комп'ютерної мережі.

Висока швидкість передавання даних у локальних мережах стимулює підвищення вимог до швидкості передавання по магістралях глобальних мереж. З цієї точки зору найбільш перспективними є волоконно-оптичні кабелі, які завдяки сучасним технологіям, дозволяють побудувати канали на швидкість від 155,52 Мбіт/с до десятків терабіт за секунду.

Стандартизована у 1988 році технологія SDH (Synchronous Digital Hierarchy) може забезпечити обмін даними по волоконно-оптичному кабелю зі швидкостями, що наведені у таблиці 2.18.

Таблиця 2.18

Рівні швидкості обміну даними з апаратурою SDH

Назва рівня	Швидкість, Мбіт/с
STM-1	155,52
STM-3	466,56
STM-4	622,08
STM-6	933,12
STM-8	1244,16
STM-12	1866,24
STM-16	2488,32
STM-64	9953,28

У стандарті SDH усі рівні швидкості мають загальну назву STM-n – Synchronous Transport Module level n. Технологія SDH апаратно сумісна з першою технологією синхронних оптичних мереж SONET (Synchronous Optical NETs), що була стандартизована ще у 1984 році. Прийнято для обох цих технологій вживати назву SONET/SDH або SDH/SONET.

Продуктивність використання волоконно-оптичних кабелів може бути значно підвищена за рахунок використання нових технологій WDM (Wave Division Multiplexing) та DWDM (Dense WDM).

Головна ідея цих технологій полягає у тому, щоб одночасно одним волокном передавати промені різних частот. До десяти сигналів-носіїв у

технологіях WDM або кілька десятків у технологіях DWDM можуть одночасно модулюватись від різних джерел інформації та об'єднуватись у одному волокні. Практична реалізація WDM стала можливою завдяки розробці оптичних підсилювачів на іонах ербію, оптичних комутаторів та мультиплексерів/демультиплексерів. Через те, що оптичні пристрої працюють набагато швидше за електронні, стало можливим у десятки і сотні разів збільшити продуктивність використання кабелю. Повна заміна електронних компонентів мережі на оптичні призвела до появи AON (All-Optical Network).

Важливою перевагою технології DWDM є забезпечення кризного передавання пакетів без проміжних перетворень у електричні сигнали та інкапсуляції. Це означає досягнення найвищої швидкості передавання інформації і повну незалежність від протоколів систем вищих рівнів, бо світловий потік на виході з AON-мережі буде таким самим, як на її вході.

РОЗДІЛ 3. БЕЗДРОТОВІ ЛОКАЛЬНІ МЕРЕЖІ СТАНДАРТІВ IEEE 802.11

22 травня 1973 р. Роберт Меткалф, співробітник дослідницького центру компанії Xerox у Пал-Альто, подав своєму керівництву доповідну записку, у якій уперше ввів слово «Ethernet» і виклав основні принципи роботи нової локальної комп'ютерної мережі, втілені пізніше в стандарті IEEE 802.3, іменованому сьогодні Ethernet'ом. Цікаво, вибираючи назву для нової технології, автор свідомо зупинився на словосполученні ether net - «ефірна мережа», передбачаючи, що через чверть століття Ethernet зможе передаватися за допомогою ефіру.

Бездротові локальні мережі передачі інформації (WLAN) розвиваються за останні п'ятнадцять років неймовірно швидко. Простота розгортання таких мереж обмежена тільки необхідністю оформлення дозвільної документації (у тих країнах, де це потрібно). По пропускій здатності вони не уступають виділеним мідним лініям. Завадостійкість, надійність і захищеність сучасних протоколів передачі зробили WLAN явищем повсюдним, а устаткування для них - масовим продуктом. Відзначимо, що поняття «локальні мережі передачі інформації» досить умовно. Як правило, маються на увазі системи, локалізовані в радіусі сотні метрів. Однак технології локальних мереж з успіхом застосовують і на відстанях до декількох десятків кілометрів.

Ринок масових пристроїв WLAN досить молодий. Перші пристрої для бездротових локальних мереж з'явилися на початку-середині 90-х років. Але вже у 1999-му обсяг продажів устаткування WLAN досяг 600-770 млн.

доларів, а до 2004 р. він склав порядку 2,2-3 млрд. доларів. Щомісяця у світі продається близько мільйона адаптерів тільки стандарту IEEE 802.11b. За експертними оцінками, до 2003 р. їх було встановлено понад 20 млн. Причому стрімко розвиваються самі технології передачі й устаткування для них - швидкості виростили від 1-2 до 54 Мбіт/с, потім переступили й бар'єр в 100 Мбіт/с. З неменшою швидкістю падає й вартість устаткування, становлячи вже десятки доларів для кінцевих пристроїв користувачів.

Роботи над єдиним стандартом локальних БСПІ розпочалися в 1989 р., коли була організована робоча група 11-го комітету IEEE 802. У липні 1997 р. у результаті роботи цієї групи був опублікований стандарт IEEE 802.11 «Специфікація фізичного рівня й рівня контролю доступу до каналу передачі бездротових локальних мереж» («Wireless LAN Medium Access Control and Physical Layer Specifications»). Він визначав архітектуру мережі, впливаючі з цього вимоги до функцій пристроїв, принципи доступу пристроїв до каналів зв'язку, формат пакетів передачі, способи аутентифікації й захисту даних. Хоча стандарт спочатку задумувався як інваріантний стосовно будь-якого частотного діапазону, на фізичному рівні він визначав три способи роботи: два радіочастотних та оптичний. В інфрачервоному діапазоні передбачалася імпульсно-позиційна модуляція, у діапазоні 2,400-2,4835 ГГц - режими модуляції з розширенням спектру методом частотних стрибків (FHSS) і методом прямої послідовності (DSSS). Швидкості обміну встановлювалися на рівні 1 й 2 Мбіт/с.

Відзначимо, що пристрої, які відповідають вихідній специфікації IEEE 802.11, не встигли отримати розвитку. Пропускна здатність провідних мереж Ethernet дуже зросла, і максимальна швидкість передачі 2 Мбіт/с, передбачена в IEEE 802.11, не задовольняла користувачів. Проблему вирішила поява стандартів (доповнень) IEEE 802.11b, 802.11a й 802.11g.

Першим став затверджений 16 вересня 1999 р. стандарт IEEE 802.11b. Він описував фізичний і MAC-рівні бездротових мереж для роботи в діапазоні 2,4 ГГц. Стандарт визначав роботу на швидкостях 1 й 2 Мбіт/с з модуляцією тільки методом DSSS. Найголовніше - він передбачав швидкості обміну до 11 Мбіт/с (а опційно - і до 33 Мбіт/с). Передача даних на швидкостях 5,5 та 11 Мбіт/с відбувається за допомогою модуляції комплементарних кодових послідовностей ССК (основний вид модуляції). Крім того, передбачалася й робота на швидкостях 22 й 33 Мбіт/с за допомогою пакетного бінарного згортувального кодування (PBCC).

Стандарт IEEE 802.11a, який описує роботу в діапазоні 5 ГГц, був прийнятий одночасно з IEEE 802.11b. У ньому використаний принципово інший, ніж в IEEE 802.11b, механізм модуляції/мультиплексування, а саме частотне мультиплексування за допомогою ортогональних несучих (OFDM). Даний метод, зокрема, досить добре зарекомендував себе в системах цифрового телевізійного мовлення DVB. Наприкінці 1999 р. були

закінчені основні роботи зі створення європейського 5 ГГц стандарту бездротових мереж HiperLan2 (HiperLan type 2), який так і не отримав масового розвитку. У червні 2003 р. був затверджений високошвидкісний (до 54 Мбіт/с) стандарт у діапазоні 2,4 ГГц - IEEE 802.11g.

Сьогодні близький до завершення стандарт IEEE 802.11n, що описує мережі зі швидкістю обміну понад 100 Мбіт/с на основі технології активних антенних систем MIMO. Розробляється мобільна версія стандарту (IEEE 802.11p) і доповнення, призначене для надання гарантованої якості зв'язку (QoS), - IEEE 802.11e.

3.1. Основні принципи побудови та функціонування мереж IEEE 802.11

Розглянемо докладніше, що являє собою стандарт IEEE 802.11 як базовий для всіх наступних специфікацій. Як і всі стандарти комітету IEEE 802, у документі IEEE 802.11 розглядаються два нижніх рівні моделі взаємодії відкритих систем (OSI): фізичний і канальний (Data Link layer). Причому останній підрозділяється на два підрівня. Верхній - Logical Link Control (LLC) - описаний у стандарті IEEE 802.2. Стандарт IEEE 802.11 розглядає тільки нижній підрівень - Medium Access Control (MAC), тобто керування доступом до каналу (до середовища передачі). Іншими словами, на фізичному рівні стандарт визначає спосіб роботи із середовищем передачі, швидкість і методи модуляції. На MAC-рівні - принцип, за яким пристрої використовують (ділять) загальний канал, способи підключення пристроїв до точок доступу і їх аутентифікації, механізми захисту даних. Оскільки стандарт IEEE 802.11 розроблявся як «бездротовий Ethernet», він передбачає пакетну передачу з 48-бітними адресами пакетів, як і будь-яка мережа Ethernet. Комітет IEEE 802 особливу увагу приділяв сумісності всіх своїх стандартів, у результаті провідні й безпроводні мережі IEEE 802 легко сполучаються одна з одною.

Коли мова заходить про радіотракт, ключове питання — частотний діапазон. IEEE 802.11 прив'язаний до існуючим у США й ряді інших країн безліцензійних частотних діапазонів. Споконвічно він був орієнтований на діапазон 2,400-2,4835 ГГц із шириною смуги 83,5 МГц. Обумовлена стандартом спектральна маска для одного каналу наведена на рис. 10.1 (потужність відраховується відносно піків функції $\sin(x)/x$). Ширина каналу на рівні -30 дБ становить 22 МГц, отже, у смузі 83,5 МГц можливо три канали, які не перекриваються.

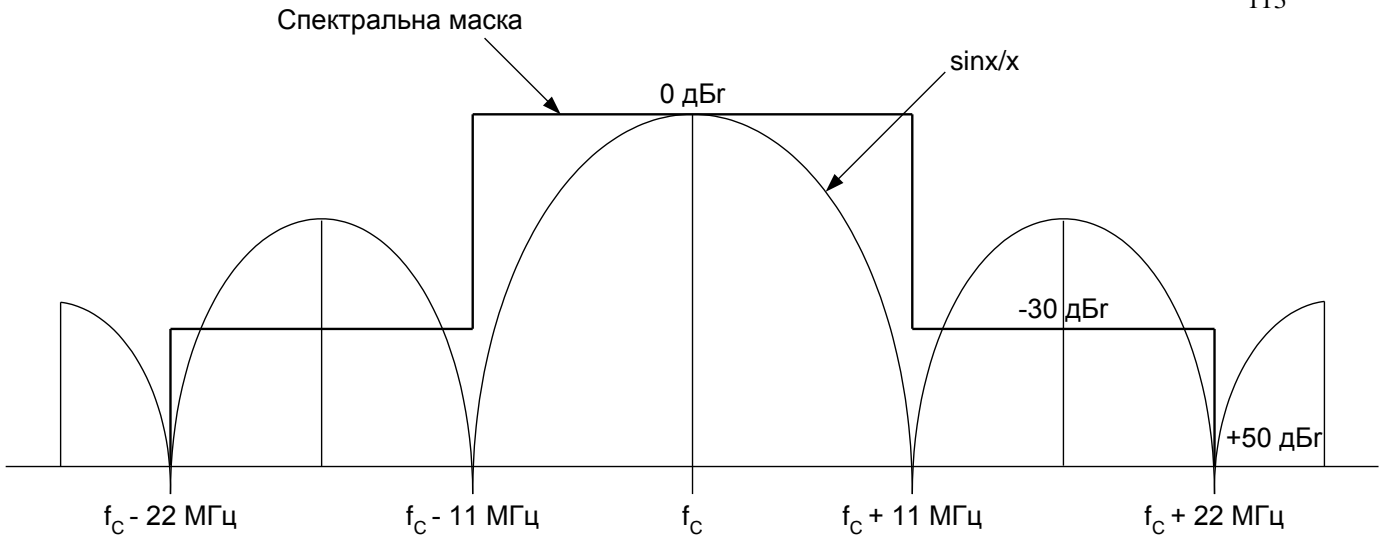


Рис. 3.1. Спектральна маска каналу мережі 802.11 при модуляції методом DSSS

Стандарт передбачає два основних способи організації локальної мережі: за принципом «рівний з рівним» (ad-hoc-мережа — рис. 3.2, а) та у вигляді структурованої мережі (рис. 3.2, б).

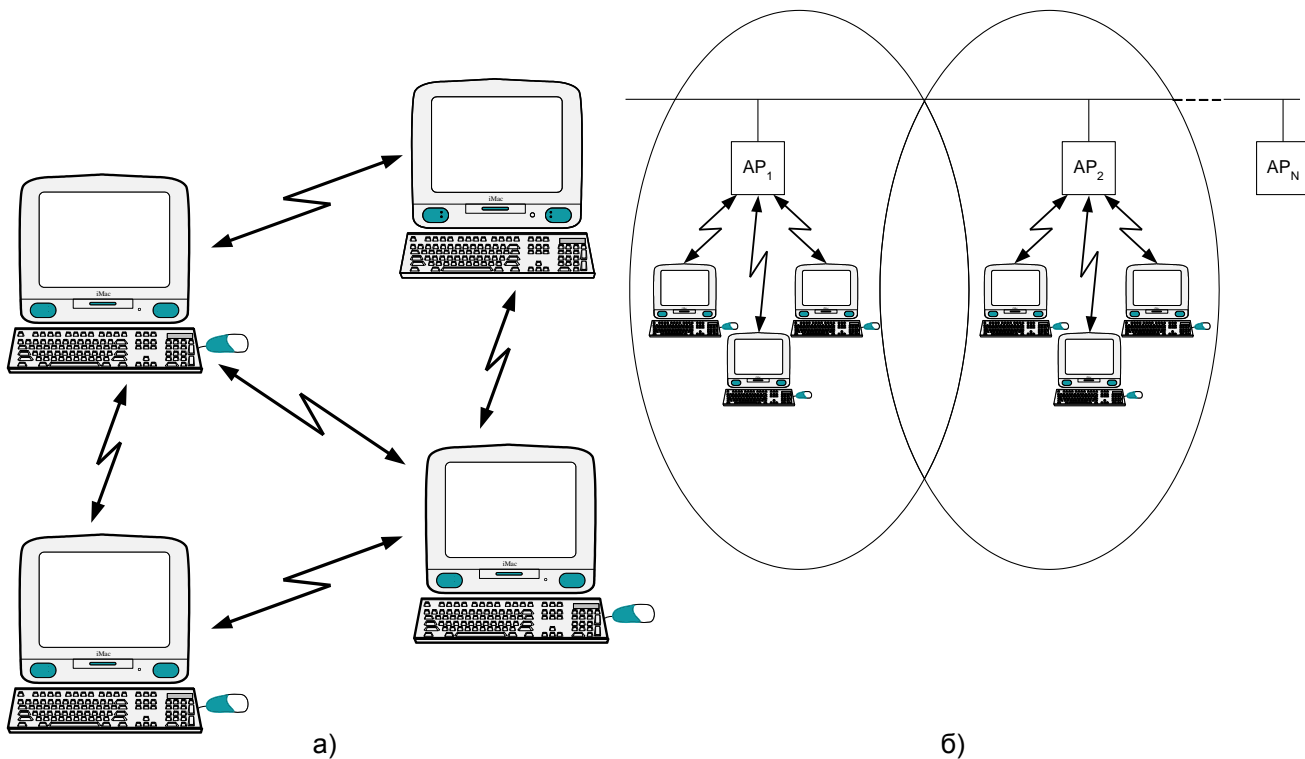


Рис. 3.2. Архітектура мережі 802.11: а - ad-hoc-мережа; б - структуровані мережі

У першому випадку зв'язок встановлюється безпосередньо між двома станціями, і ніякого адміністрування не передбачено. У випадку структурованих мереж (а як показала практика, це основний спосіб побудови мереж IEEE 802.11) у їхньому складі з'являється додатковий пристрій - точка доступу (AP - Access Point), як правило, стаціонарна й діюча на фіксованому каналі. Зв'язок між пристроями відбувається тільки через AP. Через них же можливий вихід у зовнішні проводові мережі.

У мережі IEEE 802.11 може бути декілька AP, об'єднаних проводовою мережею Ethernet. Фактично така мережа являє собою набір базових станцій із зонами обхвату, що перекриваються, . Стандарт IEEE 802.11 допускає переміщення пристроїв із зони одної AP у зону іншої (роумінг), тим самим забезпечуючи мобільність. Оскільки для мобільних станцій важливе питання ресурсу елементів живлення, у стандарті закладений спеціальний протокол керування енергоспоживанням - безпосередньо при обміні передавальний пристрій може перевести приймач у режим очікування.

Найважливіша вимога до стандартів бездротового зв'язку - безпека передачі даних. У зв'язку з цим на MAC-рівні передбачений механізм захисту даних, що включає аутентифікацію станцій і власне шифрування передаваних даних. Цей механізм повинен забезпечувати такий же рівень захисту, як і у звичайних мережах Ethernet, тому його назвали WEP (Wired Equivalent Privacy - еквівалент проводової конфіденційності). Алгоритм WEP заснований на використанні чотирьох загальних для однієї мережі секретних ключів довжиною 40 біт. Саме шифрування відбувається по алгоритму RC4 компанії RSA Security. Алгоритм використовує перемноження блоків вихідних даних на псевдовипадкову послідовність такої ж довжини, що й блок шифруємих даних. Генератор псевдовипадкової послідовності ініціалізується 64-розрядним числом, що складається з 24-розрядного вектора ініціалізації (IV - initialization vector) і 40-розрядного секретного ключа. Істотно, що якщо секретний ключ відомий пристроям мережі й незмінний, то вектор IV може змінюватися від пакета до пакета. Для захисту від несанкціонованої зміни переданої інформації кожен шифрований пакет захищається 32-розрядною контрольною сумою (ICV - integrity check value). Таким чином, при шифруванні до передаваних даних додається 8 байт: 4 для ICV, 3 для IV, і ще 1 байт містить інформацію про номер секретного ключа, який використовується (одного з чотирьох). Відзначимо, що секретний ключ може бути набагато довшим - 64, 128 біт і т.д. Це не суперечить стандарту, більше того, таке устаткування випускається, однак законодавство США перешкоджає експорту пристроїв, що підтримують шифрування даних із ключем довше 40 біт. Саме тому виробники й обмежуються 240 варіантами ключа. Додаткові методи захисту інформації й аутентифікації в мережах 802.11 описані в стандарті IEEE 802.11i (опублікований в 2004 р.).

Як ми вже відзначали, пристрої, що відповідають вихідній специфікації IEEE 802.11, практично не одержали розвитку. Тому далі будемо розглядати IEEE 802.11 з точки зору специфікації IEEE 802.11b, як першої, активно підтриманої виробниками апаратури.

3.2 MAC-рівень стандарту IEEE 802.11

Стандарт IEEE 802.11 передбачає два режими керування мережею: коли функції керування розподілені між усіма пристроями мережі IEEE

802.11 - так званий режим DCF (Distributed coordination function) - і коли вони зосереджені в одній певній точці доступу - режим PCF (Point coordination function). У режимі DCF всі пристрої працюють за принципом конкурентного доступу до каналу передачі, тобто пріоритетів не існує. Необхідність у режимі централізованого керування PCF виникає при передачі чутливої до затримок інформації (наприклад, відеопотоків), коли необхідно вводити пріоритети доступу.

Робота в режимі PCF може відбуватися тільки під керуванням спеціальної точки доступу, яка називається точкою координації (PC), і тільки в певні інтервали, які періодично повторюються. Коли мережа переходить у режим PCF, у трафіку з'являються інтервали, у яких конкурентний доступ відмінений, і весь обмін відбувається під керуванням координуючого пристрою (PC) (рис. 3.3). По завершенні такого інтервалу мережа повертається в режим DCF. Інтервали під керуванням PC слідуєть через чітко визначений період, на початку кожного інтервалу PC виставляє особливий сигнальний кадр (Beacon). PC не може передати наступний сигнальний кадр доти, доки канал не звільниться, тобто наступний «вільний від конкуренції» інтервал може початися з затримкою.

Режим PCF важливий для передачі регулярно повторюваної чутливої до затримок інформації. Він також ефективний, якщо мережі IEEE 802.11 використовуються як середовище доступу до Інтернету (або інших глобальних мереж), тобто забезпечують обмін даними між користувачами й централізованим провайдером. Однак основний принцип мереж Ethernet - це все ж таки довільний конкурентний доступ, що й робить останніми настільки простими в реалізації й експлуатації. У провідних мережах Ethernet використовується механізм множинного доступу до каналу зв'язку з контролем несучої й виявленням конфліктів (CSMA/CD - Carrier Sense Multiple Accesses with Collision Detection). Станція може почати передачу тільки якщо канал вільний. Якщо станції виявляють, що на одному каналі намагаються працювати кілька станцій, всі вони припиняють передачу й намагаються відновити її через випадковий проміжок часу. Таким чином, навіть при передачі пристрій повинен контролювати канал, тобто працювати на прийом.

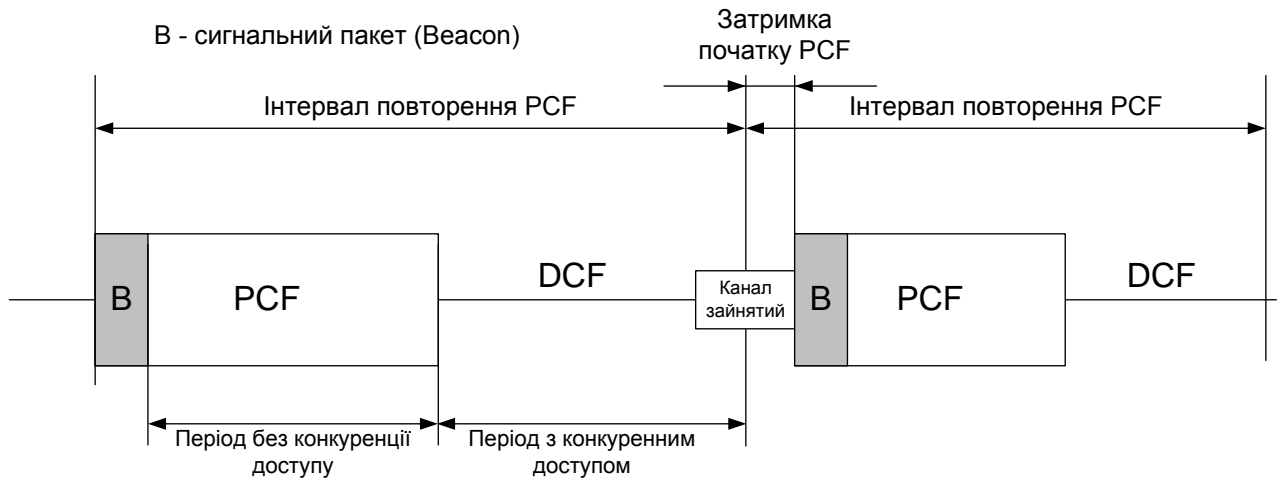
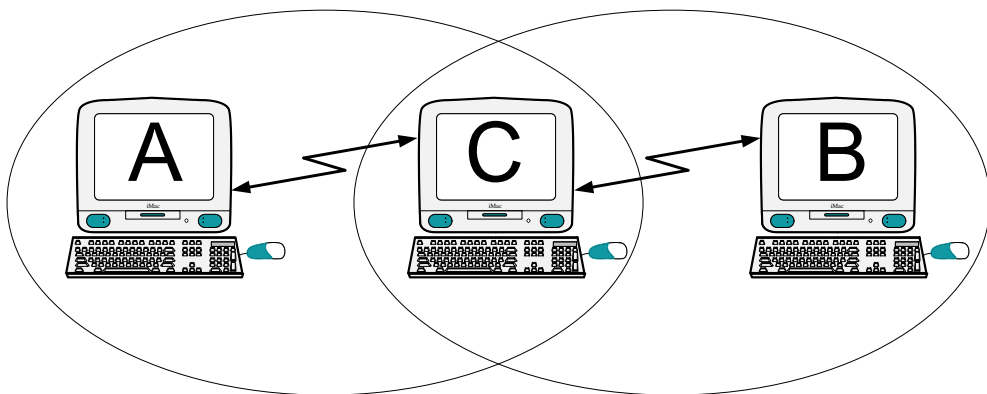


Рис. 3.3. Цикли роботи мережі в режимах з централізованим (PCF) та розподільчим (DCF) керуванням

Те, що відносно просто при проводовому зв'язку, проблематично в бездротових комунікаціях - загасання сигналу в ефірі набагато сильніше, ніж у проводі. Тому виникають дві основні проблеми. По-перше, досить складна, якщо взагалі розв'язна, задача контролю несучої передавальним пристроєм (коли воно віщає, то власний сигнал завідомо набагато потужніше, ніж сигнал віддаленого пристрою). По-друге, можлива ситуація, коли два пристрої (А і В) віддалені і не чують один одного, однак обидва попадають у зону обхвату третього пристрою - С (рис. 3.4) - так звана проблема прихованих станцій. Якщо обидва пристрої, А і В, розпочнуть передачу, то вони принципово не зможуть виявити конфліктну ситуацію й визначити, чому пакети не проходять.

Рис. 3.4. Ілюстрація проблеми прихованих станцій



Для усунення подібних проблем у специфікації IEEE 802.11 прийнятий механізм CSMA/CA (Carrier Sense Multiple Accesses with Collision Avoidance) - множинний доступ з контролем несучої й запобіганням колізій. Перед початком передачі пристрій слухає ефір і чекає, коли канал звільниться. Канал вважається вільним за умови, що не виявлено активності протягом певного проміжку часу - міжкадрового інтервалу (IFS) певного типу. Якщо протягом цього проміжку канал залишався

вільним, пристрій очікує ще протягом випадкового часу відстрочки й, якщо канал ще не зайнятий, передає пакет. Якщо пакет призначений конкретному пристрою (не широкомовна або багатоадресна передача), то приймач, успішно прийнявши пакет, посилає передавачу короткий кадр підтвердження отримання АСК (ACKnowledge). Якщо передавач не прийняв АСК, він вважає посланий пакет загубленим і повторює процедуру його передачі.

Важливо, що, якщо пристрій повторно передає пакет, для визначення незайнятості каналу він повинен використати збільшений міжпакетний інтервал (EIFS). Крім того, час відстрочки вибирається випадковим чином на деякому інтервалі. При першій спробі передачі цей інтервал мінімальний. При кожній наступній він подвоюється доти, поки не досягне заданого граничного значення. Ці міри приводять до того, що пристрій, який успішно передав пакет, має переваги в захваті каналу (хто помиляється, той довше чекає).

Перед першою спробою отримати доступ до каналу пристрій завантажує тривалість випадкового інтервалу відстрочки в спеціальний лічильник. Його значення декрементується із заданою частотою, поки канал вільний. Як тільки лічильник обнулиться, пристрій може займати канал. Якщо до обнулення лічильника канал займає інший пристрій, рахунок зупиняється, зберігаючи досягнуте значення. При наступній спробі відлік починається зі збереженої величини. В результаті невстигнувший минулого разу одержує більше шансів зайняти канал наступного разу. У проводових мережах Ethernet подібного механізму немає.

Однак описані процедури доступу не позбавляють від проблеми прихованих станцій. Для її подолання використовують два додаткових кадри: RTS (Request to Send - запит на передачу) і CTS (Clear to Send - підтвердження готовності). Пристрій, що бажає відправити пакет даних, передає адресату короткий кадр RTS. Якщо приймальний пристрій готовий до прийому, він виставляє передавачу кадр відповіді - CTS. Далі відповідно до описаного вище процедури передавачу пристрій відправляє кадр з даними й чекає підтвердження АСК.

Стандарт IEEE 802.11 передбачає два механізми контролю за активністю в каналі (виявлення несучої): фізичний і віртуальний. Перший механізм реалізований на фізичному рівні й зводиться до визначення рівня сигналу в антені й порівнянню його із граничною величиною. Віртуальний механізм виявлення несучої заснований на тому, що в передаваних кадрах даних, а також у керуючих кадрах АСК й RTS/CTS міститься інформація про час, необхідний для передачі пакета (або групи пакетів) і отримання підтвердження. Всі пристрої мережі приймають інформацію про поточну передачу й можуть визначити, скільки часу канал буде зайнятий, тобто пристрій при встановленні зв'язку всім повідомляє, на який час він резервує канал.

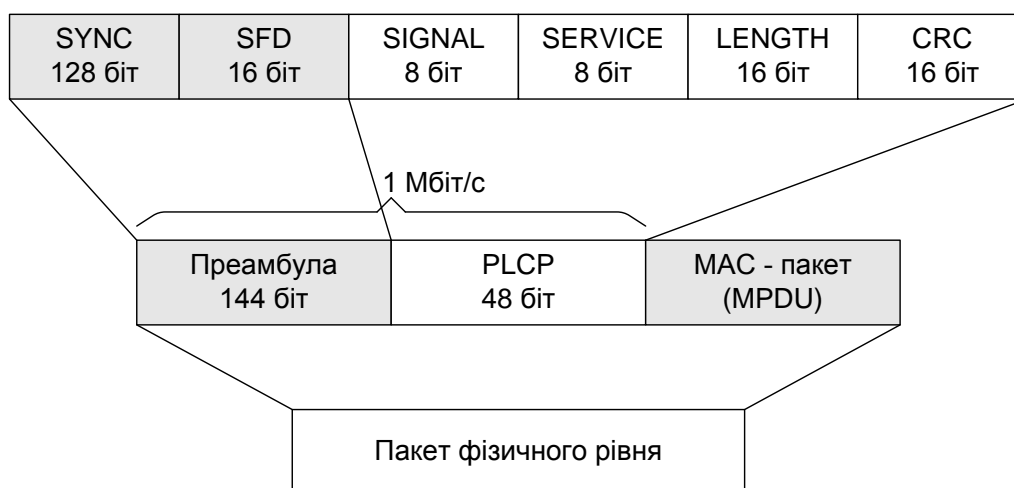


Рис. 3.6. Структура кадрів фізичного рівня мережі 802.11

У стандарті IEEE 802.11b передбачено два типи заголовків: довгий і короткий (рис. 3.7). Вони відрізняються довжиною синхро-послідовності (128 і 56 біт), способом її генерації, а також тим, що символ початку кадру в короткому заголовку передається у зворотному порядку. Крім того, якщо всі поля довгого заголовка передаються зі швидкістю 1 Мбіт/с, то при короткому заголовку препамбула транслюється на швидкості 1 Мбіт/с, інші поля заголовка - зі швидкістю 2 Мбіт/с. Іншу частину кадру можна передавати на кожній із допустимих стандартом швидкостей передачі, зазначених у полях SIGNAL й SERVICE. Короткі заголовки фізичного рівня передбачені специфікацією IEEE 802.1b для збільшення пропускної здатності мережі.

З опису процедур зв'язку мережі IEEE 802.11 видно, що «накладні витрати» у цьому стандарті вище, ніж у проводовій мережі Ethernet. Тому дуже важливо забезпечити високу швидкість передачі даних у каналі. Підвищити пропускну здатність каналу з заданою шириною смуги частот можна, розробляючи й застосовуючи більш досконалі методи модуляції. Цим шляхом пішла група розробників IEEE 802.11b.

Спочатку стандарт IEEE 802.11 передбачав роботу в режимі DSSS з використанням так називаємої баркерівської послідовності (Barker) довжиною 11 біт: $V_1 = 10110111000$. Кожен інформаційний біт заміщається своїм добутком по модулю 2 (операція «виключаюче ІЛИ») з даною послідовністю, тобто кожна інформаційна одиниця заміняється на V_1 , кожен нуль — на інверсію V_1 . У результаті біт заміняється послідовністю 11 чипів. Далі сигнал кодується за допомогою диференційної двох- або чотирьохпозиційної фазової модуляції (DBPSK або DQPSK, один або два чипи на символ відповідно). При частоті модуляції несучої 11 МГц загальна швидкість становить залежно від типу модуляції 1 і 2 Мбіт/с.



Рис. 3.7. Короткий заголовок кадрів мережі 802.11b

Стандарт IEEE 802.11b додатково передбачає швидкості передачі 11 й 5,5 Мбіт/с. Для цього використовується так звана ССК-модуляція (Complementary Code Keying — кодування комплементарним кодом). В основу даного методу лягли роботи фахівців компаній Intersil (раніше — Harris Semiconductor) і частково Agere Systems (напівпровідниковий підрозділ, виділений з Lucent Technologies). Першим, очевидно, виклав ідею бінарних комплементарних кодів Марсель Голей (М.Ж.Е. Golay), більш як півстоліття назад описавши їх принцип і методи генерації. Суть комплементарного кодування полягає у використанні двох послідовностей a і b , кожна з k елементів, з автокореляційними функціями:

$$A(i) = \sum_{j=1}^{k-i} a_j a_{j+i} \quad \text{і} \quad B(i) = \sum_{j=1}^{k-i} b_j b_{j+i}$$

де $i = 0, \dots, k-1$ — можливе зміщення. Послідовності a і b комплементарні, якщо $A(i)+B(i) = 0$ при будь-якому $i \neq 0$, і $A(0)+B(0) = 2k$. Фізична інтерпретація автокореляції зі зміщенням — одночасний прийом сигналу, що поширюється прямо і сигналу з фазовою затримкою на i елементів (чипів). Іншими словами, якщо система зв'язку, яка використовує комплементарне кодування, працює в умовах багатошляхового поширення сигналів, то в ідеалі міжсимвольна інтерференція (викликана накладанням сигналів з затримками поширення) повинна бути відсутньою, оскільки сума їх автокореляційних функцій дорівнює нулю.

Метод ССК використовує диференціальну квадратурну модуляцію (DQPSK) у радіотракті. ССК-модуляція будується на виділенні з послідовного інформаційного потоку груп по 8 біт (d_0-d_7). Ці 8 біт визначають інформаційний символ C з восьми комплексних чипів $C = [c_0, \dots, c_7]$. Використовуючи подання Ейлера, можна записати:

$c_i = e^{j\psi_i} = \cos\psi_i + j\sin\psi_i$, де ψ_i — фаза чіпа; $j = \sqrt{-1}$. Чипи є комплексними, оскільки стосовно до квадратурної модуляції дійсна та уявна складові відносяться до синфазного (I) і квадратурного (Q) каналів відповідно.

Вісім чипів інформаційного символу послідовно модулюють несучу із частотою модуляції 11 МГц. Фаза ψ_i кожного з них визначається відповідно до формули:

$$C = [c_0, \dots, c_7] = [e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, e^{-j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, e^{-j(\phi_1+\phi_2)}, e^{j\phi_1}] \quad (3.1)$$

Інакше цю формулу можна записати для вектора Ψ фаз чипів символу C :

$$\Psi = [\psi_0, \dots, \psi_7] = [\phi_1 + \phi_2 + \phi_3 + \phi_4; \phi_1 + \phi_3 + \phi_4; \phi_1 + \phi_2 + \phi_4; -(\phi_1 + \phi_4); \phi_1 + \phi_2 + \phi_3; \phi_1 + \phi_3; -(\phi_1 + \phi_2); \phi_1] \quad (3.2)$$

Елемент ϕ_1 входить у кожен чип символу, тобто змінює фазу всього символу. Фазова модуляція сигналу називається диференціальною, оскільки значення ϕ_1 поточного символу визначається щодо значення ϕ_1 попереднього символу. Зміна фази ϕ_1 задається в залежності від значень двохрозрядних двійкових чисел (дубітів) $(d_0 d_1)$. При цьому для парних символів встановлена наступна відповідність $(d_0 d_1) \rightarrow \Delta\phi_1$: $(00) \rightarrow 0$; $(01) \rightarrow \pi/2$; $(11) \rightarrow \pi$; $(10) \rightarrow -\pi/2$. Для непарних символів значення ϕ_1 додатково зміщують на π .

Як ми вже відзначали, у стандарті IEEE 802.11b за допомогою ССК кодують тільки MAC-кадр. Тому перший ССК-символ — той, що іде відразу за символами заголовка фізичного рівня. Він має номер «0», тобто є парним. Фаза останнього QPSK-символу заголовка кадру є опорною для визначення ϕ_1 першого символу інформаційного поля — до нього додається $\Delta\phi_1$. Інші три параметри мають абсолютні значення. Для швидкості 11 Мбіт/с вони визначаються як $\phi_2 = (d_2 d_3) \cdot \pi/2$; $\phi_3 = (d_4 d_5) \cdot \pi/2$; $\phi_4 = (d_6 d_7) \cdot \pi/2$, де $(d_i d_{i+1})$ — двохрозрядні двійкові числа.

Для швидкості 5,5 Мбіт/с також використовується DQPSK-модуляція, але ССК-символ (з восьми чипів) визначають не вісім, а чотири інформаційних біти (d_0-d_3) , тому й швидкість удвічі нижче. Параметр ϕ_1 обчислюється так само, як і для 11 Мбіт/с, інші інакше: $\phi_2 = d_2 \cdot \pi + \pi/2$; $\phi_3 = 0$; $\phi_4 = d_3 \pi$.

На прийомній стороні, за умови синхронного прийому, декодуючий пристрій відновлює значення $\phi_1, \phi_2, \phi_3, \phi_4$, а по них — і значення інформаційних біт. У найпростішому випадку обробка зводиться до наступних обчислень:

$$\phi_2 = \arg \left\{ r_2^* + r_3 r_4^* + r_5 r_6^* + r_7 r_8^* \right\}$$

$$\phi_3 = \arg \left\{ r_3^* + r_2 r_4^* + r_5 r_7^* + r_6 r_8^* \right\}$$

$$\phi_4 = \arg \left\{ r_5^* + r_2 r_6^* + r_3 r_7^* + r_4 r_8^* \right\}$$

$$\phi_1 = \arg \left\{ r_4 e^{-j\phi_4} + r_6 e^{-j\phi_3} + r_7 e^{-j\phi_2} + r_8 \right\}$$

де $r = [r_1, \dots, r_8]$ — прийнята 8-бітна послідовність ССК-символів. Знак * означає комплексне сполучення, тобто якщо $r_i = a + jb$, то $r_i^* = a - jb$. Функція $\arg(r) = \arctg[Im(r)/Re(r)] = \arctg(b/a)$.

У чому перевага ССК-модуляції? Як видно з формули (3.2), фази чипів символу (вектора) C визначаються на основі послідовностей Уолша-

Адамара. Якщо записати вектор $\Phi = [\varphi_1, \varphi_2, \varphi_3, \varphi_4]$, то для швидкості 11 Мбіт/с вектор $\Psi = (\Phi \times WH + B)$, де WH - верхня половина матриці Уолша-Адамара:

$$WH = \begin{bmatrix} 11111111 \\ 10101010 \\ 11001100 \\ 11110000 \end{bmatrix}$$

Вектор $B = [0, 0, 0, \pi, 0, 0, \pi, 0]$, фізично відповідний повороту фази чипів c_3 і c_6 на 180° (знаки «мінус» у формулі (3.1)), необхідний для поліпшення кореляційних властивостей кодових послідовностей. Послідовності Уолша-Адамара добре вивчені, мають відмінні автокореляційні властивості. Що важливо, кожна така послідовність мало корелює сама із собою при фазовому зміщенні - дуже корисна властивість при боротьбі з перевідбитими сигналами. Незавжди помітити, що теоретичне посилення обробки при ССК-модуляції 3 дБ (в 2 рази), оскільки без кодування комплементарним поліфазним кодом сигнал, модульований QPSK із частотою 11 Мсимвол/с, може транслювати 22 Мбіт/с. Як видно, ССК-модуляція являє собою вид блокового коду, а тому досить проста при апаратній реалізації. Сукупність цих властивостей і забезпечила ССК місце в стандарті IEEE 802.11b в якості обов'язкового виду модуляції.

На практиці важливо не тільки операційне посилення. Істотну роль грає й рівномірність розподілу символів у фазовому просторі (відстань Хеммінга) - символи повинні якнайдалі стояти один від одного, щоб мінімізувати помилки їх детектування. І з цієї точки зору ССК-модуляція не виглядає оптимальною, її реальне операційне посилення не перевищує 2 дБ. Тому спочатку пророблявся інший спосіб модуляції - пакетне бінарне згортувальне кодування РВСС (Packet Binary Convolutional Coding). Цей метод увійшов у стандарт IEEE 802.11b опційно, тобто як необов'язкова опція. Механізм РВСС (рис. 3.8) був запропонований фахівцями фірми Alantro Communications, в 2000 р., яка увійшла до складу компанії Texas Instruments. РВСС дозволяє добиватися в мережах IEEE 802.11b пропускної здатності 5,5; 11 й 22 Мбіт/с.

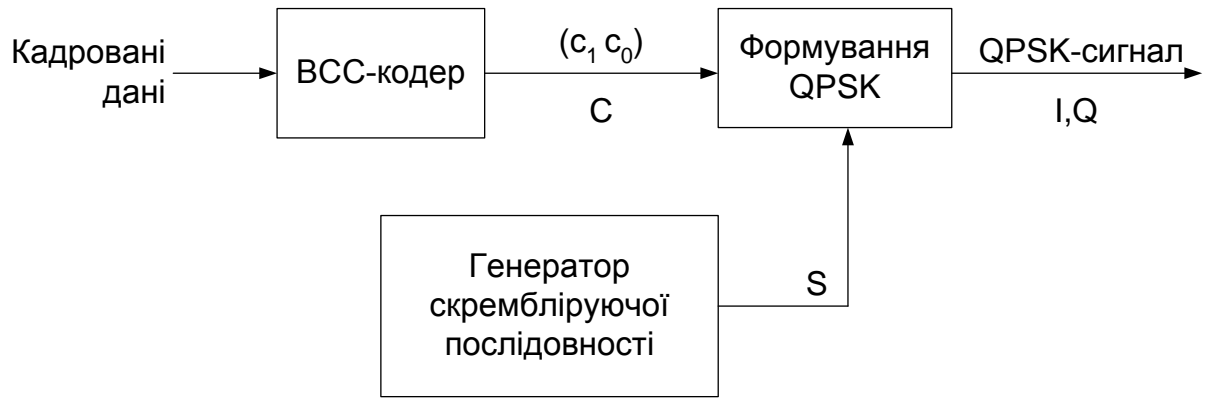


Рис. 3.8. Загальна схема RBCC-модуляції

Як випливає з назви, метод заснований на згортковому кодуванні. Для швидкостей 5,5 й 11 Мбіт/с потік інформаційних біт надходить в 6-розрядний регістр зміщення з суматорами (рис. 3.9, а). У початковий момент часу всі тригери регістра зміщення ініціалізуються нулем. У результаті кожен вихідний біт d замінюється двома бітами кодової послідовності (c_0 , c_1). При швидкості 11 Мбіт/с c_0 та c_1 задають один символ чотирьохпозиційної QPSK-модуляції. Для швидкості 5,5 Мбіт/с використовують двопозиційну BPSK-модуляцію, послідовно передаючи кодові біти c_0 та c_1 . Якщо ж потрібна швидкість 22 Мбіт/с, схема кодування ускладнюється (рис. 3.9, б): три кодових біти (c_0 - c_2) визначають один символ у восьмипозиційній 8-PSK-модуляції.

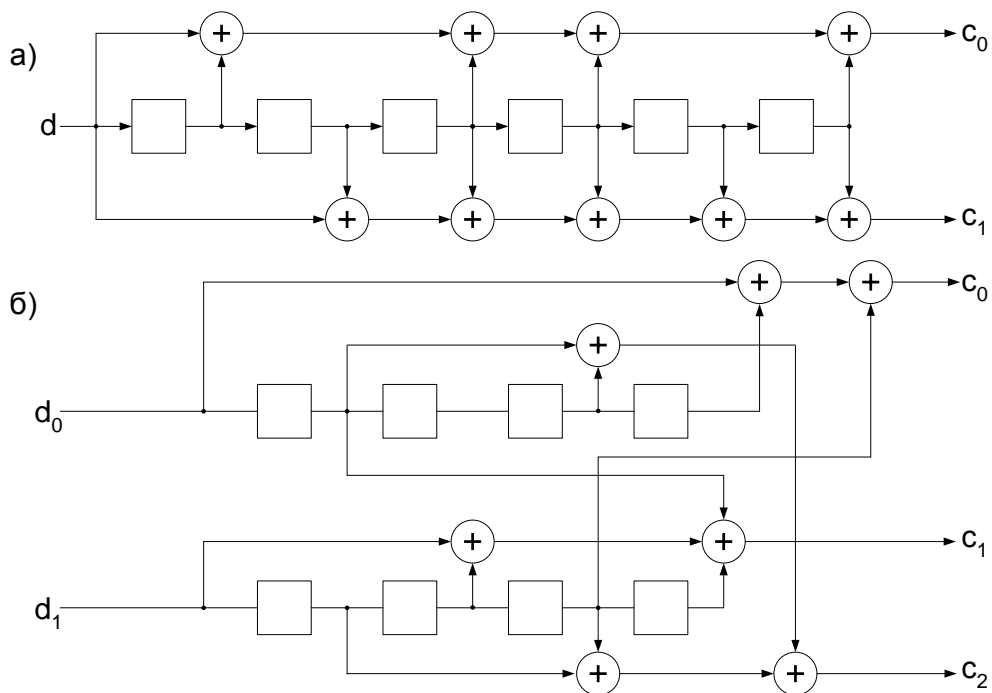
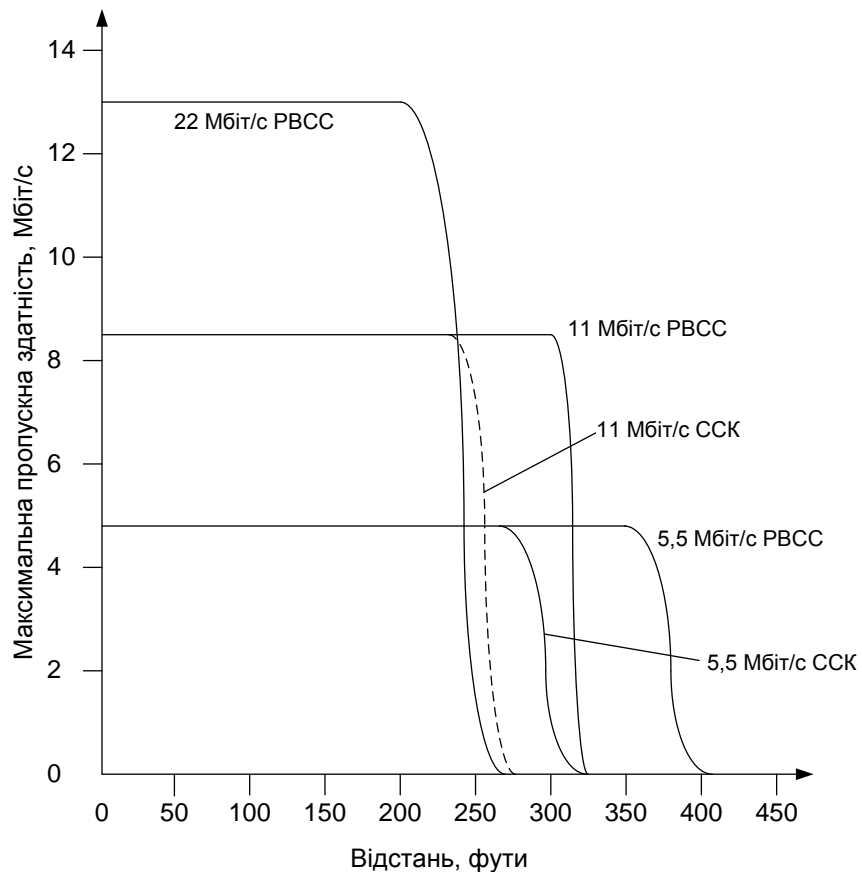


Рис. 3.9. Схема сверточного VCC-кодування: а) - для швидкостей 5,5 та 11 Мбіт/с; б) - для швидкості 22 Мбіт/с

Після формування PSK-символів відбувається скремблювання. Залежно від сигналу s (див. рис. 3.8) символ залишається без змін ($s = 0$) або його фаза збільшується на $\pi/2$ ($s = 1$). Значення s визначає 256-бітна циклічно повторювана послідовність S . Вона формується на основі початкового вектора $U=338B_{16}$, у якому рівне число нулів й одиниць. S являє собою 16 послідовних векторів U_i ($i=0, \dots, 15$), причому кожен вектор U_i циклічно зміщують вліво у порівнянні з U_{i-1} на $3i$ розряди.

У 6-розрядного регістра зміщення, який застосовується у PBCC для швидкостей 11 й 5,5 Мбіт/с, 64 можливі вихідні стани. Отже, при модуляції PBCC інформаційні біти у фазовому просторі виявляються набагато далі один від одного, ніж при CCK-модуляції. Тому PBCC і дозволяє при тих самих співвідношеннях сигнал/шум і рівні помилок вести передачу з більшою швидкістю, ніж у випадку CCK (рис. 3.10). Однак плата за більш ефективне кодування - складність апаратної реалізації даного алгоритму. Мабуть, не випадково просувати PBCC-модуляцію стала компанія Texas Instruments - ведучий виробник процесорів цифрової обробки сигналу.

Рис. 3.10. Дальність зв'язку при різноманітних способах модуляції та фіксованому загасанні в каналі (За матеріалами компанії Texas Instruments про використання IC ACX100)



3.4. Особливості стандарту IEEE 802.11a

Стандарт IEEE 802.11a з'явився практично одночасно зі стандартом IEEE 802.11b, у вересні 1999 г. Він орієнтований на роботу у діапазоні 5 ГГц та заснований на технології OFDM (Orthogonal Frequency Division

Multiplexing — мультиплексування за допомогою ортогональних несучих).

Формування OFDM-символів

Технологія OFDM означає, що одночасно інформація передається по багатьом піднесучим частотам, що утворюють канал. Ширина каналу — 20 МГц. У мережах IEEE 802.11a у 20-МГц каналі використовується 52 піднесучі, але їх номінальне число обирається з міркувань зручності перетворення Фур'є та приймається рівним 64. Таким чином, інтервал між піднесучими $\Delta f = 20 \text{ МГц} / 64 = 312,5 \text{ кГц}$, а самі піднесучі можна представити як $f_k(t) = a_k \sin[2\pi(f_0 + k\Delta f)t + \phi_k]$, де $k = -26, \dots, 26$. Центральна піднесуча f_0 не використовується (її амплітуда завжди рівна нулю). Піднесучі модулюються шляхом квадратурної амплітудно-фазової модуляції: 2-, 4-, 16- та 64-позиційної BPSK, QPSK, 16-QAM та 64-QAM, відповідно. Сигнал зручно представляти у комплексній формі

$C = a \cos x + b \sin x = A e^{jx}$, де $j = \sqrt{-1}$. Відповідно сумарний сигнал на всіх піднесучих можна записати як

$$s(t) = \sum_{k=-26}^{26} C_k e^{j2\pi(f_0 + k\Delta f)t} \quad (3.3)$$

C_k — комплексна амплітуда k -ї піднесучої, уявна та дійсна складові якої відповідають квадратурному (Q) та синфазному (I) каналам квадратурної модуляції. Значення комплексних складових обирають відповідно до діаграми Грея (рис. 3.13), виходячи з потоку інформаційних біт.

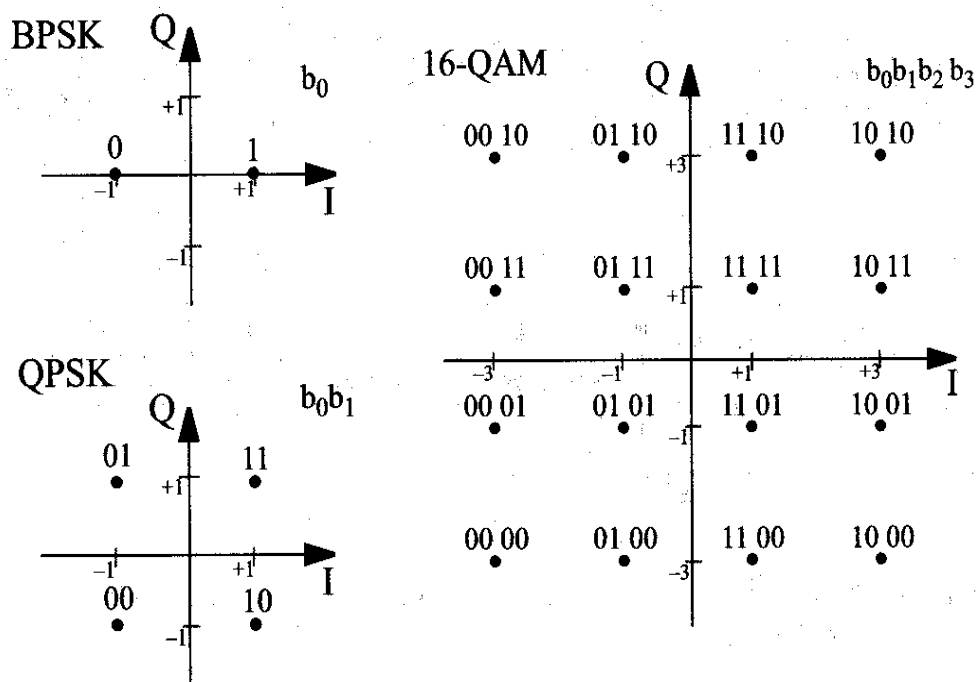


Рис. 3.13. Представлення модуляційних символів (діаграма Грея) для BPSK, QPSK та 16-QAM

OFDM-символ являє собою сукупність усіх піднесучих на дискретному інтервалі тривалістю $T_F=1/\Delta f=3,2$ мкс. Інформаційна ємність OFDM-символа визначається типом модуляції інформаційних піднесучих та їх числом. З 52 піднесучих у стандарті IEEE 802.11a для передачі даних використовуються 48, інші 4 піднесучі — пілотні. Тобто, ємність OFDM-символа складає $48 \times N_b$, де N_b — число біт в одному модуляційному символі (на одній піднесучій), що дорівнює двійковому логарифму від числа позицій модуляції. Таким чином, OFDM-символ містить від 96 до 288 біт.

Відмітимо, що OFDM-модуляція володіє потужним засобом боротьби з міжсимвольною інтерференцією, яка проявляється в тому, що через численні перевідбиття у приймачі одночасно надходять два суміжних символи — той, що прямо розповсюджується та той, що приходить із запізненням. Це призводить до втрати символів. У випадку OFDM-модуляції, яка допускає невелику швидкість передачі даних на одній піднесучій, у кожній OFDM-символ додається захисний інтервал GI. У стандарті IEEE 802.11a його тривалість дорівнює $T_F/4=0,8$ мкс. Отже, тривалість усього символу $T_S=T_{GI}+T_F=4$ мкс. Захисний інтервал транлюється на початку OFDM-символа та являє собою копію його останніх 0,8 мкс. У результаті відбитий символ, що прийшов із запізненням, потрапляє у захисний інтервал та не пошкоджує символ, який розповсюджується прямо.

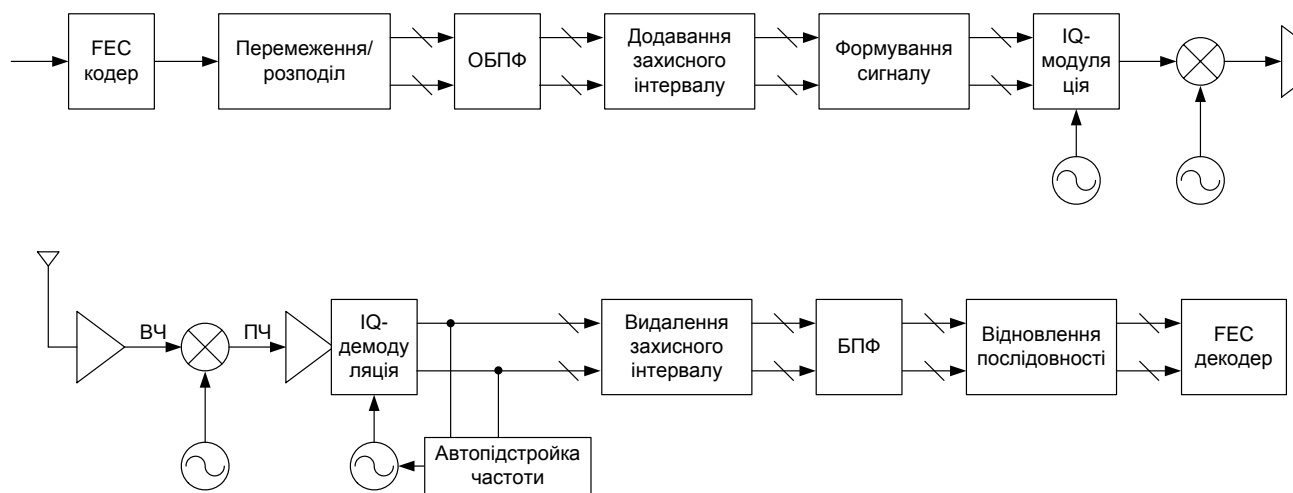


Рис. 3.14. Функціональна схема трактів прийому/передачі стандарту IEEE 802.11a

Розглянемо процедури формування вихідного сигналу у стандарті IEEE 802.11a (рис. 3.14). Вхідний потік даних (біт) перш за все, піддається скремблюванню (в даному випадку рандомізації) шляхом множення на псевдовипадкову послідовність (ПВП) з циклом повторення 127. Її

формує генератор із задаючим поліномом $G(x)=x^7+x^4+1$ та початковим значенням 1111111. При передачі конкретного пакета вектор ініціалізації генератора ПВП може бути довільним, але повинен належати ПВП. Приймач відновлює його, оскільки відомо, що останні 7 біт поля даних (молодші біти поля SERVICE заголовку, див. далі) перед скремблюванням завжди дорівнюють нулю.

Після скремблювання потік даних надходить до надточного кодера (FEC). Виходячи з обраної швидкості передачі даних, швидкість кодування може складати $1/2$, $2/3$ та $3/4$. Нагадаємо, що швидкість кодування — це відношення числа біт у пакеті до та після кодера (швидкість кодування $r=1/2$ означає, що кожний вхідний біт після кодування перетворюється у два біти). Оскільки у кодера два вихода, кожному вхідному біту x_i відповідає пара біт (y_i, z_i) . Значення швидкості кодування, відмінні від $1/2$, отримуються шляхом виключення з вихідної послідовності окремих значень y_i чи z_i , (процедура виключення).

Далі потік закодованих біт піддається перемножуванню (інтерлівінгу) — змінюється порядок біт у послідовності у межах OFDM-символа. Уся послідовність закодованих біт розбивається на блоки, довжина яких дорівнює числу біт в OFDM-символі (N_{CBPS}) при обраній швидкості передачі. У межах блоку біти нумеруються від 0 до $N_{CBPS}-1$. Потім відбувається двохстадійна перестановка. Ціль першого етапу — досягти, щоб суміжні біти кодової послідовності були на несуміжних несучих. Перший етап перемежування еквівалентний тому, що дані послідовно по рядках записуються у таблицю з 16 строк та $N_{CBPS}/16$ стовбчиків, а потім послідовно зчитуються по стовбчикам (тобто зчитуються у порядку запису, але з транспонованої таблиці).

Після другого етапу перестановки суміжні біти виявляються поперемінно в старших і молодших розрядах груп, що визначають модуляційний символ квадратурної модуляції (див. рис. 3.13). Це робиться для того, щоб сусідні біти не виявилися в молодших розрядах, надійність передачі яких набагато нижча.

Табл. 3.1. Параметри OFDM-символів для різних швидкостей передачі даних у стандарті IEEE 802.11a

Швидкість передачі даних, Мбіт/с	Модуляція	Швидкість кодування	Кодованих біт на несучу (N_{BPSC})	Кодованих біт у OFDM-символі (N_{CBPS})	Інформаційних біт у OFDM-символі (N_{DBPS})
6	BPSK	1 / 2	1	48	24
9	BPSK	3 / 4	1	48	36
12	QPSK	1 / 2	2	96	48
18	QPSK	3 / 4	2	96	72
24	16-QAM	1 / 2	4	192	96
36	16-QAM	3 / 4	4	192	144
48	64-QAM	2 / 3	6	288	192
54	64-QAM	3 / 4	6	288	216

Сформований OFDM-символ піддається зворотньому швидкому перетворенню Фур'є (ЗШПФ), у результаті чого формуються вихідні синфазний і квадратурний сигнали. До них додається захисний інтервал, після чого відбувається остаточне формування аналогового сигналу. Подальша обробка стандартна — квадратурний модулятор, гетеродин для переносу сигналу в задану область (якщо це необхідно) і вихідні підсилювачі. Якщо використається гетеродин, у формулі (3.3) $f_0=0$. У приймачі перетворення виконуються у зворотньому порядку (див. рис. 3.14).

3.5. Характеристики базового обладнання мереж Wi-Fi

Зведена таблиця характеристик базового обладнання мереж стандарту Wi-Fi представлена в табл. 3.2. В число обов'язкових увійшли параметри, принципово важливі, з точки зору авторів даного навчального посібника, для порівняння різних моделей базових станцій Wi-Fi.

Табл. 3.2

Виробник	Назва виробу	Загальні характеристики	Потужність	Функції захищеного доступу	Підтримка VLAN	Підтримка QoS	Функції контролю и управління	Допоміжні характеристики
3Com	3Com 8250 Access Point	Стандарти: 802.11b/g. Діапазон частот, ГГц: 2,4-2,4835. Швидкість передавання даних (ПД) по радіоінтерфейсу, Мбіт/с: 11-54	Потужність передавача (макс.), дБм: 17	Ідентифікація та шифрування 40/64, 128/154 біт WEP; WPA AES 256 біт, Dynamic Security Link 128 біт. Функції RADIUS-сервера (802.11x)	Так	QoS у відповідності з IEEE 802.11e	Інструментальні засоби: Wireless Infrastructure Device Manager. Site survey tool, Wireless LAN Discovery Tool, 3NS. Підтримка SNMP	-
3Com	3Com Wireless LAN AP 7250	Стандарти: 802.11b/g. Діапазон частот, ГГц: 2,4-2,4835. Швидкість передавання даних (ПД) по радіоінтерфейсу, Мбіт/с: 11-54	Потужність передавача (макс.), дБм: 17	Шифрування: 40/64, 128/154 біт WEP; WPA AES 256 біт, Dynamic Security Link 128 біт. Функції RADIUS-сервера: EAP-MD5, EAP-TLS, EAP-TTLS; MAC-/PEAP-аутентифікація; ESSID; доступ, фільтрація	Так	QoS у відповідності з IEEE 802.11e	Інструментальні засоби Wireless Infrastructure Device Manager и Wireless LAN Device Discovery. Налаштування різноманітних параметрів, діагностика та моніторинг продуктивності в будь-якій точці мережі за допомогою Web-браузера	-
3Com	3Com Office Connect Wireless 11a/b/g AP	Стандарти: 802.11a/b/g. Діапазони частот, ГГц: 2,4-2,4835 (802.11b/g), 5,150-5,825(802.11a). Усі стандартні швидкості ПД за радіоінтерфейсом	Потужність передавача (макс.), дБм: 17	Шифрування: 256 біт WPA; 40/64 та 128 біт WEP; SSID Broadcast Disable, фільтрація MAC-адресів	-	-	Інструменти мережевого адміністрування на базі Web-інтерфейсу дозволяють адміністраторам здійснювати налаштування і управління точки доступу з будь-якого місця в мережі	-
Alvarion	BreezeNET BU-DS.11 Outdoor	Стандарти: 802.11b и 802.3. Діапазон частот, ГГц: 2,4-2,4835. Швидкість передавання даних (ПД) по радіоінтерфейсу, Мбіт/с: 11	Потужність передавача, дБм: 15. Динамічне регулювання потужності від -4 дБм до +24 дБм	Списки доступу за MAC-адресами, Open System і Shared Key. Підтримка стандарту: IEEE 802.11b. Ідентифікація та шифрування: 64 біт і 128 біт RC4 WEP, механізм скремблювання	Кількість: 1 ESSID-4094 VLAN. Пріоритет VLAN: 0-7	Н/Д	Радиосканер і його можливості: робота на фіксованому каналі або сканування й автоматичний вибір каналу, виявлення устаткування, пов'язаного з мережею. Підтримка SNMP: для системи керування MIBII, DS.11, часні MIB. Підтримка LOG, Telnet. Утиліта конфігурації	Дальність: до 25 км. Архітектура: "точка - багато точок"

Cisco	AIR-AP1131 AG	Стандарти: 802.11a/b/g одночасно. Діапазони частот, ГГц: 5,15-5,25/5,25-5,35/5,725-5,825/2,412-2,497. Швидкість ПД по радіоінтерфейсу, Мбит/с: 1/2/5,5/6/9/11/12/18/24/36/48/54 (усі стандартні швидкості)	Потужність передавача (макс.), дБм: до +20, залежить від регіон, обмежень. Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так	Списки доступу: стандартні та розширені. Повна підтримка стандарту 802.1х. Функції RADIUS-сервера: так. Визначення DoS-атаки по радіоінтерфейсу: по кількості однотипних обігів від MAC, IP, SSID; порогові спрацьовування захисту, набір правил по розсиланню повідомлень і включення інструментів захисту	Кількість VLAN: до 16. Настроювання та спосіб аутентифікації до кожної VLAN	QoS у відповідності до Wi-Fi Multimedia, прототип для 802.11e	Радіосканер і його можливості: вбудований у точку доступу, визначення каналу, MAC, SSID, потужності сигналу радіопристроїв, що працюють у частотному діапазоні. Повна підтримка SNMPv1, v2c, v3, RFC 1156 MIB, RFC 1157 SNMP, RFC 1213 SNMP MIBII, RFC 3418 MIB for SNMP і т.п. Підтримка LOG, Telnet	-
-------	------------------	--	--	---	---	---	---	---

Виробник	Назва виробу	Загальні характеристики	Потужність	Функції захищеного доступу	Підтримка Vlan	Підтримка QoS	Функції контролю и управління	Допоміжні характеристики
Cisco	Aironet 1230AG	Стандарти: 802.11b/g (miniPCI - можливість заміни в майбутньому на зовнішні антени), 802.11 а (у вигляді встановлюваного модуля з інтегр. антеною). Діапазони частот, ГГц: 2,5 (ISM), 5,15-5,25 (UNII-1), 5,25-5,35 (UNII-2), 5,725-5,85 (UNII-3). Швидкість ПД по радіоінтерфейсу, Мбіт/с: 11 (802.11b), 54(802.11д й 802.11а)	Потужність передавача, дБм: 20 (802.11b/g), 15-17 (802.11а). Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так, від 0 до максимальної	Списки доступа: стандартные и расширенные. Поддержка стандарта 802.1x: да, с контролем/назначением SSID, VLAN. Функции RADIUS-сервера: встроенный/внешний для EAP-LEAP и EAP-FAST, внешний для этих и других типов аутентификации. Определение DoS-атаки по радиоинтерфейсу: да	Кількість VLAN: 16, діапазон VLAN ID: від 0 до 1023. Настроювання та спосіб аутентифікації до кожної VLAN - SSID: так, без обмежень	-	Радіосканер і його можливості: визначення каналу, MAC, SSID, потужності сигналу радіопристроїв, що працюють у частотному діапазоні. Підтримка SNMP v1, v2, v3; LOG; Telnet (у т.ч. SSH)	-
Cisco	Aironet 1130AG	Стандарти: 802.11a/b/d, інтегровані антени	Те саме	Те саме	Те саме	Те саме	Те саме	-
Cisco	AIR-AP10xx разом з контролерами серій 2000 і 4100	Стандарти: 802.11a/b/d одночасно. Діапазони частот, ГГц: 5,15-5,25/5,25-5,35/5,725-5,825/2,412-2,497. Швидкість ПД по радіоінтерфейсу, Мбіт/с: 1/2/5,5/6/9/11/12/18/24/36/48/54 (всі стандартні швидкості)	Потужність передавача (макс.), дБм: до +20, залежить від регіону, обмежень. Регулювання потужності на доступу й обмеження випромінюваної потужності для клієнтських пристроїв: так	Списки доступа: стандартні й розширені. Повна підтримка стандарту 802.1x. Функції RADIUS-сервера: функціонал, аналогічний RADIUS-серверу. Визначення DoS-атаки по радіоінтерфейсу: по кількості однотипних обігів від MAC, IP, SSID; порогови спрацювання захисту, набір правил по розсиланню повідомлень і включення інструментів захисту	Кол-во VLAN: до 16. Настройка и способ аутентификации к каждой VLAN - SSID: да	У відповідності до Wi-Fi Multimedia, прототип для 802.11e	Радіосканер і його можливості: вбудований у точку доступу, визначення каналу, MAC, SSID, потужності сигналу радіопристроїв, що працюють у частотному діапазоні. Повна підтримка SNMP v1, v2c, v3, RFC 1156 MIB, RFC 1157 SNMP, RFC 1213 SNMP MIB II, RFC 3418 MIB for SNMP і т.п. Підтримка LOG, Telnet	-

ZyXEL	G-3000 EE	Стандарти: 802.11b/g, у перспективі - 802.11a (PC-карта). Діапазон частот, ГГц: 2,4-2,4835. Швидкість ПД по радіоінтерфейсу, Мбит/с: 54	Потужність передавача, дБм: 16. Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так	Статична таблиця MAC-адресів (фільтрація, доступ). Підтримка стандарту 802.1x. Функції RADIUS-сервера: EAP-TLS, EAP-TTLS, PEAP, MD5	Кількість: 4094 VLAN, 2 ESSID. Настроювання й спосіб аутентифікації до кожної VLAN - SSID: так	Так, на рівні VLAN і 802.11e (мікропрограма)	Радіосканер і його можливості: визначення Mac-адреси клієнтів, роумінг, пошук незайнятого радіоканалу. Підтримка SNMP v1, v2; TRAP-повідомлення: включення живлення, перезавантаження, передача даних, невірне введення логіна та пароля, зупинка передачі даних. Підтримка LOG (System maintenance, System Errors, 802.1x, Wireless), Telnet	Слот розширення для 2-го радіоінтерфейсу 802.11d (встановлюється PC-карта G-110). Режим моста, повторювача. Дві знімні антени. Живлення по кабелю Ethernet (Po) та ін.
-------	-----------	---	---	---	--	--	---	--

Виробник	Назва виробу	Загальні характеристики	Потужність	Функції захищеного доступу	Підтримка VLAN	Підтримка QoS	Функції контролю и управління	Допоміжні характеристики
D-Link (постачальник - "УМД Проект. Средства радиосвязи")	DWL-2000AP+	Стандарти: 802.11b/g. Діапазон частот, ГГц: 2,4-2,4835. Швидкість ПД, Мбіт/с: до 11 (802.11b), до 22 (802.11g), до 54 (802.11n)	Потужність передавача, дБм: 16 (для 802.11b), 14 (для 802.11g). Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: н/д.	Списки доступу: н/д. Підтримка стандарту 802.1x, MD5 й TLS. Функції RADIUS-сервера: н/д. Визначення DoS-атаки по радіоінтерфейсу: Визначене користувачем шифрування даних WEP 64/128/256 біт. Захист паролем. Фільтрація MAC. Заборона широкомовлення SSID. Wi-Fi TM Protected Access	Н/д	Н/д	Н/д	Бездротова точка доступу стандарту 802.11n з високою продуктивністю. Швидкість бездротового з'єднання до 54 Мбіт/с, сумісність із бездротовим устаткуванням стандартів 802.11b/g+
D-Link	DWL-2100AP	Стандарти: 802.11b/g. Діапазон частот, ГГц: 2,4-2,4835. Швидкість з'єднання по радіоінтерфейсу, Мбіт/с: до 108	Потужність передавача, дБм: 16±2. Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так	Списки доступу: стандартні та розширені. Підтримка стандарту 802.1x. Функції RADIUS-сервера	Кількість VLAN: 3. Настроювання та спосіб аутентифікації до кожної VLAN - SSID: так	Немає	Радіосканер і його можливості: так. Підтримка SNMP v2, Telnet	Підтримка технології WDS (Wireless Distribution System), Multi SSID
D-Link	DWL-2700AP	Стандарти 802.11b/g. Діапазон частот, ГГц: 2,4-2,4835. Швидкість з'єднання по радіоінтерфейсу, Мбіт/с: до 54	Потужність передавача, дБм: 23. Регулювання потужності на крапці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так	Списки доступу: стандартні та розширені. Підтримка стандарту 802.1x. Функції RADIUS-сервера	Ні	Ні	Радіосканер і його можливості: так. Підтримка SNMP v.3, Telnet	Підтримка технології WDS, шифрування AES (Advanced Encryption Standard)
D-Link (постачальник - "УМД Проект. Средства радиосвязи")	DWL-7100AP	Стандарти IEEE: 802.11g/b/a, 802.3, 802.3u. Діапазони частот, ГГц: 2,4-2,4835 (802.11b/g), 5,15-5,875 (802.11a). Швидкість ПД по радіоінтерфейсу, Мбіт/с: 54/48/36/24/18/12/11/9/6/5,5/2/1	Потужність передавача дБм: від +14 до 18 (802.11a/d), +18 (802.11b). Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: н/д	Списки доступу: н/д. Підтримка стандарту 802.1x: так. Функції RADIUS-сервера: н/д. Визначення DoS-атаки по радіоінтерфейсу: 64/128/152 біт WEP; WPA (Wi-Fi Protected Access). Підтримка Advanced Encryption Standard (AES)	Н/д	Н/д	Н/д	Трьохрежимна, 2-діапазонна бездротова точка доступу забезпечує саму широку з можливих у точках доступу смугу пропускання для користувачів

Виробник	Назва виробу	Загальні характеристики	Потужність	Функції захищеного доступу	Підтримка VLAN	Підтримка QoS	Функції контролю и управління	Допоміжні характеристики
Proxim (постачальник - Wincom Technologies Corp.)	AP700	Стандарти 802.11 a або 802.11b/g. Діапазони частот, ГГц: 2,4-2,4835 (b/g) або 5,17-5,71 (a). Швидкість ПД по радіоінтерфейсу, Мбіт/с: 54 (802.11a/d), 11 (802.11b)	Потужність передавача, дБм: 20. Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв	Списки доступу (стандартні та розширені): підтримка фільтрації Mac-адресів. Підтримка стандарту 802. 1x. Функції RADIUS-сервера: підтримка зовнішнього RADIUS-сервера	Кількість VLAN: до 16. Номерів VLAN: 4096. Настроювання та спосіб аутентифікації до кожної VLAN - SSID: так	Так	Повнофункціональний радіосканер і його можливості: визначення каналу, MAC, SSID, потужності сигналу. Розширені можливості по виявленню "чужих" точок доступу й клієнтських пристроїв. Два види менеджменту: Standard Management (Via Web browser, Via Telnet, Via serial port (CLI), Via SNMP Manager) і Secure Management (SNMPv, https). Підтримка LOG, Telnet	Режим WDS (Wireless Distribution System). Автоматична конфігурація. Режими роботи з штатним ПЗ: Access Point, Bridge, Repeater. Дінаміч. TKIP-шифрування. WEP-шифрування 3 152-бітним ключем. Живлення по Ethernet (IEEE 802.3af)
Proxim (постачальник - Wincom Technologies Corp.)	AP4000	Стандарти 802.11a/b/d. Діапазони частот, ГГц: 2,4-2,4835 (b/d), 5,17-5,71 (a). Швидкість ПД по радіоінтерфейсу, Мбіт/с: 54 (802.11a/d), 11 (802.11b)	Потужність передавача, дБм: 20. Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв	Списки доступу (стандартні та розширені): підтримка фільтрації Mac-адресів. Підтримка стандарту 802. 1x у точці доступу та клієнтських пристроїв. Функції RADIUS-сервера: підтримка зовнішнього RADIUS-сервера	Кількість VLAN: до 16. Номерів VLAN: 4096. Настроювання та спосіб аутентифікації до кожної VLAN - SSID: так	Так	Те саме	Те саме
Enterasys Networks	Roam About Access Point 3000	Стандарти: 802.11a/b/d. Діапазони частот, ГГц: 2,4-2,4835/5. Швидкість ПД по радіоінтерфейсу, Мбіт/с: 11/54	Потужність передавача (макс.), дБм: 17 (802.11a), 20 (802.11b/g). Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так	Списки доступу: немає. Підтримка стандарту 802. 1x. Визначення DoS-атаки по радіоінтерфейсу: так	Кількість VLAN: 64. Настроювання та спосіб аутентифікації до кожної VLAN - SSID: Так	Так, MAC-адрес, Ethertype, 802.1p	Радіосканер і його можливості: Визначення сторонніх точок доступу, деасоціація клієнтів зі сторонньої точки доступу. Підтримка SNMP v3 Traps, LOG (SysLog), Telnet	-

Nortel	Nortel WLAN Access Point 2221	Стандарт 802.11b. Діапазон частот, ГГц: 2,4-2,484. Швидкість ПД по радіоінтерфейсу, Мбит/с: 11/5,5/2/1 (з автоматичним переходом)	Потужність передавача (макс.), дБм: 18. Регулювання потужності на точці доступу: н/д	Списки доступу: можливість обмежити керування точкою доступу з боку бездротового інтерфейсу. Підтримка стандарту 802.1х. Функції RADIUS-сервера: підтримка зовнішнього RADIUS-сервера	Кількість VLAN: 64	802.1р	Радіосканер і його можливості: так, визначення MAC, потужності сигналу радіоустройств. Підтримка SNMP v1, LOG, Telnet	Забезпечення додаткового рівня безпеки та мобільності - комутатор WLAN Security Switch 2250 або пристрою Nortel PVN Router
--------	--	---	---	--	-----------------------	--------	--	--

Виробник	Назва виробу	Загальні характеристики	Потужність	Функції захищеного доступу	Підтримка VLAN	Підтримка QoS	Функції контролю и управління	Допоміжні характеристики
Nortel	Nortel WLAN Access Point 2330	Стандарти 802.11a/b/g. Діапазони частот, ГГц: 5,15-5,85(802.11a), 2,4-2,484 (802.11b/g). Швидкість ПД по радіоінтерфейсу, Мбит/с: 54/48/36/24/18/12/9/6 (802.11a/д с автомат, переходом); 11/5,5/2/1 (802.11b с автомат, переходом)	Потужність передавача (макс.), дБм: 11 (802.11a), 16(802.11b/g). Регулювання потужності на точці доступу із кроком 1 дБм і обмеження випромінюваної потужності для клієнтських пристроїв	Списки доступу: стандартні та розширені (L2/3/4). Підтримка стандарту 802.1x. Функції RADIUS-сервера: так, RADIUS accounting. Визначення DoS-атаки по радіоінтерфейсу: по кількості однотипних звернень від MAC, IP, SSID; виставлення порогів спрацьовування захисту, набір правил по розсиланню повідомлень і включення інструментів захисту	Кількість VLAN: н/буд. Настроювання та спосіб аутентифікації до кожної VLAN - SSID: так	RFC 2472 DiffServ precedence; RFC 2597 DiffServ Assured Forwarding; RFC 2598 DiffServ Expedited Forwarding; IEEE 802.1p	Радіосканер і його можливості: визначення каналу, MAC, SSID, потужності сигналу радіобладнання, що працює у частотному діапазоні. Підтримка SNMP v1, v2c, набір OID, набір можливих trap-повідомлень й установка правил по їхньому відправленню. Підтримка LOG (RFC 3164 Syslog), Telnet/SSHv2	Повністю централізована архітектура з комутатором захисту WLAN Security Switch. Можливість проводити будь-які операції без настроювання кожної бездротової точки доступу в мережі
ZyXEL	G-560 EE	Стандарт: 802.11b/g. Діапазон частот, ГГц: 2,4-2,4835. Швидкість передавання даних по радіоінтерфейсу, Мбит/с: 125	Потужність передавача, дБм: 18. Регулювання потужності на точці доступу та обмеження випромінюваної потужності для клієнтських пристроїв: так	Статична таблиця Mac-адресів (фільтрація, доступ). Підтримка стандарту 802.1x. Функції RADIUS-сервера: EAP-TLS, EAP-TTLS, PEAP	Кількість: 4094 VLAN, 1 ESSID. Настроювання та спосіб аутентифікації до кожної VLAN- SSID: так	-	Радіосканер і його можливості: визначення MAC-адреси клієнтів. Підтримка LOG, Telnet	Сертифікат Wi-Fi (сумісний з обладнанням інших виробн.). Майстер настроювання. Web-інтерфейс російською мовою. Безпека 256 біт WEP, WPA. Блокування внутрішнього мережного трафіка та ін.

РОЗДІЛ 4. ПЕРСОНАЛЬНІ БЕЗДРОТОВІ МЕРЕЖІ

4.1 Технічні аспекти побудови і функціонування мереж персонального зв'язку технології BLUETOOTH

Персональні бездротові мережі передачі даних стали з'являтися порівняно недавно -- у середині 90-х років. Проте лише до кінця 90-х років розвиток мікроелектроніки дозволив проводити для таких пристроїв інтегральну елементну базу. Перспективи, що відкрилися, привели до того, що практично одночасно з'явилося відразу декілька розробок персональних безпроводних систем передачі інформації (БСП), основні з яких - це специфікації HomeRF, стандарти сімейства IEEE 802.15 (Bluetooth і IEEE 802.15.3(4)), а також технології надширокопasmугового зв'язку (UWB).

4.1.1 Стандарти Bluetooth і HomeRF

HomeRF - це назва створеної в березні 1998 року групи виробників комп'ютерного і побутового устаткування (Home Radio Frequency Working Group; у перший рік існування до неї увійшло понад 90 фірм, включаючи Intel, Compaq, Ericsson, Hewlett-Packard і Microsoft). Вона організовувалася для розробки відкритого протоколу розподіленого бездротового доступу SWAP (Shared Wireless Access Protocol), який повинен був лягти в основу радіомережі HomeRF. Згодом замість поняття SWAP в назві специфікації стали використовувати HomeRF. Перша версія специфікації HomeRF з'явилася 17 грудня 1998 року, остання (HomeRF 2.01) - 1 липня 2002 року. На цьому мета робочої групи були виконані, і в січні 2003 року вона була розформована.

Як випливає з назви, стандарт HomeRF замислювався як бездротова домашня система передачі інформації СП, аналог відомої на той час дротяної Ethernet-подібної мережі HomePNA (Home Phone Line Networking Alliance), в якості носій використала вже прокладену телефонну лінію. Для нормальної роботи мережі HomeRF необхідний host-комп'ютер (або пристрій, що виконує його функції). Ідеологія Bluetooth інша - це універсальний радіоінтерфейс, що пов'язує один з одним самі різні пристрої і що не вимагає дорогої апаратної підтримки. Проте пристрої Bluetooth сьогодні реально використовують в основному для заміни дроту радіоінтерфейсом (наприклад, як бездротова гарнітура для стільникових телефонів), не дивлячись на щонайширший спектр закладених в ньому можливостей. Ринок такого роду додатків поки у багато разів перевершує ринок мережеских пристроїв. Можливо, саме тому що чудово пропрацьований для застосування саме для мережеских завдань стандарт HomeRF поки не знайшов масового застосування. З одного боку його витісняють прості Bluetooth-пристрої, з іншою - системи стандарту IEEE 802.11, які за останні п'ять років істотно подешевшали, позбавивши тим самим

HomeRF основної перед ними переваги - низької вартості. Тому детальніше розглянемо саме стандарт Bluetooth.

Основні характеристики технологій Bluetooth і HomeRF приведені табл.4.1.

Табл. 4.1 Порівняльні характеристики технологій Bluetooth і Home RF

Показник	HomeRF	Bluetooth
Вид модуляції	Шумоподібний сигн. метод	Шумоподібний сигн. метод
Число скачків в секунду	50	1600
Потужність передавача, мВт	100	100
Швидкість обміну даними, Мбит/с	1 або 2	1
Спосіб модуляції	Двох- або чотирьохрівнева	Двохрівнева ЧМ
Кількість устройств в сети	До 127	Не обмежено
Захист інформації	Blowfish data security	40- і 64-бітне шифрування
Радіус дії, м	50	10-100

4.1.2. Архітектура і логічна структура мережі Bluetooth

Своєю появою специфікація Bluetooth зобов'язана компаніям Ericsson, IBM, Intel, Toshiba і Nokia, які в лютому 1998 року для розробки стандарту персональної безпроводної системи передачі інформації (БСПІ) організували спеціальну робочу групу SIG (Special Interest Group). Назва нової технології пов'язана з ім'ям короля Харольда I Блаатанда (у пізній транскрипції - Bluetooth, Синезуб), що об'єднав Данію з Південною Швецією і Південною Норвегією в єдине Данське Королівство. Вже в 2000 році в Bluetooth SIG входили 1883 фірми (на порядок більше, чим в групі HomeRF). Нову технологію підтримали виробники елементної бази, програмного забезпечення, портативних комп'ютерів, стільникових телефонів, звуковідтворюючої апаратури і ін. Мабуть, ім'я короля-об'єднувача принесло свої плоди. Сьогодні стандарт Bluetooth визнаний всією світовою спільнотою. Між Bluetooth SIG і IEEE була досягнута угода, відповідно до якої специфікація Bluetooth увійшла до стандарту IEEE 802.15.1 (опублікований 14 червня 2002 року) „Wireless Medium Access Control

(MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)” (Специфікації контролю доступу до бездротового каналу і фізичного рівня бездротових персональних мереж).

Специфікація Bluetooth описує пакетний спосіб передачі інформації з часовим мультиплексуванням. Радіообмін відбувається в смузі частот 2400-2483,5 МГц (у США у ряді *інших країн* - *безліцензійний* діапазон). У радіотракті застосований метод розширення спектру за допомогою частотних стрибків і дворівнева частотна модуляція з фільтром Гауса (binary Gaussian Frequency Shift Keying).

Метод частотних стрибків має на увазі, що вся відведена для передачі смуга частот підрозділяється на певну кількість підканалів шириною 1 МГц кожен (частотно-часова матриця). Канал є псевдовипадковою послідовністю стрибків по 79 або 23 радіочастотним підканалам (табл. 4.2). Кожен канал ділиться на тимчасові сегменти тривалістю 625 мкс, причому кожному сегменту відповідає певна несуча (підканал). Передавач „перескакує” з несучої на несучу синхронно з приймачем в послідовності, визначуваній номером каналу. За секунду може відбуватися до 1600 частотних стрибків. Такий метод забезпечує конфіденційність і деяку помехозахищеність передачі. Остання обумовлена тим, що якщо переданий по якому-небудь підканалу пакет не був прийнятий, то приймач повідомляє про це, і передача пакету повторюється на одному з наступних підканалів, вже на іншій частоті.

Табл. 4.2. Розділення смуги частот на підканали в стандарті Bluetooth

Країна	Діапазон. МГц	Несуча частота	Допустимі номери
Європа и США	2400.8-2483.5	2402 + κ	0... 79
Японія	2471.8-2497.8	2473 + κ	0... 23
Іспанія	2445.8-2475.8	2449 + κ	0... 22
Франція	2446.5-2483.5	2454 + κ	0... 22

Протокол Bluetooth підтримує з'єднання типу крапка-крапка і крапка-багатокрапка. Два або більш використовуючих один і той же канал пристроїв утворюють пікомережу (piconet). Один з пристроїв працює як основний (master), а інші - як підлеглий (slaves). У одній пікомережі може бути до семи активних підлеглих пристроїв, при цьому решта підлеглих пристроїв знаходиться в стані „парковки”, залишаючись синхронізованими з основним пристроєм. Взаємодія пікомереж утворює „розподілену мережу” (scatternet).

У кожній пікомережі діє тільки один основний пристрій, проте підлеглі пристрої можуть входити в різні пікомережі. Крім того,

основний пристрій однієї пікомережі може бути підлеглим в іншій (рис. 4.1).

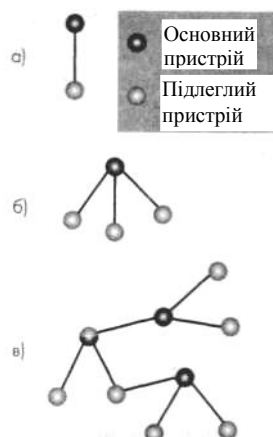


Рис. 4.1. Пікомережа з одним підлеглим пристроєм (а), кількома (б) та розподілена мережа (в)

Пікомережі не синхронізовані одна з одною за часом і частотою - кожна з них використовує свою послідовність частотних стрибків. У одній же пікомережі всі пристрої синхронізовані за часом і частотою. Псевдовипадкова послідовність стрибків унікальна для кожної пікомережі і визначається адресою її основного пристрою.

Довжина циклу псевдовипадкової послідовності - 227 елементів. В стандарті Bluetooth передбачена дуплексна передача на основі розділення в часі (time division duplexing - TDD). Основний пристрій передає пакети $f(k)$ в непарні тимчасові сегменти, а підлеглий пристрій - в парні (рис. 4.2).

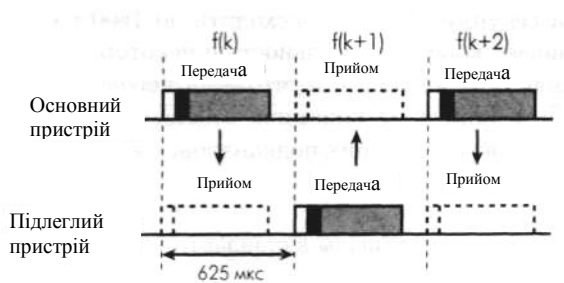


Рис. 4.2 Тимчасові діаграми роботи каналу

Пакети залежно від довжини можуть займати до п'яти тимчасових сегментів. При цьому частота каналу не міняється до закінчення передачі пакету (рис. 4.3).

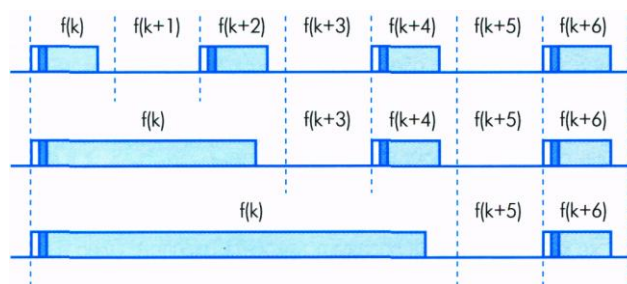


Рис. 4.3. Передача пакетів різної довжини

Протокол Bluetooth може підтримувати асинхронний канал даних, до трьох синхронних (з постійною швидкістю) голосових каналів або каналу з одночасною асинхронною передачею даних і синхронною передачею голосу. Швидкість кожного голосового каналу - 64 кбит/с в кожному напрямі, асинхронного в асиметричному режимі - до 723,2 кбит/с в прямому і 57,6 кбит/с в зворотному напрямках або до 433,9 кбит/с в кожному напрямі в симетричному режимі.

Синхронне з'єднання (SCO) можливо тільки в режимі крапка-крапка. Такий вид зв'язку застосовується для передачі інформації, чутливої до затримок, наприклад голос. Основний пристрій підтримує до трьох синхронних з'єднань, допоміжне - до трьох синхронних з'єднань з одним основним пристроєм або до двох - з різними основними пристроями.

При синхронному з'єднанні основний пристрій резервує тимчасові сегменти, наступні через так звані SCO-інтервали. Навіть якщо пакет прийнятий з помилкою, повторно при синхронному з'єднанні він не передається.

При асинхронному зв'язку (ACL) використовуються тимчасові сегменти, не зарезервовані для синхронного з'єднання. Асинхронне з'єднання можливо між основним і всіма активними підлеглими пристроями в пікомережі. Основний і підлеглий пристрої можуть підтримувати тільки одне асинхронне з'єднання. Оскільки в пікомережі може бути декілька підлеглих пристроїв, конкретний підлеглий пристрій відправляє пакет основному, тільки якщо в попередньому тимчасовому інтервалі на його адресу прийшов пакет від основного пристрою. Якщо в адресному полі ACL-паketу адреса не вказана, пакет вважається „широкомовним” - його можуть читати всі пристрої. Асинхронне з'єднання дозволяє повторно передавати пакети, прийняті з помилками (механізм ARQ - automatic repeat request).

Стандартний пакет Bluetooth містить код доступу завдовжки 72 біта, 54-бітовий заголовок і інформаційне поле завдовжки не більше 2745 біт (рис. 4.4). Проте пакети можуть бути різних типів. Так, пакет може складатися тільки з коду доступу (в цьому випадку його довжина рівна 68 бітам) або коду доступу і заголовка.

Код доступу ідентифікує пакети, що належать однієї пікомережі, а також використовується для синхронізації і реалізації процедури

запитів. Він включає преамбулу (4 біта), слово синхронізації (64 біта) і трейлер - 4 біта контрольної суми. Заголовок містить інформацію для управління зв'язком і складається з шести полів:

AM_ADDR - 3-бітова адреса активного елементу (active member address);

TYPE - 4-бітовий код типу даних;

FLOW - 1 біт управління потоком даних, що показує готовність пристрою до прийому;

ARQN - 1 біт підтвердження правильного прийому;

SEQN - 1 біт, що служить для визначення послідовності пакетів;

NC - 8-бітова контрольна сума.

Інформаційне поле залежно від типу пакетів може містити або поля голосу, або поля даних, або обидва типи полів одночасно.

Оскільки глобальна мета Bluetooth - загальне об'єднання, ця специфікація описує протоколи роботи практично на всіх рівнях моделі взаємодії відкритих систем (MBBC/OSI). Стек протоколів Bluetooth дозволяє пристроям різних стандартів взаємодіяти один з одним за допомогою даної технології.

Дотепер ми розглядали тільки фізичний рівень і рівень ланки даних, оскільки взаємодія на цих рівнях підтримується апаратно.

Протоколи верхніх рівнів, як правило, реалізуються програмно. Основні протоколи взаємодії, що входять в Bluetooth (рис. 4.4):

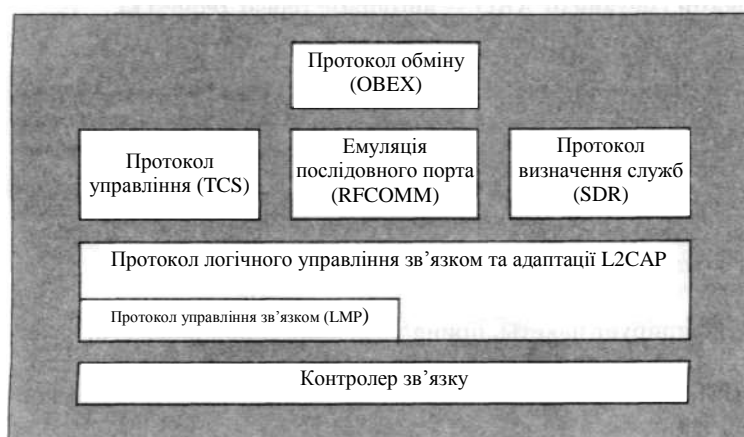


Рис. 4.4. Стек протоколів Bluetooth

- ❑ протокол управління з'єднанням (Link manager protocol). Використовується для встановлення зв'язку, управління і захисту інформації;
- ❑ протокол управління логічним з'єднанням і адаптації (Logical link control and adaptation protocol L2CAP). Забезпечує мультиплексування, сегментацію і перекомпоновувану пакетів;

- ❑ протокол визначення служб (SDP). Дозволяє ідентифікувати тип і характеристики взаємодіючого пристрою;
- ❑ протокол RFCOMM. Заснований на стандарті ETSI TS 07.10, підтримує інтерфейс RS-232, забезпечуючи емуляцію послідовного порту;
- ❑ протокол управління телефонією (TCS). Служить для організації з'єднання між пристроями для передачі голосу і даних;
- ❑ протокол обміну об'єктів OBEX. Є основою для роботи різних призначених для користувача додатків через канал Bluetooth (наприклад, електронної пошти). Він же забезпечує сумісне використання Bluetooth і інших комунікаційних інтерфейсів, наприклад IrDA (Infrared Data Association).

4.1.3. Структура пристроїв Bluetooth

Одна з необхідних умов успіху такої технології, як Bluetooth - недорога програмно-апаратна реалізація. У структуру пристроїв Bluetooth (рис. 4.5) входять радіомодуль-трансвер, контролер зв'язку (baseband-процесор) і пристрій, що управляє зв'язком, власне реалізовує протоколи Bluetooth верхніх рівнів, а також інтерфейс з термінальним пристроєм. Причому якщо трансвер і контролер зв'язки (у перших чіпсетах для Bluetooth) - це спеціалізовані мікросхеми (інтегральні або гібридні), то пристрій управління зв'язком реалізують на стандартних мікроконтролерах, сигнальних процесорах або його функції підтримують центральні процесори потужних термінальних пристроїв (наприклад, ноутбуків). Крім того, в пристроях Bluetooth застосовують інтегральні схеми (IC), використовувані в інших додатках, оскільки діапазон 2 МГц освоєний досить добре, а закладені в Bluetooth технічні рішення самі по собі особливої новизни не містять (схема модуляції - широко поширена, технологія розширення спектру методом частотних стрибків добре відпрацьована, потужність мала).



Рис. 4.5 Структура пристроїв Bluetooth

Тому не дивно, що перші чіпсети для Bluetooth включали інтегральні схеми (IC), добре знайомі по інших додатках. Так, однією з перших своє рішення для Bluetooth представила фірма Philips Semiconductors, запропонувавши комплект IC, що включає чотири мікросхеми: синтезатор UMA1022, підсилювач потужності SA2410, схему модуляції SA639 і трансивер SA2420. Дві з них - UMA1022 і SA639 - використовуються в DECT-пристроях, та і інші достатньо універсальні. Проте незабаром Philips запропонувала спеціалізований чіпсет, що підтримує специфікацію Bluetooth 1.0. Він включає однокристальний трансивер UAA3558, заснований на оригінальній технології „низької проміжної частоти” (спочатку створювався для DECT), і baseband-процесор серії Y\YS2600x. Процесор YWS26002 може працювати і з трансивером компанії Ericsson ROBY 313. Він містить ядро 32-розрядного RISC-мікроконтролера ARM7 TDMI, кодек голосу, підтримує інтерфейси UART, USB, PCM і I²C. Виготовляється процесор по 0,25-мкм КМОП-технології, тому він характеризується малою споживаною потужністю і низькою напругою: 1.8-2.5 В для цифрового ядра і 2.5-3.3 В для портів введення висновку. Одна з останніх розробок компанії Philips - повністю завершений Bluetooth-радиомодуль DGB202, побудований на базі розміщених в одному корпусі комунікаційного Bluetooth-процесора PCF87852 і трансивера UAA3559. Незабаром повинен стати доступним і перспективний baseband-процесор компанії Philips - PCD 87550 (рис.4.6).

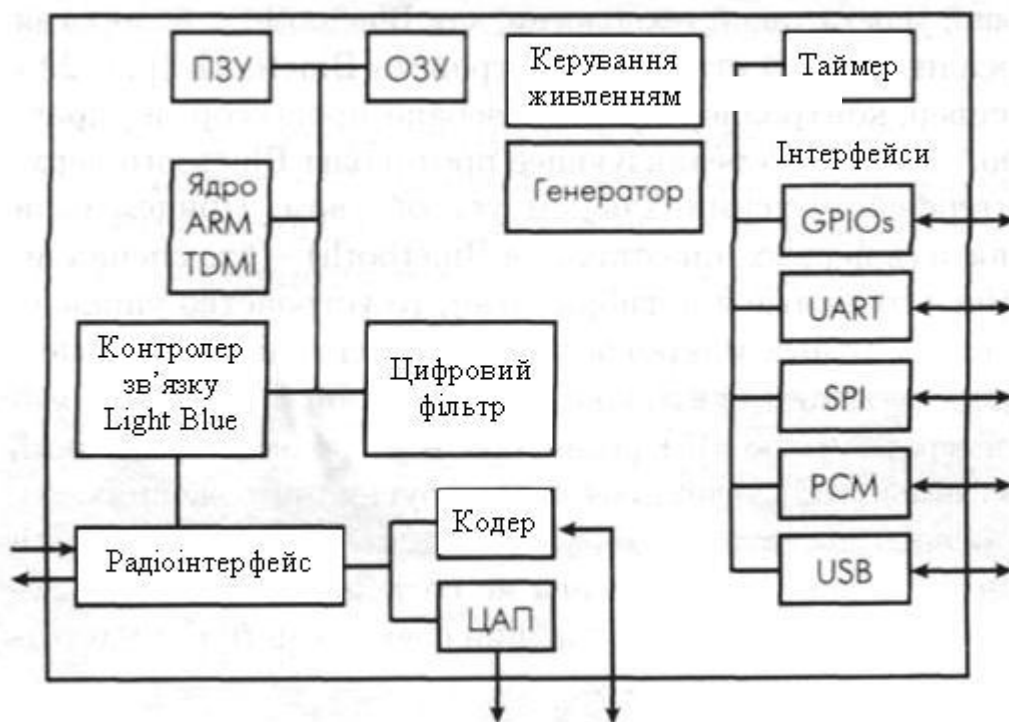


Рис. 4.6 Структурна схема Bluetooth-контроллера PCD 87550

Взагалі слід зазначити, що ядро ARM TDMI застосовується в baseband-процесорах багатьох фірм. Так, воно інтегроване в Bluetooth baseband-процесор фірми Ericsson. На основі цього ядра побудований і однокристальний контроллер Bluetooth компанії Atmel AT76C551. Його структура багато в чому аналогічна приведеною на рис. 4.6. Atmel пропонує чіпсет, що включає даний контроллер і однокристальний трансивер T2901 компанії Temic Semiconductors (яка тепер увійшла до складу Atmel). Трансивер T2901 забезпечує радіус дії до 10 м. Якщо його треба збільшити до 100 м, Atmel пропонує SiGe-ИС T7024, що включає малошумливий передпідсилювач і підсилювач потужності 23 дБм.

4.1.4 Типи антен для мереж Bluetooth

Виробляється широкий набір антен для систем Bluetooth, використовуючи керамічні матеріали з хорошими високочастотними властивостями.

Антен типу "E-Type Electrode Configuration" (рис. 4.7), добре підходять для додатків Bluetooth. Місце, потрібне для нової антени, дуже маленьке (15x3x2 мм), вона не чутлива до розташування периферійних частин, може бути виконана у вигляді високоефективної антени-кристала для Bluetooth, проста у використанні.

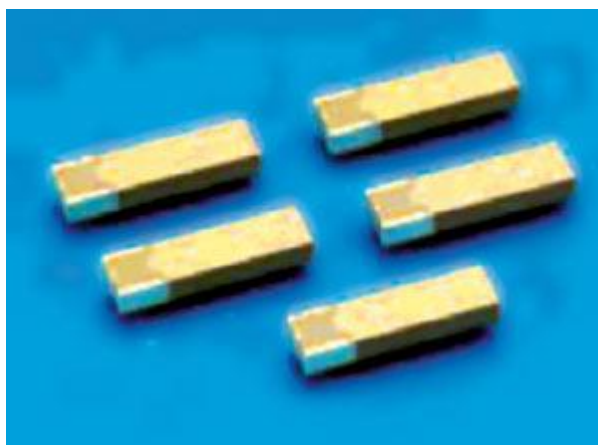


Рис. 4.7. Вид антени Hitachi Metals для Bluetooth

Фірма Antek Wireless Inc. розробила нову 2,4-ГГц антену оригінальної конструкції, яка забезпечує ефективність, що перевищує фактично будь-які технічні вимоги проекту, мініатюрна, і може бути встановлена майже в будь-який пристрій. Антена застосовна для різних додатків типу бездротової передачі відеосигналу, аудіоустаткування, головних телефонів, модемів, мобільних комп'ютерів, портативних

телефонів і інших переносних кишенькових пристроїв, що використовують протоколи Bluetooth, IEEE 802.11 і HomeRF.

Компанія Centurion International розробила внутрішню антену PIFA або різновиди плоскої антени для використання в переносних комп'ютерах, що використовують технологію Bluetooth. Нова антена дає можливість комп'ютерним фірмам - виготівникам розробити переносні пристрої, які легко зв'язуються з портативними телефонами і системами обміну повідомленнями, з'єднуються з Інтернетом на високих швидкостях передачі даних.

Murata Manufacturing Co. почала виробництво і продаж вбудованих діелектричних антен для ноутбуків, що використовують технологію Bluetooth (рис. 4.8). Розміри модуля нової серії G2 - 15x5,8x7,0 мм.



Рис. 4.8 Chip-антенна ANCG22G41 Murata

Компанія Miyazaki Matsushita Electric Industrial Co. Ltd. Випускає надкомпактну антену для Bluetooth-пристроїв (рис. 4.9). Антена виконана на керамічній основі і має розміри 5x1,2x1,2 мм. Це найменша антена в індустрії Bluetooth. Характеристики антени наступні: робоча частота 2,4 ГГц, коефіцієнт посилення -2 dBi, коефіцієнт стоячої хвилі по напрузі (КСВН) 2,0.

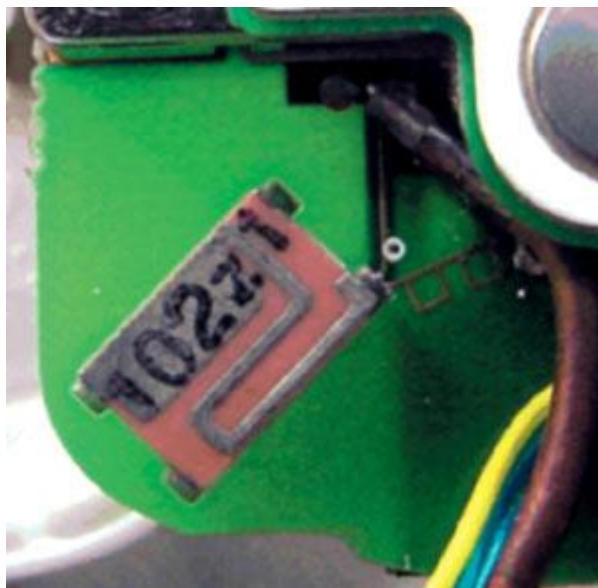


Рис. 4.9. Керамічна антенна в корпусі мобільного телефону

TDK Corp випускає дві півхвильові антени невеликого розміру (7 на 7 мм) (рис. 4.10) для використання у виробках на основі технології Bluetooth. Антена CANPB0715 має коефіцієнт посилення -5 dBi, а антена CANPB0716 - 3 dBi. Більшість інших малих антен є чвертьхвильовими. Їх використання можливо тільки в крупніших мобільних пристроях, таких як ноутбуки, де здійснюється заземлення на корпус пристрою. Для мобільних телефонів було потрібно розробка півхвильових антен.

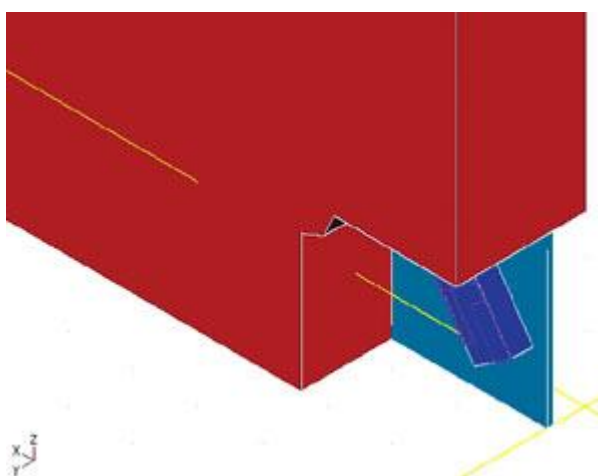


Рис. 4.10 3D-вид антени Bluetooth в металевому корпусі мобільного телефону

4.2 Високошвидкісні персональні мережі стандарту IEEE 802.15.3(3a)

4.2.1 Специфікація IEEE 802.15.3

Стандарт IEEE 802.15.3 описує роботу малої бездротової системи передачі інформації (БДПІ) - пікомережі (piconet). Пікомережа у стандарті IEEE 802.15.3 - це так названа ad hoc -- система, у якій кілька незалежних пристроїв можуть безпосередньо взаємодіяти один з одним. Радіус зони дії однієї пікомережі, як правило, не перевищує 10 м. Основні вимоги до неї - висока швидкість передачі даних, проста інфраструктура, легкість встановлення з'єднання й входження в мережу, наявність засобів захисту даних і надання для певних типів даних з'єднання з гарантованими параметрами передачі (гарантія якості обслуговування, QoS).

Пікомережа (рис. 4.11) може поєднувати кілька пристроїв, один з яких виконує функції керування (координатор пікомережі - piconet coordinator, PNC). Стандарт також передбачає можливість формування так званих дочірніх пікомереж й описує взаємодію між незалежними сусідніми пікомережами.

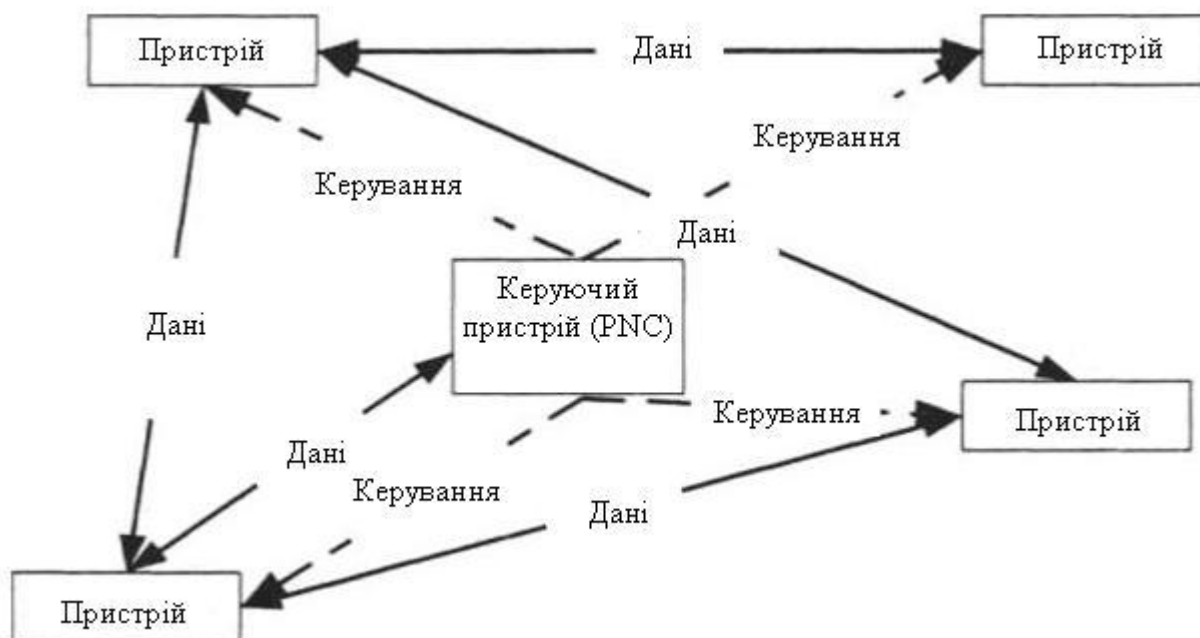


Рис. 4.11. Структура пікомережі IEEE 802.15.3

У пікомережі можливий обмін як асинхронними, так й ізохронними (потоківими) даними. До останнього відносяться, наприклад, звук і відео. Весь інформаційний обмін у пікомережі заснований на послідовності суперкадрів (superframe - термінологія стандартів IEEE 802.15). Кожен суперкадр (мал. 4.12) включає керуючий сегмент (beacon), інтервал конкурентного доступу (contention access period - CAP) і набір тимчасових інтервалів (каналів), призначених певним пристроям. PCN визначає границі всіх інтервалів і розподіляє канали між пристроями.

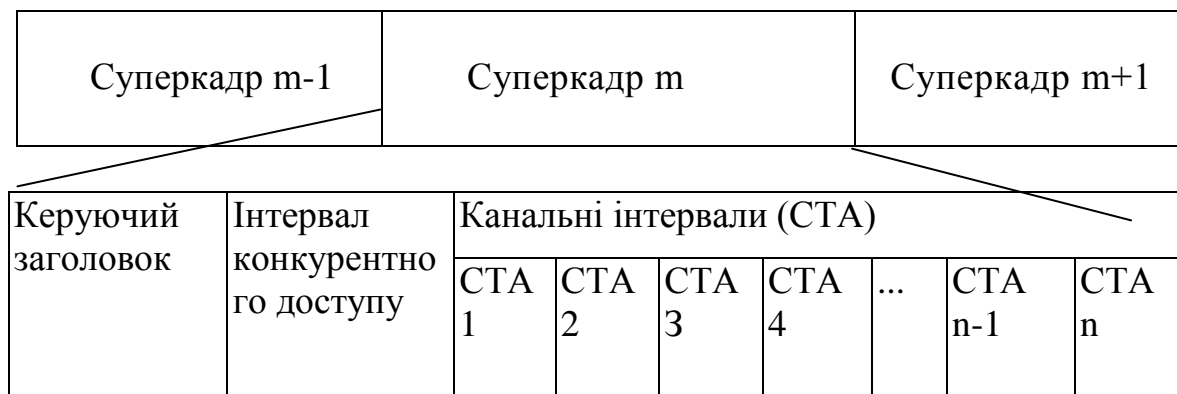


Рис. 4.12. Структура суперкадрів фізичного рівня мережі IEEE 802.15.3

Під час САР доступ до каналу надається на основі механізму контролю несучої із запобіганням колізій - CSMA/CA (як і в стандарті IEEE 802.11), тобто хто перший встиг зайняти канал, той і працює. У цей період передаються команди або асинхронні дані.

Канальні інтервали (СТА) координатор пікомережі призначає кожному пристрою або групі пристроїв по попередньому запиті з їх боку. У керуючому сегменті задається момент початку й тривалість кожного СТА. Призначення каналного інтервалу для якого-небудь пристрою означає, що ніхто інший у цей момент не може працювати на передачу. СТА можуть динамічно розподілятися в суперкадрі (для асинхронних й ізохронних даних) або бути фіксованими (тільки для ізохронних даних).

Специфікація фізичного каналу в документі IEEE 802.15.3 наведена тільки для діапазону 2400-2483,5 МГц. Вона передбачає п'ять припустимих швидкостей передачі (табл. 4.3). Швидкість 22 Мбіт/с є базовою, її зобов'язані підтримувати всі пристрої IEEE 802.15.3. При роботі на цій швидкості дані не кодуються. В інших випадках дані перед формуванням модуляційних символів кодуються за допомогою згорточного кодера із трирозрядним здвиговим регістром (так названа модуляція за допомогою гратчастого коду з вісьма станами). При цьому в кодері до вхідного набору з 1/3/4/5 біт (при QPSK/16-QAM 32-QAM 64-QAM) додається кодовий біт з виходу трирозрядного здвигового регістра.

Табл. 4.3. Модуляція й швидкості передачі даних у мережах IEEE 802.15.3 у діапазоні 2,4 ГГц

Тип модуляції	Швидкість передачі даних, Мбіт/с
QPSK	11
DQPSK	22
16-QAM	33
32-QAM	44
64-QAM	55

Стандарт IEEE 802.15.3 вимагає, щоб пристрої могли працювати в кожному з п'яти можливих частотних каналів (табл. 4.4). Причому передбачається два каналних плани - режим високої щільності (чотири канали в припустимому діапазоні) і режим сумісності з мережею стандарту IEEE 802.11b (три дозволених канали). Це означає, що кожен пристрій перед початком роботи сканує діапазон, знаходить вільні канали, визначає наявність працюючої мережі 802.11b.

Табл. 4.4. Розподіл каналів у мережах IEEE 802.15.3

Номер каналу	Центральна частота, МГц	Режим високої щільності	Режим сумісності з IEEE 802.11b
1	2412	✓	✓
2	2428	✓	
3	2437		✓
4	2445	✓	
5	2462	✓	✓

4.2.2 Надшвидкодючі персональні мережі IEEE 802.15.3a

Специфікацію IEEE 802.15.3 не встигли затвердити (а відбулося це 12 червня 2003 року), як увесь телекомунікаційний світ став чекати появи нового стандарту — IEEE 802.15.3a. Мова йде про розробку принципів побудови пікомережі зі швидкістю обміну 110-480 Мбіт/с і вище — до 1320 Мбіт/с. Досягти настільки високих швидкостей можна тільки збільшуючи спектральну ширину каналу, переходячи в область так названої Надширокосмугові зв'язку (НШС, UWB). У США це стало можливим після 14 лютого 2002 року, коли федеральна комісія зв'язку (FCC) США дозволила застосування надширокосмугових пристроїв усередині приміщень в діапазоні 3100-10600 МГц при максимальній

щільності потужності випромінювання $7.41 \cdot 10^{-14} \text{Вт / Гц}$ ($-41,3 \text{дБм/МГц}$).

У результаті в 2002 році утворилася дослідницька група Tg3a, у яку увійшли представники практично всіх найбільших напівпровідникових і телекомунікаційних фірм. Незабаром з'явилися дві конкуруючі пропозиції по технології НШС-передачі - на основі ортогональних кодів (так званий мультісмуговий множинний доступ за допомогою ортогональних несучих, MB-OFDM) і шляхом розширення спектра сигналу методом прямої послідовності (DS-UWB). Першу пропозицію підтримувала більшість фірм на чолі з гігантами Texas Instruments та Intel (у березні 2003 року було створене навіть спеціальне об'єднання MBOA - Multiband OFDM Alliance). Табір прихильників другого очолили компанії Motorola й XtremeSpectrum.

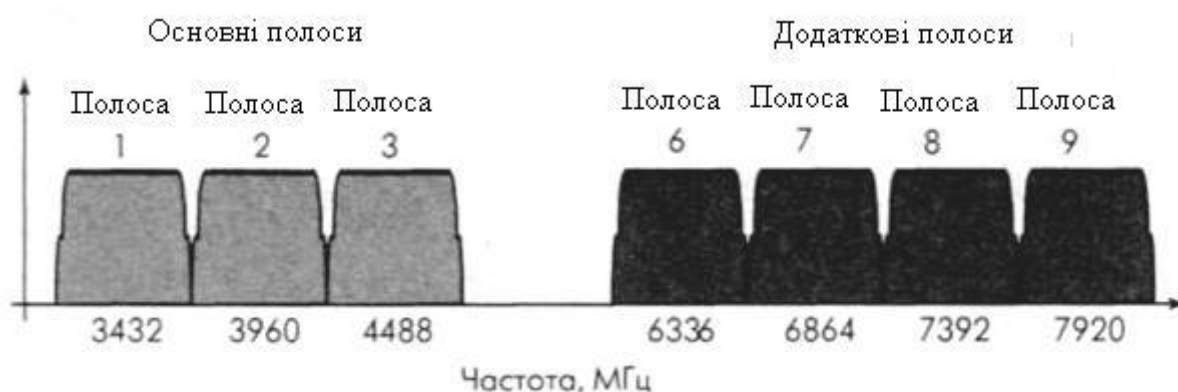


Рис. 4.13. Пропонований розподіл каналів у стандарті IEEE 802.3a в США

Суть її полягає в тому, що весь дозволений діапазон ділиться на смуги шириною 528 МГц. У стандартному режимі передбачено три смуги, у розширеному - сім (рис. 4.13). Кожна смуга, у свою чергу, ділиться на 128 піднесучих частот, із кроком 4,125 МГц. З них використовуються 122:100 для модуляції даних. 12 піднесучих - пілотні та ще 10 - захисні. Кожна піднесуча модулюється за допомогою QPSK. Один OFDM-символ містить 100 або 200 кодованих біт (100 у випадку, коли однаково модулюються дві піднесучі, симетричні щодо центральної). Період проходження символів - 312,5 нс. Дотепер усе відповідає звичайній OFDM. Мультисмуговість означає, що наступний символ може передаватися в іншій частотній смузі за жорстко визначеною схемою для кожного логічного каналу.

Послідовність переходу з однієї смуги частот на іншу називають частотно-тимчасовим кодом. Поки передбачено чотири таких коди (каналу) (табл. 4.5). Крім переходу із частоти на частоту, передбачений режим, коли один символ може передаватися кілька разів (два або чотири). Наприклад, код $1 \rightarrow 2 \rightarrow 3 \rightarrow 1 \rightarrow 2 \rightarrow 3$ означає, що перший OFDM-символ передається в смугах 1 й 2, другий OFDM-символ — у смугах 3 й 1, третій — у смугах 2 й 3.

Табл. 4.5. Частотно-тимчасові коди

Номер логічного каналу	Режим трьох смуг	Режим семи смуг
1	$1 \rightarrow 2 \rightarrow 3 \rightarrow 1 \rightarrow 2 \rightarrow 3$	$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7$
2	$1 \rightarrow 3 \rightarrow 2 \rightarrow 1 \rightarrow 3 \rightarrow 2$	$1 \rightarrow 7 \rightarrow 6 \rightarrow 5 \rightarrow 4 \rightarrow 3 \rightarrow 2$
3	$1 \rightarrow 1 \rightarrow 2 \rightarrow 2 \rightarrow 3 \rightarrow 3$	$1 \rightarrow 4 \rightarrow 7 \rightarrow 3 \rightarrow 6 \rightarrow 2 \rightarrow 5$
4	$1 \rightarrow 1 \rightarrow 3 \rightarrow 3 \rightarrow 2 \rightarrow 2$	$1 \rightarrow 3 \rightarrow 5 \rightarrow 7 \rightarrow 2 \rightarrow 4 \rightarrow 6$

Обмін інформацією відбувається кадрами (пакетами). Кадр складається із преамбули (набору синхронізуючих послідовностей), заголовка (керуюча інформація) і поля даних. Преамбула й заголовок завжди транслюються з найменшою з можливих швидкостей - 55 Мбіт/с. Наявність чотирьох логічних каналів означає, що в безпосередній близькості можуть працювати принаймні чотири пікомережі. Для цього кожному логічному каналу відповідає унікальний вид синхрорядності в преамбулі.

Таким чином, запропонована комбінація OFDM та відомого механізму частотних стрибків (FH). У результаті, залежно від швидкості кодування й числа повторів символів і формується спектр швидкостей від 55 до 480 Мбіт/с. Змінюючи вид модуляції, можна досягти й більших швидкостей. Так, застосування 16-QAM при тій же схемі кодування дасть уже $480 \times 2 = 960$ кбіт/с. Інший шлях полягає у використанні для передачі одночасно трьох діапазонів - тоді при QPSK і швидкості згорткового кодування $3/4$ досягається швидкість $480 \times 3 = 1440$ Мбіт/с.

Проблема в тім, що метод частотних стрибків - не найефективніший з точки зору використання спектрального діапазону. Опоненти MB-OFDM вказують, що прихильники даної технології у своїх вимірах середньої

потужності випромінювання передавача усереднюють її по часовому інтервалу порядку 1 мс. Цей час відповідає тривалості трьох символів. Реально ж при використанні механізму повторів (і при вимірах) символ в одному субканалі за цей час передається тільки один раз. У результаті щільність потужності випромінювання при роботі передавача може перевершувати припустимі (Федеральною комісією зв'язку США) - 41,3 дБм/МГц. А це вже серйозна проблема, оскільки мова йде про сигнал зі смугою понад 500 МГц.

Прихильники технології DS-UWB пропонують для розширення спектра класичний метод прямої послідовності. При цьому кожен біт замінюється спеціальною кодовою послідовністю довжиною до 24 біт. Передбачено два види модуляції - двійкова фазова BPSK (один біт на символ) і так названа 4ВОК-МОДУЛЯЦІЯ (модуляція на основі чотирьох ортогональних двійкових кодів. Відомий варіант ВОК-метод ССК, основний вид модуляції в стандарті IEEE 802.11b). 4ВОК - фактично варіант квадратурної модуляції, один 4ВОК-символ містить 2 біти.

Весь діапазон мовлення розбитий на дві зони: 3,1-4,85 ГГц (нижній діапазон) і від 6,9 до 9,7 ГГц (верхній діапазон). У кожному діапазоні передбачено по шість каналів пікомережі (із кроком 39 МГц у нижньому діапазоні починаючи з 3900 МГц і із кроком 78 МГц - у верхньому починаючи з 7800 ГГц). Тільки чотири канали нижнього діапазону із центральними частотами 3939, 3978, 4017 й 4056 МГц вважаються обов'язковими для підтримки кожним пристроєм, інші канали - додаткові. Частота проходження модуляційних символів у кожному каналі дорівнює 1/3 його центральної частоти. Залежно від швидкості попереднього кодування, виду модуляції й довжини кодової послідовності швидкість передачі даних може скласти 28, 55, 110, 220, 500, 660, 1000 й 1320 Мбіт/с.

Відзначимо, що суперечки прихильників двох підходів до реалізації НШС-пікомереж тривають із 2003 року. Виробники надвеликих інтегральних схем (НВІС) готові почати випуск необхідних компонентів (а деякі вже почали), і ситуація повинна незабаром розв'язатися. Тим більше що вже з'являються пропозиції, як об'єднати дві ці технології й без особливих витрат робити двухмодові пристрої, що підтримують і MB-OFDM, і DS-UWB.

Недавно з'явилися перші чипсети стандарту IEEE 802.15.3. Так, Freescale Semiconductor, дочірня компанія фірми Motorola, випустила чипсет XS110 із трьох мікросхем - трансівера з ВЧ-трактом, baseband-процесора (комунікаційний процесор, що виконує всі перетворення фізичного рівня, включаючи ЦАП/ АЦП) і MAC-контролера. Максимальна швидкість, забезпечувана модемом на основі цього чипсета, - 114 Мбіт/с (тобто мова йде про версії стандарту на основі технології DS-UWB). Енергія, споживана чипсетом, - 750 мВт, напруга живлення - 3,3 В. Загальна потужність випромінювання в смузі частот 3,1-10,6 ГГц - менш 1 мВт. Мікросхеми виготовлені на основі 0,18-мкм КМОП- і SiGe-технології.

4.3 Низькошвидкісні мережі стандарту IEEE 802.15.4 (ZigBee)

Однак світ відчуває потребу не тільки в мережах з найвищими швидкостями передачі даних. Для дуже широкого спектра завдань досить низької швидкості обміну - аби тільки мережні пристрої були максимально простими, дешевими, з наднизьким споживанням енергії й нескладним механізмом підключення до мережі. Скажемо, для інтерактивних ігор не потрібна швидкість обміну з комп'ютерів понад 250 кбіт/с, а різноманітні завдання автоматизації й системи збору інформації й зовсім не вимагають швидкостей передачі понад 20 кбіт/с.

Для рішення даного кола завдань і був розроблений стандарт низьшвидкісних БДП IEEE 802.15.4. Його розроблювачем виступив альянс компаній (Inven-sys, Honeywell, Mitsubishi Electric, Motorola, Philips), що назвав себе ZigBee - (від Zig-zag - зигзаг й Bee - бджола). Малося на увазі, що топологія мережі буде нагадувати зигзагоподібну траєкторію польоту бджоли від квітки до квітки. Під такою своєрідною назвою технологія ZigBee й одержує все більше поширення.

Стандарт IEEE 802.15.4 (ZigBee) передбачає роботу в трьох діапазонах: один канал 868,0-868,6 МГц (для Європи), 10 каналів у діапазоні 902-928 МГц (крок центральних частот 2 МГц, сама нижня з них - 906 МГц) і 16 каналів у діапазоні 2400-2483,5 МГц (крок центральних частот 5 МГц, сама нижня з них - 2405 МГц) (табл. 4.6).

Табл. 4.6. Частотні діапазони і швидкості передачі в мережах IEEE 802.15.4

Частотний діапазон, МГц	Чіпова швидкість, Кчіп/с	Модуляція	Бітова швидкість, кбіт/с	Швидкість символів, Ксимволів/с
868-868.6	300	BPSK	20	20
902-928	600	BPSK	40	40
2400-2483.5	2000	O-QPSK	250	62.5

У радіоканалі використаний метод широкосмугової передачі з розширенням спектра прямою послідовністю (DSSS). Модуляція й розширювальні послідовності для діапазонів 868/915 й 2450 МГц різні.

У діапазоні 2450 МГц потік немодульованих даних розбивається на групи по чотири біта. Кожна група замінюється однією з 16 квазіортогональних послідовностей довжиною 32 біта (чіпа). Послідовності наведені в стандарті. Модуляція даних - квадратурна фазова (QPSK). Парні чіпи квазіортогональної послідовності (починаючи з нульового) модулюють синфазний (I) канал, непарні - квадратурний (Q) канал. У результаті послідовність у квадратурному каналі зміщена щодо синфазного на період одного чіпа, тому модуляція називається Offset-QPSK (QPSK зі зрушенням). Тривалість імпульсу після квадратурного модулятора вдвічі більше, ніж

тривалість одного чіпа (форма імпульсу - половина періоду синусоїди із частотою, вдвічі меншої частоти чіпів).

В діапазоні 868/915 МГц потік даних піддається диференціальному кодуванню за схемою $E_i = E_{i-1} \oplus R_i$, $E_0 = 0$. Тут R_i й E_i — біти до й після кодування відповідно. Далі відбувається заміна кожного біта розширювальною послідовністю довжиною 15 біт («1» замінюється на 0537_{16} , «0» — на інверсну послідовність $7AC8_{16}$). Далі перетворений потік даних передається в радіоканал за допомогою двухпозиційної фазової модуляції (BPSK). Форма імпульсу при цьому відповідає так названому припіднятому косинусу, у цьому випадку — функції виду $[\sin(x)]/[x(1-x^2)]$, де $x = 2\pi f_{\text{чипов}}t$, $t = 0..1/f_{\text{чипов}}$.

Мережа стандарту IEEE 802.15.4 містить два типи пристроїв - так названі повнофункціональні (FFD) і пристрої зі зменшеною функціональністю (RFD). Їхня основна відмінність: FFD можуть установлювати з'єднання з будь-якими пристроями, RFD - тільки з FFD. У кожній пікомережі (PAN) повинен бути пристрій - координатор PAN. Його функції може виконувати тільки FFD. Мережа, що складається з одного FFD і декількох RFD, утворить топологію типу «зірка». Якщо в мережі декілька FFD, топологія може бути більш складною - типу однорангової мережі (мережі рівноправних пристроїв, peer-to-peer) «кожний з кожним» (рис. 4.14) або об'єднання декількох зіркоподібних кластерів (рис. 4.15). Але в кожному випадку одне з FFD виконує функцію координатора мережі. Кожному пристрою мережі привласнюється 64-розрядна адреса. Відзначимо, що стандарт передбачає взаємодію пристроїв не тільки в рамках однієї PAN, але й між різними сусідніми PAN (для чого й потрібна розвинена система адресації). Для спрощення обміну усередині мережі координатор PAN може привласнювати пристроям більш короткі 16-розрядні адреси. У цьому випадку для міжмережевої взаємодії використовуються 16-розрядні ідентифікатори мереж, також призначувані координатором.

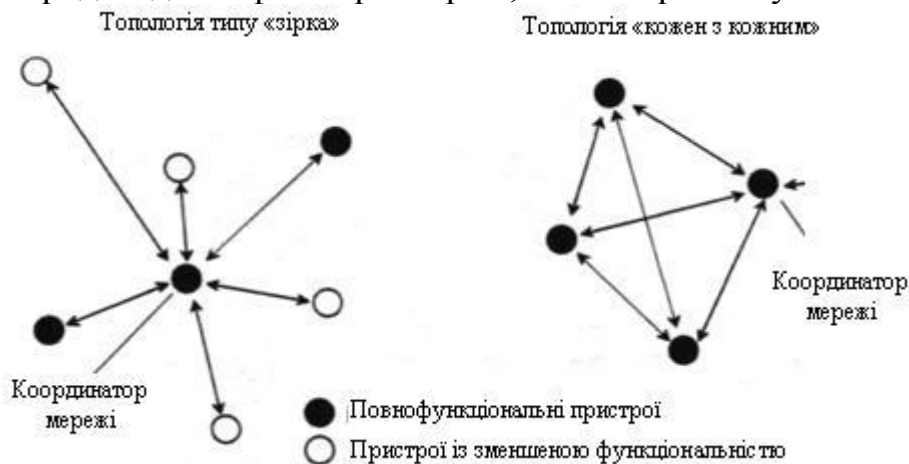


Рис. 4.14. Топологія мережі IEEE 802.15.4 типу «зірка» й «рівний з рівним»

Інформаційний обмін у пікомережі відбувається за допомогою послідовності суперфреймів. У загальному випадку суперфрейм включає керуючий інтервал (beacon), за ним йде інтервал конкурентного доступу (CAP) відповідно до механізму CSMA/CA і період призначеного доступу. Останній містить набір часових інтервалів, призначених певним пристроям, чутливим до затримок, для передачі даних (гарантовані тайм-слоти, GTS), наприклад, для

зв'язку бездротового маніпулятора «миша» з комп'ютером. Керуючий інтервал передає тільки координатор PAN. Відзначимо, що в суперфреймі може не бути ні керуючого інтервалу, ні GTS. Загалом, структура суперфреймів аналогічна прийнятій в стандарті IEEE 802.15.3.

Кожен пристрій передає інформацію за допомогою фреймів (пакетів). Вони можуть бути чотирьох типів - керуючі (beacon frame), фрейми даних, фрейми підтвердження прийому даних і фрейми команд MAC-рівня. Фрейми фізичного рівня (рис.4.16) містять заголовок із синхропослідовністю та інформацією про розмір фрейму (до 127 байт) а також поле даних - пакет MAC-рівня. Останній містить заголовок з усією необхідною інформацією про фрейм (тип, наявність криптозахисту, необхідність підтвердження прийому й т.п.), адреси й ідентифікатори пристрою - відправника та одержувача, власне поле даних і перевірочну контрольну суму (мал. 4.17). Сама процедура обміну інформацією може використовувати пакети підтвердження прийому даних (якщо втрата пакета критична).

- Координатор мережі
- Керуючий пристрій (вершина) кластера (CLH)
- Пристрій мережі

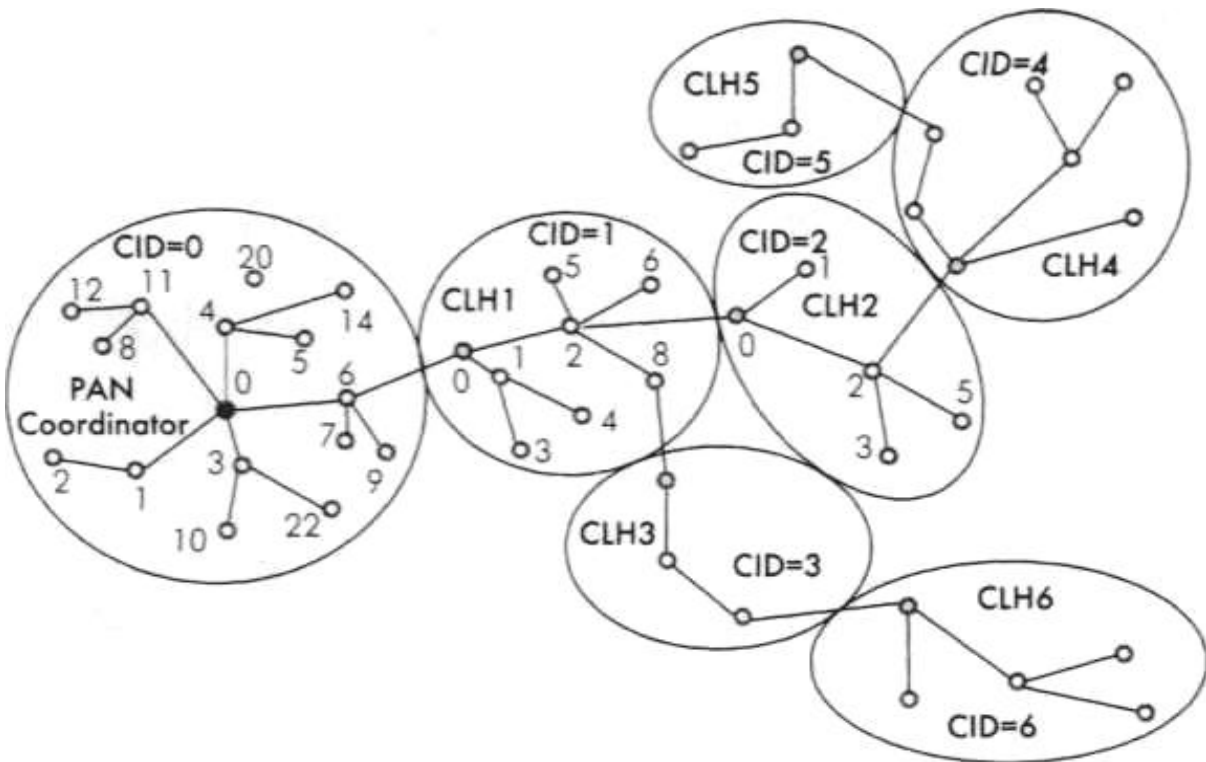


Рис. 4.15. Об'єднання декількох кластерів в мережі IEEE 802.15.4

Заголовок синхронізації		Заголовок фізичного рівня		Поле даних
Преамбула	Маркер початку фрейму	Довжина фрейму	Зарезервовано	
4 байти	1 байт	7 біт	1 біт	Довільно

Рис. 4.16. Структура пакетів фізичного рівня стандарту IEEE 802.15.4

Заголовок MAC-рівня						Поле даних	Перевірочна послідовність
Контроль кадру	Номер послідовності	Ідентифікатор мережі призначення	Ідентифікатор пристрою призначення	Ідентифікатор мережі джерела	Адреса джерела		
						Адресні поля	
2 байти	1 байт	0/2 байта	0/2/8 байт	0/2 байта	0/2/8 байт	Довільно	2 байти

Рис. 4.17. Структура пакетів MAC-рівня стандарту IEEE 802.15.4

Для IEEE 802.15.4 (ZigBee) чіпсети виробляє уже досить широкий ряд виробників. Характерний продукт тієї ж компанії Freescale Semiconductor - однокристальний модем MC13192 для діапазону 2,4 ГГц. Це - закінчене рішення бездротового модему. Пристрій містить інтерфейс із мікроконтролером і може застосовуватися в безлічі задач.

РОЗДІЛ 5. МЕРЕЖІ ШИРОКОСМУГОВОГО БЕЗДРОТОВОГО ДОСТУПУ СІМЕЙСТВА СТАНДАРТІВ IEEE 802.16 (WiMAX)

5.1 Структура та особливості стандарту IEEE 802.16-2004

5.1.1 Загальні аспекти

Новий документ – це компіляція вже існуючих стандартів, проте з достатньо серйозними змінами і уточненнями в окремих розділах. Головним чином вони торкнулися розділів, що входили раніше в IEEE 802.16a. Стандарт описує принципи побудови мереж регіонального масштабу в діапазонах до 66 ГГц – точніше, їх фізичний і MAC-рівні. Для цього передбачено п'ять режимів (табл.5.1).

Табл. 5.1 - Режими стандарту IEEE 802.16-2004

Режим	Частотний діапазон, ГГц	Опції	Метод дуплексування
WirelessMAN-SC	10-66		TDD/FDD
WirelessMAN-SCa	<11	AAS/ARQ/STC/ Mesh	TDD/FDD
WirelessMAN-OFDM	<11	AAS/ARQ/STC/Mesh	TDD/FDD
WirelessMAN-OFDMA	<11	AAS/ARQ/STC/ Mesh	TDD/FDD
WirelessHUMAN	<11, безліцензійний діапазон (в США і Європі)	DFS/AAS/ARQ/Mesh/STC	FDD

З них тільки WirelessMAN-SC призначений для роботи в діапазоні 10–66 ГГц. Він орієнтований на магістральні мережі ("точка-точка", "точка-багатоточка"), що працюють в режимі прямої видимості (тому що загасання таких високочастотних сигналів при віддзеркаленні дуже велике) з типовими швидкостями потоку даних (bit stream) 120 Мбіт/сек і шириною каналу близько 25 МГц. Це фактично описаний в документі IEEE 802.16-2001 радіоінтерфейс широкосмугового доступу з модуляцією однієї несучої на канал (SC – single carrier).

Решта режимів розроблена для діапазонів нижче 11 ГГц. Один з них – WirelessMAN-SCa – це "низькочастотна" варіація WirelessMAN-SC (з рядом додаткових механізмів, зокрема допускається 256-позиційна квадратурна модуляція 256-QAM). Інший, WirelessHUMAN, призначений для роботи в безліцензійних діапазонах (головним чином в США). Зате два режими, що залишилися, – WirelessMAN-OFDM і WirelessMAN-OFDMA – це принципово нові по відношенню до IEEE 802.16-2001 методи, і на них ми і зосередимо увагу.

Відзначимо, що всі режими діапазону нижче за 11 ГГц відрізняють три характерні деталі – це механізми автоматичного запиту повторної передачі (ARQ – automatic repeat request), підтримка роботи з адаптивними антенними системами (AAS – adaptive antenna system) і просторово-часове кодування (STC – space time coding) при роботі з AAS. Крім того, крім централізованої архітектури "точка-багатоточка", в діапазоні нижче за 11 ГГц передбачена підтримка архітектури

Mesh-мережі ("мережі" – децентралізованої мережі взаємодіючих одна з одною систем). Фактично Mesh-мережа є аналогом локальних ad-hoc-мереж стандарту IEEE 802.11. Примітно, що якщо в документі IEEE 802.16а йшлося про діапазон 2–11 ГГц, то в новому стандарті нижня межа так чітко не оговорюється (згадується "як правило, не нижче 1 ГГц").

Ще одна особливість стандарту – режим WirelessHUMAN (High-speed Unlicensed Metropolitan Area Network). Фактично він є адаптацією описаних в стандарті IEEE 802.16-2004 режимів для роботи в безліцензійних діапазонах частот (мабуть, в зоні 5–6 ГГц). Основні відмінності WirelessHUMAN – це використання тільки тимчасового дуплексування, режим динамічного розподілу частот (DFS – dynamic frequency selection) і механізм кризової нумерації частотних каналів. Проте оскільки в Україні безліцензійних діапазонів в гігагерцовій області немає, і нічого подібного нам не загрожує, детально зупинятися на даному режимі не будемо.

Принципово, що істотна увага в стандарті IEEE 802.16-2004 приділена якості обслуговування (QoS), а також механізмам захисту даних і з'єднань. Враховуючи, що IEEE 802.16-2004 принципово орієнтований на роботу в ліцензійних діапазонах, а також його фактично загальносвітове визнання (у Європі він прийнятий ETSI під ім'ям HiperMAN) і підтримку провідних виробників телекомунікаційного обладнання (що об'єдналися в WiMAX Forum), можна з великим ступенем впевненості припустити, що найближчими роками нас чекає нова хвиля "бездротової революції". І по своєму розмаху вона може перевершити хвилі, породжені появою персональних комп'ютерів і стільникових телефонів.

5.1.2 Фізичний рівень стандарту IEEE 802.16-2004

На фізичному рівні стандарт IEEE 802.16-2004 передбачає три принципово різні методи передачі даних: метод модуляції однієї несучої SCa канал (SC – single carrier), метод модуляції за допомогою ортогональних несучих OFDM (orthogonal frequency division multiplexing) і метод мультиплексування (множинного доступу) за допомогою ортогональних несучих OFDMA (orthogonal frequency division multiple access).

Режим OFDM – це метод модуляції потоку даних в одному частотному каналі (шириною 1–2 МГц і більше) із центральною частотою f_c . Розподіл же на канали – частотне. Нагадаємо, що при модуляції даних за допомогою ортогональних несучих у частотному каналі виділяються N піднесучих так, що

$$f_k = f_c + k\Delta f \quad (5.1)$$

де k – ціле число з діапазону $\left[-N/2, N/2 \right]$ (у цьому випадку $k \neq 0$).

Відстань між ортогональними несучими

$$\Delta f = 1/T_b \quad (5.2)$$

де T_b – тривалість передачі даних у символі.

Крім даних OFDM-символ включає захисний інтервал тривалістю T_g .

Отже, загальна тривалість OFDM-символу (Рис. 5.1):

$$T_s = T_b + T_g \quad (5.3)$$

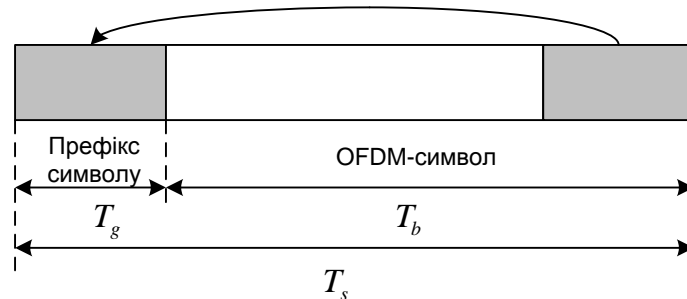


Рис. 5.1 - OFDM-символ

Захисний інтервал являє собою копію кінцевого фрагменту символу. Його тривалість T_g може становити 1/4, 1/8, 1/16 і 1/32 від T_b .

Кожна піднесуча модулюється самостійно за допомогою квадратурної амплітудної модуляції. Загальний сигнал обчислюється методом зворотного швидкого перетворення Фур'є (ЗШПФ) як

$$s(t) = \text{Re} \left\{ e^{i2\pi f_c t} \sum_{k=-N/2}^{N/2} c_k e^{i2\pi k \Delta f (t - T_g)} \right\}, \quad 0 < t < T_s \quad (5.4)$$

де c_k – комплексне представлення символу квадратурної модуляції (QAM-символу).

Комплексне подання зручно, оскільки генерація радіосигналу відбувається за допомогою квадратурного модулятора відповідно до виразу:

$$s_k(t) = I_k \cos 2\pi f_c t - Q_k \sin 2\pi f_c t \quad (5.5)$$

де I_k і Q_k – синфазне й квадратурне (ціле й мниме) значення комплексного символу, відповідно.

Для роботи алгоритмів ШПФ/ЗШПФ бажано, щоб кількість точок відповідало 2^m . Тому число несучих вибирають рівним мінімальному числу $N_{FFT} = 2^m$, що перевершує N . У режимі OFDM стандарту IEEE 802.16-2004 $N = 200$, відповідно $N_{FFT} = 256$. З них 55 ($k = -128 \dots -101$ і $101 \dots 127$) утворюють захисний інтервал на границях частотного діапазону каналу. Центральна частота каналу ($k = 0$) і частоти захисних інтервалів не використовуються (тобто амплітуди відповідних їм сигналів дорівнюють нулю). З інших 200 несучих вісім частот – пілотні (з індексами $\pm 88, \pm 63, \pm 38, \pm 13$), інші розбиті на 16 підканалів по 12 несучих у кожному, причому в одному підканалі

частоти розташовані не підряд. Наприклад, підканал 1 складають несучі з індексами -100, -99, -98, -37, -36, -35, 1, 2, 3, 64, 65, 66. Розподіл на підканали необхідно, оскільки в режимі WirelessMAN-OFDM передбачена (опціонально) можливість роботи не у всіх 16, а в одному, двох, чотирьох і восьми підканалах – деякий прообраз схеми множинного доступу OFDMA. Для цього кожний підканал і кожна група підканалів мають свій індекс (від 0 до 31).

Тривалість корисної частини T_b OFDM-символу залежить від ширини смуги каналу BW і системної тактової частоти (частоти дискретизації) F_s ; $F_s = N_{FFT}/T_b$. Співвідношення $F_s/BW = n$ нормується, і залежно від ширини смуги каналу приймає значення 86/75 (BW кратно 1,5 МГц), 144/125 (BW кратно 1,25 МГц), 316/275 (BW кратно 2,75 МГц), 57/50 (BW кратно 2 МГц) і 8/7 (BW кратно 1,75 МГц і у всіх інших випадках).

Захисний інтервал при OFDM-модуляції – потужний засіб боротьби з міжсимвольними перешкодами (міжсимвольної інтерференції, MCI), що виникають внаслідок неминучих у міських умовах перевідбиттів і багатопроменевого поширення сигналу. MCI приводить до того, що в приймачі на сигнал, що поширюється прямо, накладається перевідбитий сигнал, що містить попередній символ. При модуляції OFDM перевідбитий сигнал попадає в захисний інтервал і шкоди не заподіює. Однак цей механізм не запобігає внутрішньосимвольній інтерференції – накладення сигналів з тим самим символом, що прийшов з фазовою затримкою. У результаті інформація може повністю спотворитися або (наприклад, при фазовому зрушенні на 180°) просто зникнути. Для запобігання втрати інформації при пропаданні окремих символів або їхніх фрагментів стандарт IEEE 802.16-2004 передбачає ефективні засоби канального кодування.

Кодування даних на фізичному рівні включає три стадії – рандомізацію, завадостійке кодування й перемежування.

Рандомізація – це множення блоку даних на псевдовипадкову послідовність (ПВП), що формує генератор ПВП із задаючим поліномом виду $1 + x^{14} + x^{15}$.

У низхідному потоці генератор ПВП ініціалізується з початком кадру за допомогою кодового слова 4A8016. Починаючи із другого пакету кадру генератор ПВП ініціалізується на основі ідентифікаційного номера базової станції BSID, ідентифікатора профілю пакета DIUC (downlink interval usage code) і номера кадру (рис. 5.2).

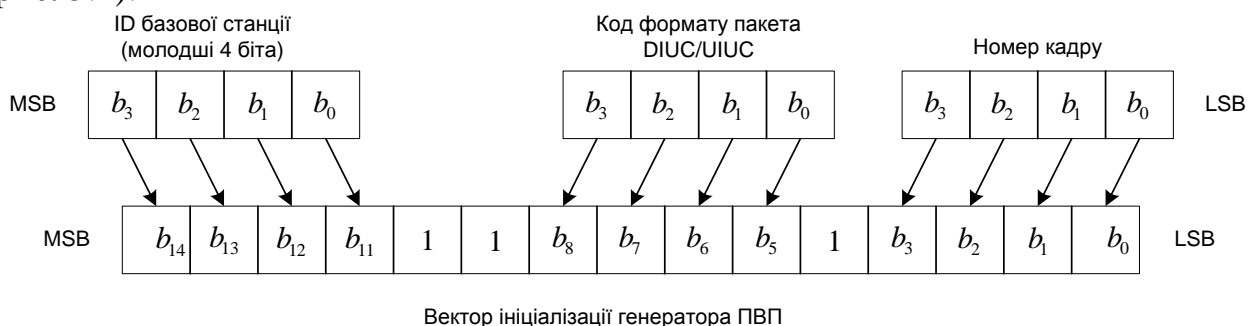


Рис. 5.2 Формування вектора ініціалізації генератора ПВП для рандомізації низхідного каналу

У висхідному потоці все відбувається аналогічно, з тією лише різницею, що ініціалізація генератора ПВП за схемою, яка наведена на рис.5.2, відбувається з першого пакета (замість DIUC використовується UIUC – uplink interval usage code).

Кодування даних передбачає каскадний код із двома стадіями – кодер Ріда-Соломона з поля Галуа GF (256) і згортковий кодер. У базовому виді код Ріда-Соломона оперує блоками вихідних даних по 239 байт, формуючи з них кодований блок розміром 255 байт (додаючи 16 перевірочних байт). Такий код здатний відновити до 8 пошкоджених байт. Оскільки реально використовуються блоки даних меншої довжини K , перед ними додаються $239 - K$ нульових байт. Після кодування ці байти знищуються. Якщо необхідно скоротити число перевірочних слів так, щоб зменшити число відновлюваних байт T , використовуються тільки $2T$ перших перевірочних байтів. Обов'язкові для підтримки в IEEE 802.16-2004 варіанти каскадного коду наведені в табл. 5.2.

Табл. 5.2 Каскадні коди

Модуляція	Блок даних до кодування, байт	Кодер Ріда-Соломона	Швидкість кодування загорткового коду	Сумарна швидкість кодування	Блок даних після кодування, байт
BPSK	12	(12,12,0)	1/2	1/2	24
QPSK	24	(32,24,4)	2/3	1/2	48
QPSK	36	(40,36,2)	5/6	3/4	48
16-QAM	48	(64,48,8)	2/3	1/2	96
16-QAM	72	(80,72,4)	5/6	3/4	96
64-QAM	96	(108,96,6)	3/4	2/3	144
64-QAM	108	(120,108,6)	5/6	3/4	144

Після кодера Ріда-Соломона дані надходять у згортковий кодер (рис. 5.3) з породжуючими послідовностями (генераторами коду) $G_1 = 171_8$ (для виходу X) і $G_2 = 133_8$ (для Y) - так званий стандартний код NASA. Його базова швидкість кодування – 1/2, тобто з кожного вхідного біта він формує пару кодованих біт X і Y . Упускаючи з послідовності пар елементи X_i або Y_i , можна отримувати різні швидкості кодування. Так, швидкості 2/3 відповідає послідовність $(X_1 Y_1 Y_2)$, швидкості 3/4 – $(X_1 Y_1 Y_2 X_3)$, 5/6 – $(X_1 Y_1 Y_2 X_3 Y_4 X_5)$.

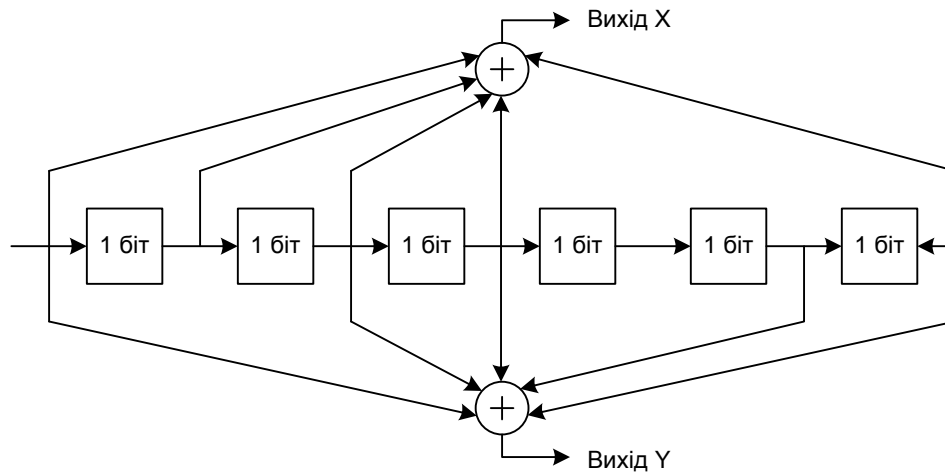


Рис. 5.3 Схема згорткового коду

Кодер Ріда-Соломона не використовується із двопозиційною модуляцією BPSK (наприклад, при початковій ініціалізації АС або запиті смуги). Він також пропускається, коли використовується частина субканалів OFDM. У цьому випадку швидкість загорткового кодування приймається рівною загальній швидкості кодування (див. табл. 5.2) (відповідно, розмір вихідного блоку даних множиться на число субканалів, які використовуються, поділене на 16).

Крім описаного механізму кодування стандарт передбачає опціональне застосування блокових турбо-кодів (заснованих на кодах Хемінга й контролі парності) і загорткових турбо-кодів.

Після кодування слідує процедура перемежування – перемішування біт у межах блоку кодованих даних, що відповідає OFDM-символу. Ця операція проводиться у дві стадії. Ціль першої – зробити так, щоб суміжні біти виявилися рознесеними по несуміжним несучим. На другій стадії суміжні біти виявляються рознесеними в різні половини послідовності. Все це робиться для того, щоб при групових помилках у символі пошкоджувалися несуміжні біти, які легко відновити при декодуванні. Перемежування реалізується відповідно до формул:

$$m_k = \left(N_{cbps} / 12 \right) - \left\langle \text{mod } 12 \right\rangle \left\lfloor \left\langle / 12 \right\rangle \right\rfloor \quad (5.6)$$

$$j_k = s - \left\lfloor \left\langle m_k / s \right\rangle \right\rfloor + \left(m_k + N_{cbps} - \left\lfloor \left(12m_k / N_{cbps} \right) \right\rfloor \right) \text{mod } s \quad (5.7)$$

$$k = 0 \dots N_{cbps} - 1 \quad (5.8)$$

де m_k і j_k – номер вихідного k -го біта після першої й другої стадії перемежування, відповідно

N_{cbps} – число кодованих біт в OFDM-символі (при заданому числі субканалів)

s – 1/2 числа біт на несучу (1/2/4/6 біт для BPSK/QPSK/16-QAM/64-QAM, відповідно, для BPSK $s = 1$)

функція $\text{floor}(x)$ – це найбільше ціле число, що не перевершує x

функція $x \bmod r$ – залишок від x/r .

Після перемежування розпочинається стадія модуляції. Виходячи з обраної схеми модуляції (BPSK/QPSK/16-QAM/64-QAM), блок представляється у вигляді послідовності груп біт, що відповідають модуляційним символам (по 1/2/4/6 біт). Кожній групі ставиться у відповідність значення Q і I з векторних діаграм Грея (рис 5.4), які потім використовуються при безпосередній модуляції несучої. Для усереднення амплітуд квадратурних символів використовуються нормалізовані значення Q і I , тобто помножені на коефіцієнти c (для QPSK $c = 1/\sqrt{2}$, для 16-QAM $c = 1/\sqrt{10}$, для 64-QAM $c = 1/\sqrt{42}$).

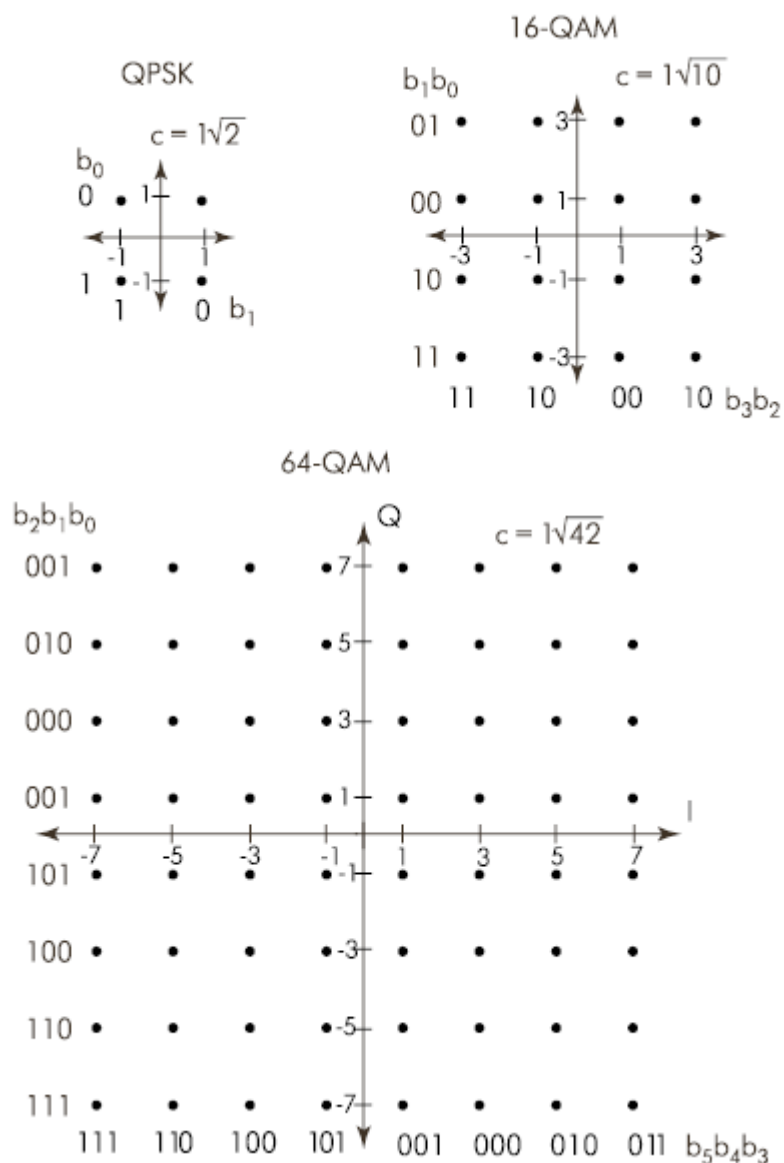


Рис. 5.4 Векторні діаграми Грея (представлення модуляційних символів) для BPSK, QPSK, 16-QAM та 64-QAM

Пілотні несучі модулюються за допомогою BPSK. Значення сигналів на цих несучих визначаються на підставі бінарної ПВП w_k з задаючим поліномом $x^{11} + x^9 + 1$, причому в низхідному субкадрі k - номер символу відносно початку кадру, у висхідному - номер символу відносно початку пакета (Рис. 5.5).

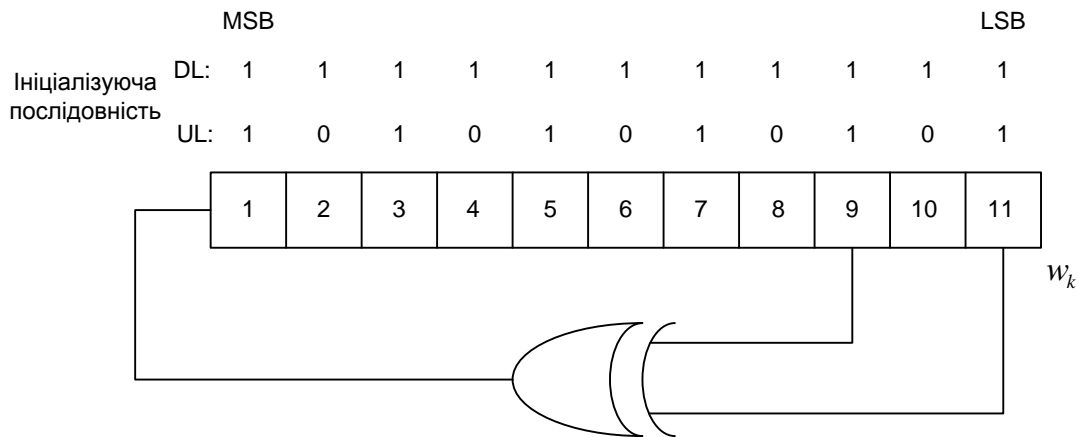


Рис. 5.5 Генерація модулюючої послідовності для пілотних несучих

Ініціалізуючі слова генератора ПВП для низхідного й висхідного потоків різні ($8FF_{16}$ і 555_{16} , відповідно). Власне, значення BPSK-символів обчислюються як:

$$c_{-88} = c_{-38} = c_{63} = c_{88} = 1 - 2w_k \quad (5.9)$$

$$c_{-63} = c_{-13} = c_{13} = c_{38} = 1 - 2\bar{w}_k \quad (5.10)$$

у низхідному каналі й

$$c_{-88} = c_{-38} = c_{13} = c_{38} = c_{63} = c_{88} = 1 - 2w_k \quad (5.11)$$

$$c_{-63} = c_{-13} = 1 - 2\bar{w}_k \quad (5.12)$$

у висхідному.

Після визначення модуляційних символів за допомогою ЗШПФ обчислюється сам радіосигнал і передається в передавач. При прийомі всі процедури проводять у зворотному порядку.

У режимі OFDM на фізичному рівні для мереж з архітектурою "точка-багатоточка" інформаційний обмін відбувається за допомогою послідовності кадрів (фреймів). Кожний фрейм (Рис 5.6) ділиться на два субкадра – низхідний (DL – від БС до АС) і висхідний (UL – від АС до БС). Поділ на висхідний і спадний канали – як часове (TDD), так і частотне (FDD). В останньому випадку DL і UL транслуються одночасно, у різних частотних діапазонах.

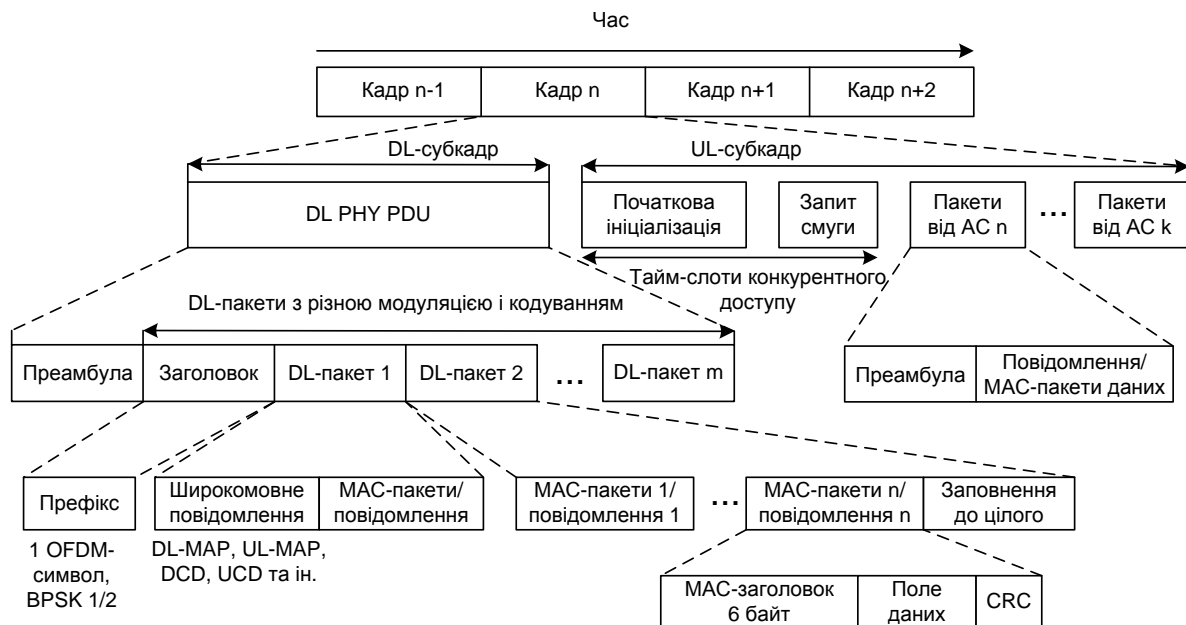


Рис. 5.6 Структура OFDM-символу при часовому дуплексу ванні

Низхідний субкадр включає керуючу преамбулу, заголовок кадру (FCH – frame control header) і послідовність пакетів даних. Преамбула в низхідному каналі – посилка із двох OFDM-символів (довга преамбула), призначена для синхронізації. Перший OFDM-символ використовує несучі з індексами, кратними 4, другий – тільки парні несучі (модуляція – QPSK).

За преамбулою слідує керуючий заголовок кадру – один OFDM-символ з модуляцією BPSK і стандартною схемою кодування (швидкість кодування – 1/2). Він містить так званий префікс кадру спадного каналу (DLFP – Downlink Frame Prefix), що описує профіль і довжину першого (або декількох початкових) пакета в DL-субкадрі.

У перший пакет входять широкомовні повідомлення (призначені всім AC) – карти розташування пакетів DL-MAP, UL-MAP, дескриптори низхідних/висхідних каналів DCD/UCD, інша службова інформація. Кожний пакет має свій профіль (схема кодування, модуляція й т.д.) і передається за допомогою цілого числа OFDM-символів. Точки початку й профілі всіх пакетів, крім першого, утримуються в DL-MAP.

Низхідний субкадр містить інтервал конкурентного доступу, що включає періоди для початкової ініціалізації AC (входження в мережу) і для запиту смуги передачі. Далі слідує тимчасові інтервали, призначені базовою станцією певним абонентським станціям для передачі. Розподіл цих інтервалів (точки початку) утримується в повідомленні UL-MAP. AC у своєму часовому інтервалі починає трансляцію з передачі короткої преамбули (один OFDM-символ, використовує тільки парні несучі). За ним слідує, власне, інформаційний пакет, сформований на MAC-рівні.

Тривалість OFDM-кадрів може становити 2,5; 4; 5; 8; 10; 12,5; і 20 мс. Заданий базовою станцією період побудови кадрів не може змінюватися, оскільки в цьому випадку потрібна буде ресинхронізація всіх AC.

Запит на встановлення з'єднання не відрізняється від загальноприйнятого в стандарті IEEE 802.16, за винятком додаткового режиму «концентрованого» запиту (Region-Focused). Він призначений тільки для станцій, здатних працювати з окремими субканалами. У цьому режимі в інтервалах конкурентного доступу (заданих в UL-MAP) АС може передати короткий 4-розрядний код на одному із 48 субканалів, кожний з яких включає чотири несучі. Усього передбачено вісім кодів. Код і номери каналу АС вибирає випадковим чином.

Отримавши кодове повідомлення, БС надає АС інтервал для передачі «звичайного» запиту на надання доступу (заголовок запиту MAC-рівня) – якщо це можливо. Однак, на відміну від інших механізмів, БС в UL-MAP не вказує ідентифікатор станції, що її запросила, а приводить номера коду запиту, підканалу, а також порядковий номер інтервалу доступу, протягом якого був переданий запит. По цих параметрах АС і визначає, що інтервал для запиту смуги передачі призначений їй. Вибір моменту для передачі 4-розрядного коду запиту доступу відбувається випадковим чином, по описаному вище алгоритму звертання до каналу конкурентного доступу.

Відзначимо, що в режимі OFDM каналний ресурс може надаватися не тільки в часовій області, але в окремих підканалах (групах підканалів), якщо БС і абонентські станції підтримують таку можливість. Одне з найбільш важливих застосувань такої опції – Mesh-мережа.

5.1.3 MAC-рівень стандарту IEEE 802.16-2004

Обладнання стандарту IEEE 802.16-2004 покликане формувати транспортне середовище для різних додатків (сервісів), тому перше завдання, що вирішується в IEEE 802.16-2004, – це механізм підтримки різноманітних сервісів верхнього рівня. Розробники стандарту прагнули створити єдиний для всіх додатків протокол MAC-рівня, незалежно від особливостей фізичного каналу. Це істотно спрощує зв'язок терміналів кінцевих користувачів з міською мережею передачі даних – фізично середовища передачі в різних фрагментах WMAN можуть бути різні, але структура даних єдина. У одному каналі можуть працювати (не одночасно) сотні різних терміналів ще більшого числа кінцевих користувачів. Цим користувачам необхідні найрізноманітніші сервіси (додатки) – потоки голосу і даних з тимчасовим розділенням, з'єднання по протоколу IP, пакетна передача мови через IP (VoIP) і т.д. Більш того, якість послуг (QoS) кожного окремого сервісу не повинна змінюватися при роботі через мережі IEEE 802.16-2004. Алгоритми і механізми доступу MAC-рівня повинні упевнено вирішувати всі ці задачі.

Структурно MAC-рівень IEEE 802.16-2004 підрозділяється на три підрівні (Рис. 5.7):

- підрівень перетворення сервісу CS (Convergence Sublayer);
- основний підрівень CPS (Common Part Sublayer);
- підрівень захисту PS (Privacy Sublayer).

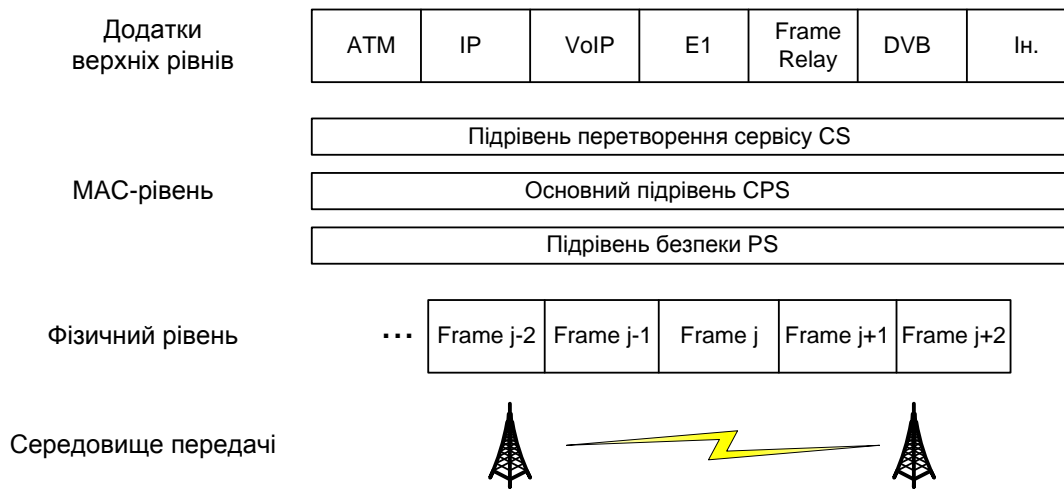


Рис. 5.7 Структура MAC-рівня

На підрівні захисту реалізуються функції, що забезпечують криптозахист даних і механізми аутентифікації/запобігання несанкціонованого доступу. Для цього передбачені два основні компоненти – набір алгоритмів криптозахисту і протокол управління ключем шифрування. Ключ кожної АС базова станція може передавати в процесі авторизації, використовуючи схему роботи “клієнт (АС) – сервер (БС)”.

На підрівні перетворення сервісу відбувається трансформація потоків даних протоколів верхніх рівнів для передачі через мережі IEEE 802.16-2004. Для кожного типу додатків верхніх рівнів стандарт передбачає свій механізм перетворення, але на сьогодні описані і увійшли до специфікації IEEE 802.16-2004 тільки два – для роботи в режимі АТМ і для пакетної передачі. Під пакетною передачею передбачають достатньо широкий набір різних протоколів, включаючи ІР. Мета роботи на CS-підрівні – оптимізація потоків даних кожного додатку верхнього рівня, що передаються, з урахуванням їх специфіки. Тому найважливіше завдання, що вирішується на даному підрівні, – класифікація пакетів/комірок. Від результатів її рішення залежить і оптимізація потоків, що передаються, і виділення смуги пропускання для кожного з них.

Для оптимізації потоків, що транслюються, передбачений спеціальний механізм видалення фрагментів заголовків PHS, що повторюються (Payload Header Suppression). Дійсно, і в АТМ, і в пакетному режимі дані передаються окремими порціями – комітками і пакетами, відповідно. Кожна така порція даних складається, в загальному випадку, із заголовка і поля даних – фіксованих розмірів для АТМ (5 і 48 байт, відповідно) і достатньо довільних при пакетній передачі. У багатьох випадках заголовки пакетів і комірок містять інформацію, яка повторюється, і являється зайвою при трансляції за допомогою протоколу IEEE 802.16-2004. Механізм PHS дозволяє позбавитися передачі надмірної інформації: на передаючому кінці пакети додатків відповідно до певних правил перетворюються в структури даних MAC-рівня IEEE 802.16-2004, на приймальному – відновлюються.

На основному підрівні MAC формуються пакети даних (MAC PDU – MAC Protocol Data Unit, блоки даних MAC-рівня), які потім передаються на фізичний

рівень і транслюються через канал зв'язку. Пакет MAC PDU (далі – PDU) включає заголовок і поле даних (його може і не бути), за яким може слідувати контрольна сума CRC (Рис. 5.8).

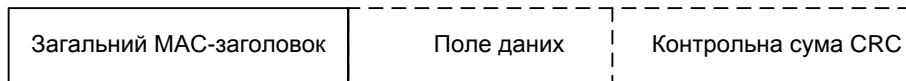


Рис. 5.8 Пакет MAC-рівня

Заголовок PDU займає 6 байт і може бути двох типів – загальний і заголовок запиту смуги пропускання. Загальний заголовок використовується в пакетах, у яких присутнє поле даних. У загальному заголовку вказується ідентифікатор з'єднання CID, тип і контрольна сума заголовка, а також приводиться інформація про поле даних (табл. 5.3).

Табл. 5.3 Структура загального заголовку MAC PDU

Структура загального заголовку MAC PDU (від старшого до меншого біта)	
Поле	Довжина, біт
тип заголовку = 0 (ознака загального заголовку)	1
ознака шифрування поля даних	1
тип поля даних	6
не використовується	1
ознака наявності CRC	1
індекс ключа шифрування	2
не використовується	1
довжина пакета, включаючи заголовок (в байтах)	11
ідентифікатор з'єднання CID	16
контрольна сума заголовку (задаючий поліном $g(D) = D^8 + D^2 + D + 1$)	8

Заголовок запиту смуги застосовується, коли АС просить у БС виділити або збільшити їй смугу пропускання в низхідному каналі. При цьому в заголовку вказується CID і розмір необхідної смуги (у байтах, без урахування заголовків фізичних пакетів). Поля даних після заголовків запиту смуги може не бути.

Поле даних може містити підзаголовки MAC, керуючі повідомлення і, власне, дані додатків верхніх рівнів, перетворені на CS-підрівні. У стандарті

описано три типу MAC-підзаголовків – упаковки, фрагментації і управління наданням каналу. Підзаголовок упаковки використовуються, якщо в полі даних одного PDU містяться декілька пакетів верхніх рівнів; підзаголовок фрагментації – якщо, навпаки, один пакет верхнього рівня розбитий декілька PDU. Підзаголовок управління наданням каналу призначений, щоб АС повідомляла БС про зміну своїх потреб в смузі пропускання (число байт у висхідному каналі для певного з'єднання, повідомлення про переповнювання вихідної черги в АС, вимога регулярного опитування з боку БС для з'ясування потрібної смуги).

Керуючі повідомлення – це основний механізм управління системою IEEE 802.16-2004. Всього зарезервовано 256 типів керуючих повідомлень, з них 30 описано в стандарті IEEE 802.16-2004. Опис профілів пакетів, управління доступом, механізми криптозахисту, динамічна зміна роботи системи і т.д. – всі функції управління, запиту і підтвердження реалізуються через керуючі повідомлення. Розглянуті вище карти висхідного/низхідного каналів (UL-/DL-MAP) також є керуючими повідомленнями. Формат керуючих повідомлень простий – поле типу повідомлення (1 байт) і поле даних (параметрів).

5.1.4 Керування з'єднаннями в мережах IEEE 802.16-2004

Ключовим моментом в стандарті IEEE 802.16-2004 є поняття “сервісного потоку” і пов'язані з ним поняття “з'єднання” і “ідентифікатор з'єднання” (CID). Оскільки система IEEE 802.16-2004 – лише транспортне середовище, її інфраструктура фактично формує комунікаційні канали для потоків даних різних додатків верхніх рівнів (сервісів) – передача відеоданих, АТМ-потоки, IP-потоки, передача телефонних мультимплексованих пакетів типу Е1 і т.д. Кожний з таких додатків володіє своїми вимогами до швидкості передачі, надійності (якості обслуговування), криптозахисту і т.д. Відповідно, і дані кожного додатку слід передавати через транспортне середовище з урахуванням цієї специфіки.

Сервісним потоком в стандарті IEEE 802.16-2004 називається потік даних, пов'язаний з певним додатком. У цьому контексті з'єднання – це встановлення логічного зв'язку на MAC-рівнях на передаючій і приймальній стороні для передачі сервісного потоку. Кожному з'єднанню привласнюється 16-розрядний ідентифікатор CID, з яким однозначно зв'язані тип і характеристики з'єднання. Зокрема, по запиту надання/зміни смуги пропускання зі сторони АС базова станція відразу розуміє, з яким сервісним потоком має справу і які умови передачі йому потрібно забезпечити. Так, при початковій ініціалізації в мережі кожної АС призначається три CID для службових повідомлень трьох рівнів. Принципово, що одна АС може встановлювати безліч різних з'єднань з різними CID. Характерний приклад – коли зв'язок крупного офісу з телекомунікаційним вузлом організований через систему IEEE 802.16-2004. В цьому випадку одна АС в офісі може підтримувати абсолютно різні додатки – телефонію, телебачення, доступ в Інтернет і т.д. Кожний з цих додатків пред'являє свої вимоги до QoS і швидкостей передачі, які потрібно задовольнити. За допомогою CID базова станція дізнається, з чим має справу, і надає необхідний ресурс.

Не менш важливим для розуміння ідеології IEEE 802.16-2004 є принцип надання доступу до каналу по запиту Demand Assigned Multiple Access (DAMA). Жодна АС не може нічого передавати, окрім запитів на реєстрацію і надання каналу, поки БС не дозволить їй цього – тобто відведе часовий інтервал у висхідному каналі і вкаже його розташування в карті UL-MAP. Абонентська станція може запрошувати як певний розмір смуги в каналі, так і просити про зміну вже наданого їй каналного ресурсу.

Запити смуги можуть бути як епізодичними для БС, так і планованими. У першому випадку запити реалізуються за допомогою пакетів, що складаються із заголовка запиту, які передаються на конкурентній основі в спеціально виділеному для них інтервалі висхідного каналу. Процедура планових запитів смуги у висхідному каналі називається опитуванням (polling) – БС як би опитує АС про їх потреби. Реально це означає, що базова станція надає конкретній АС інтервал для передачі запиту про надання/зміну смуги, тобто ніякої конкуренції вже немає.

Опитування може бути у реальному часі – інтервали для запиту надаються АС з тим же періодом, з яким у неї може виникнути потреба в зміні умов доступу (наприклад, в кожному кадрі). Цей режим зручний для додатків, коли пакети даних слідує з фіксованим періодом, але їх розмір не стабільний (наприклад, відео-MPEG). Інший варіант опитування – поза “реальним часом”. В цьому випадку БС надає АС інтервал для запиту також періодично, але період цей істотно більший – наприклад, 1 сек. Характерний додаток, для якого ефективний цей механізм, – FTP-протокол.

Для додатків, у яких періодичність і розмір пакетів фіксовані (наприклад, в телефонії шина Е1), передбачений механізм доступу до каналу без вимоги (Unsolicited Grant Service – UGS). В цьому випадку БС із заданим періодом надає АС для передачі даних інтервали фіксованого розміру, відповідні швидкості потоку даних. Якщо в ході роботи АС потрібно змінити умови доступу, вона робить це за допомогою спеціального MAC-підзаголовку управління наданням каналу. У цьому підзаголовку є спеціальний прапор “опитай мене”, встановивши який, АС просить у БС інтервал для запиту нової смуги. Істотно, що в згаданому підзаголовку є спеціальний біт індикації переповнення вихідного буфера передавача АС, що приводить до втрати даних (slip). БС може відреагувати на появу цього сигналу, наприклад, збільшивши смугу для даної АС.

5.1.5 Mesh-мережі

Формально Mesh-мережа – це вид топології мережі IEEE 802.16-2004. Основна відмінність Mesh-мережі від архітектури "точка-багатоточка" полягає в тому, що якщо в останньому випадку АС може спілкуватися тільки з БС, то в Mesh-мережі можливо взаємодія безпосередньо між АС. Оскільки мережі стандарту IEEE 802.16-2004 орієнтовані на роботу з широкими частотними каналами, Mesh-мережі увійшли до стандарту зовсім не з метою створення однорангових локальних мереж – для цього є стандарти групи IEEE 802.11. Причина в іншому – необхідний інструмент побудови широкосмугової мережі, в якій трафік може передаватися по ланцюжку з декількох станцій, ліквідовуючи

тим самим проблеми передачі за відсутності прямої видимості. Відповідно і всі механізми управління, що в принципі дозволяють побудувати децентралізовану розподілену мережу, орієнтовані все ж таки на деревовидну архітектуру, з виділеною базовою станцією (основний вузол) і домінуючими потоками БС-АС.

У Mesh-мережі всі станції (вузли) формально рівноправні. Проте практично завжди обмін трафіку Mesh-мережі із зовнішнім оточенням відбувається через один певний вузол (Рис. 5.9).

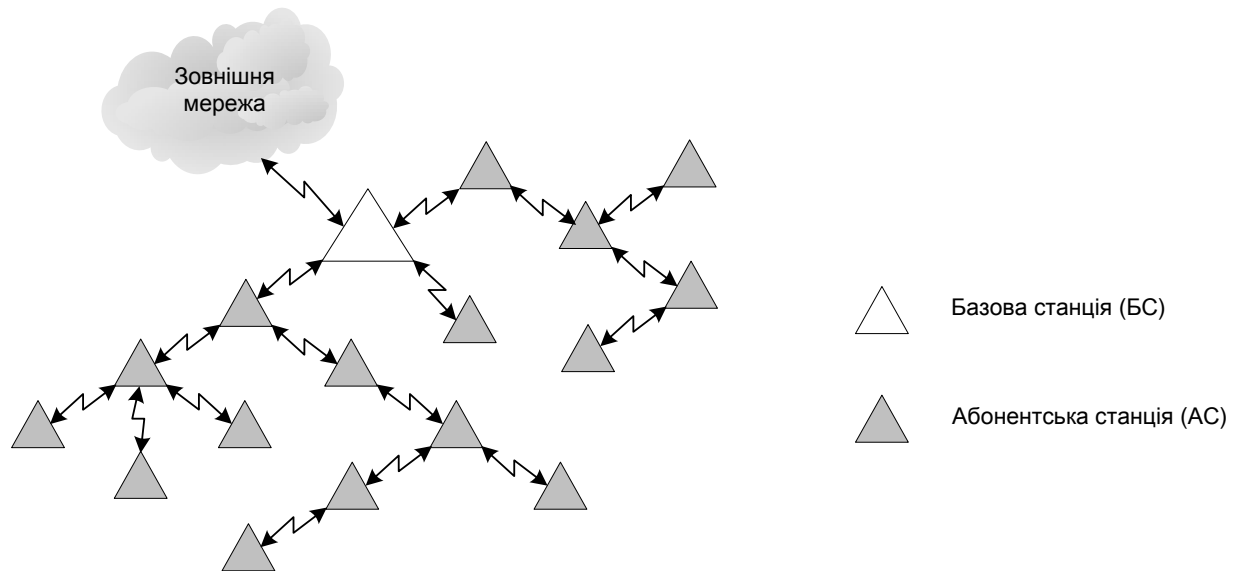


Рис. 5.9 Приклад Mesh-мережі

Такий вузол називають базовою станцією Mesh-мережі, саме на нього покладається частина необхідних для управління Mesh-мережею функцій. При цьому управління доступом може відбуватися або на основі механізму розподіленого управління, або централізованим способом, під управлінням БС. Можлива і комбінація цих методів.

Базове поняття в Mesh-мережі – сусіди. Під сусідами певного вузла розуміють всі вузли, які можуть встановлювати з ним безпосереднє з'єднання. Всі вони утворюють сусідське оточення. Вузли, пов'язані із заданим вузлом через сусідські вузли, називають сусідами другого порядку. Можуть бути сусіди третього порядку і т.д.

У Mesh-мережі немає поняття висхідних/низхідних каналів. Весь обмін відбувається за допомогою кадрів. Станції передають повідомлення або у відведені їм часові інтервали (відповідно до попереднього призначення каналів), або отримують доступ до каналів довільним (випадковим) чином. Кожен вузол має унікальну 48-розрядну MAC-адресу. Крім того, для ідентифікації усередині Mesh-мережі станціям привласнюється 16-розрядний мережевий ідентифікатор. Кожен вузол постійно зберігає список даних про всіх своїх сусідів (з вказівкою віддаленості, сектори для направленої антени, показової необхідної потужності передавача для зв'язку, затримки розповсюдження сигналу і т.п.) і транслює його в мережу із заданою періодичністю. На підставі сукупності цих списків від кожного з вузлів і відбувається управління мережею.

Кадр Mesh-мережі ділиться на керуючий субкадр і субкадр даних (Рис. 5.10).

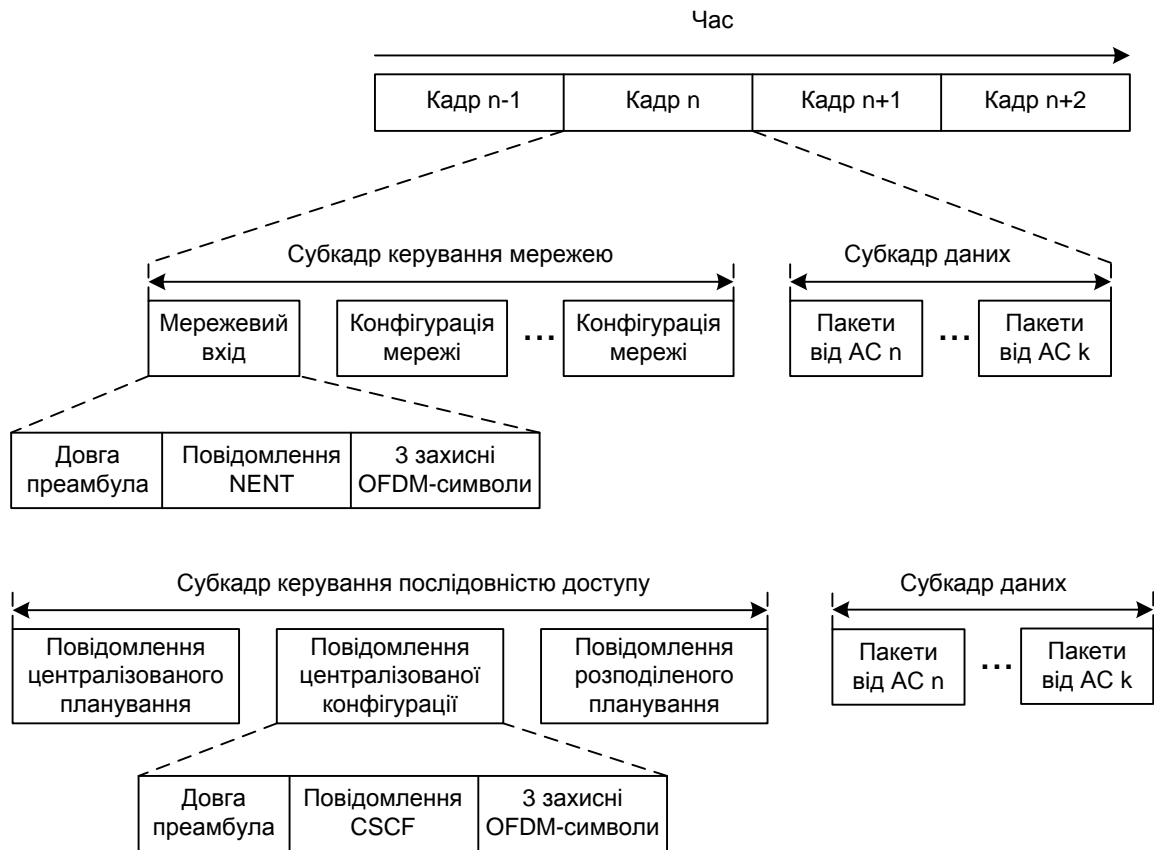


Рис. 5.10 Структура кадру Mesh-мережі

Довжина керуючого субкадру – змінна величина, що задається БС. Керуючий субкадр представляє собою набір пакетів MAC-рівня з тією різницею, що відразу після загального заголовку MAC-пакету слідує підзаголовок Mesh-мережі. Керуючий субкадр, залежно від реалізованих функцій, може бути двох типів – управління мережею (network control) і управління послідовністю доступу до каналів зв'язку (schedule control). У субкадрах завжди використовується модуляція QPSK із швидкістю кодування 1/2.

Субкадри управління включають інтервали для підключення до мережі нових пристроїв (Network entry – "мережевий вхід") і повідомлення "конфігурація мережі", які слідують за ними. Повідомлення типу "конфігурація мережі" містять всю необхідну інформацію про склад мережі. Вони ж реалізують процедури управління. Ці повідомлення генерує кожен вузол і транслює по мережі через своє сусідське оточення. Серед інформації, яка передається – списки сусідів кожного вузла, ідентифікаційний номер БС і число її сусідів, номер логічного каналу для передачі графіка доступу до каналів, віддаленість вузла (ранг сусідства) від БС і т.д. За допомогою таких повідомлень із заданою періодичністю транслюється дескриптор мережі – таблиця, що повністю описує поточні параметри мережі. Серед них – тривалість кадрів, довжина керуючого субкадру, число інтервалів для повідомлень децентралізованого розподілу ресурсів, періодичність проходження субпакетів розподілу ресурсів, профілі пакетів, тип кодування, відповідність

логічних каналів фізичним і т.п. Дескриптор мережі передається від базової станції її сусідському оточенню, від нього – вузлам з наступним рангом сусідства і т.д. Періодичність передачі дескриптора мережі нормована.

"Мережевий вхід" – це інтервал, протягом якого новий вузол може послати повідомлення (NENT) про свій намір підключитися до мережі (аналог інтервалу конкурентного доступу в мережі "точка-багатоточка"). Перед цим він повинен прийняти повідомлення про конфігурацію мережі, вибрати вузол для підключення, синхронізуватися з ним і лише потім відправляти запит. У відповідь вузол або відмовить в доступі, або призначить новому вузлу мережевий ідентифікатор, канал і часовий інтервал для проведення процедур аутентифікації.

Розподіл каналних ресурсів в Mesh-мережі може бути централізованим і децентралізованим (розподіленим). У свою чергу децентралізований розподіл буває координованим з БС і не координованим.

Децентралізований розподіл ресурсів передбачає, що розподіл відбувається в межах однієї групи сусідів (тобто між станціями, здатними безпосередньо зв'язуватися один з одним). При координованому децентралізованому розподілі вузли обмінюються між собою спеціальними повідомленнями управління розподілом (distributed scheduling – DSCH). Координованість полягає в тому, що період видачі таких повідомлень кожною станцією визначений і відомий її сусідам. Координовані DSCH-повідомлення передаються в субкадрах управління послідовністю доступу в обумовлених в мережевому дескрипторі інтервалах. Некоординовані DSCH-повідомлення передаються в субкадрі даних.

DSCH-повідомлення – це запити на отримання каналного ресурсу і повідомлення з відповіддю з наданням (підтвердженням) вільного ресурсу (часового інтервалу в субкадрі даних). Ресурс надається сусідом під конкретне з'єднання.

Централізований розподіл ресурсів передбачає деревовидну топологію мережі з БС у вершині. Воно реалізоване за допомогою двох типів повідомлень – централізованої конфігурації CSCF і централізованого планування CSCH. Ці керуючі повідомлення розміщуються на початку субкадру управління графіком доступу. Використовуючи повідомлення централізованого планування CSCH, кожен вузол визначає потребу в трафіку своїх дочірніх вузлів (тобто трафік яких від (до) БС проходить через даний вузол) і повідомляє свою потребу вищестоящому вузлу – аж до БС. Проаналізувавши потребу, БС розсилає повідомлення CSCH, інформуючи кожен вузол про виділену йому смугу пропускання (у біт/с) у висхідному і низхідному напрямках. Виходячи з цих даних, кожен вузол вже сам запрошує (або призначає) розташування пакетів в субкадрі даних у (для) своїх сусідських вузлів за допомогою повідомлень децентралізованого планування DSCH.

Повідомлення централізованої конфігурації CSCF формуються БС і транслюються по мережі для інформування всіх її вузлів про поточний стан. CSCF включає таку інформацію, як число доступних логічних каналів і їх перелік, перелік вузлів в мережі з вказівкою числа дочірніх вузлів для кожного з них, а також профілі висхідних/низхідних пакетів для кожного дочірнього вузла.

5.1.6 Формат заголовку MAC-рівня

В стандарті IEEE 802.16-2004 визначений набір керуючих повідомлень MAC. Ці повідомлення транспортуються в блоках даних MAC PDU. Блок даних MAC-кадру містить заголовок й опціональні поля даних та CRC. Формат MAC блоку даних (PDU) представлений на рис.5.11.

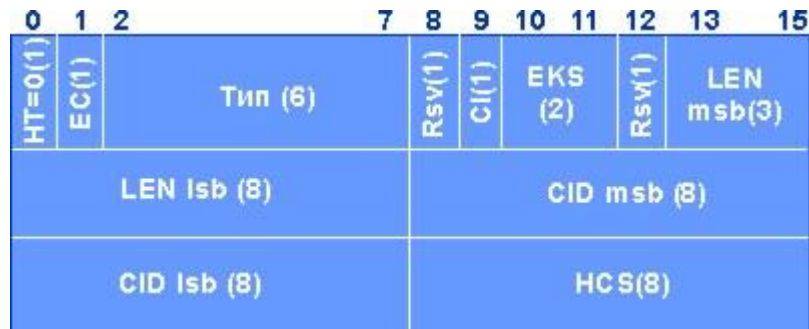


Рис. 5.11 Формат MAC-заголовка (біт 0 є старшим)

Опис полів MAC-заголовків наведений в табл. 5.4.

Табл. 5.4. Опису полів MAC-заголовка

Ім'я поля	Довжина в бітах	Опис
CI	1	Індикатор CRC 1= CRC додається до поля даних 0= CRC відсутній
CID	16	Ідентифікатор з'єднання
EC	1	Керування шифруванням 0= поле даних не зашифрованої 1= дані зашифровані
EKS	2	Послідовність ключів шифрування Індекс ключа шифрування трафіку й вектор ініціалізації для шифрування поля даних. Поле має сенс при EC=1
HCS	8	8-бітова контрольна торба заголовка. Утворюючий поліном: $g(D)=D^8+D^2+D+1$.
HT	1	Тип заголовка. Буде встановлений рівним нулю.
LEN	11	Довжина в байтах поля даних і MAC-заголовка
Тип	6	Поле вказує на тип поля даних, що включає підзаголовки

Значення поля *тип* для спадного каналу представлені в таблиці нижче

Табл. 5.5. Значення поля *тип* для спадного каналу

Тип	Опис
0x00	Підзаголовків немає
0x01	Зарезервовано
0x02	Підзаголовок упакований
0x03	Зарезервовано
0x04	Є підзаголовок фрагментації
0x05-0x3F	Зарезервовано

Значення поля *тип* для висхідного каналу представлені в таблиці нижче

Табл. 5.6. Значення поля *тип* для висхідного каналу

Тип	Опис
0x00	Підзаголовків немає
0x01	Є підзаголовок Grant Management (основне керування)
0x02	Є підзаголовок упаковання
0x03	Присутні підзаголовки Grant Management й упаковання
0x04	Є підзаголовки фрагментації й Grant Management
0x05-0x3F	Зарезервовано

Блок даних (PDU) запиту смуги містить заголовок запиту смуги пропущення й позбавлений поля даних. Формат заголовка показаний на рис. 5.12. Запит смуги має наступні властивості:

Запит смуги має наступні властивості:

- Довжина заголовка завжди має 6 байт
- Поле ЄС встановлюється рівним нулю (відсутність шифрування)
- CID указує на потік, для якого запитується смуга висхідного каналу (uplink).
- Поле запиту смуги BR визначає запитуваних байт.
- Припустимими типами для запитів смуги є 000000 для інкрементації й 000001 для агрегування.

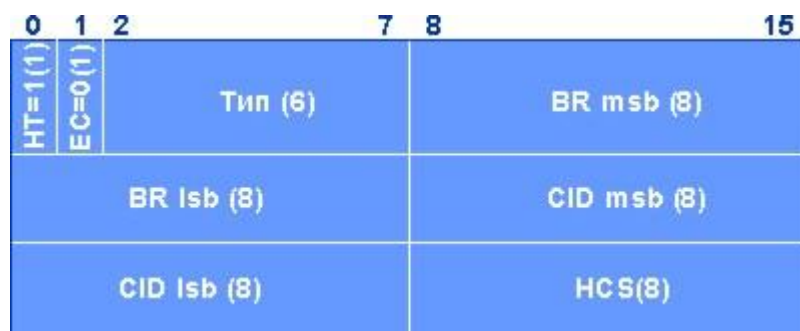


Рис. 5.12. Формат заголовка запроса смуги частот

Поля заголовка запиту смуги визначені в таблиці. Кожен заголовок кодується, починаючи з полів HT й ЄС. Кодування цих полів улаштовано так, що перший байт MAC-заголовка ніколи не повинен містити код 0xFF.

Табл. 5.7. Поля заголовка запиту смуги

Ім'я поля	Довжина в бітах	Опис
BR	16	Запит смуги Число байтів запитуваної SS смуги висхідного каналу. Запитий ставитися до даного CID.
CID	16	Ідентифікатор з'єднання
EC	1	Завжди дорівнює нулю
HCS	8	8-бітова контрольна торба заголовка. Утворюючий поліном: $g(D)=D^8+D^2+D+1$.
HT	1	HT = 1.
Тип	6	Поле вказує на тип заголовка запиту смуги

Можуть бути присутнім три типи підзаголовків MAC (фрагментації й керування). Якщо підзаголовки фрагментації й керування присутні одночасно, то підзаголовок керування міститься першим. Підзаголовки впакування й фрагментації несумісні.

Структура підзаголовка фрагментації (FSH) представлена в таблиці 5.8.

Табл. 5.8. Структура підзаголовка фрагментації (FSH)

Синтаксис	Розмір	Опис
Підзаголовок фрагментації() {		
FC	2 біти	
FCN	3 біти	
Зарезервовано для використання з CS	3 біти	
}		

Поля підзаголовка фрагментації описано в таблиці 5.9.

Табл. 5.9. Поля підзаголовка фрагментації

Ім'я поля	Довжина в бітах	Опис
FC	2	Керування фрагментацією Індицирує стан поля даних (PDU): 00 = фрагментації немає 01 = останній фрагмент 10 = перший фрагмент 11 = проміжний фрагмент
FCN	3	Порядковий номер фрагмента Визначає порядковий номер поточного фрагмента SDU. Це поле збільшується на 1 (по модулі 8) для кожного фрагмента, включаючи не фрагментовані SDU.

Підзаголовок керування GM (Grand Management) містить два байти й використовується SS, щоб реалізувати керування смугою, необхідної BS. Структура підзаголовка керування представлена в таблиці 5.10.

Табл. 5.10. Структура підзаголовка керування

Синтаксис	Розмір	Опис
Підзаголовок Grant Management () {		
if(тип служби диспетчеризації = UGS) {		
SI	1 біт	
PM	1 біт	
Зарезервовано	14 біт	Установлюється рівним 0
}		
else {Комбінований запит}	16 біт	
}		

Опис полів підзаголовка керування представлений в табл. 5.11.

Табл. 5.11. Опис полів підзаголовка керування

Ім'я поля	Довжина в бітах	Опис
PBR	16	Комбінований запит Число байт, запитаних SS для смуги висхідного каналу. Запит смуги ставиться до CID і не включає поля заголовка фізичного рівня.
PM	1	Реєстрація (poll-me) 0 = ніяких дій 1 = використовується SS для запиту реєстрації смуги.
CI	1	Індикатор зсуву (slip) 0 = ніяких дій 1 = використовується SS для вказівки зсуву можливостей висхідного каналу стосовно довжини черги в цьому каналі.

Коли використовується впакування, MAC дозволяє впакувати трохи SDU в один блок MAC PDU. При впакуванні декількох MAC SDU різної довжини, кожний з них забезпечується своїм підзаголовком упакування. Формат підзаголовка впакування описаний у табл. 5.12.

Табл. 5.12. Формат підзаголовка впакування

Синтаксис	Розмір	Опис
Підзаголовок упакування () {		
FC	2 біти	
FSN	3 біти	
Довжина	11 біт	
}		

Опис полів підзаголовка керування представлений в табл.5.13.

Табл. 5.13. Опис полів підзаголовка керування

Ім'я поля	Довжина в бітах	Опис
FC	2	Керування фрагментацією Вказує стан фрагментації поля даних: 00 = без фрагментації 01 = останній фрагмент 10 = перший фрагмент 11 = проміжний фрагмент
FSN	3	Порядковий номер фрагмента Визначає номер фрагмента SDU. Це поле збільшується на 1 (по модулі 8) для кожного фрагмента.
Довжина	11	Довжина в байтах MAC SDU або SDU фрагмента, включаючи двухбайтовий підзаголовок упакування.

Повідомлення керування MAC

Визначено набір керуючих повідомлень MAC. Ці повідомлення транспортуються в блоках даних MAC PDU. Всі керуючі повідомлення MAC починаються з поля *тип повідомлення* й можуть містити додаткові поля. Керуючі повідомлення для базових, ширококомовних і вихідних з'єднань (initial ranging) не можуть бути фрагментовані, або впаковані. Керуючі повідомлення первинного з'єднання можуть бути впаковані й/або фрагментовані. Значення поля, тип повідомлення представлені в табл. 5.14. Керуючі повідомлення не можуть передаватися через транспортні з'єднання.

Табл. 5.14. Значення поля *тип* (керуючих повідомлень MAC)

Тип	Ім'я повідомлення	Опис повідомлення	З'єднання
0	UCD	Дескриптор висхідного каналу	Широкомовне
1	DCD	Дескриптор спадного каналу	Широкомовне
2	DL-MAP	Визначення доступу до спадного каналу	Широкомовне
3	UL-MAP	Визначення доступу до висхідного каналу	Широкомовне
4	RNG-REQ	Запит діапазону	Вихідне або базове
5	RNG-RSP	Відгук діапазону	Вихідне або базове
6	REG-REQ	Запит реєстрації	Первинне керування

7	REG-RSP	Відгук реєстрації	Первинне керування
8	Зарезерв.		
9	PKM-REQ	Запит керування ключем конфіденційності	Первинне керування
10	PKM-RSP	Відгук на запит керування ключем конфіденційності	Первинне керування
11	DSA-REQ	Запит додавання динамічного сервісу	Первинне керування
12	DSA-RSP	Відгук додавання динамічного сервісу	Первинне керування
13	DSA-ACK	Підтвердження додавання динамічного сервісу	Первинне керування
14	DSC-REQ	Запит зміни динамічного сервісу	Первинне керування
15	DSC-RSP	Відгук зміни динамічного сервісу	Первинне керування
16	DSC-ACK	Підтвердження зміни динамічного сервісу	Первинне керування
17	DSD-REQ	Запит анулювання динамічного сервісу	Первинне керування
18	DSD-RSP	Відгук анулювання динамічного сервісу	Первинне керування
19		Зарезервовано на майбутнє	
20		Зарезервовано на майбутнє	
21	MCA-REQ	Запит мультикастингового присвоєння	Базове
22	MCA-RSP	Відгук мультикастингового присвоєння	Базове
23	DBPC-REQ	Запит зміни профілю спадного каналу	Базове
24	DBPC-RSP	Відгук зміни профілю спадного каналу	Базове
25	RES-CMD	Команда скидання	Базове
26	SBC-REQ	Запит базових можливостей SS	Базове
27	SBC-RSP	Відгук базових можливостей SS	Базове
28	CLK-CMP	Порівняння показань мережних годин SS	Широкомовне
29	DREG-CMD	Команда реєстрації або її скасування	Базове
30	DSX-RVD	Повідомлення одержання DSx	Первинне керування
31	TFTP-CPLT	Повідомлення завершення конфігураційного файлу TFTP	Первинне керування
32	TFTP-REP	Відгук завершення конфігураційного	Первинне

		файлу TFTP	керування
33-255		Зарезервовано на майбутнє	

Повідомлення дескриптора спадного каналу (DCD)

DCD періодично передається BS, щоб визначити характеристики фізичного спадного каналу. Параметри, що впливають за ID каналу, і число змін конфігурації представляються у форматі TLV, де поля типу й довжини мають довжину один байт. Формат повідомлення DCD описаний у табл. 5.15.

Табл. 5.15. Формат повідомлення DCD

Синтаксис	Розмір	Опис
DCD_Message_Format () {		
Тип керуючого повідомлення = 1	8 біт	
Ідентифікатор спадного каналу	8 біт	
Число змін конфігурації	8 біт	
Інформація про канал у форматі TLV	перем.	
Початок секції, специфічної для PHY {		
for(i=1; i<=n; i++) {		Для кожного профілю спадного каналу з 1 до n
Downlink_Burst_Profile}		Залежить від PHY
}}}		

BS сформує DCD у форматі табл. 5.15, включаючи всі перераховані нижче параметри:

Число змін конфігурацій

Інкрементується BS на 1 по модулі 256 для будь-якої зміни параметра каналу із заданим дескриптором. Якщо значення цього лічильника надалі DCD залишається тим же, SS може вирішити, що інші поля не змінилися й ігнорувати частину, що залишилася, повідомлення.

Ідентифікатор спадного каналу

Ідентифікатор спадного каналу, до якого ставиться повідомлення. Цей ідентифікатор довільно обирається BS та є унікальним для заданого домену підрівня MAC.

Параметри повідомлення, які впливають за числом змін конфігурації, кодуються у форматі TLV.

Downlink_Burst_Profile має комбіноване кодування TLV, що сполучена з DIUC (Downlink Interval Usage Code) використовуваного фізичного каналу. Кожен Downlink_Burst_Profile являє собою неупорядкований список атрибутів PHY,

закодованих у форматі TLV. Кожному інтервалу за допомогою повідомлення DL-MAP ставиться у відповідність DIUC.

Кожен Downlink_Burst_Profile у повідомленні DCD містить наступні параметри:

- Тип модуляції
- Тип коду FEC
- Довжина останнього коду
- Поріг обов'язкового виходу DIUC
- Поріг мінімального запису DIUC
- Присутність преамбули

Якщо тип коду FEC дорівнює 1, 2 або 3 Downlink_Burst_Profile буде містити також

- RS байти даних (DO)
- RS байти парності (R)

Якщо тип коду FEC дорівнює 2, то Downlink_Burst_Profile буде містити тип коду ВСС. Якщо ж тип коду FEC дорівнює 4, то Downlink_Burst_Profile буде містити тип коду ряду ВТС, тип коду стовпчика й тип інтерлівінга ВТС.

Повідомлення прив'язки спадного каналу (DL-MAP)

Повідомлення DL-MAP визначає доступ до інформації про спадний канал. Якщо довжина повідомлення не дорівнює цілому числу байтів, значення поля LEN у заголовку MAC округляється до найближчого цілого. Формат повідомлення DL-MAP описаний у табл. 5.16. Повідомлення містить наступні параметри:

Синхронізація РНУ

Поле синхронізації РНУ залежить від специфікації фізичного каналу.

Лічильник DCD

Відповідає числу змін конфігурації DCD.

Ідентифікатор BS

Ідентифікатор базової станції являє собою 48-бітовий код, що однозначно визначає BS. Старші 24 біта є ідентифікатором оператора.

Число елементів

Число наступних інформаційних елементів

Кодування іншої частини DL-MAP залежить від специфікації РНУ, цієї частини може й не бути.

Табл. 5.16. Формат повідомлення DL-MAP

Синтаксис	Розмір	Опис
DL-MAP_Message_Format() {		
Тип керуючого повідомлення = 2	8 біт	
Поле синхронізації PHU	перем.	
Лічильник DCD	8 біт	
Ідентифікатор BS	48 біт	
Число елементів DL-MAP n	16 біт	
Початок секції, специфічної для PHU {		
For(i=1; i<=n; i++) {		Для кожного елемента DL-MAP з 1 до n
DL-MAP_Information_Element()	перем.	
if!(границя байта) {		
4 біти заповнювача }		До границі байта
}}}		

Повідомлення дескриптора висхідного каналу

Дескриптор висхідного каналу (UCD) періодично передається BS, для того щоб визначити характеристики фізичного висхідного каналу. Окреме повідомлення UCD передається для кожного висхідного каналу. BS передає повідомлення UCD у форматі, показаному в таблиці 5.17. Повідомлення містить наступні параметри:

Лічильник змін конфігурації

Збільшується BS на 1 (по модулі 256), щораз, коли виробляється зміна будь-якого параметра каналу з даним дескриптором. Якщо значення лічильника для чергового UCD залишається тим же, SS вирішує, що інші поля не змінені й можна ігнорувати частину, що залишилася, повідомлення.

Розмір мінідомена

Розмір n мінідоменів для висхідного каналу в одиницях фізичних доменів. Припустимими значеннями є $n=2^m$, де m дорівнює цілому з діапазону 0-7.

Ідентифікатор висхідного каналу

Ідентифікатор каналу, до якого ставиться повідомлення. Ідентифікатор довільно вибирається BS й є унікальним у межах домена субрівня MAC.

Початок відстроки передачі

Розмір вихідного вікна відстроки для вихідного суперництва за діапазон, виражений через ступінь 2. Значення n може лежати в інтервалі 0-15 (старші біти можуть не використатися й прирівнюватися нулю).

Кінець відстроки передачі

Розмір кінцевого вікна відстрочки передачі для вихідного суперництва за діапазон, виражений через ступінь 2. Значення n може лежати в інтервалі 0-15 (старші біти можуть не використатися й прирівнюватися нулю).

Запит початку відстрочки

Запит розміру вихідного вікна відстрочки для даних вихідного суперництва за діапазон, виражений через ступінь 2. Значення n може лежати в інтервалі 0-15 (старші біти можуть не використатися й прирівнюватися нулю).

Кінець відстрочки передачі

Запит розміру кінцевого вікна відстрочки передачі для вихідного суперництва за діапазон, виражений через ступінь 2. Значення n може лежати в інтервалі 0-15 (старші біти можуть не використатися й прирівнюватися нулю).

Табл. 5.17. Формат повідомлення UCD

Синтаксис	Розмір	Опис
UCD_Message_Format () {		
Тип керуючого повідомлення = 0	8 біт	
Ідентифікатор висхідного каналу	8 біт	
Лічильник змін конфігурації	8 біт	
Розмір мінідомена (minislot)	8 біт	
Початок відстрочки передачі	8 біт	
Кінець відстрочки передачі	8 біт	
Запит початку відстрочки	8 біт	
Запит кінця відстрочки	8 біт	
Інформація про канал у кодуванні TLV	перем.	
Початок секції, специфічної для RHY {		
For(i=1; i<=n; i++) {		Для кожного профілю висхідного каналу з 1 до n
Uplink_Burst_Profile }	перем.	
} }		

Щоб забезпечити гнучкість, інші параметри повідомлення кодуються у форматі TLV.

Uplink_Burst_Profile має комбіноване кодування TLV, що сполучена з UIUC (Uplink Interval Usage Code) використовуваного фізичного каналу. Кожен Uplink_Burst_Profile являє собою неупорядкований список атрибутів RHY, закодованих у форматі TLV. Кожному інтервалу за допомогою повідомлення UL-MAP ставиться у відповідність UIUC.

5.2 Мережі WiMAX мобільного доступу IEEE 802.16e

Загальні відомості про стандарт IEEE 802.16e

Версія стандарту IEEE 802.16e, опублікована на сайті Intel Corporation, визначене як тимчасове доповнення до стандарту IEEE 802.16-2004 для локальних і регіональних обчислювальних мереж. У стандарті IEEE 802.16e дані доповнення для фізичного й MAC-рівнів керування доступом для змішаних, стаціонарних і мобільних операцій на ліцензованих частотах, описані відмінності радіоінтерфейса для стаціонарних і мобільних систем широкосмугового бездротового доступу.

Зауваження

Вказівки для редагування, що втримуються в стандарті 802.16e у вигляді доповнень/виправлень, визначають, як привести матеріал до існуючого базового стандарту IEEE Std 802.16-2004.

Вказівки для редагування відзначені *напівжирним курсивом*. Використано наступні вказівки: *змінити*, *видалити*, *вставити* й *замінити*. *Змінити* використовується для внесення невеликих виправлень в існуючий текст або таблиці. Вказівка для редагування визначає місце зміни й описує, що саме потрібно змінити, використовуючи закреслювання (для видалення старого матеріалу) і підкреслення (для додавання нового матеріалу). *Видалити* використовується для видалення існуючого матеріалу. *Вставити* використовується для додавання нового матеріалу, не зачіпаючи при цьому вужеві існуючий матеріал. Вставка тексту може зажадати перенумерації. У цьому випадку вказівки по перенумерації дані у вказівці для редагування. *Замінити* використовується для внесення істотних змін у текст, розділи параграфу, таблиці або малюнки шляхом видалення існуючого матеріалу й заміни його новим. Редакторські замітки не будуть перенесені в майбутні видання, тому що зміни будуть наведені у відповідність базовому стандарту.

5.2.1. Загальний огляд

Предметний охват: Даний документ вносить у стандарт IEEE Std 802.16-2004 доповнення, що дозволяють підтримувати абонентські пункти, що рухаються із транспортною швидкістю, і, таким чином, точно визначає систему змішаного, стаціонарного й мобільного широкосмугового бездротового доступу. Визначено функції підтримки передачі обслуговування між базовими станціями на високому рівні. Дія обмежена ліцензованими частотами, що підходять для мобільного зв'язку до 6 ГГц. Певні стандартом IEEE Std 802.16-2004 характеристики абонента зміні не підлягають.

Ціль: Даний стандарт покликаний розширити ринок рішень для широкополосного бездротового доступу, використовуючи переваги власної мобільності бездротових засобів. Він заповнить розрив між дуже високою швидкістю передачі даних у бездротових локальних обчислювальних мережах і

високорухомих системах стільникового зв'язку. Він буде підтримувати стаціонарні й мобільні служби як для підприємництва, так і для споживчого ринку.

5.2.2. Базова мережна модель для мобільних систем зв'язку

При описі процедур функціонування мережі й пристроїв у стандарті 802.16e використані додаткові терміни й визначення.

Визначення

Мобільна станція користувача MSS: Мобільний термінал користувача, що підтримує режим передачі обслуговування (хендовера) при переході із зони обслуговування однієї базової станції в зону обслуговування іншої базової станції. Мобільний термінал може бути встановлений на транспортному засобі, що рухається. Використається й інше визначення: **рухлива станція (mobile station, MS):** станція в мобільній службі, використання якої передбачається під час руху або зупинок у невизначених крапках.

Анкерна BS: Анкерна BS повинна виділяти ресурси для MSS. т. е. призначені основні CID, CID первинного керування, CID вторинного керування й інформаційні CID для MSS. MSS повинна бути завжди синхронізована з BS. MSS повинна виконувати визначення відстані тільки до анкерної BS. Для FBSS АЛЕ анкерна BS є обслуговуючою BS, що призначена для передачі/одержання даних к/от MSS із заданим фреймом. Для SHO MSS відслідковує анкерну BS з метою одержання контрольної інформації DL, тобто DL_MAP, UL_MAP, FCH і широкомовних повідомлень DL.

Для SHO або FBSS, що підтримують MSS, це BS, де зареєстровано MSS, з якої вона синхронізована, здійснює визначення відстані й відслідковує контрольну інформацію в DL. Для FBSS, що підтримують MSS, це обслуговуюча BS, що призначено для передачі/одержання даних к/от MSS із заданим фреймом.

Сусідня BS: Для будь-якої MSS сусідня BS — це BS (на відміну від обслуговуючої BS), що сходиться передача якої може бути дитектована MSS.

Обслуговуюча BS: Для будь-якої рухливої абонентської станції (MSS) обслуговуюча BS — це BS, у якій MSS має саму останню завершену реєстрацію при вході в мережу або по завершенні АЛЕ.

Цільова BS: BS, у якій MSS має намір зареєструватися по закінченні АЛЕ.

Активний набір: Активний набір застосуємо до SHO й FBSS. Активний набір містить список активних BS для MSS. Активний набір управляється MSS й BS.

Активна BS: Активна BS інформована про можливості MSS, параметрах безпеки, службових потоках і повній інформації в контексті MAC. Для SHO MSS передає/одержує дані к/от всіх активних BS в активному наборі.

Індекс FA: Призначення логічного індексу FA, обумовленого мережею. Призначення індексу FA використовується в комбінації з конфігураційною інформацією, обумовленої оператором, що надається MSS методами, огляд яких виходить за рамки даного стандарту.

Швидке перемикання BS (fast BS switching, FBSS): Перемикання BS, що використовує розмаїтість вибору й швидкий механізм комутації для поліпшення якості з'єднання. MSS тільки передає/одержує дані к/от однієї з активних BS (анкерних BS) із заданим фреймом. Анкерна BS може мінятися від фрейму до фрейму, залежно від схеми вибору BS.

Нерухома абонентська станція (fixed subscriber station, FSS): Абонентська станція, що не підтримує встановлення зв'язку, перебуваючи в русі.

Призначення частот (frequency assignment, FA): Призначення частот (FA) означає логічне завдання центральної частоти DL і пропускну здатності каналу, повідомлюваних BS.

Передача обслуговування (handover, АЛЕ): Процес, при якому MSS переміщується з радіоінтерфейса, надаваного однієї BS, у радіоінтерфейс, надаваний інший BS. Визначено два варіанти АЛЕ:

- АЛЕ з перемиканням з розривом до включення: АЛЕ, при якому цільова BS починає обслуговування після розриву зв'язку з попередньої обслуговуючої BS;
- АЛЕ з перемиканням з розривом після включення: АЛЕ, при якому цільова BS починає обслуговування до розриву зв'язку з попередньої обслуговуючої BS.

Період огляду: Період часу, призначений для відстеження MSS сусідньої BS з метою визначення можливостей BS для здійснення АЛЕ.

Передача обслуговування зі збереженням з'єднання (soft handover, SHO):

Передача обслуговування, при якій дві або більше BS передають MSS однакові MAC/PHY PDU у той самий відрізок часу, щоб MSS могла здійснити додавання рознесених сигналів. SHO в UL визначена як дві або більше BS, що одержують (детектуючі, що декодують) від MSS у той самий відрізок часу. Додавання рознесених сигналів з одержуваних PHY фреймів виробляється серед BS.

Ключ шифрування групового ключа (group key encryption key, GKEK): записаний аббревіатурою GKEKEK, що отриманий від АК.

Ключ шифрування групового трафіка (group traffic encryption key, GTKK): записаний аббревіатурою GKEK.

Об'єкти

Базова мережна модель містить у собі групи BS (base station, базова станція), що надають мережні послуги (не обов'язково суміжних) для авторизації MSS. В географічному регіоні. Групи BS, які розділяють адміністративну приналежність і підключені до магістралі, ставляться до мережі провайдера. В одному регіоні може співіснувати, безліч мереж провайдерів з різною конструкцією, виконанням, володінням/керуванням. Мережі провайдера можуть застосовувати спеціалізовані сервери для AAA (Authorization, Authentication and Accounting - Авторизація, Аутентифікація й Облік), керування, постачання й виконання інших функцій. Сервери, відповідальні за ці функції, скрізь у даній специфікації називаються серверами аутентифікації й авторизації послуг (ASA-сервери). Провайдер може розгорнути один або безліч ASA-серверів централізованим або розподіленим образом. Операції між базовими станціями й ASA-серверами не обговорені. На рис. 5.13 показана еталонна мережна модель у площині керування.

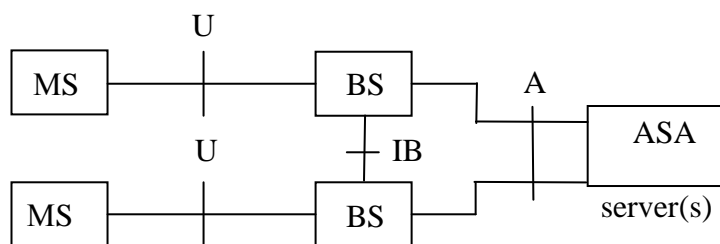


Рис. 5.13. Логічна еталонна мережна модель, площина керування

У площині керування мережної моделі присутні базові крапки, показані в табл. 5.18. Об'єкти, пов'язані з мобільністю, описані в табл. 5.19.

Таблиця 5.18. Базові крапки в площині керування

Базова крапка	Елементи, зазначені в 802.16e	Коментарі
U	Операції MAC- (разом з CS) і PHY-рівнів, включаючи обмін повідомленнями для підтримки мобільності	
IB	Повідомлення, передані від однієї BS до іншої	Транспортний протокол точно не визначений
A	Повідомлення, що виконують функцію аутентифікації й авторизації послуг MSS	Транспортний протокол точно не визначений

Таблиця 5.19. Об'єкти, пов'язані з мобільністю

Об'єкт	Опис
MSS	Mobile Subscriber Station — станція рухливого абонента, містить MAC-(CS) і PHY -рівні
BS	Base Station — базова станція

ASA-сервер(ы)	Authentication and Service Authorization Server - сервер аутентифікації й авторизації послуг обслуговує всю мережу оператора. Ці сервери необов'язкові й можуть бути впроваджені як розподілені об'єкти *
---------------	---

Залежно від конфігурації мережі провайдера й адміністративної політики MSS може здійснювати передачу обслуговування (АЛЕ, handover) від однієї BS до іншої. Схема мережі провайдера для керування передачею обслуговування може бути локалізована у відповідних BS або ж може бути розподілена й/або містити в собі ASA-сервери.

На рис. 5.14 показаний приклад, де дві BS підключені до магістралі оператора. BS#1 - обслуговуюча BS для MSS. BS#2 - сусідня BS. Якщо MSS наближається ближче до BS#2, як це доведено зафарбованою стрілкою, то BS#2 може стати цільовий BS для передачі обслуговування.

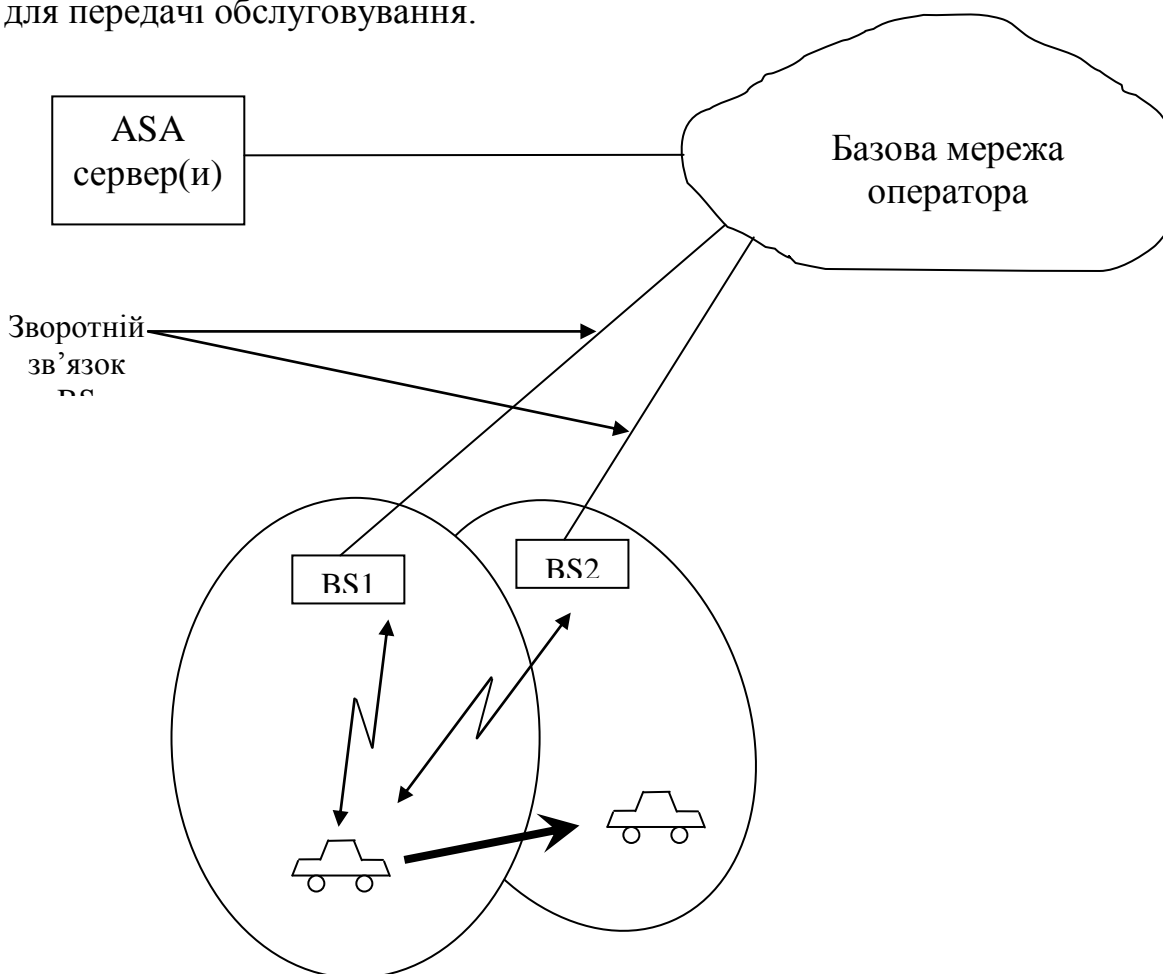


Рис. 5.14. Приклад мережної моделі передачі обслуговування

Процес передачі обслуговування, при якому MSS переміщається із зони з радіоінтерфейсом, надаваним однією базовою станцією, у зону з радіоінтерфейсом, надаваним іншою базовою станцією, визначений у специфікації 6.3.20.2 стандарту IEEE 802.16e.

Підтримка передачі обслуговування визначається полем *тип* = 19 у форматі кадру. Це поле показує (див. табл. 5.20), який(е) тип(и) АЛЕ підтримують BS й MSS. Біт зі значенням 0 означає "не підтримує", а значення 1 - "підтримує".

Таблиця 5.20. Бітові значення підтримки передачі обслуговування

Тип	Довжина	Значення	Область визначення
19	1	Bit #0: SHO/FBSS АЛЕ не підтримується, коли значення " 1 ". Коли цей біт встановлен на " 1 ", BS повинна ігнорувати всі інші біти.	REG_REQ REG_RSP

Таблиця 5.20 (закінчення)

Тип	Довжина	Значення	Область визначення
		Bit #1: FBSS/SO DL RF ущільнення підтримується з контрольним одиночним MAP від вузловий BS, коли цей біт установлений в " 1 ". Bit #2: FBSS/SO DL RF ущільнення підтримується з контрольними MAP від всіх активних BS, коли цей біт установлений в " 1 ". Bit #3: SHO DL плавне ущільнення підтримується з контрольним одиночним MAP від вузловий BS, коли цей біт установлений в " 1 ". Bit #4: SHO DL плавне ущільнення підтримується з контрольними MAP від всіх активних BS, коли цей біт установлений в " 1 ". Bit #5: FBSS/SO UL одиночна передача. Bit #6: SHO UL множинна передача. Bit #7: службові, повинні установлений в нуль	

Тривалість інформації (табл. 5.21) про з'єднання MSS, що буде утримана в обслуговуючої BS, визначається значенням RTM (Resource Retain Time). BS повинна запустити таймер Resource Retain Time по повідомленню від MSS про майбутню спробу здійснити АЛЕ за допомогою MOB_NO-IND або по виявленню обриву зв'язку з MSS. Одиниця цього значення - 100 мс.

Таблиця 5.21. Тривалість утримання інформації при хендовері

Тип	Довжина	Значення	Область визначення
50	2	Кратно 100 мс. 200 мс рекомендується, як значення за замовчуванням	REG_RSP

Процес передачі обслуговування при хендовері представлений алгоритмами, наведеними на рис. 5.15-5.17.

Передача обслуговування по запиті MSS

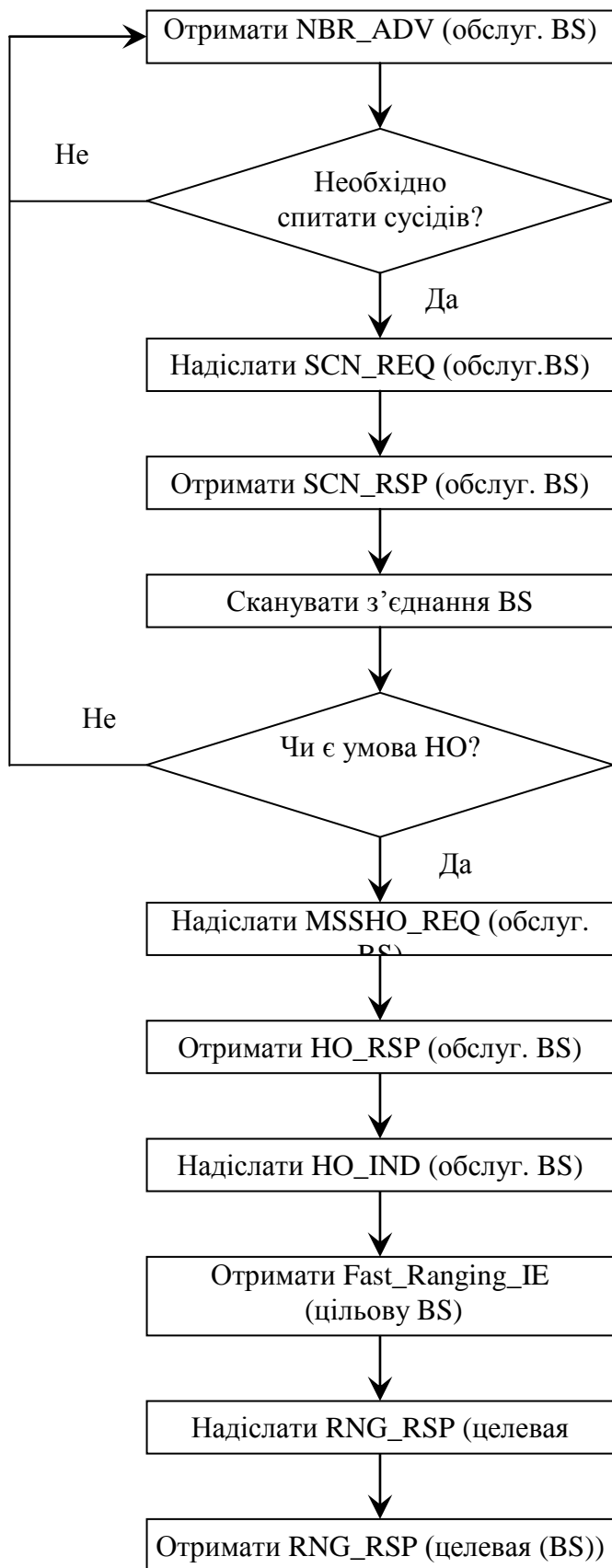


Рис. 5.15. Блок-схема процесу HO в MSS по запиті MSS

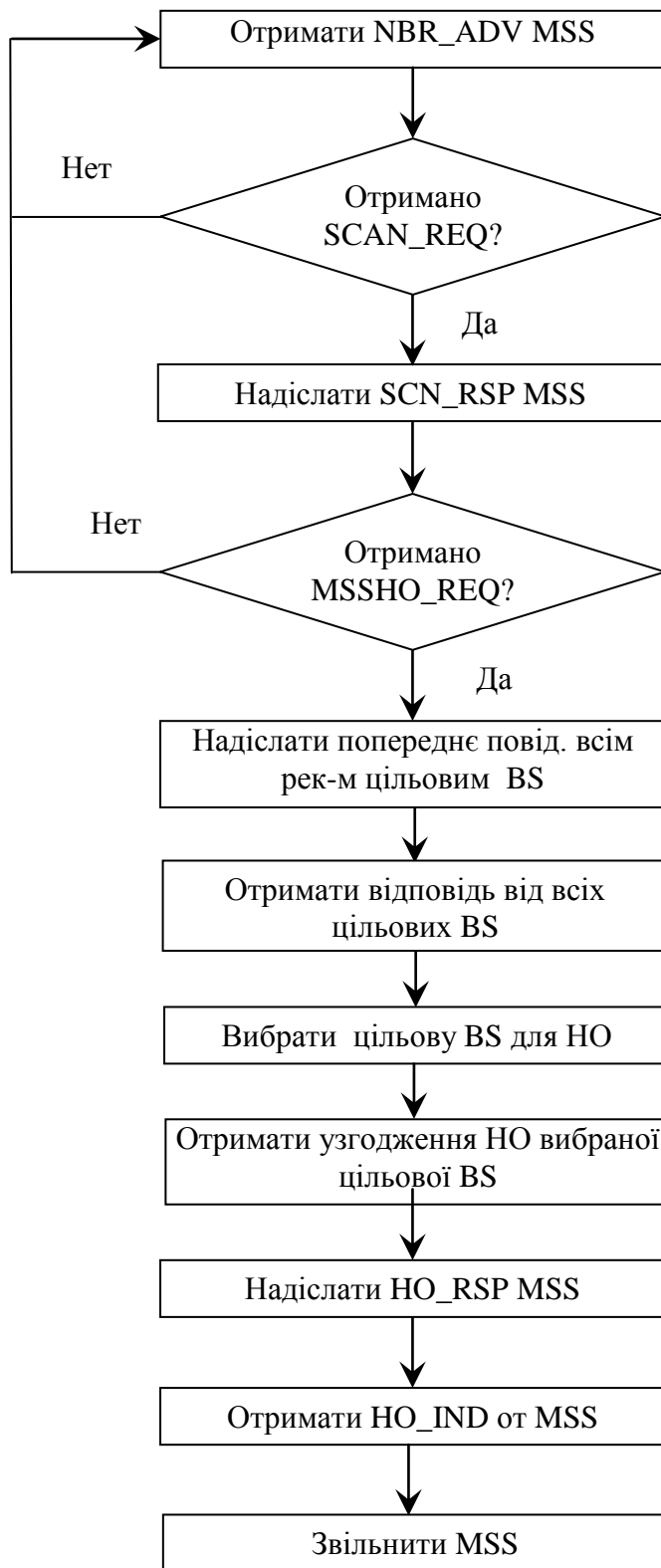


Рис. 5.16. Блок-схема процесу АЛЕ в обслуговуючій BS по запиті MSS

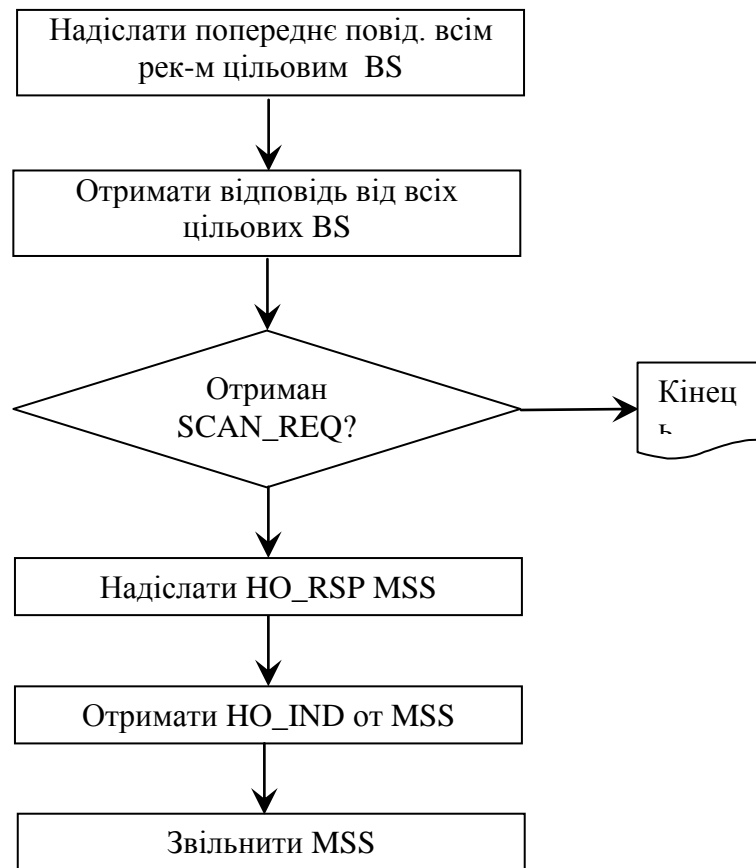


Рис. 5.17. Блок-схема процесу АЛЕ в обслуговуючій BS по запиті MSS

Передача обслуговування по запиті BS

Блок-схема процесу АЛЕ в MSS по запиті BS представлена на мал. 6.26.

Блок-схема процесу АЛЕ в обслуговуючій BS по запиті BS представлена на рис 6.27.

5.2.3. Визначення дальності на основі OFDMA

У випадках використання мережі WirelessMAN-OFDMA PHY рівень MAC може призначати одиночний канал для визначення дальності користувальницької станції від базової. Визначення дальності необхідно для організації хендовера й керування потужністю передавачів. Така процедура може бути ініційована з боку мобільної станції. Канал визначення дальності складається з однієї або більше груп по шести суміжних підканалів у кожній групі. Групи визначені, починаючи з першого підканала. Канал визначення дальності може бути складений також з восьми суміжних підканалів.

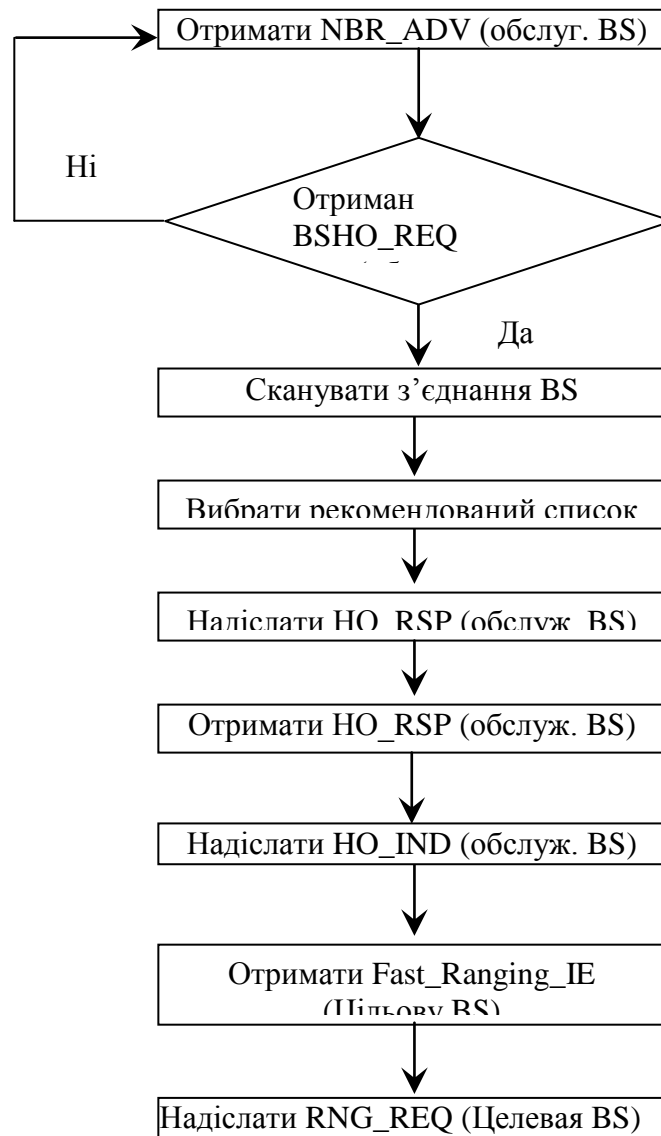


Рис. 5.18. Блок-схема процесу АЛЕ в MSS по запиті BS

Індекси підканалів, що становлять канал визначення дальності, зазначені в повідомленні UL MAP. Щоб виконати процедуру визначення дальності, кожен користувач довільно вибирає для передачі один з кодів визначення дальності з банку заданих двійкових кодів. Ці коди потім за допомогою двійкової фазової маніпуляції модулюються в, що піднесуть усередині каналу визначення дальності з розрахунку один біт на що піднесе.

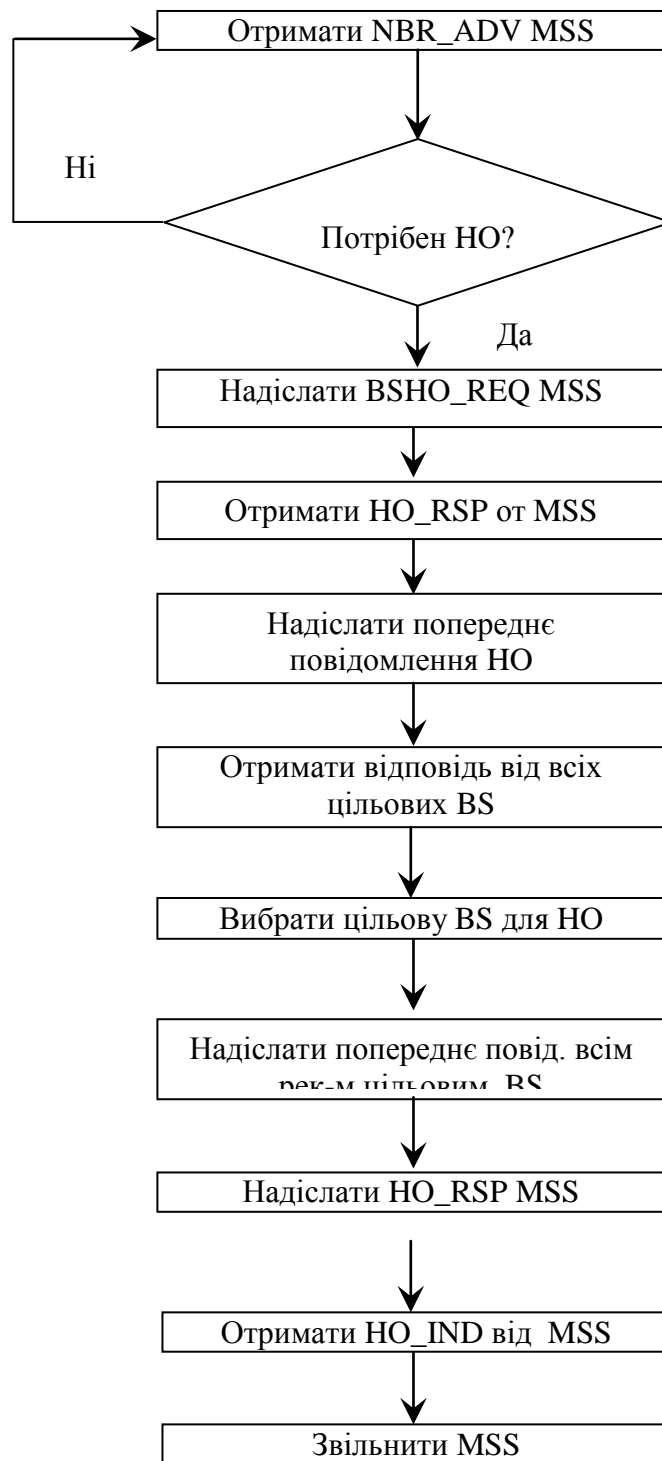


Рис. 5.19. Блок-схема процесу АЛЕ в обслуговуючій BS по запиті BS

У деяких обставинах, таких як повторний вхід у мережу до іншій BS, у ситуації припинення обслуговування, коректування місця розташування в неробочому режимі або швидкому відновленні виклику, які вимагають більше UL-ресурсів для RNG-REQ через додатковий 23 байтів, що додають до довжини кортежу НМАС, мобільна станція може використати в процедурі хендовера код визначення дальності BS, що одержує АЛЕ -код визначення дальності, повинна

виділити більшу пропускну смугу для MSS, достатню для того, щоб відправити RNG-REQ з кортежем HMAC.

Число доступних кодів визначення дальності — 256. Вони пронумеровані 0..255. Кожна BS використає підгрупу цих кодів, де підгрупа визначається числом S , $0 < S < 256$. Група кодів буде перебувати між 5 й $((S + O + N + M + L) \bmod 256)$.

- Перші W генеруючих кодів призначені для початкового визначення дальності. Наприклад, за замовчуванням у випадку двох підканалів у каналі визначення дальності, синхронізація PRBS 144 а $(S \bmod 256)$ раз до 144 х $((S + L) \bmod 256)$ — 1 раз.
- Наступні M кодів — для періодичного визначення дальності. Наприклад, за замовчуванням у випадку двох підканалів у каналі визначення дальності синхронізація PRBS 144 х $((S + N) \bmod 256)$ раз до 144 л $((S + N + M) \bmod 256)$ — 1 раз.
- Наступні L кодів — для запиту смуги пропущення. Наприклад, за замовчуванням у випадку двох підканалів у каналі визначення дальності синхронізація PRBS 144 а $((S + N + M) \bmod 256)$ раз до 144 ч $((S + N + M + L) \bmod 256)$ — 1 раз.
- Наступні PPO кодів — для визначення дальності при передачі обслуговування. Наприклад, за замовчуванням у випадку двох підканалів у каналі визначення дальності синхронізація PRBS 144 х $((S + N + M + L) \bmod 256)$ раз до 144 х $((S + N + M + L + PPO) \bmod 256)$ — 1 раз.

Для 128-краткової FFT BS може виділити менш 6 (або 8 у випадку необов'язкової PUSC або AMC) підканалів для визначення дальності/ розміщення BW-запиту. В цьому випадку MSS повинна пред'явити код визначення дальності, як показано нижче (начебто виділені 6/8 підканалів), але модулювати тільки тональні сигнали, розташовані в підканалів (так що останні біти кодів визначення дальності не передаються).

При первісному входженні користувальницької станції в мережу будь-який MSS, що бажає синхронізуватися із системним каналом, робить початкове визначення дальності. Передача при початковому визначенні дальності (або визначенні дальності при передачі обслуговування) здійснюється під час двох безупинно наступних один за одним символів.

Той самий код (X) визначення дальності передається по каналі визначення дальності під час кожного символу без фазових розривів між двома символами. Ілюстрація тимчасової області передачі коду при початковому визначенні дальності (або визначенні дальності при передачі обслуговування) показана на рис. 5.20.

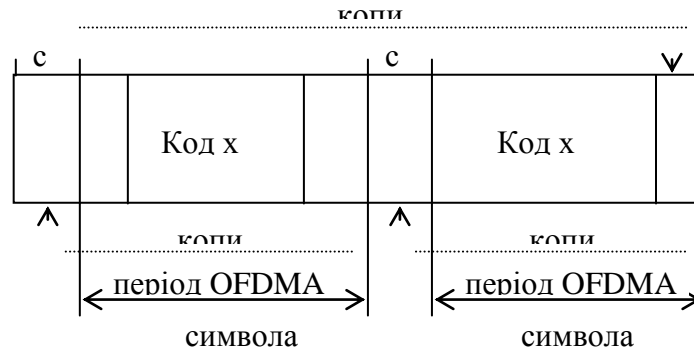


Рис. 5.20. Передача коду при початковому визначенні дальності для OFDMA

BS може виділити два сусідніх слота початкові визначення дальності (або визначення дальності при передачі обслуговування), у які MSS повинен передати коди початкового визначення дальності (початковий код завжди повинен бути кратним 2), як показано на мал. 5 21.

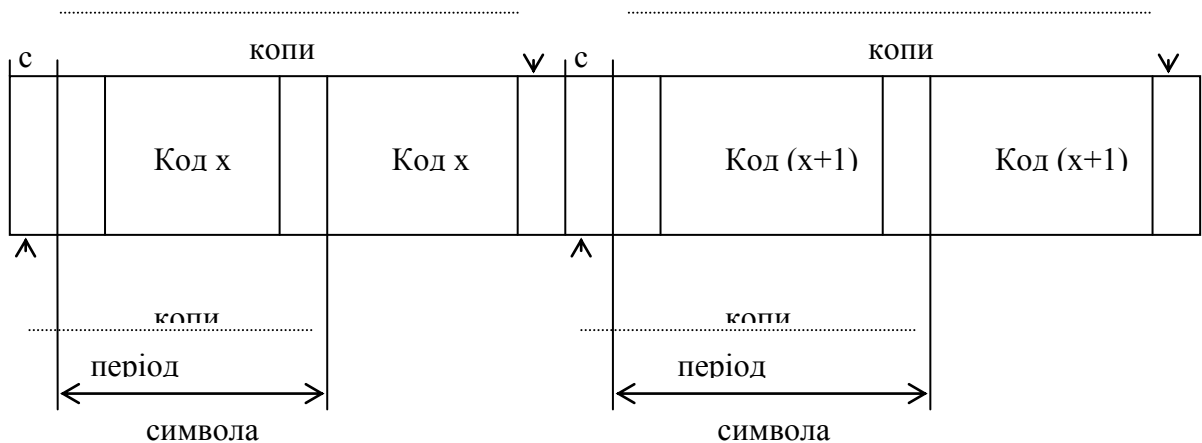


Рис. 5.21. Передача коду при початковому визначенні дальності для OFDMA з використанням двох послідовних початкових кодів визначення дальності

5.2.4. Попередня аутентифікація

Після обміну HO-REQ/RSP мобільної абонентської станції може знадобитися попередня аутентифікація, що впливає на швидку передачу обслуговування. MSS, що потрібно попередня аутентифікація, повинна передати PKM_PREAUTH-REQ. Базова станція, прийнявши повідомлення PKM-AUTH-REQ, повинна відповісти повідомленням PKM-PREAUTH-RSP або повідомленням PKM_PREAUTH-REJECT. BS може відправити надаване добровільно повідомлення PKM AUTH-RSP. PKM-PREAUTH-RSP показує, що обрана BS постачено РМК, що зіставляє дійсність падаючої запит MSS.

Попередньо аутентифікована MSS може пропустити процедури авторизації й стадії EAP при вході в мережу. Матеріал первинного ключа доступний в BS, і

MSS повинна розрахувати РМК, як це визначено в ієрархії ключів 7.X.X.X. Отже, обчислення АК буде засноване на РМК, а не на РАК, що погодиться із правилами обчислення в ключовій ієрархії РКМv2.

5.2.5. Механізм керування потужністю

Механізм керування потужністю реалізується за допомогою розімкнутої системи, у якій відсутній зворотний зв'язок по взаємному регулюванню потужності між BS й MSS. Керування потужністю в розімкнутій системі виробляється за допомогою команд PCS RSP. Потужність на кожній під несучій повинна підтримуватися передачею UL. Таке керування потужністю розімкнутої системи повинне бути застосоване до всіх пакетів при з'єднанні "нагору".

$$L + C/N + NI < 10 \log_{10}(R) + \text{Offset_SS}_{\text{perSS}} + \text{Offset_BS}_{\text{perSS}},$$

де:

- P — рівень потужності TX (dBm) на під несучу для поточної передачі;
- L — теоретичні втрати при поширенні UL. Містять у собі коефіцієнт підсилення антени при прийомі/передачі й втрати на трасі;
- C/N — нормоване відношення "несуча/шум" коефіцієнта модуляція/FEC для поточної передачі, як представлено в таблиці 332 стандарту. Таблиця 332 може бути модифікована UCD (заміна нормованого C/N). На додаток, значення нормованого відношення C/N для області UL ASK й QPSK 1/3 також можуть бути отримані за допомогою UCD;
- R — кількість повторень для коефіцієнта модуляції/FEC;
- NI — теоретичний середній рівень потужності (dBm) шуму й інтерференції на піднесе в BS;
- $\text{Offset_SS}_{\text{perSS}}$ — поправочний член для відводу потужності, обумовленого SS. Він управляється SS. Початкове значення дорівнює нулю;
- $\text{Offset_BS}_{\text{perSS}}$ — поправочний член для відводу потужності, обумовленого SS. Він управляється BS за допомогою повідомлень керування потужністю. Початкове значення дорівнює нулю.

Фактичні установки потужності повинні бути квантовані до найближчого застосовного значення, як це зазначено в специфікації (8.4.12.1). Для кожної передачі SS повинна обмежувати потужність для відповідності спектральним маскам і вимогам EVM. SS може регулювати $\text{Offset_SS}_{\text{perSS}}$ у межах діапазону:

$$\text{Offset_Bound}_{\text{lower}} \leq \text{Offset_SS}_{\text{perSS}} \leq \text{Offset_Bound}_{\text{upper}}$$

де:

- $\text{Offset_Bound}_{\text{upper}}$ — верхня границя $\text{Offset_SS}_{\text{perSS}}$;
- $\text{Offset_Bound}_{\text{lower}}$ — нижня границя $\text{Offset_SS}_{\text{perSS}}$.

Або ж $Offset_SS_{perSS}$ може обновлятися автоматично на основі квитирування/негативного квитирування пакетів у з'єднанні "нагору" усередині обумовленого діапазону.

На додаток BS може управляти $Offset_BS_{perSS}$ використовуючи повідомлення PCS_RSP (пункт стандарту 6.3. 2.3.58), Швидке Керування Потужністю (FPC. Fast Power Control) повідомлення (пункт стандарту 6.3. 2.3.34) і Керування Потужністю IE (пункт стандарту 8.4. 5.4. 5). У цьому режимі повинні накопичуватися значення керування потужністю, що доставляють повідомленнями керування потужністю від PMC_RSP, що віддає розпорядження SS про використання керування потужністю розімкнутої системи. Накопичене значення керування потужністю повинне бути використане для $Offset_BS_{perSS}$.

Спектральна нерівномірність передавача не повинна виходити за межі маски. Абсолютна різниця між сусідніми піднесучими не повинна перевищувати 0,1 дБ, за винятком випадків навмисного посилення або блокування що піднесуть, звукових символів CS1T і невиділених підканалів скорочення PAPR.

Чутливість приймача при різних видах модуляції повинна відповідати значенням, наведеним у табл. 5.22.

Таблиця 5.22. Умови SNR для приймача.

Модуляція	Коефіцієнт кодування	SNR приймача, дБ
QPSK	1/2	9,4
	3/4	11,2
16-QAM	1/2	16,4
	3/4	18,2
64-QAM	2/3	22,7
	3/4	24,4

5.2.6. Шифрування відновлень CID

MSS має кодову таблицю, що дозволяє обновити потік обслуговування й інформацію про з'єднання, щоб MSS могла продовжити користування послугою після передачі її обслуговування нової BS. Значення поля *tin* у форматі кадру при відновленні (CID update) дорівнює 16.

Таблиця значень TLV (табл. 5.23) повинна з'являтися в кожному TLV при CID update.

Таблиця 5.23. Значення полів при відновленні CID

Ім'я	Тип (1 байт)	Довжина (1 байт)	Значення (змінна довжина)
New_CID	16.1	2	Новий CID після передачі обслуговування нової BS
Old_CID	16.2	2	Старий CID перед передачею обслуговування від старої BS

Наступний елемент (табл. 5.24) TLV може з'являтися в ЦЮ update TLV.

Таблиця 5.24. Значення полів в CID update TLV

Ім'я	Тип (1 байт)	Довжина (1 байт)	Значення (змінна довжина)
Connection Info (інформація про з'єднання)	16.3	змінна	Якщо зміниться кожний з параметрів потоку обслуговування, то в кодуєч TLV додаються змінні параметри потоку обслуговування. Cobnection_Info - це складене значення TLV, що інкапсулює змінні параметри потоку обслуговування. Всі правила й настроювання до параметрів при використанні в повідомленні DSC-RSP, застосовуються також до інформації, інкапсульованої в TLV

5.2.7. Порядок розподілу IP-адрес

Порядок розподілу IP-адрес визначається значенням $min = 23$ відповідно до табл. 5.25.

Таблиця 5.25. Розподіл IP-адрес

Тип	Довжина	Значення
23	1	bit #0: DHCP bit #1: Мобільний IPv4 bit #2: DHCPv6 bit #3: IPv6 Stateless Address Autoconfiguration bits #4-7: службові, повинне бути установлене-установлено в нуль

5.2.8. Формування кадру OFDMA

У режимі OFDMA активні що піднесуть підрозділяються на підмножини що піднесуть. Кожна підмножина називається підканалом. У лінії вниз підканал може призначатися для різних груп приймачів. У лінії нагору передавачу може приписуватися один або більше підканалов, кілька передавачів можуть передавати одночасно. Що піднесуть, формуючі один підканал, можуть (не обов'язково повинні) бути сусідніми по частоті.

Символ розділяється по логічним підканалам, щоб підтримувати масштабованість множинного доступу й розширену обробку антенного сигналу.

Вихідні параметри:

- BW -номінальна ширина підканала;
- $N_{\text{исп}}$ — число використовуваних підканалів, що включає користувачів із прямою видимістю;
- n — фактор дискретизації. Це параметр разом з BW й $N_{\text{исп}}$ визначає рознесення що піднесуть і тривалість корисного символу. Значення встановлюється рівним $8/7$;
- G — це відношення тривалості циклічного префікса до корисного часу. Можуть підтримуватися співвідношення $1/32$, $1/16$, $1/8$ й $1/4$.

Одержувані параметри, обумовлені з вихідних:

- N_{FFT} — це найменший ступінь підстави 2, більша чим $N_{\text{исп}}$;
- F_{Δ} — поріг від $(n \cdot BW/8000) \times 8000$ — частота дискретизації;
- $\Delta f = F_s/N_{\text{FFT}}$ — рознесення що піднесуть;
- $T_b = 1/\Delta f$ -тривалість корисної частини символу;
- $T_g = G \cdot T_b$ — тривалість циклічного префікса; f
- $T_s = T_b + T_g$ — тривалість символу OFDMA;
- T_b/N_{FFT} -період дискретизації.

Слот й область даних

Слот на фізичному рівні OFDMA визначений вказівкою часу й розміру підканала. Підканали є мінімально можливими одиницями розміщення даних. Розмір слота залежить від структури символу OFDMA, що різна в лінії нагору або вниз в FUSC й PUSC і для розподіленої перестановки що піднесуть, і для перестановки сусідніх що піднесуть.

- Для лінії вниз в FUSC, що використає розподілену перестановку що піднесуть, один слот - це один підканал для одного OFDMA-символу.
- Для лінії вниз в PUSC, що використає розподілену перестановку що піднесуть, один слот — це підканал на 2 OFDMA-символи.
- Для лінії нагору PUSC, що використає одну з комбінацій що піднесуть, один слот - це один підканал на три символи OFDMA.
- Для ліній униз і нагору, що використають перестановку сусідніхпіднесучих, один слот - це один подканал на один символ OFDMA.

Область даних в OFDMA — це двовимірне розміщення групи наступних один за одним підканали у групі, що йдуть один за одним символів OFDMA. Область даних може передаватися від BS як передача на 1 або групу SS.

Сегмент — це підрозділ безлічі що нараховує підканали OFDMA, що може включати взагалі всі підканали. Один сегмент використовується для організації передачі одного екземпляра MAC.

Зони перестановки — це кількість наступних один за одним символів OFDMA у лініях нагору й униз, які піддаються перестановкам (переміщенням) при формуванні тих або інших підканалів.

У ліцензованих смугах частот використовується FDD або TDD SS може бути з HFDD (напівдуплекс) у неліцензованому TDD.

У стандарті 802.16-2004 наведена структура кадру OFDMA у режимі з тимчасовим дуплексуванням (мал. 5 22).

При установці TDD фреймова структура складається з передач BS й SS. Кожен фрейм передачі в D-link починається із преамбули, за якої треба період передачі DL і період передачі UL. У кожному фреймі TTG й RTG повинні бути вставлені між DL й UL і наприкінці кожного фрейму, щоб дозволити BS повернутися у вихідну готовність до передачі.

В OFDMA (TDD) підтримується також кадрова структура передачі як в BS, так й в SS. Кожен кадр передачі в обох напрямках починається із преамбули, що визначає період передачі на лініях DL й UL. У кожному фреймі як в BS, так й в SS, уведений захисний інтервал RTG (Receive/Transmit Gap), TTG (Transmit/Receive Transition Gap) для переходу від передачі до прийому й навпаки, щоб передавачі на кожній стороні могли відключитися й підготуватися до передачі/прийому наступної пачки. В TDD- і HFDD-системах SS має можливість передавати в проміжку часу між інтервалами SSRTG й SSTTG, а базова станція в цей час не передає.

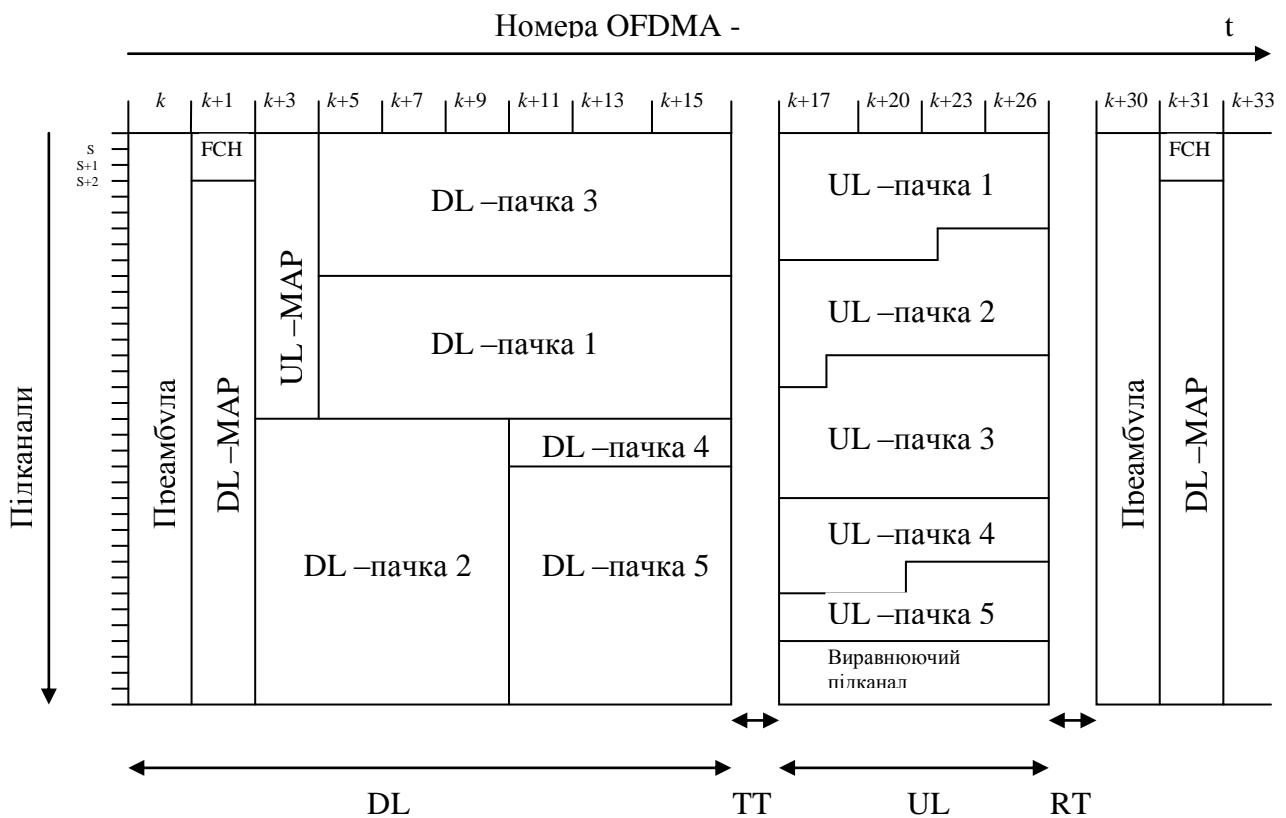


Рис. 5.22. Структура кадру OFDMA (TDD)

Виділення підканалів на висхідному напрямку може виконуватися по двох варіантах. У режимі часткового використання наявних підканалів PUSC (Partial Usage of Subchannels), коли на передачу можуть бути виділені будь-які підканали, і в режимі повного використання всіх підканалів FUSC (Full Usage of Subchannels). Перші два переданих підканала називаються контрольним заголовком фрейму FCH (Frame Control Header). FCH будуть передані на перших двох підканалах у першому символі даних з повторенням в 4-х фреймах. Використається модуляція QPSK зі швидкістю кодування 1/2 в PUSC-зоні. FCH містить DL-фреймовий префікс і повідомлення про довжину DL-MAP-повідомлення, що відразу ж треба за DL-фреймовим префіксом. OFDMA-кадр може включати безліч зон, таких як PUSC й FUSC.

5.3 Ринок мережевого та абонентського обладнання стандарту IEEE 802.16 в Україні та країнах СНД

Практично весь цей сегмент вітчизняного ринку зайнятий закордонними компаніями, що повною мірою пояснюється активною позицією західних вендорів відносно розробки й маркетингу нових систем зв'язку. Кілька російських компаній також заявили про роботу зі створення апаратур нового стандарту, однак інформації про закінчені продукти повністю розробки Росії поки немає.

Нижче коротко представлені учасники ринку України та країн СНД обладнання фіксованого широкосмугового радіодоступу стандарту 802.16 і HiperACCESS, а в табл. 5.26 приводяться основні технічні характеристики їхньої продукції.

Airspan Networks

Компанія Airspan Networks в 2004 р. почала поставки обладнання радіодоступу AS4030 (стандарт 802.16a). У цей час Airspan пропонує ціле сімейство продуктів AS.MAX, розроблених у відповідності зі стандартом 802.16. Дане сімейство включає чотири системи: HiperMAX, MacroMAX, MicroMAX і PrimeMAX, що функціонують у діапазонах 3,5 і 5,8 ГГц.

Alvarion

Компанія Alvarion, чия продукція вже кілька років є присутнім на українському ринку абонентського радіодоступу, пропонує свою останню розробку - платформу BreezeMAX стандарту 802.16a, що функціонує в діапазоні 3,5 ГГц.

Aperto Network

Фірма Aperto заявила про розробку сімейства обладнання PacketMAX стандарту 802.16-2004, що працює в діапазонах 2,5; 3,5 і 5,8 ГГц. У сімейство входять три типи базових станцій: PacketMAX 5000, PacketMAX 3000 і PacketMAX 2000, які відрізняються пропускною здатністю й використовуваними інтерфейсами. Лінійка абонентського обладнання містить у собі п'ять типів терміналів з різними наборами користувальницьких інтерфейсів.

Axxcelera Broadband Wireless

Компанія Axxcelera розробляє обладнання Excel-Max™ стандарту 802.16-2004 діапазонів 3,3-3,8 і 5 ГГц. У діапазоні 3,3-3,8 ГГц працює обладнання ExcelMax™-FD, що використовує частотний дуплекс, і обладнання ExcelMax™-TD, що використовує часовий дуплекс. У системі АВ Max™, що працює в діапазоні 5 ГГц, застосовується метод тимчасового дуплекса.

Marconi

Marconi - єдиний із включених у цей огляд виробників, що випускає обладнання радіодоступу відповідно до вимог європейського стандарту HiperACCESS. Система AXR призначена для високошвидкісної передачі даних в IP- і АТМ-мережах, для збору й передачі трафіка від базових станцій до контролерів базових станцій у мережах мобільного зв'язку за допомогою стандартизованих інтерфейсів "користувач - мережа". На базі обладнання AXR можуть бути побудовані мережі типу "крапка - крапка" у діапазонах 26, 28 і 32 ГГц і "крапка - багато крапок" у діапазонах частот 3,5; 3,7 і 10,5 ГГц. Дальність зв'язку в режимі "крапка - крапка" досягає 20 км.

Motorola

Продовжуючи лінію продуктів широкосмугового радіодоступу під маркою Canopy™, фірма Motorola розробляє систему Canopy™ WiMAX, що відповідає стандарту 802.16-2004, яка функціонує в діапазоні 3,5 ГГц. Передбачається, що система буде підтримувати мобільних абонентів після модернізації з урахуванням вимог стандарту 802.16e. Радіус зони обслуговування абонентських пристроїв, розташовуваних усередині приміщення (IDU), у режимі непрямой видимості (NLOS) становить 3 км.

Proxim

Компанія Proxim заявила про розробку обладнання Tsunami MP. 16 стандарту 802.16-2004. Обладнання функціонує у двох діапазонах: 3,5 ГГц (ширина радіоканалів 3,5 і 7 МГц) і 5,8 ГГц (канали 5 і 10 МГц).

Redline Communications

Redline Communications однієї з перших в 2004 р. почала поставку системи радіодоступу AN-100 (стандарт 802.16a), що функціонує в діапазоні 3,5 ГГц. У цей час фірма заявила про випуск обладнання радіодоступу RedMAX (AN-100U) діапазону 3,5 ГГц, що відповідає стандарту 802.16-2004.

Siemens

Один з найбільших виробників обладнання зв'язку Siemens продемонстрував на виставці "Связь-Эспокомм-2005" систему SkyMAX, що відповідає стандарту 802.16-2004 і функціонує в діапазонах 2,3; 2,5 і 3,5 ГГц.

SR Telecom

В 2002 р. компанія SR Telecom однієї з перших вийшла на ринок країн СНД з обладнанням, що використовує в радіоканалі технологію OFDM, - Angel FWA. На його основі була розроблена система Summetry, що відповідає стандарту 802.16.

Terabeam Wireless

У компанії Terabeam Wireless розробляється устаткування Тега-Мах™, у якому для підтримки рівнів MAC і PHY стандарту 802.16-2004 використовується

процесор MB87M3400 виробництва Fujitsu.

Wi-LAN

Wi-LAN пропонує обладнання радіодоступу стандарту 802.16a -Libra 5800, що функціонує в діапазоні 5,8 ГГц. У цей час фірма заявила про випуск системи Libra MX діапазону 3,5 ГГц, що відповідає вимогам 802.16-2004.

Таблиця 5.26 Короткі технічні характеристики обладнання стандартів IEEE 802.16 і ETSI HiperACCESS

Найменування обладнання	HiperMAX	MacroMAX	MicroMAX	PrimeMAX	EasyST(абон. станція)	ProSm(абон. станція)	AS4030	BreezeMAX
Фірма-виробник	Airspan Networks	Airspan Networks	Airspan Networks	Airspan Networks	Airspan Networks	Airspan Networks	Airspan Networks	Alvarion
Країна	Великобританія	Великобританія	Великобританія	Великобританія	Великобританія	Великобританія	Великобританія	Ізраїль
Відповідність стандарту	IEEE 802.16-2004, с можливістю розширення до 802.16e	IEEE 802.16-2004, з можливістю розширення до 802.16e	IEEE 802.16-2004, с можливістю розширення до 802.16e	IEEE 802.16-2004	IEEE 802.16-2004, с можливістю розширення до 802.16e	IEEE 802.16-2004, с можливістю розширення до 802.16e	IEEE 802.16a	IEEE 802.16a
Конфігурація	P-M-P	P-M-P	P-M-P	P-M-P	-	-	P-M-P	P-M-P
Радіус зони обслуговування, км	Н/д	Н/д	Н/д	Н/д	Н/д	Н/д	До 45	Н/д
Параметри радіо інтерфейсу								
Радіотехнологія	OFDM	OFDM	OFDM	OFDM	OFDM	OFDM	OFDM	OFDM/TDMA
Діапазон частот, ГГц	3,4-3,6	3,4-3,6	3,4-3,6; 5,8	3,4-3,6; 5,8	3,4-3,6; 5,8	3,4-3,6; 5,8	3,4-3,6	3,4-3,6
Ширина радіоканалу, МГц	1,75; 3,5; 5; 7; 10	1,75; 3,5; 5	1,75; 3,5; 7; 10	7; 10; 24; 20	1,75; 3,5; 7; 10	1,75; 3,5; 7; 10	3,5; 7; 14	1,75; 3,5
Метод дуплекса	FDD/TDD	FDD/TDD	FDD/TDD	TDD/HD-FDD	TDD/HD-FDD	TDD/HD-FDD	TDD/HD-FDD	FDD
Конфігурація зони обслуговування	До 6 секторів	До 6 секторів	До 6 секторів	До 6 секторів	-	-	До 6 секторів	-
Використовувани типи модуляції	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM
Потужність передатчика, дБм	До 32	До 37	До 27	23	24	До 23	До 23	28 ±1
Чутливість приймача, дБм	-100	-100	-100	-90	-98	-98	-88(QPSK1/2; BER = 10 ⁻⁹)	-100
Опції радіо-інтерфейсу	AAC; SDMA; SFIR; MIMO; Sub-channelling	MIMO; Sub-channelling	MIMO; DFS; Sub-channelling	Н/д	AAC; SDMA; MIMO; SFIR; DFS; Sub-channelling	AAC; SDMA; MIMO; SFIR; DFS; Sub-channelling	Н/д	Н/д
Характеристики IP								
Характеристики IP	802.1d self-learning bridge; IP4 і IP6; 802.1Q VLAN; MIR/CIR; DiffServ; Packet IPv6 over 802.3/Ethernet; Packet IPv4 over 802.1Q; Packet IPv6 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ; Packing	802.1d self-learning bridge; IP4 і IP6; 802.1Q VLAN; MIR/CIR; DiffServ; Packet IPv6 over 802.3/Ethernet; Packet IPv4 over 802.1Q; Packet IPv6 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ; Packing	802.1d self-learning bridge; IP4 і IP6; 802.1Q VLAN; MIR/CIR; DiffServ; Packet IPv6 over 802.3/Ethernet; Packet IPv4 over 802.1Q; Packet IPv6 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ; Packing	802.1d self-learning bridge; IP4 і IP6; 802.1Q VLAN; MIR/CIR; Packet IPv6 over 802.3/Ethernet; Packet IPv4 over 802.1Q; Packet IPv6 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ	802.1d self-learning bridge; IP4 і IP6; 802.1Q VLAN; MIR/CIR; DiffServ; Packet IPv6 over 802.3/Ethernet; Packet IPv4 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ; Packing	802.1d self-learning bridge; IP4 і IP6; 802.1Q VLAN; MIR/CIR; DiffServ; Packet IPv6 over 802.3/Ethernet; Packet IPv4 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ; Packing	Transparent Bridge; 802.1q VLAN; 802.1p; SLA (Max. reserved traffic rate; Min. reserved traffic rate; Max. latency); rt-PS; nrt-PS; Best Effort; ARQ	802.3 CSMA/CD; 802.1Q; 802.1p; IP DiffServ Code; Points DSCP; Static/Dynamic IP (DHCP); PPPo/PPTP client; RIP1/2; VPN (IPSec; PPTP<2P Pass Through)

Захист інформації									
Захист інформації	Data Encryption AES CCM; TIK Encryption AES 128/1024	Data Encryption AES CCM; TIK Encryption AES 128/1024	Data Encryption AES CCM; TIK Encryption AES 128/1024	Data Encryption AES CCM; TIK Encryption AES 128/1024	Data Encryption AES CCM; TIK Encryption AES 128/1024	Data Encryption AES CCM; TIK Encryption AES 128/1024	3 DES	WEP encryption 64 і 128 bit	
Користувальницький і мережвий інтерфейси									
Мережвий інтерфейс	100Base-T/ 1000Base-T	100Base-T	100Base-T/ 1000Base-T	10/100Base-T; 4(8) E1	-	-	10/100Base-T; 4(8) E1	10/100Base-T	
Користувальницький інтерфейс	10/100Base-T; 802.11g (Wi-Fi); POTs з RGW	10/100Base-T; 802.11g (Wi-Fi); POTs з RGW	10/100Base-T; 802.11g (Wi-Fi); POTs з RGW	10/100Base-T; 4(8) E1	10/100Base-T; 802.11g (Wi-Fi); POTs з RGW	10/100Base-T; 802.11g (Wi-Fi); POTs з RGW; E1	10/100Base-T; 4(8) E1	1(4) 10/100Base-T; 1 або 2RJ1; 802.11b/g	
Джерело живлення									
Напруга живлення, В	-48 (DC)	220 (AC)	220 (AC); -48 (DC)	220 (AC); -48 (DC)	90-264 (AC); -6 (DC)	220 (AC); -48 (DC)	220 (AC); -48 (DC)	220 (AC); -48 (DC)	
Споживана потужність, Вт	250 на сектор	250 на сектор	25 на сектор	250 на сектор	6-8	10	75 на сектор	200 на сектор	
Фірм-виробник	<i>Aperto Networks</i>	<i>Axxcelera Broad-band Wireless</i>		<i>Marconi</i>	<i>Motorola</i>	<i>Nateks</i>	<i>Proxim</i>	<i>Redline Communications</i>	
Країна	США	США	США	Германія	США	Росія	США	Канада	
Відповідність стандарту	IEEE 802.16-2004	IEEE 802.16-2004, з можливістю розширення до 802.16 e		HiperAccess	IEEE 802.16-2004, с возм. расш. до 802.16e	IEEE 802.16a	IEEE 802.16-2004	IEEE 802.16-2004	
Конфігурація	P-M-P	P-M-P, P-T-P	P-M-P	P-M-P	P-M-P	P-M-P	P-M-P	P-M-P	
Радіус зони обслуговування, км	Н/д	Н/д	До 30	До 20	17	До 45	Н/д	Н/д	
Параметри радіоінтерфейса									
Радіотехнологія	OFDM	OFDM	OFDM	TDM/TDMA	OFDMA	OFDM	OFDM	OFDM	
Діапазон частот, ГГц	2,5-2,7; 3,3-3,8; 5,425-5,725; 5,725-5,925	5,25-5,85	3,3-3,8	24,5-26,5; 27,5-29,5	3,3-3,65; 3,6-3,8	3,4-3,6	2,496-2,690; 5,725-5,850; 5,470-5,725	3,4-3,8 3,4-3,6;	
Ширини радіо-каналу, МГц	2-10; 5,5; 20 (1,75; 3,5; 7; 14 у перспективі)	5; 10; 15; 20	1,75; 3,5; 7; 10	7; 14; 28	3,5; 7	3,5; 7; 14	3,5; 5; 7; 10	3,5; 7; 14	
Метод дуплекса	TDD	TDD	FDD (Excel-Max-FD) і TDD (ExcelMax-TD)	FDD	H-FDD/TDD	TDD/HD-FDD	TDD	TDD і HD-FDD	
Конфігурація зони обслуговування	До 6 секторів	До 6 секторів	До 6 секторів	До 4 секторів	-	До 6 секторів	-	До 6 секторів	
Використовувані типи модуляції	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	QPSK; 16QAM; 64QAM	QPSK; 16QAM; 64QAM	QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	
Потужність передавача, дБм	20 (28 у перспективі)	36 (ЭИИМ)	38	22	10 Вт (ЭИИМ)	До 23	До 28	До 23	
Чутливість приймача, дБм	-100	-100	-100	-87,5 (QPSK2/3; BER = 10 ⁻⁶)	-	-88 (QPSK1/2; BER = 10 ⁻⁹)	-95	-90 (QPSK1/2; BER = 10 ⁻⁶)	
Опції радіо-інтерфейсу	AFS; DFS	MIMO; DFS; Sub-channelling	Sub-channelization; Space Time Coding/Diversity (MIMO)	Н/д	Н/д	Н/д	Н/д	Н/д	
Характеристики IP									
Характеристики IP	IP Routing; OSPF; RIPv2; VLSM; CIDR DHCP (client and relay agent); VLAN; Bridging; PPP; Service Classes (Continuous Grant; Real/Non Real Time; Best Effort)	802.1d self-learning bridge; IP4 і IP6; 802.1 Q VLAN; MIR/CIR; DiffServ; Packet Pw6 over 802.3/ Ethernet; Packet IPv4 over 802.1 Q; IPv4 over 802.1Q; Packet IPv6 over 802.1Q; Pauload Header Suppression; Multicast Polling; ARQ; Packing			802.1Q VLAN	802.1Q VLAN	Transparent Bridge; 802.1 q VLAN; 802.1p;SLA(Max. reserved traffic rate; Min. reserved traffic rate; Max. latency); rt-PS; nrt-PS; Best Effort; ARQ	802.1 Q VLAN; Bridging (802.1 D); Routing (RIP v1 and v2);802.1D/802.1Q/802.1p priority; Best Effort; Universal Grant Services; Realtime Polling; Non-Realtime Polling	Transparent Bridge; 802.1q VLAN; 802.1 p; SLA (Max. reserved traffic rate; Min. reserved traffic rate; Max. latency); rt-PS; nrt-PS; Best Effort; ARQ
Захист інформації									
Захист інформації	3 DES; AES CCM 128 і 1024	Data Encryption AES CCM; TIK Encryption AES 128/1024		Н/д	Н/д	3 DES	DES (56 bit) або AES (128 bit)	DES; 3 DES	
Користувальницький і мережвий інтерфейси									

Мережевий інтерфейс	100Base-T	100Base-T/ 1000Base-T	100Base-T, повний дуплекс на сектор 10/100Base-T; POTS (RJ11), E1 (RJ45) і Wi-Fi (802,11a/b/g) через зовнішні пристрої	STM1 ATM,E1 ATM/IMA/TDM, 10/100 Base-T	-	10/100Base-T; 4(8) E1	10/100Base-T	10/100Base-T; Д0 8 E1
Користувальницький інтерфейс	10/100 Base-T; до 8 POTS; AP 802.11a,b,g	10/100Base-T		E1 ATM/IMA/TDM, Ethernet 10/ 100Base-T	-	10/100Base-T; 4(8) E1	10/100Base-T	10/100Base-T; до 8 E1
Джерело живлення								
Напруга живлення, В	220 (AC); -48 (DC)	-48 (DC)	220 (AC); -48 (DC)	-48 (DC)	-	220 (AC); -48 (DC)	220 (AC)	220 (AC); -48 (DC)
Споживана потужність, Вт	380	Підлягає визначенню	Підлягає визначенню	Н/д	-	75 на сектор	До 32 на сектор	Н/д
Фірма-виробник	<i>Redline Communications</i>	<i>Redline Communications</i>	<i>Siemens Mobile</i>	<i>SR-Telecom</i>	<i>Terabeam Wireless</i>	<i>Wi-LAN</i>	<i>Wi-LAN</i>	<i>Wi-LAN</i>
Країна	Канада	Канада	Германія	Канада	США	Канада	Канада	Канада
Відповідність стандарту	IEEE 802.16-2004	IEEE 802.16-2004	IEEE 802.16-2004, с можливістю розширення до 802.16e	IEEE 802.16-2004	IEEE 802.16-2004	IEEE 802.16-2004	IEEE 802.16a	IEEE 802.16a
Конфігурація	P-M-P	P-M-P	P-M-P	P-M-P	P-to-P	P-M-P	P-to-P	P-M-P
Радіус зони обслуговування, км	Н/д	Н/д	Н/д	До 50	Н/д	До 30	До 66	До 35
Параметри радіоінтерфейса								
Радіо-технологія	OFDM	OFDM	OFDM/TDMA	OFDM	OFDM	W-OFDM	W-OFDM	W-OFDM
Діапазон частот, ГГц	3,4-3,6	3,4-3,6	2,3/2,4; 3,4-3,8	3,3-3,8	4,94-4,99; 5,725-5,850	3,4-3,6	5,8	5,8
Ширина радіо-каналу, МГц	3,5; 7	3,5; 7	1,75; 3,5; 7; 14	1,75; 3,5	20	3,5; 7	10 (12,5 канальний рознос)	10 (12,5 канальний рознос)
Метод дуплекса	TDD і HD-FDD	TDD/HD-FDD	FDD/TDD	FDD	TDD	FDD	TDD	TDD
Конфігурація зони обслуговування	-	-	До 4 секторів	До 6 секторів	-	До 6 секторів	-	До 6 секторів
Використовувані типи модуляції	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	BPSK; QPSK; 16QAM; 64QAM	QPSK	BPSK; QPSK; 16QAM; 64 QAM	BPSK; QPSK; 16QAM	BPSK; QPSK; 16QAM
Потужність передавача, дБм	До 20	До 20	35	31	До 23	До 30	Від-3 до+17	Від-3 до+17
Чутливість приймача, дБм	-90 (QPSK1/2; BER = 10 ⁻⁶)	-90 (QPSK1/2; BER = 10 ⁻⁶)	-98 (3,5 МГц; BER = 10 ⁻⁶)	-97 (1/2BPSK; 3,5 МГц)	-86	-91 (3,5 МГц; BPSK; BER = 10 ⁻⁶)	-84 (BPSK; BER = 10 ⁻⁶)	-84 (BPSK; BER = 10 ⁻⁶)
Опції радіоінтерфейсу	Н/д	Н/д	Н/д	MIMO; Space-time Coding; Hybrid ARQ; Sub-channelling	Н/д	Н/д	Н/д	Н/д
Характеристики IP								
Характеристики IP	Transparent Bridge; 802.1q VLAN; 802.1p, TOS/ DSCP and L2/L3 addressstratfic prioritization	Transparent Bridge; 802.1q VLAN; 802.1p, TOS/ DSCP and L2/L3 addressstratfic prioritization	Layer2 802..1p; Layer3 IP DSCP; NAPT; DHCP; PPPo; Unsolicited Grant Service; rt-PS; nrt-PS; Best Effort; ARQ	802.1 d; IP4; PPPo; L2TP; PPT; IPsec; MPLS; 802.1Q VLAN; DiffServ; Broadcast/ Multicast Flood Control; Traffic priority marking; Latency and jitter control	IP router; Ethernet bridge; TurboCell Polling Protocol; Adaptive Dynamic polling algorithm; SuperPacket Agg-regation; RADIUS Authentication; RIP II; MAC address; Protocol ID	802.1q VLAN Compliance; Bridge functionality; Net- work Filtering (MAC address, IP address, IP subnet); CIR/MBR; IPTOS	802.1q VLAN Compliance; Bridge functiona- lity; Network Filtering (MAC& IP); CIR/MBR	802.1q VLAN Compliance; Bridge functiona- lity; Network Filtering (MAC& IP); CIR/MBR
Захист інформації								
Захист інформації	DES; AES	DES; AES	DES; 3 DES	Н/д	DES (56 біт); AES (128 біт)	Н/д	Н/д	Н/д
Користувальницький і мережевий інтерфейси								

Мережевий інтерфейс	-	-	10/100/1000Base-T; STM-1 GFP; 2x Gigabit Ethernet; Nx1	100Base-T; до 16E1	10/100Base-T	10/100Base-T; E1 (опція)	10/100Base-T	10/100Base-T
Користувальницький інтерфейс	До 4 10/100Base-T; до 4 POTS (FXO/FXS)	До 4 10/100Base-T; 1xe1; до 4POTS (FXO/FXS)	1(4)10/100Base-T; 2 POTS(E1;AP (Wi-Fi) - опція)	10/100 Base-T; POTS	10/100Base-T	10/100Base-T; E1 (опція)	10/100Base-T	10/100Base-T
Джерело живлення								
Напруга живлення, В	220 (AC)	220 (AC)	220 (AC)	-48 (DC)	220 (AC)	220 (AC); -48 (DC)	Н/д	Н/д
Споживана потужність, Вт	Н/д	Н/д	50+140 (на сектор)	1550 на 6 секторів	16	350	30	30

Література

1. Шахнович И. Сети городского масштаба: решения рабочей группы IEEE 802.16 – в жизнь! – ЭЛЕКТРОНИКА: НТБ, 2003, №8, с.50.
2. IEEE Std IEEE 802.16a-2003. IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 2: "Medium Access Control Modifications and Additional Physical Layer Specifications for 2–11 GHz". – IEEE, 1 April 2003.
3. IEEE Std IEEE 802.16-2001 IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. – IEEE, 8 April 2002.
4. IEEE Std IEEE 802.16c-2002. IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 1: Detailed System Profiles for 10–66 GHz. – IEEE, 15 January 2003.
5. IEEE Std IEEE 802.16™-2004 (Revision of IEEE Std IEEE 802.16-2001). IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. – IEEE, 1 October 2004.
6. Шахнович И. Стандарт широкополосного доступа IEEE 802.16 для диапазонов ниже 11 ГГц // Электроника НТБ, 2005, №1, с. 8-14.
7. Шахнович И. Беспроводные локальные сети. Анатомия стандартов IEEE 802.11 // Электроника НТБ, 2005, №1, с. 16-18.
8. Вишневикий В.М. и др. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
9. Гургенидзе А. Беспроводные сети: реальные перспективы // Connect, 2005, №8, с. 42-47.

10. Ханс-Петер Петри, Бернд Фридрихс WiMAX: новая звезда на небосклоне беспроводной связи // Connect, 2005, №6, с.166-170.
11. Перспективы развития WiMAX: далекие или близкие // Connect, 2005, №8.
12. Лукоев О. WiMAX – беспроводные безграничные возможности // Connect, 2005, №6.
13. Гармонов А.В. и др. Технический обзор стандарта IEEE 802.16 // Мобильные системы, 2005, №6, с. 16-24.
14. Буров Є. Комп'ютерні мережі. 2-е оновлене і доповн. вид. – Львів: БаК, 2003. – 584 с.
15. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. СПб: ПИТЕР, 2003. – 864 с.
16. Дуглас К. Компьютерные сети и Internet. Диалектика, 2002. – 640 с.
17. Закер К. Компьютерные сети. ВHV-СПб, 2001. – 1008 с.
18. Microsoft Corporation. Сети TCP/IP. Ресурсы Microsoft Windows 2000 Server/ Пер.с англ. Издательско-торговый дом «Русская редакция», 2001. – 784 с.
19. Патий Е. GPRS: Интернет в кармане // Сети и телекоммуникации. – 2003. – №10 (37). – С.68-78.
20. Сирота Л. “Удлинитель” для оптоволоконна // Сети и телекоммуникации. – 2003. – №8-9 (35-36). – С.16-22.
21. Горностаев Ю.М., Соколов В.В., Невдяев Л.М. Перспективные спутниковые системы связи. – М.: «Горячая линия Телеком» МЦНТИ, 2000. – 132 с.
22. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы: 4-е изд., перераб. и доп. – М.: ДМК Пресс, 2002. – 640 с.
23. Возенкрафт Д., Джекобс И. Теоретические основы техники связи. – М.: Мир, 1969. – 640 с.
24. Котельников В.А. Теория потенциальной помехоустойчивости. – М.: Госэнергоиздат, 1956. – 240 с.
25. Волобоев Б.А. Методи проектування інформаційного простору будівельної галузі України // Будівництво України. – 2004. – №5. – С.5-6.
26. Боговіс В.Є., Вишняков В.М., Тарасюк Д.М. Елементи корпоративної інформаційної мережі будівельного комплексу України // Будівництво України. – 2004. – №5. – С.18-19.

27. Wireless Broadband Communications: Some Research Activities in Singapore / K.C. Chua, K.V. Ravi, B. Bensaou, T.C. Peh // IEEE Communications Magazine. - 1999.- Vol. 37, nr 11.- P. 84-90.

28. Drewes C., Aicher W., Hausner J. The Wireless Art and Wired Force of Subscriber Access // IEEE Communications Magazine.- 2001.- Vol. 39, nr 5.- P. 118-124.

29. Мамаев Н.С., Мамаев Ю.Н., Теряв Б.Г. Цифровое телевидение.- М.: Горячая линия – Телеком, 2001. – 180 с.

30. Ohmori S., Yamao Y., Nakajima N. The Future Generations of Mobile Communications Based on Broadband Access Technologies // IEEE Communications Magazine. - 2000.- Vol. 38, nr 12.- P. 134-142.

31. Mikkonen J., Corrado C., Evcı C. Emerging wireless broadband networks // IEEE Communications Magazine.-1998.-Vol. 36, nr 2.- P. 112-117.

32. Гассанов Л.Г., Шевченко Д.Д., Шермаревич В.Г. Интегрирование телекоммуникационных услуг в беспроводных сетях на основе широкополосных сигналов // Материалы 10-й Международная Крымская Микроволновая конференция КрыМиКо-2000 «СВЧ-техника и телекоммуникационные технологии», 11-15 сент.- Севастополь: «Вебер», 2000.- С. 81-82.

33. Москалюк А. TeleSym: мобильная связь «на халяву» // Компьютерное обозрение.- 2002.- № 39.- С. 66.

34. New high-rate wireless LAN standards / R. van Nee, G. Awater, M. Morikura, H. Takanashi and etc. // IEEE Communications Magazine.-1999.-Vol. 37, nr 12.- P. 82-88.

35. Keyholes, Correlations, and Capacities of Multielement Transmit and Receive Antennas / D. Chizhik, G. Foschini, M. Gans, and R. Valenzuela // IEEE Trans. on Wireless Communications. – 2002.- Vol. 1, nr 2.- P. 361-368.

36. Detection Algorithm and Initial Laboratory Results using the V-BLAST Space-Time Communication Architecture / G. D. Golden, G. J. Foschini, R. A. Valenzuela, P. W. Wolniansky // Electronics Letters. – 1999.- Vol. 35, nr 1.- P. 14-15.

37. Ильченко М.Е., Кравчук С.А. Перспективы развития телекоммуникаций // Материалы 11-й Международной конференции КрыМиКо'2001 «СВЧ-техника и телекоммуникационные технологии», 10-14 сентября 2001 г., Севастополь, Крым, Украина.- Севастополь: «Вебер», 2001.- С. 237-240.

38. Микроволновые технологии в телекоммуникационных системах / Т.Н. Нарытник, В.П. Бабак, М.Е. Ильченко, С.А. Кравчук.- Киев: Техника, 2000.- 304 с.

39. Palmer D., Germon R., Evans D. BWA Standardisation: A European view // N-WEST Tutorial.- 1998.- 7 p.

40. Микроволновая интегрированная телерадиоинформационная система / Т.Н. Нарытник, В.Н. Денисенко, М.Е. Ильченко и др. // Радиоэлектроника.- 1999.- Т.42, №11. – С.40-50. (Изв. вузов).

41. Кравчук С.А., Липатов А.А. Современные телекоммуникационные технологии диапазона миллиметровых волн // Материалы 12-й Международной конференции КрымМиКо'2002 «СВЧ-техника и телекоммуникационные технологии», 9-13 сентября 2002 г., Севастополь, Крым, Украина.- Севастополь: «Вебер», 2002.- С. 41-42.

42. Мостовой В.И. Сотовое телевидение – новейшая технология широкополосного радиодоступа // Материалы 12-й Международной конференции КрымМиКо'2002 «СВЧ-техника и телекоммуникационные технологии», 9-13 сентября 2002 г., Севастополь, Крым, Украина.- Севастополь: предприятие «Вебер», 2002.- С. 3-8.

43. Ильченко М.Ю., Кайдено М.М., Кравчук С.О. Цифрові мережі з інтеграцією послуг на основі мікрохвильової телекомунікаційної розподільчої системи // Матеріали 2-го міжнародного конгресу “Розвиток інформаційного суспільства в Україні”, 4-6 грудня 2001 р., Київ, Україна.- К.: ТОВ “Сак Лтд.”, 2002.- С. 87-95.

44. Микроволновые устройства телекоммуникационных систем. В 2 т. Том 2: Устройства приемного и передающего трактов. Проектирование устройств и реализация систем / М.З. Згуровский, М.Е. Ильченко, С.А. Кравчук, Т.Н. Нарытник, Ю.И. Якименко.- К.: ИВЦ “Видавництво “Політехніка”, 2003.- 616 с.

45. Wireless Optical Transmission of Fast Ethernet, FDDI, ATM, and ESCON Protocol Data Using the TerraLink Laser Communication System / I.I. Kim, R. Stienger, J.A. Koontz etc. // Optical Engineering.- 1998.- Vol. 37, nr 12.- P. 3143-3155.

47. Begley D.L. Laser Cross-Link Systems and Technology // IEEE Communications Magazine.-2000.-Vol. 38, nr 8.- P. 126-132.

48. Слюсар В. Ультразвуковая техника на пороге третьего тысячелетия.- Электроника: НТБ, 1999, № 5, с. 50–53.

49. Слюсар В. Цифровое формирование луча в системах связи: будущее рождается сегодня. – Электроника: НТБ, 2001, № 1, с. 6–12.

50. Слюсар В. Цифровые антенные решетки: будущее радиолокации. – Электроника: НТБ, 2001, № 3, с. 42--46.

51. Слюсар В. Схемотехника цифрового диаграммообразования. Модульные решения. – Электроника: НТБ, 2002, № 1, с. 46–52.

52. Слюсар В.И. Идеология построения мультистандартных базовых станций перспективных систем связи. – Радиоэлектроника (Изв. вузов), 2001, № 4, с. 3–12.
53. Інформаційні матеріали сайту: www.metawave.com.
54. Super Capacity Solution. The World's First GSM Adaptive Array Solution. – www.airnetcom.com.
55. Інформаційні матеріали сайту: www.arraycom.com
56. Слюсар В. И. Схемотехника цифрового диаграммообразования. Модульные решения. – ЭЛЕКТРОНИКА: НТБ, 2002, № 1, с.46–52.
57. Слюсар В. И. Smart-антенны пошли в серию. – ЭЛЕКТРОНИКА: НТБ, 2004, № 1, с.52 – 55.13. 12-Bit, 40/65 MSPS Quad A/D Converter MAX1127. – <http://www.maxim-ic.com/>.
58. Сиверс М.А., Галкин С.Л., Григорьев М.С., Певцов Н.В., Рыжков А.Е. Современные системы радиодоступа. СПб, Судостроение, 2001.
59. Бабков В.Ю., Вознюк М.А., Петраков В.А., Рыжков А.Е., Сиверс М.А. Передача информации в системах подвижной связи / СПбГУТ. СПб, 1999.
60. Столлингс В. Беспроводные линии связи и сети. М.-СПб: Вильямс, 2003.
61. Шиллер Й. Мобильные коммуникации. М.-СПб: Вильямс, 2002.
62. Бабков В.Ю., Никитин А.Н., Осенний К.Н., Сиверс М.А. Системы мобильной связи с кодовым разделением каналов. СП.: ТРИАДА, 2003.
63. Дингес С.И. Мобильная связь: технология DECT. М.: СОЛОН-Пресс, 2003.
64. Архипкин В.Я., Архипкин А.В. Bluetooth. Технические требования. Практическая реализация. Применение. М.: Мобильные коммуникации. 2004.
65. Молта Дейв. Развитие БЛВС // Сети и системы связи. 2004. №1. С. 30 - 33.
66. Інформаційні матеріали сайту журналу Сети: <http://www.osp.ru/nets>
67. Інформаційні матеріали сайту журналу Сети и системы связи: <http://ccc.ru>
68. Інформаційні матеріали сайту журналу Mobile News Review: <http://www.mobilenews.ru>
69. Інформаційні матеріали сайту журналу Russian Mobile: <http://www.mobilemag.spb.ru>

70. Інформаційні матеріали сайту Telecoms Virtual Library
<http://www.analysys.com/vlib>
71. Інформаційні матеріали сайту ETSI (Європейський інститут стандартів в області телекомунікацій) - стандарти DECT, HIPERLAN и др.
<http://www.etsi.org>
72. Інформаційні матеріали сайту IEEE-SA (Международный институт электро и радиоинженеров - Standard Association) <http://grouper.ieee.org/groups/802/11/>.
73. Інформаційні матеріали сайту по Bluetooth: <http://www.bluetoothweb.com>
74. Інформаційні матеріали сайту по Bluetooth: <http://www.bluetoothsig.org>
75. Інформаційні матеріали сайту по IEEE 802.11 <http://www.80211-planet.com/news/>
76. Інформаційні матеріали сайту по HIPERLAN2 <http://www.hiperlan2.com>
77. Інформаційні матеріали сайту Wi-Fi Alliance: <http://www.wi-fi.org>
78. Інформаційні матеріали сайту по Wi-Fi (точки доступу): <http://www.wi-fizone.org>
79. Інформаційні матеріали сайту Ericsson: <http://www.ericsson.com>
80. Інформаційні матеріали сайту Nokia: <http://www.nokia.com>
81. Інформаційні матеріали сайту Siemens: <http://www.siemens.de>
82. Інформаційні матеріали сайту Cisco: <http://www.cisco.com>
83. Інформаційні матеріали сайту Proxim: <http://www.proxim.com>
84. Інформаційні матеріали сайту Symbol: <http://www.symbol.com>
85. Інформаційні матеріали сайту Airespace: <http://www.airespace.com/>
86. Інформаційні матеріали сайту Alvarion: <http://www.alvarion.com/>
87. Інформаційні матеріали сайту WiMAX Forum org: :
<http://www.wimaxforum.org/>
88. Інформаційні матеріали сайту компанії «Украинские новейшие технологии»: www.alternet.com.ua/
89. Інформаційні матеріали сайту www.wireless.ru.

90. Ильченко М.Е., Бунин С.Г., Войтер А.П. Сотовые радиосети с коммутацией пакетов. К.: Наукова думка, 2003, 266с.
91. Бунін С.Г., Войтер А.П. Мережа ДИСКРЕТ з пакетною комутацією. -УСИМ, N5, 1983, с.37-44
92. Бунін С.Г., Войтер А.П., Пилипчак С.І. Децентралізовані протоколи множинного доступу з асинхронним резервуванням. – УСИМ, N6, 1990, с.34-40.
93. Кантор Л.Я., Поволоцкий И.С. Системы персонального рухомого зв'язку через низькоорбитальні ШСЗ //Вестник связи, N11, 1994, с.6-10.
94. Гуськов Г.Я., Галицкий А.В., Рыбальченко Ю.М. та ін. Глобальна супутникова система зв'язку // Кур'єр. -МЕРЕЖІ, січень-лютий 1992, с.11-17.
95. Михайлов М.К. та ін.. Перспективні напрямки розвитку бездротових телекомунікаційних технологій // Праці УНДІРТ, №1 (41), 2005, с. 3-6.
96. Домбровский Д.А. Перспективы развития систем беспроводного доступа в диапазоне частот 5 ГГц в Украине // Праці УНДІРТ, №1 (41), 2005, с. 30-35.
97. Олейник В.Ф., Сайко В.Г., Булгач С.В. Радиотелекоммуникационные технологии мобильных систем: теоретические основы и практическое применение. Том 1. Системы сотовой подвижной радиосвязи. К.: ГУИКТ, 2004, 307 с.
98. Олейник В.Ф., Сайко В.Г., Булгач С.В. Радиотелекоммуникационные технологии мобильных систем: теоретические основы и практическое применение. Том 2. Системы профессиональной и спутниковой связи, абонентского радиодоступа. К.: ГУИКТ, 2004, 388 с.
99. Олейник В.Ф., Сайко В.Г., Булгач С.В. Мобильные радиотелекоммуникационные системы специального назначения. К.: ГУИКТ, 2004, 102 с.
100. Бабак В.П. та ін.. Обробка сигналів у радіоканалах цифрових систем передавання інформації. К.: книжкове видання НАУ, 2005, 476с.
101. Сайко В.Г. Беспроводное общение новой эпохи // Сети и телекоммуникации, 2000, №4, с. 40-45.
102. Delivering Voice and Data: Comparing CDMA2000 and GSM|GPRS|EDGE|UMTS. By: The CDMA Development Group, December 2005, www.cdg.org.
103. Програма переходу України до систем рухомого зв'язку 3-го покоління // Зв'язок, 2002, №5(37), с. 2-5.

104. Гряник М.В., Пасічник С.Г. Напрямки розвитку в Україні систем рухомого зв'язку 3-го покоління // Зв'язок, 2002, №5(37), с. 13-19.
105. Грицунь Б.Е., Гряник М.В., Пасечник С.Г., Фролов В.И. Особенности внедрения систем сотовой связи 3-го поколения в Украине // Праці УНДІРТ, 2006, №1(45)-2(46), с. 79-81.
106. Іванов В.А., Севостьяненко А.В. Перспективи розвитку в Україні технологій стільникового радіозв'язку наступних поколінь // Праці УНДІРТ, 2006, №1(45)-2(46), с. 82-83.
107. Мазурков М.І. та ін.. Системи телекомунікацій. Одеса: ТЕС, 2005, 288с.
108. Гайдук О.В. та ін.. Радіотелекомунікаційні технології: радіопередавальні та радіоприймальні пристрої. Ніжин: Видавництво «Аспект-Поліграф», 2007, с.320.
109. Інформаційні матеріали робочої групи 802.16 розміщений за адресою <http://grouper.ieee.org/groups/802/16/index.html>.
110. Інформаційні матеріали сайту: www.timedomain.com
111. Інформаційні матеріали сайту: www.miltispectral.com/history.html
112. Хармут Х. Теорія секвентного аналізу. М.: Мир, 1980. – 574с.
113. Хармут Х. Несинусоидальные волны в радиолокации и радиосвязи. – м.: Радио и связь, 1985. – 376с.
114. Бунин С.Г. Несинусоидальные сигналы в системах передачи информации // Процессоры и системы обработки сигналов: Сб. науч. тр. – К.: Ин-т кибернетики. – 191. -- с. 9-13.
115. Бунин С.Г. Назад к Герцу? // Радио. – 1990. -- №7. с.17-20.