

І. Р. Арсенюк, А. А. Яровий

КОМП'ЮТЕРНІ МЕРЕЖІ

Частина 3

Навчальне видання

**Арсенюк Ігор Ростиславович
Яровий Андрій Анатолійович**

**КОМП'ЮТЕРНІ МЕРЕЖІ
Частина 3**

Навчальний посібник

Редактори: І. Городенська
О. Ткачук

Оригінал-макет підготовлено І. Арсенюком

Підписано до друку 06.02.2017 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різнографічний. Ум. друк. арк. 5,7.
Наклад 50 пр. Зам. № 2017-022.

Вінницький національний технічний університет,
навчально-методичний відділ ВНТУ.
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, к. 2201.
Тел. (0432) 59-87-36.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному
університеті в комп'ютерному інформаційно-видавничому центрі
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-87-38.
publish.vntu.edu.ua; email: kivc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Міністерство освіти і науки України
Вінницький національний технічний університет

І. Р. Арсенюк, А. А. Яровий

КОМП'ЮТЕРНІ МЕРЕЖІ
Частина 3

Навчальний посібник

Вінниця
ВНТУ
2017

УДК 004.732(075)
ББК 32.973.202я73
А85

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 5 від 25 грудня 2014 р.)

Рецензенти:

А. М. Петух, доктор технічних наук, професор

Л. І. Тимченко, доктор технічних наук, професор

С. М. Захарченко, кандидат технічних наук, доцент, сертифікований інструктор мережевої академії Cisco

Арсенюк, І. Р.

А85 Комп'ютерні мережі. Частина 3 : навч. посіб. / І. Р. Арсенюк, А. А. Яровий. – Вінниця : ВНТУ, 2017. – 85 с.

У третій частині посібника розглянуто технології локальних комп'ютерних мереж Ethernet, Fast Ethernet, Gigabit Ethernet, 10 G Ethernet, Wi-Fi. Зокрема, розглянуто фізичні рівні технологій, методи доступу до середовища передачі даних. Приділено увагу технологіям Token Ring, FDDI та 100VG-AnyLAN.

Посібник розроблено відповідно до плану кафедри й програми дисципліни «Комп'ютерні мережі», може бути використаний під час вивчення дисциплін «Корпоративні і глобальні комп'ютерні мережі» та «Мережеві інформаційні технології».

УДК 004.732(075)
ББК 32.973.202я73

ЗМІСТ

ТЕХНОЛОГІЇ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ	4
1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОТОКОЛІВ ЛОКАЛЬНИХ МЕРЕЖ	4
2 СІМЕЙСТВО ТЕХНОЛОГІЙ ETHERNET	8
2.1 Технологія Ethernet.....	8
2.1.1 Доступ до середовища передачі даних	8
2.1.2 Кадри технології Ethernet	15
2.1.3 Розрахунок продуктивності Ethernet	16
2.1.4 Специфікації фізичного середовища Ethernet	18
2.2 Технологія Fast Ethernet	19
2.2.1 Загальні відомості	19
2.2.2 Продуктивність Fast Ethernet	20
2.2.3 Специфікації фізичного середовища Fast Ethernet	20
2.3 Технологія Gigabit Ethernet	25
2.3.1 Загальні відомості	25
2.3.2 Продуктивність Gigabit Ethernet	27
2.3.3 Специфікації фізичного середовища стандарту Gigabit Ethernet 30.....	29
2.4 Технологія 10-Gigabit Ethernet	30
Контрольні запитання	32
3 ТЕХНОЛОГІЯ БЕЗПРОВОДОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ WI-FI	35
3.1 Загальні відомості	35
3.2 Основні елементи та режими функціонування Wi-Fi.....	36
3.3 Технологія колективного доступу CSMA/CA	41
3.4 Формати кадрів стандарту IEEE 802.11	50
3.5 Основні різновиди стандарту IEEE 802.11	53
Контрольні запитання	67
4 ІНШІ ТЕХНОЛОГІЇ ПРОВОДОВИХ ЛОКАЛЬНИХ МЕРЕЖ	68
4.1 Технологія Token Ring	68
4.1.1 Загальні відомості	68
4.1.2 Метод доступу до розділюваного середовища	68
4.1.3 Фізичний рівень технології Token Ring	70
4.2 Технологія FDDI	72
4.2.1 Загальні відомості та основні характеристики технології	72
4.2.2 Метод доступу у FDDI	75
4.2.3 Відмовостійкість технології FDDI	75
4.2.4 Фізичний рівень технології FDDI	76
4.3 Технологія 100VG-AnyLAN	77
Контрольні запитання	80
СЛОВНИК ТЕРМІНІВ	81
ЛІТЕРАТУРА	84

ТЕХНОЛОГІЇ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Локальні комп'ютерні мережі (ЛКМ), на відміну від інших типів комп'ютерних мереж, покривають невеликі географічні території (до 1000–2000 м²) та призначені для обслуговування конкретного підприємства або організації. На відміну від глобальних, локальні мережі погано масштабуються (дозволяють лише у невеликих межах змінювати як власні розміри, так і збільшувати кількість вузлів) та належать до мереж закритого типу, що надають доступ лише працівникам даного підприємства чи організації. Також доцільно зазначити, якщо на початковому етапі розвитку мереж ЛКМ значно випереджали глобальні за швидкістю передачі даних та за якістю і кількістю надаваних сервісів та послуг, то сьогодні ситуація кардинально змінилася: глобальні комп'ютерні мережі, як правило, надають набагато ширший спектр послуг, і швидкості у їхніх магістральних каналах суттєво перевищують швидкості локальних мереж.

Нижче розглянемо деякі технології провідних і безпроводних ЛКМ, їх основні характеристики та особливості.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОТОКОЛІВ ЛОКАЛЬНИХ МЕРЕЖ

Основна мета, яку ставили перед собою розробники перших локальних комп'ютерних мереж (КМ) у другій половині 70-х років ХХ ст., полягала у знаходженні простого й дешевого рішення для об'єднання у мережу декількох десятків комп'ютерів, що знаходяться в межах однієї будівлі. Для спрощення і здешевлення апаратних і програмних рішень розробники зупинилися на використанні загального (спільного, розділюваного) середовища передачі даних, яке передбачало спільне використання кабелів усіма комп'ю-терами мережі в режимі поділу часу [1].

Цей метод зв'язку було апробовано в другій половині 60-х років у радіомережі АЛОНА Гавайського університету, яка працювала за методом випадкового доступу, коли кожен вузол міг почати передачу в будь-який момент часу. Якщо ж вузол не отримував підтвердження протягом певного тайм-ауту, то надсилав пакет знову. Аналогом загального радіосередовища є, наприклад, сегмент коаксіального кабелю, до якого паралельно приєднуються усі вузли мережі і при передачі сигналів одним з передавачів усі приймачі отримують один і той же сигнал, як і при використанні радіохвиль [1].

Використання розділюваного середовища передбачає, що кожен вузол може надсилати дані не в будь-який момент часу, а лише коли загальне середовище передачі вільне й дозволяє спростити логіку роботи вузлів мережі: оскільки у кожен момент часу виконується тільки одне передавання,

зникає необхідність в буферизації кадрів у транзитних вузлах і самих транзитних вузлах. Отже, немає необхідності у складних процедурах управління потоком та боротьби з перевантаженнями. Унаслідок простоти така ідея доступу до середовища знайшла застосування як у мережах Ethernet (де коаксіальний кабель є загальним для усіх вузлів мережі), так і в мережах Token Ring та FDDI (де доступ до середовища передачі виконується за певним алгоритмом і передавати одночасно може лише один вузол).

Основним недоліком техніки роділюваного середовища є погана масштабованість, оскільки пропускна спроможність розподіляється між усіма вузлами мережі. І як тільки коефіцієнт використання загального середовища перевищує деякий поріг, черги до середовища починають зростати нелінійно, і мережа втрачає працездатність (так, наприклад, у мережах ALOHA значення цього порога складає 18%, в Ethernet – близько 30%, а у мережах Token Ring і FDDI – біля 60–70%) [1].

Алгоритм керування доступом до середовища є однією з найважливіших характеристик будь-якої технології локальних КМ. У технології Ethernet як подібний алгоритм застосовується метод випадкового доступу CSMA/CD. Основним його недоліком є суттєве зниження корисної пропускної здатності мережі при зростанні навантаження. А основною перевагою – простота, яка сприяла найвищій популярності й найбільшому відсотку використання саме цієї технології.

Технології Token Ring і FDDI використовують метод маркерного доступу, заснований на передачі від вузла до вузла особливого кадру – маркера (токена) доступу. При цьому право доступу до поділюваного кільця отримує лише той вузол, який має маркер доступу. Цей, більш детермінований характер доступу технологій Token Ring і FDDI визначив ефективніше використання розділюваного середовища, ніж для технології Ethernet, але водночас і ускладнив обладнання.

Технологія 100VG-AnyLAN передбачає більш справедливий розподіл пропускної спроможності мережі, ніж у метода CSMA/CD, і підтримує пріоритетний доступ для синхронних додатків. Проте ця технологія була створена занадто пізно – у середині 90-х років, коли переваги й доступність комутованих локальних мереж «скасували» сам принцип поділу середовища (у провідних мережах) [1].

Відмова від розділюваного середовища (на користь комутованих середовищ) фактично анулювала такий компонент технології локальних КМ (ЛКМ) як метод доступу, унаслідок чого стали зникати відмінності між технологіями ЛКМ. Оскільки під час застосування комутаторів усі зв'язки між вузлами є індивідуальними, комутовані версії мереж Ethernet і Token Ring працюють подібно, розрізняються лише формати кадрів цих технологій.

Перші стандарти технологій ЛКМ були фірмовими. Це було незручно для користувачів і для виробників мережевого обладнання. Для виправлення вказаної ситуації в інституті IEEE було організовано комітет з питань стандартизації технологій ЛКМ. Цей комітет мав номер 802, і сімейство стандартів, яке він прийняв, отримало назву IEEE 802.x. Ці стандарти містили рекомендації щодо проектування нижніх рівнів ЛКМ.

Питаннями стандартизації технологій ЛКМ займався й інститут ANSI, який для оптоволоконних мереж розробив стандарт FDDI для швидкості передачі даних 100 Мбіт/с.

Структуру стандартів IEEE 802.x наведено на рис. 1.1. Стандарти робочої групи 802.1 є загальними. У наш час ці стандарти продовжують розвиватись. Вони описують найбільш високорівневі функції ЛКМ. Тут даються визначення локальних мереж та їх властивостей, стандарти побудови складніших мереж на основі базових технологій, описується взаємодія різних технологій.

Робочі групи 802.3, 802.4, 802.5 і т. д. відповідають за стандартизацію конкретної технології. Так, наприклад, група 802.3 займалася технологією Ethernet, 802.4 – Token Bus, 802.5 – Token Ring, 802.11 – безпроводовими ЛКМ, 802.12 – ЛКМ з методом доступу за вимогою з пріоритетами (Demand Priority Access) 100VG-AnyLAN.

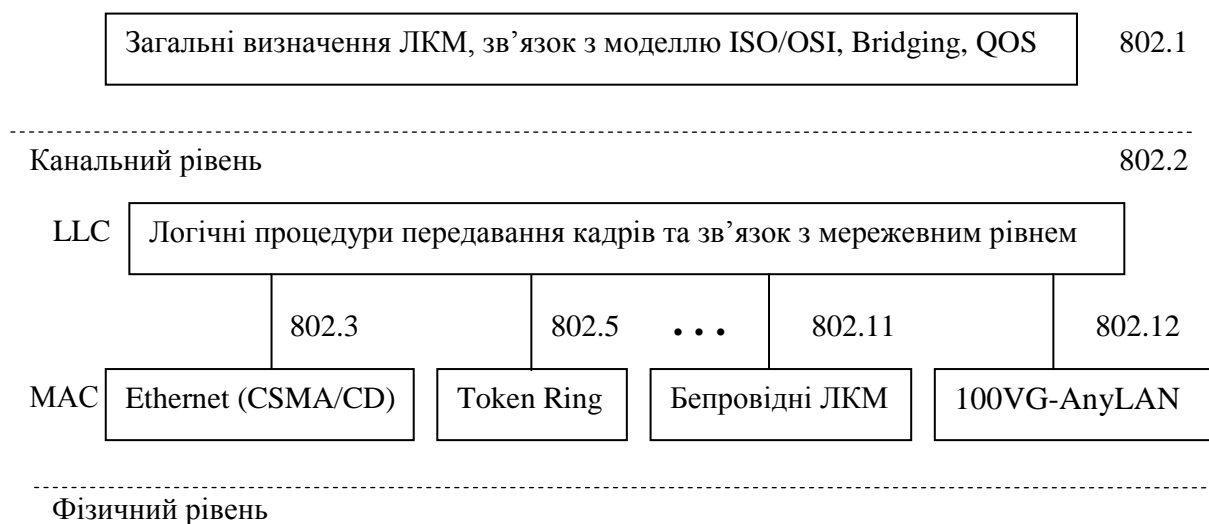


Рисунок 1.1 – Структура стандартів IEEE 802.x

З рис. 1.1 бачимо, що для кожної технології є загальний рівень 802.2, який існує завдяки тому, що комітет 802 розділив функції каналного рівня моделі OSI на два рівні: керування логічним каналом (Logical Link Control, LLC) та керування доступом до середовища (Media Access Control, MAC).

Рівень MAC вирішує питання забезпечення доступу до середовища передачі, а також надсилання кадрів між кінцевими вузлами за допомогою функцій та пристроїв фізичного рівня. Рівень LLC забезпечує для технологій ЛКМ потрібну якість послуг транспортної служби, надсилаючи кадри або дейтаграмним способом, або за допомогою процедур з установами з'єднання та відновленням кадрів.

Протокол LLC займає проміжний рівень між мережевими протоколами та протоколами рівня MAC. Мережеві протоколи надають для протоколу LLC через міжрівневий інтерфейс пакети з адресною інформацією про вузол призначення та вимоги до якості транспортних послуг. Протокол LLC

інкапсулює пакет у кадр LLC, доповнюючи його певними службовими полями і, передусім, через міжрівневий інтерфейс передає свій кадр (разом з адресною інформацією про вузол призначення) відповідному протоколу рівня MAC, який інкапсулює кадр LLC у свій кадр (наприклад, кадр Ethernet).

Послуги LLC

Відповідно до стандарту 802.2, рівень керування логічним каналом LLC надає верхнім рівням три типи послуг [1]:

1) LLC1 – послуга без установлення з'єднання й без підтвердження отримання даних;

2) LLC2 – послуга з установленням з'єднання й підтвердженням отримання даних;

3) LLC3 – послуга без установлення з'єднання, але з підтвердженням отримання даних.

Послуга LLC1 передбачає дейтаграмний режим роботи, який надає користувачеві засіб для передачі даних з мінімумом витрат. Зазвичай вона використовується, коли функції відновлення даних після помилок і впорядкування даних виконуються протоколами вищерозташованих рівнів, тому немає потреби дублювати їх на рівні LLC.

Послуга LLC2 надає користувачеві можливість перед початком передачі будь-якого блоку даних встановити логічне з'єднання і (якщо потрібно) виконати процедури відновлення після помилок та впорядкування потоку цих блоків у рамках установленого з'єднання.

Послуга LLC3 використовується у випадках, коли часові витрати на встановлення логічного з'єднання перед надсиланням даних неприйнятні, а підтвердження про коректність прийому даних є необхідним. Такі випадки зустрічаються, наприклад, при використанні мереж у системах реального часу, що керують промисловими об'єктами

Використання однієї з цих послуг LLC залежить від стратегії розробників конкретного стека протоколів. Наприклад, у стеках TCP/IP та IPX/SPX рівень LLC завжди працює в режимі LLC1. А в стеку Microsoft/IBM, заснований на протоколі NetBIOS/NetBEUI, часто використовується режим LLC2. Цей же режим використовується також стеком протоколів SNA (коли на нижньому рівні застосовується технологія Token Ring).

2 СІМЕЙСТВО ТЕХНОЛОГІЙ ETHERNET

Технологія Ethernet у наш час є застарілою і, фактично, майже не використовується внаслідок низької швидкості передачі даних (10 Мбіт/с). Наразі у локальних мережах широко використовуються такі її нащадки: Fast- та Gigabit-Ethernet, що мають швидкості у 10 та 100 разів вищі, ніж в Ethernet. Проте в даному посібнику технологія Ethernet розглядається, оскільки є класичною, і саме вона дозволяє зрозуміти, з чого виходили розробники під час вирішення того чи іншого питання.

2.1 Технологія Ethernet

2.1.1 Доступ до середовища передачі даних

З моменту створення мережі Ethernet працювали в режимі колективного доступу (напівдуплексний режим). Через деякий час з'явилася можливість роботи в дуплексному (повнодуплексному) режимі роботи, який, фактично, відрізняється від першого та має вищу продуктивність. У цьому підрозділі розглянемо обидва вищевказані режими роботи.

Режим колективного доступу

У класичних мережах Ethernet до кабелю (який відіграє роль загальної шини) підключають усі вузли – і він працює в режимі колективного доступу (Multiply Access). Метод доступу до середовища передачі даних у таких мережах отримав назву методу колективного доступу з розпізнаванням носійної частоти і виявленням колізій (*carrier sense multiply access with collision detection, CSMA/CD*). Одночасно усі вузли такої мережі мають можливість миттєво (з урахуванням затримки поширення сигналу фізичним середовищем) отримати дані, які почав надсилати будь-який з вузлів на загальну шину (ЗШ) (рис. 2.1)

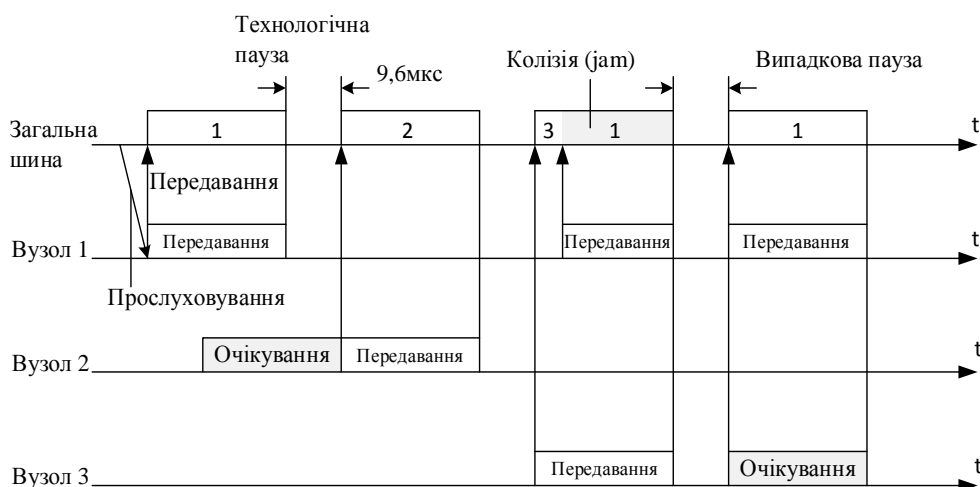


Рисунок 2.1 – Метод випадкового доступу CSMA/CD

Усі дані, що надсилаються мережею, розташовуються у кадри визначеної структури й забезпечуються унікальною адресою вузла призначення. Для того, щоб передати кадр, вузол повинен переконатися, що середовище доступу вільне. Це досягається прослуховуванням основної гармоніки сигналу, яка також називається несучою частотою (*carrier-sense, CS*). Ознакою незайнятості середовища є відсутність у ньому несучої частоти, що при манчестерському способі кодування (використовується у мережах Ethernet) дорівнює 5–10 МГц, залежно від послідовності бітів, що надсилаються у даний момент часу [1].

Якщо середовище вільне, то вузол має право почати передачу кадру. Цей кадр зображено на рис. 2.1 першим. Вузол 1 виявив, що середовище вільне, і почав передавати свій кадр. У класичній мережі Ethernet на коаксіальному кабелі сигнали передавача вузла 1 поширюються в обидва боки так, що їх отримують усі вузли мережі. Кадр даних завжди супроводжується преамбулою (*preamble*), яка складається з 7 байтів, які у двійковій системі числення мають вигляд 10101010, і 8-го байта у вигляді 10101011. Преамбула потрібна для входження приймача у побітовий і побайтовий синхронізм з передавачем.

Усі вузли, підключені до кабелю, можуть розпізнати факт передачі кадру, і той вузол, який бачить власну адресу в заголовках кадру, записує його вміст у власний внутрішній буфер. Далі обробляє отримані дані, передає їх власним протоколам стека, а потім надсилає у кабель кадр-відповідь. Адреса станції джерела міститься у вихідному кадрі, тому станція-одержувач знає, кому варто надіслати відповідь.

Під час надсилання кадру вузлом 1 вузол 2 також намагався почати передачу свого кадру (див. рис. 2.1), однак визначив, що середовище зайняте, і тому змушений чекати, поки вузол 1 не завершить передачу кадру.

Після завершення передачі кадру усі вузли мережі повинні витримати міжкадровий інтервал (*Inter Packet Gap, IPG*) або технологічну паузу в 9,6 мкс (або 96 bt, де bt – бітовий інтервал. 1 bt – це час передачі одного біта), яка потрібна для приведення мережевих адаптерів у вихідний стан та для запобігання монопольного захоплення середовища одним вузлом. Після завершення IPG вузли мають право почати передачу свого кадру, оскільки середовище вільне. Унаслідок затримки поширення сигналу кабелем не всі вузли одночасно фіксують факт завершення передачі кадру вузлом 1.

У наведеному прикладі вузол 2 дочекався завершення передачі кадру вузлом 1, зробив паузу (9,6 мкс) і почав надсилати свій кадр.

Виникнення колізії

Механізм прослуховування середовища й пауза між кадрами не гарантують уникнення ситуації, коли дві або більше станції одночасно вирішують, що середовище вільне й починають надсилати свої кадри. Кажуть, що

в такій ситуації відбувається колізія (collision), тому що вміст двох (або більшої кількості) кадрів зіштовхується на загальному кабелі й відбувається перекручування інформації. Даний факт відображено у складовій «Base (band)», присутньої у назвах усіх фізичних протоколів технології Ethernet (наприклад, 10Base-2, 10Base-T). Baseband network означає мережу з немодульованою передачею, у якій повідомлення надсилаються у цифровій формі по єдиному каналу і без частотного поділу [1].

Колізія – це нормальна ситуація у роботі мережі Ethernet, яка виникає внаслідок розподіленого характеру мережі. У прикладі, зображеному на рис. 2.2, колізію спричинило одночасне надсилання даних вузлами 3 і 1. Для виникнення колізії не обов'язково, щоб кілька станцій почали передачу абсолютно одночасно. Найімовірніше колізія виникає внаслідок того, що перший вузол починає надсилати раніше другого, але до останнього сигналу першого просто не встигають дійти і він, вирішивши, що середовище вільне, також надсилає свій кадр.

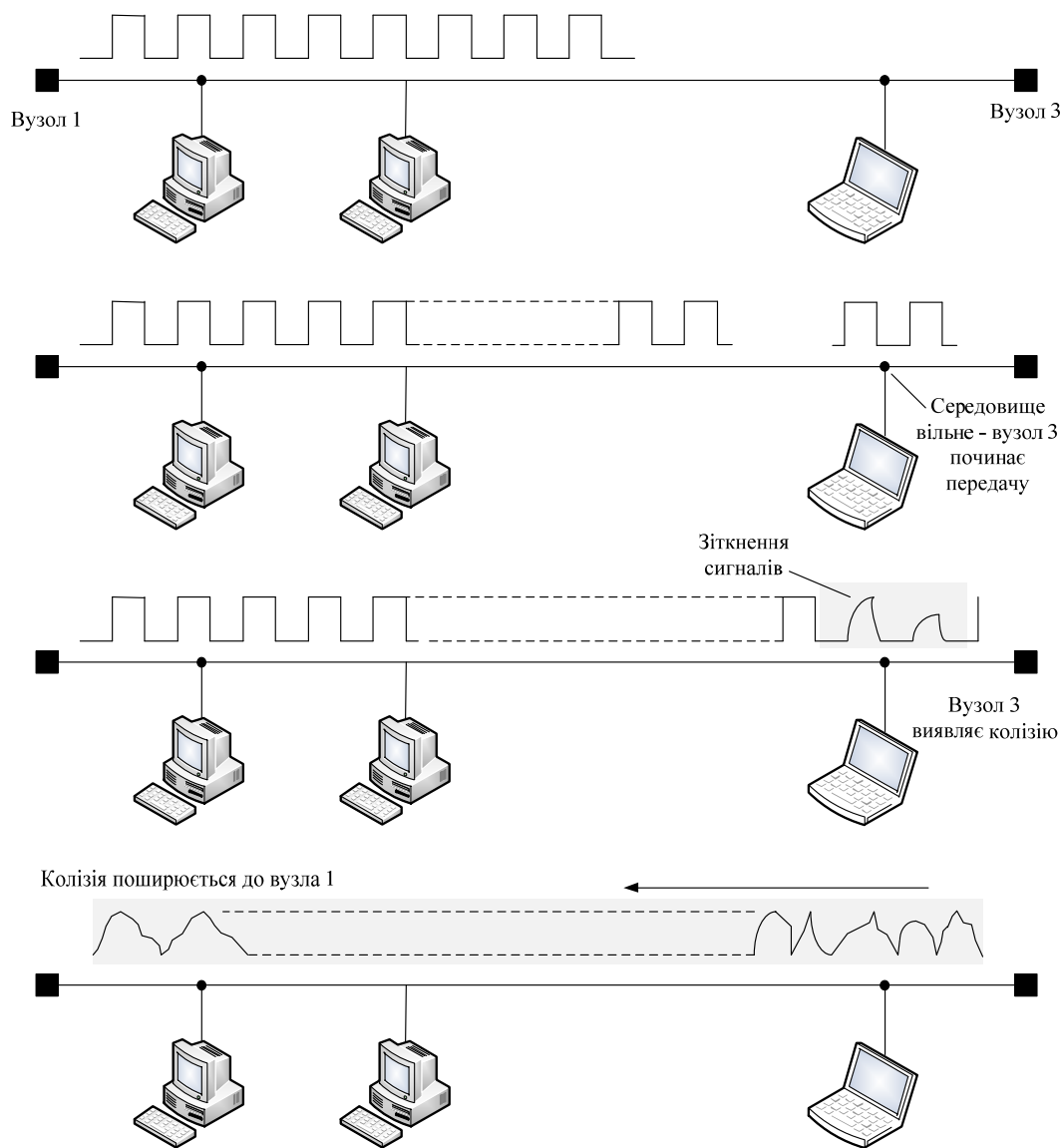


Рисунок 2.2 – Схема виникнення й розповсюдження колізії

Для коректного процесу оброблення колізії, усі станції одночасно спостерігають за сигналами у кабелі. Якщо сигнали, які передаються, і ті, що спостерігаються, відрізняються, то фіксується колізія (*collision detection, CD*). Для збільшення ймовірності якнайшвидшого виявлення колізії усіма вузлами мережі, вузол, що виявив колізію, у довільному місці перериває надсилання свого кадру й підсилює колізію, надсилаючи у мережу спеціальну jam-послідовність довжиною 32 біти. Після цього станція, що передає, виявивши колізію, повинна припинити передачу і зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища і надсилання кадру [1].

Випадкова пауза Y вибирається за таким алгоритмом:

$$Y = D \cdot L,$$

де D – інтервал відтермінування, дорівнює 512 бітовим інтервалам (бітовий інтервал позначається як bt і відповідає часу між появою двох послідовних біт даних у кабелі; для швидкості 10 Мбіт/с значення бітового інтервалу дорівнює 0,1 мкс);

L – ціле число, вибране з однаковою ймовірністю з діапазону $[0, 2N]$, де N – номер повторної спроби передачі даного кадру ($N = 1, 2, \dots, 10$).

Після десятої спроби інтервал, з якого вибирається пауза, не збільшується, отже, випадкова пауза може приймати значення від 0 до 52,4 мс. Якщо 16 послідовних спроб передачі кадру спричиняють колізію, то передавач повинен припинити спроби й відкинути цей кадр [1].

Очевидно, що метод доступу CSMA/CD має ймовірнісний характер, і ймовірність успішного отримання у своє розпорядження загального середовища залежить від завантаженості мережі. Зрозуміло, що при значній інтенсивності колізій корисна пропускна спроможність мережі Ethernet різко падає, а для зменшення інтенсивності виникнення колізій потрібно або зменшити трафік (наприклад, зменшенням кількості вузлів у сегменті), або підвищити швидкість роботи мереж.

Варто зауважити, що метод доступу CSMA/CD взагалі не гарантує вузлу, що він коли-небудь зможе отримати доступ до середовища. При невеликому завантаженні мережі ймовірність такої ситуації невелика, а у випадку його збільшення – вона також зростає. Зазначений недолік – плата за надзвичайну простоту методу, яка зробила технологію Ethernet найдешевшою (інші методи доступу – маркерний доступ мереж Token Ring і FDDI, метод Demand Priority мереж 100VG-AnyLAN – не мають такого недоліку).

Час подвійного обертання й розпізнавання колізій

Необхідною умовою коректної роботи мережі Ethernet (при напівдуплексному режимі роботи) є чітке розпізнавання колізій усіма вузлами мережі. Якщо деякий вузол, який передає, не розпізнає колізію і вирішить, що кадр даних переданий ним правильно, то цей кадр буде втрачено. Через накладення сигналів при колізії інформація кадру спотвориться, і його буде відбраковано вузлом-приймачем. Перекручену інформацію буде надіслано

повторно певним протоколом верхнього рівня (наприклад, транспортним або прикладним), але повторне передавання повідомлення протоколами верхніх рівнів відбудеться через значно більший інтервал часу (іноді навіть через кілька секунд) порівняно з мікросекундними інтервалами, якими оперує протокол Ethernet. Тому якщо колізії не будуть надійно розпізнаватися вузлами мережі Ethernet, це призведе до помітного зниження корисної пропускної здатності даної мережі [1].

Для надійного розпізнавання колізій має виконуватися співвідношення:

$$T_{\min} \geq PDV,$$

де T_{\min} – час передачі кадру мінімальної довжини;

PDV – час, за який сигнал колізії встигає розповсюдитися до найвіддаленішого вузла мережі. Оскільки в іншому випадку сигнал повинен пройти двічі між найвіддаленішими вузлами мережі (в один бік проходить невикривлений сигнал, а на зворотному шляху поширюється вже спотворений колізією сигнал), то цей час називається часом подвійного обертання (*Path Delay Value, PDV*).

При виконанні цієї умови вузол, що надсилає, повинен встигати виявляти колізію, яку спричиняє передача певного кадру, ще до того, як він завершить його передавання. Виконання даної умови залежить від довжини найменшого кадру, пропускної здатності мережі, а також довжини кабельної системи мережі й швидкості поширення сигналу в кабелі.

Усі параметри протоколу Ethernet (у тому числі мінімальна довжина кадру й максимальна відстань між вузлами у сегменті мережі) підібрані так, щоб при нормальній роботі вузлів мережі колізії завжди чітко розпізнавалися. У стандарті Ethernet прийнято, що мінімальна довжина поля даних кадру становить 46 байтів (що разом зі службовими полями дає мінімальну довжину кадру 64 байти, а разом з преамбулою – 72 байти або 576 бітів). Звідси може бути визначено обмеження на відстань між станціями.

У мережі Ethernet час передачі кадру мінімальної довжини дорівнює 575 бітових інтервалів, отже, час подвійного обертання (враховуючи, що швидкість передачі тут становить 10 Мбіт/с) повинен бути меншим ніж 57,5 мкс. Відстань, яку сигнал може пройти за цей час, залежить від типу кабелю і для товстого коаксіального кабелю дорівнює приблизно 13280 м. Враховуючи, що за цей час сигнал повинен пройти лінією зв'язку (ЛЗ) двічі, відстань між двома вузлами не повинна бути більшою ніж 6635 м. У стандарті величина цієї відстані обрана суттєво меншою, з урахуванням інших більш суворих обмежень [1].

Одне з таких обмежень пов'язане з гранично допустимим згасанням сигналу. Для забезпечення необхідної потужності сигналу під час його проходження між найвіддаленішими вузлами сегмента – максимальна довжина безперервного сегмента товстого коаксіального кабелю з урахуванням внесеного ним згасання обрана у 500 м. У такому разі умови розпізнавання колізій виконуватимуться з великим запасом для кадрів будь-якої стандартної довжини, у тому числі й 72 байти (час подвійного обер-

тання кабелем 500 м становить 43,3 бітових інтервали). Тому мінімальна довжина кадру могла би бути ще меншою. Однак розробники технології не стали зменшувати мінімальну довжину кадру, враховуючи багатосегментні мережі, які будуються з декількох сегментів, з'єднаних повторювачами [1].

Повторювачі збільшують потужність переданих із сегмента у сегмент сигналів, і стає можливим використання мережі значно більшої довжини, що складається з декількох сегментів. У коаксіальних реалізаціях Ethernet розробники обмежили максимальну кількість сегментів у мережі п'ятьма, що насамперед обмежує загальну довжину мережі 2500 м. Навіть у такій багатосегментній мережі умова виявлення колізій виконується з великим запасом. У дійсності часовий запас істотно менший, оскільки повторювачі також вносять у поширення сигналу додаткову затримку в кілька десятків бітових інтервалів. Крім того, параметри кабелю та повторювачів мають деякі відхилення.

У результаті врахування усіх цих та низки інших чинників було ретельно підібрано співвідношення між мінімальною довжиною кадру й максимально можливою відстанню між вузлами мережі (цю відстань називають також максимальним діаметром мережі), що забезпечує надійне розпізнавання колізій.

Зі збільшенням швидкості передачі кадрів, що має місце у більш нових стандартах, які базуються на методі доступу CSMA/CD (наприклад, Fast Ethernet), максимальна відстань між станціями мережі зменшується пропорційно збільшенню швидкості передачі. У стандарті Fast Ethernet вона становить близько 210 м, а у Gigabit Ethernet вона була б обмежена 25 м, якби розробники стандарту не здійснили деяких заходів щодо збільшення мінімального розміру пакета.

У табл. 2.1 наведено значення основних параметрів процедури передачі кадру стандарту 802.3, які не залежать від реалізації фізичного середовища. Зауважимо, що кожен варіант фізичного середовища технології Ethernet додає до цих обмежень свої, суворіші обмеження, які також мають виконуватися [1].

Таблиця 2.1 – Параметри рівня MAC Ethernet

Параметри	Значення
Бітова швидкість передачі даних	10 Мбіт/с
Інтервал відстрочки	512 bt
Міжкадровий інтервал (IPG)	9,6 мкс
Максимальна кількість спроб передачі	16
Максимальна кількість зростання діапазону паузи	10
Довжина jam-послідовності	32 біти
Максимальна довжина кадру (без преамбули)	1518 байтів
Мінімальна довжина кадру (без преамбули)	64 байти
Довжина преамбули	64 біти
Мінімальна довжина випадкової паузи після колізії	0 bt
Максимальна довжина випадкової паузи після колізії	524 000 bt
Максимальна відстань між вузлами мережі	2500 м
Максимальна кількість вузлів у мережі	1024

Дуплексний режим роботи

Дуплексний канал зв'язку (на відміну від напівдуплексного) підтримує передачу у двох напрямках одночасно. Але для такої передачі потрібна підтримка дуплексного зв'язку на фізичному рівні. Таку підтримку забезпечують два основних типи середовища – оптичне волокно та скручена пара (за винятком інтерфейсу 100Base-T4, який буде розглянуто нижче). Відповідна логічна топологія повинна бути «точка–точка». Проте наявність дуплексного середовища – не достатня умова існування дуплексного каналу. Наприклад, якщо використати як комунікаційний пристрій концентратор (у нього логічна топологія типу «шина») – він принципово не зможе підтримувати дуплексний режим, і одночасне передавання двох сигналів одним сегментом призведе до виникнення колізії, виявленої на рівні MAC. Тобто, для забезпечення дуплексної роботи, і порти вузлів, і порти комутаторів, і середовище передачі повинні її підтримувати. Тоді на рівні MAC паралельно функціонують приймальний і передавальний модулі, які також у дуплексному режимі взаємодіють з вищими рівнями.

Під час дуплексного режиму роботи передачі немає потреби у підтримці механізму CSMA/CD, що суттєво спрощує алгоритм передачі (тепер він полягає в тому, що вузол готує кадр для передачі; встановлює число спроб у нуль; очікує на спливання IGP з моменту останньої передачі й починає передачу; завершує передачу й встановлює статус передачі «передачу завершено»). Приймальний модуль при цьому працює без змін. Відсутність спеціальних додаткових вимог до дуплексної передачі та спрощення рівня MAC призвело до того, що багато фірм почали з 1995 року постачати комутатори та мережеві карти, що підтримують дуплексний режим. Стандартизація дуплексного Ethernet відбулася в 1997 році.

Перевагами дуплексного режиму роботи є:

- відсутність колізій;
- скорочення затримки при передачі за рахунок зникнення потреби в очікуванні припинення сигналу, що приймається (а от потреба у витримванні $IPG = 96 \text{ bt}$ між послідовними передачами кадрів залишилася);
- підвищення вдвічі ефективної смуги пропускання до 20 Мбіт/с для Ethernet;
- підвищення продуктивності роботи мережі при великому завантаженні (до 98%) по кожному з каналів;
- відсутність обмежень на довжину сегментів між вузлами мережі (наприклад, оптичний сегмент на одномодовому волокні між двома комутаторами може мати довжину до 100 км. А за наявності оптичних підсилувачів відстані можуть мати глобальний масштаб);
- краще функціонування додатків, критичних до затримок (наприклад, мультимедійний зв'язок, відеоконференції).

2.1.2 Кадри технології Ethernet

Існує декілька стандартів формату кадру Ethernet. Практично в обладнанні Ethernet використовується лише один з них – кадр Ethernet DIX, що також називають кадром Ethernet II за номером останнього стандарту DIX. Цей формат наведено на рис. 2.3.

6 байтів	6 байтів	2 байти	46 – 1500 байтів	4 байти
DA	SA	T	Дані (+ заповнювач)	FCS

Рисунок 2.3 – Формат кадру Ethernet DIX II

Розглянемо поля заголовка кадру.

DA (Destination Address) – MAC-адреса вузла призначення.

SA (Source Address) – MAC-адреса вузла відправника. Потрібна для того, щоб вузол отримувач знав, від кого надійшов кадр і кому потрібно на нього відповісти. Прийняття рішення про відповідь покладено не на протокол Ethernet, а на протоколи верхніх рівнів. Ethernet може виконати таку дію, якщо з мережевого рівня надійде відповідна вказівка.

Поле T (Type, або EtherType) містить умовний код протоколу верхнього рівня, дані якого розташовуються в полі даних кадру (наприклад, протоколу IP відповідає шістнадцяткове значення 08-00). Це поле потрібно для підтримування інтерфейсних функцій мультиплексування й демуплексування кадрів під час взаємодії з протоколами верхніх рівнів.

Поле даних може містити від 46 до 1500 байтів. Якщо ж довжина даних менша ніж 46 байтів, то це поле доповнюється заповнювачем до мінімального розміру. Така операція потрібна для коректної роботи методу доступу Ethernet.

Поле контрольної послідовності кадру (Frame Check Sequence, FCS) складається з 4 байтів контрольної суми, яка обчислюється за алгоритмом CRC-32.

Кадр Ethernet DIX (II) не відображає поділ каналного рівня Ethernet на рівень MAC і рівень LLC: його поля підтримують функції обох рівнів. Наприклад, інтерфейсні функції поля T стосуються функцій рівня LLC, усі інші поля підтримують функції рівня MAC.

Існують ще три стандарти формату кадру Ethernet:

– кадр 802.3/LLC є стандартом комітету IEEE 802 і побудований відповідно з прийнятим розбиттям функцій каналного рівня на рівень MAC і LLC. Тому остаточний кадр є вкладенням кадру LLC (визначається стандартом 802.2) у кадр MAC (визначається стандартом 802.3);

– кадр Raw 802.3 або Novell 802.3 з'явився в результаті зусиль компанії Novell з прискорення розробки свого стека протоколів в мережах Ethernet;

– кадр Ethernet SNAP став результатом діяльності комітету 802.2 з приведення попередніх форматів кадрів до деякого загального стандарту й надання кадру необхідної гнучкості для обліку в майбутньому можливостей додавання полів або зміни їх призначення.

Варто зазначити, що кадри останніх трьох форматів фактично не використовуються сьогодні, унаслідок більш складного формату, який виявився непотрібним в умовах снування єдиної технології каналного рівня. Тому розглядати їх у межах даного навчального посібника недоцільно.

2.1.3 Розрахунок продуктивності Ethernet

Кількість оброблюваних кадрів Ethernet за секунду часто вказується як основна характеристика продуктивності комутаторів та маршрутизаторів. Визначимо чисту максимальну пропускну здатність сегмента Ethernet у кадрах за секунду в ідеальному випадку, коли у мережі немає колізій і додаткових затримок, внесених комутаторами та маршрутизаторами. Такий показник допомагає оцінити вимоги до продуктивності комунікаційних пристроїв, оскільки в кожен порт пристрою за одиницю часу не може надходити більше кадрів, ніж це дозволяє зробити відповідний протокол.

Очевидно, для комунікаційного обладнання найважчим режимом є обробка кадрів мінімальної довжини, оскільки на обробку кожного кадру комутатор або маршрутизатор витрачає приблизно однаковий час. А кількість кадрів мінімальної довжини, що надходять на пристрій за одиницю часу, більша, ніж кадрів будь-якої іншої довжини. Інша характеристика продуктивності комунікаційного устаткування – біт за секунду використовується рідше, оскільки вона не говорить про те, якого розміру кадри при цьому обробляв пристрій, а на кадрах максимального розміру досягти високої продуктивності, вимірюваної у бітах в секунду, набагато легше.

Розрахуємо максимальну продуктивність сегмента Ethernet у кількості переданих кадрів (пакетів) мінімальної довжини за секунду (при вказанні пропускну спроможності мереж терміни «кадр» і «пакет», зазвичай, використовуються як синоніми, і, відповідно, аналогічними є й одиниці вимірювання продуктивності frames-per-second, fps і packets-per-second, pps.).

Для розрахунку потрібно згадати, що розмір кадру мінімальної довжини разом із преамбулою становить 72 байти (576 бітів), тому на його передачу витрачається 57,6 мкс. Додавши міжкадровий інтервал, який становить 9,6 мкс, отримуємо, що період проходження кадрів мінімальної довжини становить 67,2 мкс. Звідси максимально можлива пропускну спроможність сегмента Ethernet – 14 880 кадрів за секунду. Проте ця величина може бути менша за рахунок очікування вузлами доступу до середовища (як внаслідок його продуктивної зайнятості, так і в результаті наявності колізій, що призводять до необхідності повторних передач кадрів).

Кадри максимальної довжини технології Ethernet займають 1500 байтів, разом зі службовою інформацією – 1518 байтів, а з преамбулою – 1526 байтів (12208 бітів). Отже, враховуючи час міжкадрового інтервалу отримуємо, що максимально можлива пропускну здатність сегмента Ethernet для кадрів максимальної довжини становитиме 813 кадрів за секунду.

Тепер розрахуємо, яку максимальну корисну пропускну здатність мають сегменти Ethernet при використанні кадрів різного розміру. Зауважимо, що корисна пропускну здатність протоколу – це швидкість передачі користувачьких даних, які переносяться полем даних кадру. Ця пропускну здатність завжди менша від номінальної бітової швидкості протоколу Ethernet за рахунок таких факторів:

- службової інформації кадру;
- міжкадрових інтервалів (IPG);
- очікування доступу до середовища.

Отже, для кадрів мінімальної довжини корисна пропускну здатність дорівнює:

$$C_{к.мін} = 14880 \cdot 46 \cdot 8 = 5,48 \text{ Мбіт/с},$$

що набагато менше ніж 10 Мбіт/с. Проте необхідно пам'ятати, що кадри мінімальної довжини використовуються переважно для передачі квитанцій, отже, до передачі даних файлів ця швидкість відношення не має.

Для кадрів максимальної довжини корисна пропускну здатність дорівнює:

$$C_{к.мах} = 813 \cdot 1500 \cdot 8 = 9,76 \text{ Мбіт/с},$$

що дуже близько до номінальної швидкості протоколу. Ще раз акцентуємо, що такої швидкості можна досягти тільки тоді, коли двом вузлам у мережі Ethernet інші вузли не заважають, що буває досить рідко.

При використанні кадрів середнього розміру з полем даних у 512 байтів пропускну спроможність мережі становитиме 9,29 Мбіт/с, що теж досить близько до граничної пропускну здатності у 10 Мбіт/с.

Варто зазначити, що отримані вище значення продуктивності мережі є дещо завищеними, адже на продуктивність, крім розміра кадру, впливає й багато інших факторів, основними серед яких є [2, 3, 4]:

- використовувані комунікаційні протоколи та їх параметри;
- топологія мережі та використовуване комунікаційне обладнання;
- інтенсивність виникнення й характер помилкових ситуацій (у тому числі й колізій);
- конфігурація програмного й апаратного забезпечення кінцевих вузлів;
- ступінь завантаженості процесорів.

Відношення поточної пропускну спроможності мережі до її максимальної пропускну спроможності називається коефіцієнтом використання мережі (*network utilization*). Під час визначення поточної пропускну спроможності береться до уваги передавання мережею будь-якої інформації (як користувачької, так і службової). Коефіцієнт є важливим показником для технологій середовищ, що поділяються, оскільки при випадковому характері методу доступу високе значення коефіцієнта використання часто говорить

про низьку корисну пропускну спроможність мережі (тобто швидкості передачі призначених користувацьких даних), де дуже багато часу вузли витрачають на процедуру отримання доступу й повторні передачі кадрів після колізій.

2.1.4 Специфікації фізичного середовища Ethernet

Унаслідок того, що сьогодні технологія Ethernet є застарілою, у межах даного посібника доцільно стисло розглянути специфікації її фізичного середовища (детальніше це питання розглянуто, наприклад, у [1]).

Відомі такі фізичні специфікації технології Ethernet.

– **Стандарт 10Base-5** передбачає використання коаксіального кабелю діаметром 0,5 дюйма (називається «товстий» коаксіал) з хвильовим опором 50 Ом. Максимальна довжина сегмента становить 500 м без повторювачів. Для збільшення діаметра мережі передбачається використання до чотирьох повторювачів (тоді довжина мережі зростає до 2 500 м.). Проте лише до трьох сегментів з п'яти можуть підключатися кінцеві вузли, а між навантаженими сегментами повинні бути ненавантажені сегменти (правило «5-4-3»). Мережа, побудована за таким стандартом вважається класичним Ethernet.

– **Стандарт 10Base-2** передбачає використання коаксіального кабелю діаметром 0,25 дюйма (називається «тонкий» коаксіал) з хвильовим опором 50 Ом. Максимальна довжина сегмента становить 185 м без повторювачів. Збільшення діаметра мережі може бути здійснено за правилом «5-4-3» аналогічно стандарту 10Base-5.

– **Стандарт 10Base-T** передбачає застосування кабелю на основі неекранованої скрученої пари (*Unshielded Twisted Pair, UTP*). Дозволяє реалізувати зіркоподібну топологію на основі концентратора. Відстань між концентратором і кінцевим вузлом не повинна перевищувати 100 м. Для збільшення діаметра мережі передбачається використання до чотирьох хабів (правило чотирьох хабів).

– **Стандарт 10Base-F** передбачає застосування волоконно-оптичного кабелю. Топологія аналогічна топології стандарту 10Base-T. Є декілька варіантів цієї специфікації:

- FOIRL (відстань – до 1 000 м),
- 10Base-FL (відстань – до 2 000 м),
- 10Base-FB (відстань – до 2 000 м).

Число 10 у зазначених вище назвах позначає бітову швидкість передачі даних цих стандартів – 10 Мбіт/с; слово Base (Baseband) – метод передачі на одній базовій частоті 10 МГц (на відміну від методів, які використовують кілька носійних частот і називаються Broadband – широкополосними); останній символ у назві стандарту фізичного рівня – тип кабелю.

Основні характеристики фізичних інтерфейсів стандарту IEEE 802.3 наведено у табл. 2.2

Таблиця 2.2 – Фізичні інтерфейси стандарту Ethernet

Характеристика	10Base5	10Base2	10Base-T	10Base-FL
Середовище передачі	Товстий коаксіальний кабель	Тонкий коаксіальний кабель	Скручена пара UTP категорії 3 і вище	БОВ (довжина хвилі 850 нм або 1310 нм) або ООВ (довжина хвилі 1310 нм)
Порт пристрою	AUI	BNC	RJ-45 (MDI або MDI-X)	ST
Фізичне кодування	Манчестерський код			Манчестерський код on-off
Фізична топологія	Шина	Шина	Зірка, дерево	Зірка, дерево
Логічна топологія	Шина	Шина	Шина	Шина
Довжина сегмента	До 500 м	До 185 м	до 100 м	до 2000 м для БОВ, до 100 км для ООВ*

Примітка. Скорочення БОВ та ООВ означають багатомодове та одномодове оптичне волокно, відповідно; MDI та MDI-X – інтерфейс мережевої карти та інтерфейс портів повторювача або комутатора; * – під час використання ООВ довжина сегмента обмежується максимальним діаметром колізійного домена Ethernet, а якщо зв'язок здійснюється між двома комутаторами в дуплексному режимі передачі, то відстань може досягати 100 км.

2.2 Технологія Fast Ethernet

2.2.1 Загальні відомості

Класичний Ethernet (швидкість передачі 10 Мбіт/с) влаштував більшість користувачів протягом 15 років. Проте на початку 90-х років почала відчуватися його недостатня пропускна спроможність і виникла необхідність у розробці технології, яка б мала продуктивність 100 Мбіт/с та була б такою ж ефективною (у співвідношенні ціна–якість) як Ethernet. У результаті пошуків і досліджень фахівці розділилися на два табори, кожен з яких запропонував нову технологію: Fast Ethernet і 100VG-AnyLAN, які відрізняються ступенем спадкоємності з класичним Ethernet [1].

У 1992 році група виробників мережевого обладнання, разом з такими лідерами технології Ethernet, як SynOptics та 3Com утворили некомерційне об'єднання Fast Ethernet Alliance для розробки стандарту нової технології, що повинна була максимально зберегти особливості технології Ethernet. Пропозиція Fast Ethernet Alliance забезпечувала спадкоємність й узгодженість мереж 10 Мбіт/с і 100 Мбіт/с, зберігши метод випадкового методу доступу CSMA/CD.

Другий табір (мав підтримку значно меншої кількості виробників у мережевій індустрії, ніж Fast Ethernet Alliance) очолили компанії Hewlett-Packard, AT&T (потім і IBM), які вирішили усунути деякі відомі недоліки технології Ethernet. Вони запропонували абсолютно новий метод доступу *Demand Priority* – пріоритетний доступ за вимогою, який суттєво змінював

правила поведінки вузлів у мережі, а тому не міг вписатися у технологію Ethernet і стандарт 802.3. Унаслідок цього для його стандартизації було організовано новий комітет IEEE 802.12.

За період з кінця 1992 року по кінець 1993 року група IEEE вивчила вищевказані 100-мегабітні рішення і восени 1995 року ці обидві технології стали стандартами IEEE. Комітет IEEE 802.3 прийняв специфікацію Fast Ethernet як стандарт 802.3u, що є не самостійним стандартом, а лише доповненням до існуючого стандарту 802.3. А комітет 802.12 прийняв технологію 100VG-AnyLAN (розглянута в підрозділі 4.3 посібника), яка використовує новий метод доступу Demand Priority і підтримує кадри двох форматів – Ethernet і Token Ring. Проте через деякий час технологія 100VG-AnyLAN перестала використовуватися, здебільшого внаслідок того, що була набагато складнішою за Fast Ethernet, а також внаслідок переведення локальних мереж на повністю комутовані версії (відмова від розділюваного середовища передачі, концентраторів), що, фактично, звело нанівець переваги технології 100VG-AnyLAN.

2.2.2 Продуктивність Fast Ethernet

Характеристики продуктивності Fast Ethernet залежать від багатьох факторів. Оцінимо корисну пропускну спроможність Fast Ethernet для кадрів мінімальної та максимальної довжини. Розмірковуючи (як і у випадку Ethernet зі швидкістю 10 Мбіт/с) та враховуючи, що у Fast Ethernet формат кадру залишився незмінним (як і в Ethernet), бітова швидкість збільшилася в 10 разів, а міжкадровий інтервал зменшився в 10 разів, отримуємо такі характеристики:

- максимальна швидкість протоколу в кадрах за секунду (для кадрів мінімальної довжини з полем даних 46 байтів) становить 148 800;
- корисна пропускну здатність для кадрів мінімальної довжини дорівнює 54,8 Мбіт/с;
- корисна пропускну здатність для кадрів максимальної довжини (поле даних 1500 байтів) дорівнює 97,6 Мбіт/с.

Варто зауважити, що як і у випадку мережі Ethernet, на продуктивність Fast Ethernet, крім розміру кадру, впливає і багато інших параметрів. Детальніше про оцінку продуктивності можна дізнатися з [4].

2.2.3 Специфікації фізичного середовища Fast Ethernet

Усі відмінності технології Fast Ethernet від Ethernet мають місце на фізичному рівні, а рівні MAC і LLC у них залишилися тими ж, і їх описують колишні глави стандартів 802.3 і 802.2. Тому доцільно розглянути лише фізичний рівень Fast Ethernet.

Порівняно з Ethernet технологія Fast Ethernet має дещо складнішу структуру фізичного рівня (рис. 2.4) і в ній передбачено використання трьох варіантів кабельних систем:

- волоконно-оптичний багатомодовий кабель (використовуються два волокна);
- скручена пари категорії 5 (використовуються дві пари);
- скручена пари категорії 3 (використовуються чотири пари).

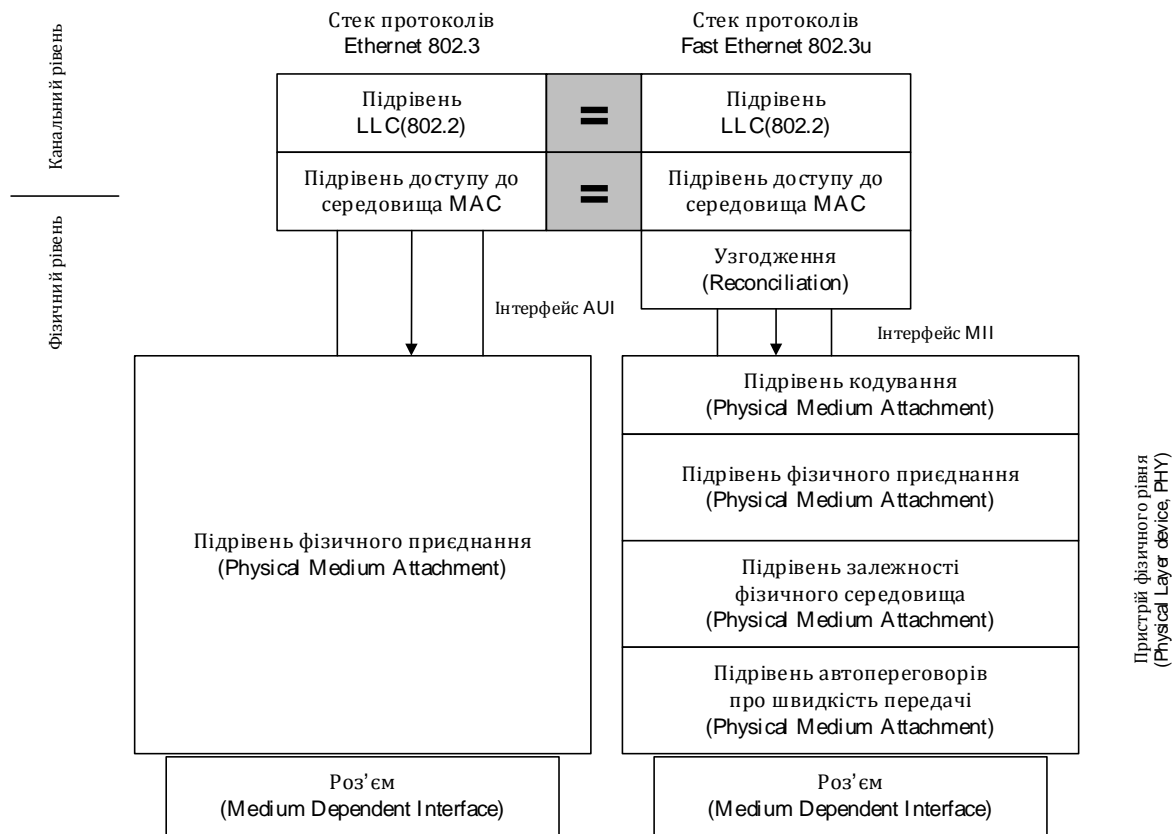


Рисунок 2.4 – Відмінності технологій Ethernet і Fast Ethernet

Коаксіальний кабель у число середовищ передачі даних технології Fast Ethernet не потрапив, оскільки на невеликих відстанях скручена пара категорії 5 дозволяє передавати дані з тією же швидкістю, що й коаксіальний кабель, але у першому випадку мережа виходить дешевшою та зручнішою в експлуатації. На великих же відстанях у коаксіального кабелю вирає оптичне волокно, оскільки має набагато більшу ширину смуги пропускання і не потребує високих витрат на пошук й усунення несправностей, які характерні для великих кабельних коаксіальних систем.

Варто зазначити, що ще у середині 1990-х років у ЛКМ починають широко використовувати комутатори, і протокол Fast Ethernet може працювати у повнодуплексному режимі, у якому немає обмеження на загальну довжину мережі, а залишаються тільки обмеження на довжину фізичних сегментів, що з'єднують сусідні пристрої (вузол – комутатор, комутатор – комутатор).

Офіційний стандарт 802.3u установив три різні специфікації для фізичного рівня Fast Ethernet:

- **100Base-TX** – для двопарного кабелю на основі неекранованої скрученої пари UTP категорії 5 або екранованої скрученої пари STP типу 1;
- **100Base-FX** – для багатомодового оптоволоконного кабелю з двома волокнами;
- **100Base-T4** – для кабелю з чотирьох пар на основі неекранованої скрученої пари UTP категорії 3 або вище.

Для усіх вищевказаних трьох стандартів формати кадрів технології Fast Ethernet не відрізняються від форматів кадрів технологій 10-мегабітного Ethernet. Міжкадровий інтервал (IPG) дорівнює 0,96 мкс, а бітовий інтервал дорівнює 10 нс. Усі часові параметри алгоритму доступу (інтервал відтермінування, час передачі кадру мінімальної довжини тощо), вимірюються у бітових інтервалах, які залишилися старими, тому зміни у розділі стандарту, що стосуються рівня MAC, не вносилися. Ознакою вільного стану середовища є передача по ньому символу простою джерела (Idle) – відповідного надлишкового коду (а не відсутність сигналів, як у стандартах Ethernet 10 Мбіт/с).

Фізичний рівень має три елементи:

- рівень узгодження (*reconciliation sublayer*), який потрібен для того, щоб рівень MAC, розрахований на інтерфейс AUI, мав змогу працювати з фізичним рівнем через інтерфейс MII;
- незалежний від середовища інтерфейс (*Media Independent Interface, MII*);
- пристрій фізичного рівня (*Physical layer device, PHY*), який складається з підрівнів:
 - логічного кодування даних, що перетворює байти, які надходять від рівня MAC, у символи коду 4В/5В (для 100Base-FX/TX) або 8В/6Т (для 100Base-T4);
 - фізичного приєднання й підрівня залежності від фізичного середовища (PMD), що забезпечують формування сигналів відповідно до методу фізичного кодування, наприклад, NRZI (для 100Base-T4/FX) або MLT-3 (для 100Base-TX) (детальніше про фізичне кодування можна дізнатися у першій частині цього посібника);
 - автопереговорів, що дозволяє двом портам, які взаємодіють автоматично вибрати найефективніший режим роботи, наприклад, напівдуплексний чи повнодуплексний (цей підрівень є факультативним).

Інтерфейс MII підтримує незалежний від фізичного середовища спосіб обміну даними між підрівнями MAC і PHY. Цей інтерфейс за призначенням аналогічний інтерфейсу AUI класичного Ethernet, за винятком того, що інтерфейс AUI розташовувався між підрівнем фізичного кодування сигналу (для будь-яких варіантів кабелю використовувався однаковий метод фізичного кодування – манчестерський код) і підрівнем фізичного приєднання до середовища, а інтерфейс MII розташовується між підрівнем MAC і підрівнями кодування сигналу, яких у стандарті Fast Ethernet є три: FX, TX, T4.

Специфікації 100Base-FX/TX

Сьогодні широко використовуються мережі специфікацій 100Base-FX і 100Base-TX. Оскільки між ними є багато спільного, то загальні для двох специфікацій властивості нижче подаються під узагальненою назвою 100Base-FX/TX.

Тоді як Ethernet зі швидкістю передачі 10 Мбіт/с використовує лише фізичне кодування (манчестерське) для представлення даних при передачі по кабелю, у стандарті Fast Ethernet це кодування вже не використовується, оскільки не є ефективним за такої швидкості. Замість нього тут застосовується і логічне кодування, і фізичне (рішення з одним фізичним кодуванням знайдено не було). Як логічне застосовується кодування 4В/5В (кожні 4 біти вихідного коду замінюються на 5 бітів. Така надлишковість дозволяє відбракувати помилкові символи), а як фізичне – або NRZI (у 100Base-FX), або MLT-3 (у 100Base-TX).

Як зазначалося вище, ознакою вільного стану середовища у Fast Ethernet є передача по ньому символу Idle, що має вигляд п'яти двійкових одиниць (11111) коду 4В/5В. Для відокремлення кадру від символів Idle на початку кадру використовується комбінація символів Start Delimiter (пара символів J (11000) і K (10001). SFD (*start frame delimiter*) означає початок кадру. Після завершення кадру перед першим символом Idle вставляється символ T (01101) (рис. 2.5).

Преамбула Idle	JK	Преамбула	SFD	DA	SA	L	Дані	CRC	T	Преамбула Idle
Середовище вільне		Кадр Fast Ethernet								Середовище вільне

Рисунок 2.5 – Неперервний потік даних специфікації 100Base-FX/TX

На відміну від специфікації 100Base-FX, у 100Base-TX використовується функція автопереговорів (*Auto-negotiation*) для вибору режиму роботи порту. Автопереговори дозволяють двом фізично з'єднаним пристроям обрати зручний режим роботи. Звичайно автопереговори відбуваються у випадку використання мережевого адаптера, який може працювати на швидкостях 10 і 100 Мбіт/с.

Взагалі визначено 5 різних режимів роботи, що можуть підтримувати пристрої 100Base-TX/T4 на скручених парах:

- 1) 10Base-T;
- 2) дуплексний режим 10Base-T;
- 3) 100Base-TX;
- 4) 100Base-T4;
- 5) дуплексний режим 100Base-TX.

Режим 10Base-T має найнижчий пріоритет у переговорному процесі, а дуплексний режим 100Base-TX – найвищий. Переговорний процес відбувається при ввімкненні живлення пристрою, а також може бути ініційований у будь-який момент модулем керування пристрою.

Пристрій, що почав процес автопереговорів, надсилає своєму партнеру пачку спеціальних імпульсів Fast Link Pulse burst (FLP), у якій міститься восьмибітне слово, що кодує запропонований режим взаємодії, починаючи з найпріоритетнішого, який підтримується даним вузлом. Якщо вузол-партнер підтримує функцію auto-negotiation і може підтримувати запропонований режим, він відповідає пачкою імпульсів FLP, у якій підтверджує даний режим, і на цьому переговори закінчуються. Якщо ж вузол-партнер може підтримувати менш пріоритетний режим, то він вказує його у відповіді, і цей режим вибирається як робочий. Таким чином, завжди вибирається найбільш пріоритетний загальний режим вузлів.

Вузол, що підтримує тільки технологію 10Base-T, кожні 16 мс надсилає манчестерські імпульси для перевірки цілісності лінії, що зв'язує його із сусіднім вузлом. Такий вузол не розуміє запит FLP, що робить йому вузол з функцією Auto-negotiation, і продовжує надсилати свої імпульси. Вузол, який отримав у відповідь на запит FLP лише імпульси перевірки цілісності лінії, розуміє, що його партнер може працювати тільки за стандартом 10Base-T, та встановлює цей режим роботи й для себе.

Специфікація 100Base-T4

Версія 100Base-T4 була тимчасовою, оскільки дозволяла у 10 разів підвищити швидкість класичного Ethernet, використовуючи поширені на той час кабельні системи категорії 3. Передусім розробники цієї технології мали за мету фізичну специфікацію, найбільш близьку до специфікацій 10Base-T і 10Base-F. У подальшому більшість організацій досить швидко замінила їх на кабельні системи категорії 5 – і потреба у вищевказаній версії відпала.

Підвищення загальної пропускної здатності у 100Base-T4 досягається за рахунок одночасної передачі потоків бітів по усіх чотирьох парах кабелю. Як логічне кодування тут використовується 8В/6Т (воно має вузький спектр сигналу і при швидкості 33 Мбіт/с вкладається у смугу 16 МГц скрученої пари категорії 3; при кодуванні 4В/5В спектр сигналу в цю смугу не вкладається), де кожні 8 бітів інформації рівня MAC кодуються шістьма трійковими цифрами (*ternary symbols*), що мають три стани. Кожна трійкова цифра має тривалість 40 нс. Група з шести трійкових цифр потім передається на одну з трьох передавальних скручених пар незалежно і послідовно. Четверта пара завжди використовується для прослуховування несучої частоти з метою виявлення колізії. Швидкість передачі даних по кожній із трьох пар для передачі дорівнює 33,3 Мбіт/с, тому загальна швидкість протоколу 100Base-T4 – 100 Мбіт/с. Водночас через прийнятий спосіб кодування швидкість зміни сигналу на кожній парі дорівнює всього 25 Мбод, що і дозволяє використовувати скручену пару категорії 3. Як фізичне кодування у специфікації 100Base-T4 використовується NRZI.

Фізичні інтерфейси стандарту Fast Ethernet (IEEE 802.3u) та їх основні характеристики наведено у табл. 2.3.

Таблиця 2.3 – Фізичні інтерфейси стандарту Fast Ethernet

Фізичний інтерфейс	100Base-FX	100Base-TX	100Base-T4
Середовище передавання	Оптичне волокно	Скручена пара UTP категорії 5	Скручена пара UTP категорії 3, 4, 5
Порт пристрою	Duplex SC	RJ-45	RJ-45
Логічне кодування	4B/5B	4B/5B	8B/6T
Фізичне кодування	NRZI	MLT-3	NRZI
Кількість скручених пар або волокон	2 волокна	2 скручені пари	4 скручені пари
Довжина сегмента	до 412 м (БОВ), до 2 км (БОВ при ДРП), до 100 км (ООВ при ДРП)	до 100 м	до 100 м

Примітка. Скорочення БОВ та ООВ означають багатомодове та одномодове оптичне волокно відповідно, а ДРП – дуплексний режим передачі.

2.3 Технологія Gigabit Ethernet

2.3.1 Загальні відомості

Досить швидко після появи на ринку продуктів Fast Ethernet під час побудови корпоративних мереж відчувалися деякі обмеження. У багатьох випадках сервери підключені по 100-мегабітному каналу перевантажували магістралі мереж, які також працювали на швидкості 100 Мбіт/с. Виникла потреба у підвищенні швидкостей.

Основна ідея розробників стандарту Gigabit Ethernet полягала в максимальному збереженні ідей класичної технології Ethernet при досягненні бітової швидкості у 1000 Мбіт/с. Для цього було вирішено: зберегти формати кадрів; зберегти напівдуплексну версію протоколу, що підтримує метод доступу CSMA/CD; залишити ті основні види кабелів, на яких працювали мережі Ethernet та Fast Ethernet (у тому числі оптичне волокно, скручена пара UTP категорії 5, екранована скручена пара) [1].

Незважаючи на те, що у Gigabit Ethernet не стали реалізовувати нові функції, підтримка навіть досить простих функцій класичного стандарту Ethernet на швидкості 1 Гбіт/с вимагала вирішення декількох досить складних завдань [1]:

– *Забезпечення прийняттого діаметра мережі для роботи на розділюваному середовищі.* У зв'язку з обмеженнями, що накладаються методом CSMA/CD на довжину кабелю, версія Gigabit Ethernet для розділюваного середовища допускала б довжину сегмента усього в 25 м при збереженні незмінними розміру кадрів й усіх параметрів методу CSMA/CD. А оскільки є велика кількість застосувань, що вимагають діаметра мережі хоча б 200 м, необхідно було розв'язувати цю задачу за рахунок якомога менших змін у технології Fast Ethernet.

– *Досягнення бітової швидкості 1000 Мбіт/с на оптичному кабелі.* Технологія Fibre Channel, фізичний рівень якої був узятий за основу оптоволоконної версії Gigabit Ethernet, забезпечує швидкість передачі даних лише 800 Мбіт/с.

– *Використання кабелю скрученої пари.* Таку задачу, на перший погляд, здається, не можна розв'язати, адже навіть для 100-мегабітних протоколів потрібні досить складні методи кодування, щоб укласти спектр сигналу в смугу пропускання кабелю.

Для вирішення цих завдань розробникам технології Gigabit Ethernet довелося внести зміни не тільки в фізичний рівень, як це було у випадку Fast Ethernet, а й у рівень MAC.

З метою розробки протоколу максимально подібного до Ethernet, але з бітовою швидкістю 1000 Мбіт/с IEEE влітку 1996 року оголосило про створення групи 802.3z.

Досвід передавання даних на гігабітних швидкостях вже був. У територіальних мережах таку швидкість забезпечувала технологія SDH, а в локальних – Fibre Channel. Остання використовувалася переважно для підключення високошвидкісної периферії до великих комп'ютерів і забезпечувала передачу даних по волоконно-оптичному кабелю зі швидкістю, близькою до гігабітної. Саме метод кодування 8B/10B, застосовуваний у технології Fiber Channel, і був прийнятий як перший варіант фізичного рівня Gigabit Ethernet.

Стандарт 802.3z остаточно був прийнятий у 1998 році. А роботи щодо реалізації Gigabit Ethernet на скрученій парі категорії 5 були передані проблемній групі 802.3ab через складність забезпечення гігабітної швидкості на цьому типі кабелю, розрахованому на підтримку швидкості 100 Мбіт/с. Проблемна група 802.3ab успішно виконала це завдання, і версію Gigabit Ethernet для скрученої пари категорії 5 також було прийнято.

Забезпечення прийнятного діаметра мережі для роботи в розділюваному середовищі

Для розширення максимального діаметра мережі Gigabit Ethernet до 200 м у напівдуплексному режимі розробники технології зробили достатньо логічні кроки, в основі яких було відоме співвідношення часу передачі кадру мінімальної довжини і часу обороту (PDV).

Мінімальний розмір кадру було збільшено (без урахування преамбули) з 64 до 512 байтів (4096 бітів). Відповідно час обороту також можна було збільшити до 4095 бітових інтервалів, що при використанні одного повторювача зробило допустимим діаметр мережі близько 200 м (без повторювача довжина лінії зв'язку зменшується до 100 м).

Для збільшення довжини кадру до потрібного для нової технології значення мережевий адаптер повинен доповнити поле даних до 448 байтів так званім розширенням (рис. 2.6), яке має вигляд поля, заповненого нулями.

Тобто формально мінімальний розмір кадру не змінився: він, як і раніше, дорівнює 64 байти (512 бітів). Це пояснюється тим, що поле розширення розташовується після поля контрольної суми кадру (FCS). Відповідно, значення цього поля не включається в контрольну суму й не враховується при вказанні довжини поля даних у полі довжини. Поле розширення необхідне для коректного виявлення колізій.

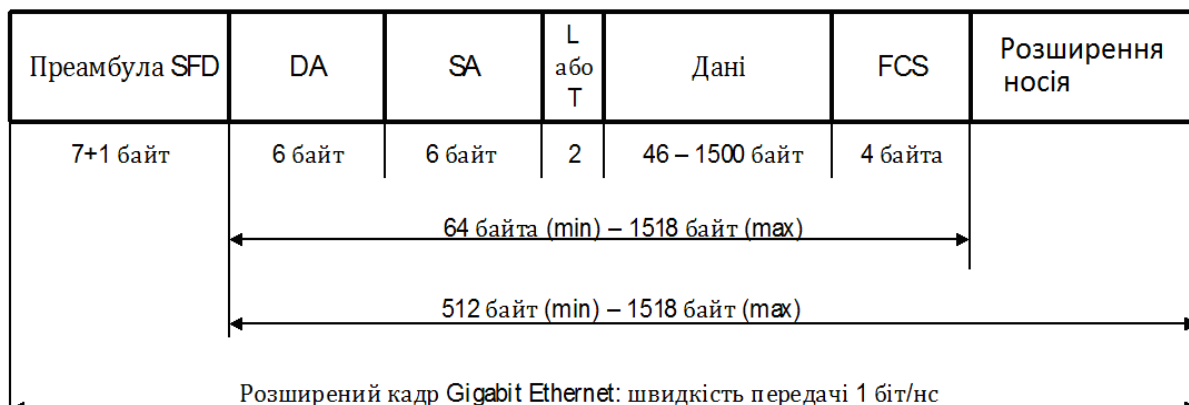


Рисунок 2.6 – Кадр Gigabit Ethernet з полем розширення носія:

SFD (*Start of Frame Delimiter*) – обмежувач початку кадру;
 DA (*Destination Address*) – адреса призначення;
 SA (*Source Address*) – адреса джерела; L (*Long*) – довжина поля даних;
 T (*Type*) – тип поля даних; FCS (*Frame Check Sequence*) – контрольна послідовність кадру

2.3.2 Продуктивність Gigabit Ethernet

Характеристики продуктивності Gigabit Ethernet залежать від того, чи використовує комутатор режим передавання кадрів з розширенням або надсилає їх у режимі пульсації. В останньому випадку на періоді пульсації ми отримуємо характеристики, які в 10 разів відрізняються від характеристик Fast Ethernet:

- максимальна швидкість протоколу в кадрах у секунду (для кадрів мінімальної довжини з полем даних 46 байтів) становить 1 488 000 кадрів;
- корисна пропускна здатність для кадрів мінімальної довжини дорівнює 548 Мбіт/с;
- корисна пропускна здатність для кадрів максимальної довжини (поле даних 1500 байтів) дорівнює 976 Мбіт/с.

Gigabit Ethernet на основі скрученої пари категорії 5

Як відомо, кожна пара кабелю категорії 5 має гарантовану смугу пропускання до 100 МГц. Для передавання таким кабелем даних зі швидкістю 1000 Мбіт/с було вирішено організувати паралельне передавання одночасно всіма чотирма парами кабелю. Це знизило швидкість передавання

даних по кожній парі до 250 Мбіт/с. Однак і для такої швидкості необхідно було придумати метод кодування зі спектром, що не перевищує 100 МГц. Код 4В/5В (використовується у Fast Ethernet) не дозволяє розв'язати поставлену задачу. Крім того, кожна нова версія повинна підтримувати не тільки класичний напівдуплексний, а й дуплексний режим. На перший погляд, здається, що одночасне використання чотирьох пар позбавляє мережу можливості працювати в дуплексному режимі, тому що не залишається вільних пар для одночасної передачі даних у двох напрямках (від та до вузла). Однак проблемна група 802.3ab знайшла шляхи вирішення обох проблем.

Для кодування даних було використано код РАМ5 з п'ятьма рівнями потенціалу: -2, -1, 0, +1, +2. У цьому випадку за один такт по одній парі передається $\log_2 5 = 2,322$ бітів інформації. Отже, для досягнення швидкості 250 Мбіт/с тактову частоту 250 МГц можна зменшити у 2,322 рази (до 108 МГц). Розробники стандарту вирішили використовувати вищу частоту – 125 МГц. При цій тактовій частоті код РАМ5 має спектр менший ніж 100 МГц, а отже, може бути надісланий без спотворень по кабелю катюго-рії 5. Крім того, у кожному такті передається не $2,322 \cdot 4 = 9,288$ біт інформації, а 8 бітів. У результаті сумарна швидкість передачі становить 1000 Мбіт/с. Передавання рівно 8 бітів у кожному такті досягається за рахунок того, що під час кодування інформації використовуються не усі $5^4 = 625$ комбінацій коду РАМ5, а лише 256 (2^8). Решту комбінацій приймач використовує для контролю прийнятої інформації і виділення правильних комбінацій на тлі шуму.

Для організації дуплексного режиму розробники специфікації 802.3ab застосували техніку виділення сигналу із сумарного. Два передавачі працюють назустріч один одному по кожній з чотирьох пар в одному і тому ж діапазоні частот (рис. 2.7). Н-образна схема гібридної розв'язки дозволяє приймачу та передавачу одного і того ж вузла використовувати одночасно скручену пару як для прийому, так і для передавання.

Для відокремлення прийому сигналу від власного приймач віднімає з результувального сигналу відомий йому свій сигнал. Це досить складна операція, і для її виконання використовуються спеціальні процесори цифрової обробки сигналу (*Digital Signal Processor, DSP*).

Варіант технології Gigabit Ethernet на скрученій парі розширив процедуру автопереговорів, введена стандартом 100Base-T, за рахунок того, що туди ще додали дуплексний і напівдуплексний режими роботи на швидкості 1000 Мбіт/с. Тому порти багатьох комутаторів Ethernet на скрученій парі є універсальними, і можуть працювати на будь-якій з трьох швидкостей: 10, 100 або 1000 Мбіт/с.

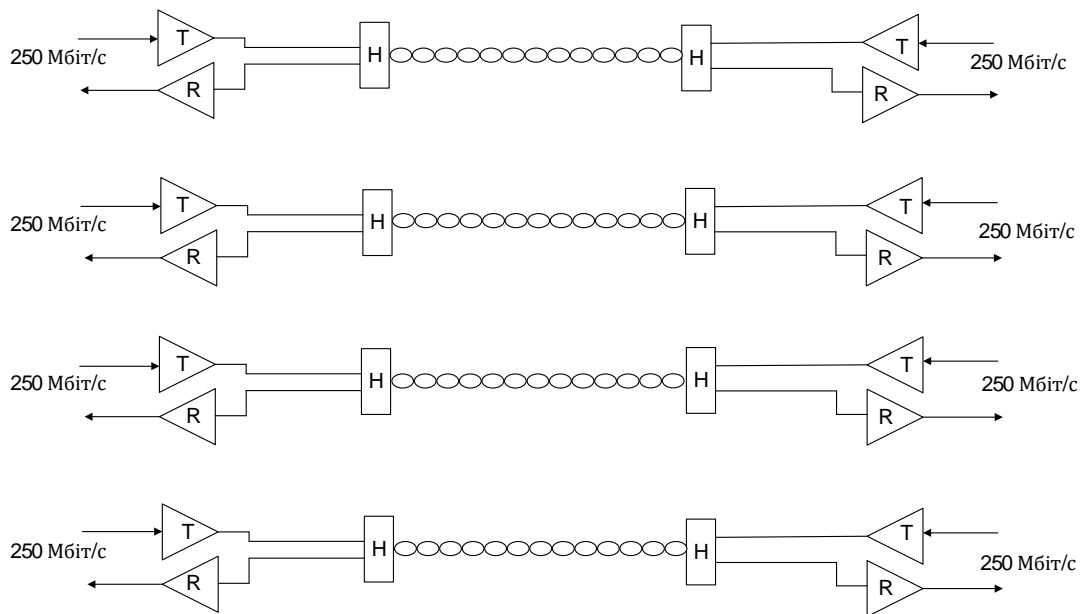


Рисунок 2.7 – Двонаправлене передавання чотирма парами UTP категорії 5

2.3.3 Специфікації фізичного середовища стандарту Gigabit Ethernet

У стандарті 802.3z визначено такі типи фізичного середовища:

- одномодовий волоконно-оптичний кабель;
- багатомодовий волоконно-оптичний кабель 62,5/125;
- багатомодовий волоконно-оптичний кабель 50/125;
- екранований збалансований мідний кабель.

Для передавання даних традиційним для КМ багатомодовим волоконно-оптичним кабелем стандарт вказує на застосування випромінювачів, що працюють на двох довжинах хвиль: 1300 і 850 нм. Застосування світлодіодів з довжиною хвилі 850 нм пояснюється тим, що вони набагато дешевші, ніж світлодіоди, які працюють на хвилі 1300 нм, хоча при цьому максимальна довжина кабелю зменшується, оскільки загасання багатомодового оптоволокна на хвилі 850 м удвічі вище, ніж на хвилі 1300 нм. Проте можливість здешевлення надзвичайно важлива для такої, загалом дорогої, технології, як Gigabit Ethernet.

Для багатомодового оптоволокна стандарт Gigabit Ethernet визначає специфікації 1000Base-SX і 1000Base-LX. У першому випадку використовується довжина хвилі 850 нм (S означає Short Wavelength), а в другому – 1300 нм (L – Long Wavelength). Специфікація 1000Base-SX дозволяє використовувати тільки багатомодовий кабель, при цьому його максимальна довжина становить близько 500 м.

Для специфікації 1000Base-LX як джерела випромінювання завжди застосовується напівпровідниковий лазерний діод довжиною хвилі 1300 нм. Специфікація 1000Base-LX дозволяє працювати як з багатомодовим (максимальна відстань до 500 м), так і з одномодовим кабелем (максимальна відстань залежить від потужності передавача та якості кабелю і може становити декілька десятків кілометрів).

Як середовище передачі даних у специфікації 1000Base-SX визначено екранований збалансований мідний кабель з хвильовим опором 150 Ом. Максимальна довжина сегмента – 25 м, тому це рішення підходить тільки для з'єднання обладнання, розташованого в одній кімнаті. Варто зауважити, що в наш час цей стандарт фактично не використовується і його замінено на 1000Base-T.

У стандарті 802.3ab (специфікація 1000Base-T) як фізичне середовище визначено скручену пару категорії 5e. Нагадаємо, що у передачі даних беруть участь 4 пари; швидкість передачі даних – 250 Мбіт/с по кожній парі; як метод кодування використовується PAM5; частота основної гармоніки становить 62,5 МГц; довжина сегмента мережі становить до 100 метрів.

Специфікацію 1000BASE-TX було створено Асоціацією телекомунікаційної промисловості (*Telecommunications Industry Association, TIA*) і опубліковано у березні 2001 року як «Специфікація фізичного рівня дуплексного Ethernet 1000 Мб/с симетричних кабельних систем категорії 6» (ANSI/TIA/EIA-854-2001). Стандарт використовує роздільні пари: одну – на прийом, іншу – на передачу. Це суттєво спрощує конструкцію приймально-передавальних пристроїв. Іншою істотною відмінністю 1000BASE-TX є відсутність схеми цифрової компенсації наведень і зворотних перешкод, у результаті чого складність, рівень енергоспоживання та ціна процесорів є нижчими, ніж у процесорів стандарту 1000BASE-T. Але для стабільної роботи тут потрібна високоякісна кабельна система. Тому 1000BASE-TX може використовувати лише кабель категорії 6. На основі даного стандарту створено велику кількість продуктів для промислових мереж.

2.4 Технологія 10-Gigabit Ethernet

Стандарт 10-Gigabit Ethernet (10G Ethernet) має позначення IEEE 802.3ae і є поправкою до основного тексту стандарту 802.3. Формат кадру тут залишився незмінним, при цьому розширення кадру, уведене у стандарті Gigabit Ethernet, не використовується, оскільки немає необхідності забезпечувати розпізнавання колізій [1].

Стандарт 802.3ae описує кілька нових специфікацій фізичного рівня, які взаємодіють з рівнем MAC за допомогою нового варіанту підрівня узгодження. Цей підрівень забезпечує для усіх варіантів фізичного рівня 10G Ethernet єдиний інтерфейс XGMII (eXtended Gigabit Medium Independent Interface – розширений інтерфейс незалежного доступу до гігабітного середовища), який передбачає паралельний обмін 4 байтами, що утворюють чотири потоки даних.

На рис. 2.8 наведено структуру інтерфейсів 10G Ethernet для фізичного рівня, що використовує оптичне волокно. Як бачимо, є три групи таких фізичних інтерфейсів: 10GBase-X, 10Gbase-R і 10GBase-W, що відрізняються способом кодування даних. У 10Base-X застосовується код 8B/10B, а у двох інших – 64B/66B. Усі вони для передачі даних використовують оптичне середовище [1].

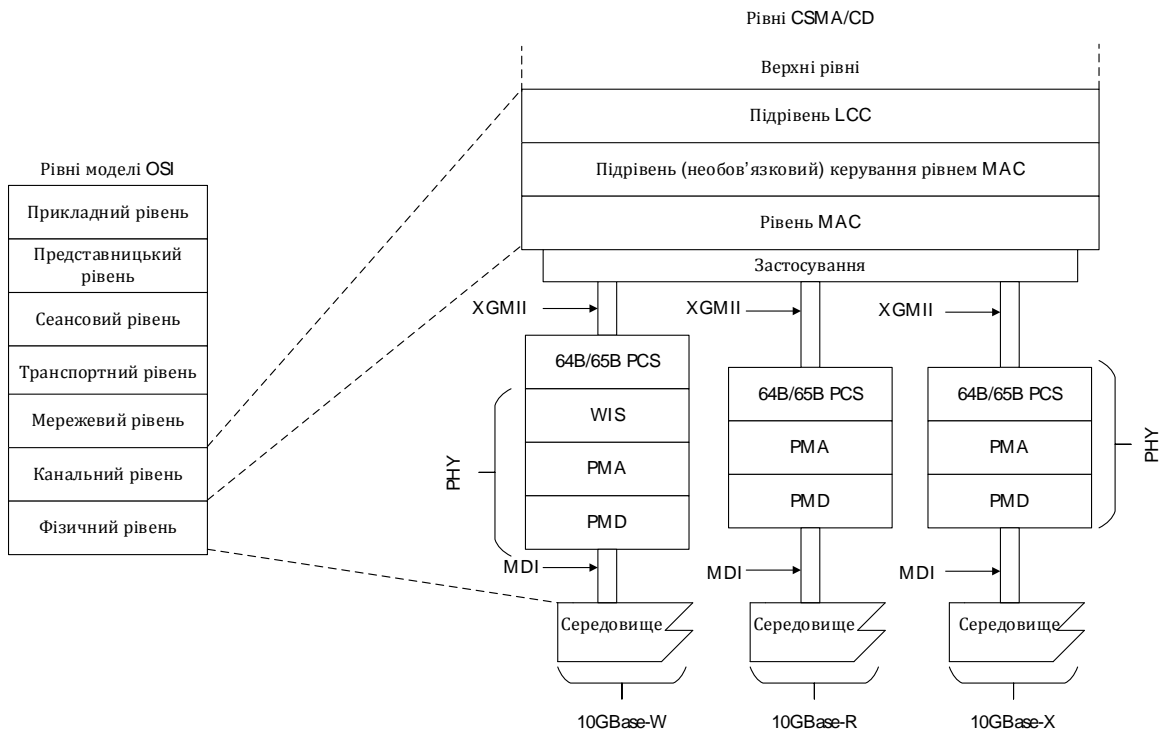


Рисунок 2.8 – Три групи фізичних інтерфейсів 10G Ethernet

Група 10GBase-X у даний час складається з одного інтерфейсу підрівня PMD – 10GBase-LX4. Літера L говорить про те, що інформація передається за допомогою хвиль другого діапазону прозорості, тобто 1310 нм. Інформація в кожному напрямку передається одночасно за допомогою чотирьох хвиль (що відображає цифра 4 в назві інтерфейсу), які мультиплексується на основі техніки WDM (рис. 2.9). Кожен з чотирьох потоків інтерфейсу XGMII передається в оптичному волокні зі швидкістю 2,5 Гбіт/с.

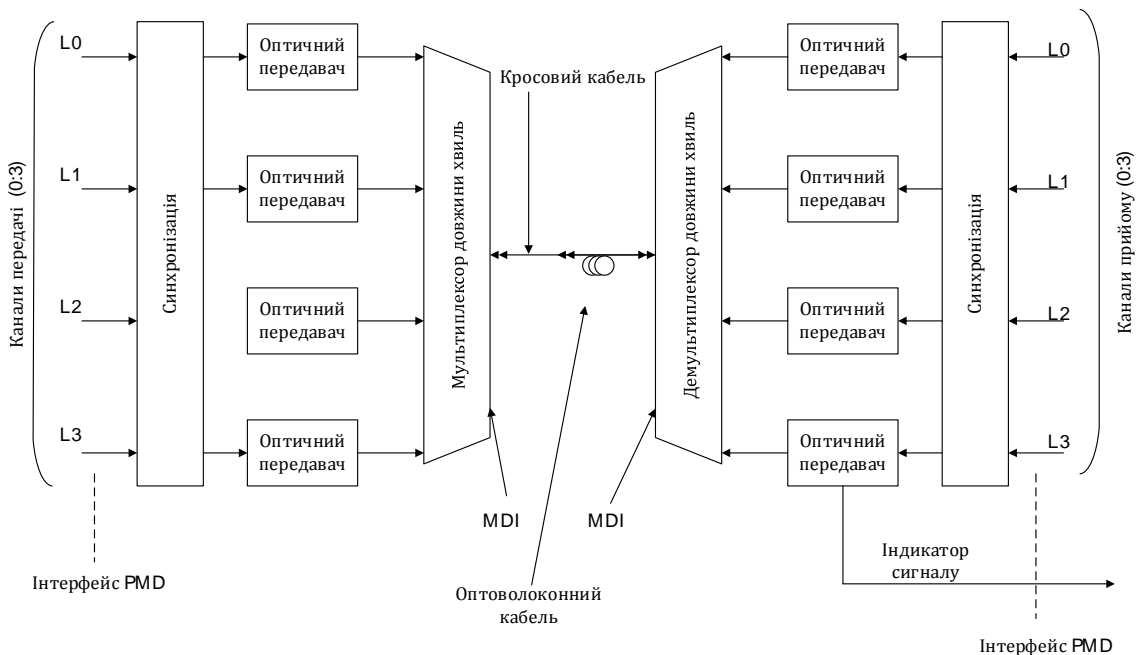


Рисунок 2.9 – Інтерфейс 10GBase-LX4

Максимальна відстань між передавачем і приймачем стандарту 10GBase-LX4 на багатомодовому оптичному волокні дорівнює 200–300 м (залежно від смуги пропускання волокна), на одномодовому – 10 км.

У кожній з груп 10GBase-W і 10GBase-R може бути три варіанти під-рівня PMD: S, L і E залежно від використовуваного для передавання інформації діапазону хвиль – 850, 1310 або 1550 нм відповідно. Отже, існують інтерфейси 10GBase-WS, 10GBase-WL, 10GBase-WE та 10GBase-RS, 10GBase-RL, 10GBase-RE. Кожен з них передає інформацію за допомогою однієї хвилі відповідного діапазону.

На відміну від 10GBase-R, фізичні інтерфейси групи 10GBase-W забезпечують швидкість передавання й формат даних, що сумісні з інтерфейсом SONET STS-192/SDH STM-64. Пропускна здатність інтерфейсів групи W дорівнює 9,95328 Гбіт/с, а ефективна швидкість передавання даних – 9,58464 Гбіт/с. Оскільки швидкість передавання інформації у цієї групи інтерфейсів нижча, ніж 10 Гбіт/с, вони можуть взаємодіяти тільки між собою, тобто з'єднання, наприклад, інтерфейсів 10GBase-RL і 10GBase-WL неможливе.

Інтерфейси групи W за електричними характеристиками не цілком сумісні з інтерфейсами SONET STS-192/SDH STM-64, тому для з'єднання мереж 10G Ethernet через первинну мережу SONET/SDH у мультиплексорів первинної мережі повинні бути спеціальні 10-гігабітні інтерфейси, сумісні зі специфікаціями 10GBase-W. Підтримка обладнанням 10GBase-W швидкості 9,95328 Гбіт/с забезпечує принципову можливість передачі трафіку 10G Ethernet через мережі SONET/SDH у кадрах STS-192/STM-64.

Фізичні інтерфейси, що працюють у вікні прозорості E, забезпечують передавання даних на відстані до 40 км, що дозволяє розгортати не лише локальні мережі, а й мережі мегаполісів. Це знайшло відображення у поправках до початкового тексту стандарту 802.3.

У 2006 році було прийнято специфікацію 10G Base-T, яка дає можливість використовувати кабелі скрученої пари категорії 6 або 6а. У першому випадку максимальна довжина кабелю не повинна перевищувати 55 м, а у другому – 100 м, що є традиційним для локальних мереж.

Контрольні запитання

1. Поясніть, чому розробники перших ЛКМ як середовище передачі даних обрали загальне середовище передачі даних?
2. Наведіть та стисло охарактеризуйте переваги й недоліки використання у КМ загального середовища передачі даних.
3. Перерахуйте відомі Вам технології ЛКМ.
4. Наведіть структуру стандартів IEEE 802.x.
5. Поясніть функції рівня MAC.
6. Поясніть функції рівня LLC.

7. Охарактеризуйте три типи послуг LLC. У яких випадках доцільно використовувати той чи інший тип послуги LLC?
8. Яке позначення IEEE має стандарт Ethernet?
9. Наведіть часову діаграму та поясніть сутність методу доступу до середовища передачі даних, що використовувався у перших мережах Ethernet.
10. Поясніть, що таке «колізія». Чому виникають колізії у мережах Ethernet?
11. Наведіть алгоритм, який використовується у мережах Ethernet для виходу з колізії.
12. Чому для мереж Ethernet дуже важливою є умова надійного розпізнавання колізій?
13. Чим пояснюється той факт, що мінімальний розмір кадру в стандарті 10Base-5 був обраний у 64 байти?
14. Поясніть, з яких міркувань обрана максимальна довжина фізичного сегмента в стандартах Ethernet?
15. У чому полягають функції преамбули й початкового обмежувача кадру в стандарті Ethernet?
16. Наведіть структуру кадру Ethernet та поясніть зміст кожного його поля.
17. Наведіть особливості роботи мереж Ethernet у дуплексному режимі роботи. Які переваги цього режиму відносно напівдуплексного режиму?
18. Яке фізичне кодування використовується у технології Ethernet? Наведіть діаграму сигналу відповідно цього кодування для заданої бітової комбінації.
19. Наведіть та охарактеризуйте відомі Вам специфікації фізичного середовища мережі Ethernet.
20. Наведіть розрахунок продуктивності мережі Ethernet, Fast Ethernet та Gigabit Ethernet. Поясніть, які проблеми несуть занадто довгі кадри, а також у чому полягає неефективність коротких кадрів.
21. Перерахуйте фактори (крім розміра кадру) і як вони впливають (у якісному аспекті) на продуктивність мережі Ethernet.
22. Наведіть розрахунок продуктивності мережі Ethernet, враховуючи, що в кадри інкапсулюються пакети, а в пакети – сегменти, які мають певні службові поля.
23. Яке позначення IEEE має стандарт Fast Ethernet?
24. Коли було прийнято специфікацію Fast Ethernet? Поясніть, чому виникла необхідність у розробці технології Fast Ethernet.
25. Вкажіть спільне та відмінне в технологіях Ethernet та Fast Ethernet.
26. Наведіть структуру фізичного рівня технології Fast Ethernet.
27. Наведіть та охарактеризуйте специфікації фізичного рівня технології Fast Ethernet.
28. Поясніть, у чому сутність функції автопереговорів. Перерахуйте режими роботи, які можуть вибрати пристрої Fast Ethernet у процесі таких автопереговорів.

29. Наведіть та охарактеризуйте фізичні коди, які використовуються в технології Fast Ethernet. Наведіть діаграми сигналів відповідно цих фізичних кодів для довільної бітової комбінації.

30. Наведіть логічні коди, які використовуються у технології Fast Ethernet та поясніть, з якою метою вони використовуються.

31. Наведіть загальну характеристику технології Gigabit Ethernet.

32. Яке позначення IEEE має стандарт Gigabit Ethernet?

33. Наведіть основні проблеми, з якими зіштовхнулися розробники технології Gigabit Ethernet, а також основні шляхи вирішення цих проблем.

34. Наведіть та охарактеризуйте логічне та фізичне кодування, яке використовується в технології Gigabit Ethernet.

35. Наведіть структуру розширеного кадру, що використовується в технології Gigabit Ethernet.

36. У контексті технології Gigabit Ethernet поясніть, що таке «режим пульсацій» і з якою метою він використовується. Що називають довжиною пульсації?

37. Які режими роботи можуть бути обрані під час автопереговорів для пристроїв Gigabit Ethernet?

38. Наведіть та охарактеризуйте специфікації фізичного середовища стандарту Gigabit Ethernet.

39. Яке позначення IEEE має стандарт 10G Ethernet?

40. Яке логічне кодування використовується в технології 10G Ethernet?

41. Наведіть та охарактеризуйте специфікації фізичного рівня технології 10G Ethernet.

42. Поясніть аббревіатуру «MTU». Укажіть максимально допустимі значення MTU для мереж: Ethernet, Fast Ethernet, Gigabit Ethernet та 10G Ethernet.

3 ТЕХНОЛОГІЯ БЕЗПРОВОДОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ WI-FI

3.1 Загальні відомості

Wi-Fi (абревіатура Wi-Fi походить від англійського «*Wireless Fidelity*», що означає «безпроводова точність»). Ця назва була дана технології безпроводової передачі даних за аналогією з терміном Hi-Fi (*High Fidelity*), що означає «висока точність») – це сучасна бездротова технологія з'єднання комп'ютерів у мережу або підключення їх до Інтернету. Сегмент Wi-Fi-мережі може використовуватися як самостійна мережа або як складова частина більш складної мережі, що містить як безпроводові, так і звичайні проводові сегменти.

Варто зазначити, що в наш час безпроводові локальні комп'ютерні мережі (*Wireless Local Area Network, WLAN*) дуже широко використовуються у багатьох сферах людської діяльності. Це пояснюється тим, що WLAN мають низку переваг перед звичайними кабельними мережами [14, 16]:

- WLAN-мережа може виявитися єдиним виходом, якщо неможливе прокладання кабелю для звичайної мережі. Так, наприклад, коли постає завдання з'єднати у КМ вузли, що розділені певними перешкодами (наприклад, водними перешкодами, стінами та стелями будинків у яких недопустимо або недоцільно прокладати кабелі);

- WLAN-мережу можна досить швидко розгорнути, що дуже зручно, наприклад, в умовах роботи поза офісом, або при проведенні презентацій;

- користувачі мобільних пристроїв, при підключенні до локальних безпроводових мереж, можуть легко переміщуватися у межах діючих зон мережі (наприклад, коли співробітники повинні переміщуються територією під час робочого дня з метою обслуговування клієнтів або для збирання певної інформації);

- швидкості сучасних безпроводових мереж досить високі, що дозволяє їх використовувати для вирішення дуже широкого спектра завдань.

Водночас необхідно пам'ятати й про основні обмеження WLAN, якими, як правило, є:

- набагато більша схильність до впливу перешкод;

- складніша процедура забезпечення безпеки інформації, що передається мережею;

- дещо менша, ніж у провідних ЛКМ, швидкість передачі (хоча нові стандарти вже долають такий недолік).

Потрібно зазначити також, що для забезпечення сумісності апаратури WLAN різних виробників було розроблено низку стандартів, що одночасно виконувалися органами стандартизації трьох регіонів:

у США – Інститутом інженерів електротехніки й електроніки (*Institute of Electrical and Electronics Engineers, IEEE*);

у Європі – Європейським інститутом стандартів електрозв'язку (*European Telecommunications Standards Institute, ETSI*);

у Японії – Асоціацією радіопромисловості та бізнесу (Association of Radio Industries and Business, ARIB).

Найпопулярнішим серед цих стандартів став IEEE. Він має номер 802.11 (див. рис. 1.1) і відомий під назвою Wi-Fi. Тому далі зупинимося саме на цьому стандарті.

3.2 Основні елементи та режими функціонування Wi-Fi

Для побудови безпроводової мережі Wi-Fi використовують точки доступу Wi-Fi та адаптери Wi-Fi (далі – точки доступу та адаптери).

Точка доступу (*Access Point, AP*) – це окремий мікрокомп'ютерний пристрій з приймально-передавальним радіотрактом. Вона виконує роль комутатора, забезпечуючи взаємодію та обмін інформацією між безпроводовими адаптерами, а також зв'язок з провідним сегментом мережі. Такий зв'язок виконується через мережевий інтерфейс (*Uplink Port*). Через цей же інтерфейс може здійснюватися й налаштування точки доступу (ТД).

ТД може використовуватися як для підключення до неї клієнтів (базовий режим точки доступу), так і для взаємодії з іншими точками доступу для побудови розподіленої мережі (*Wireless Distributed System, WDS*). Це режими безпроводового моста «точка–точка» і «точка–багато точок», безпроводовий клієнт і повторювач.

Адаптер (АД) – це пристрій, який підключається через слот розширення PCI, PCMCIA, CompactFlash або через порт USB 2.0. АД фактично виконує ту ж функцію, що й мережевий адаптер (карта) у провідній мережі й слугує для підключення комп'ютера користувача до безпроводової мережі. Варто зазначити, що усі сучасні ноутбуки та кишенькові персональні комп'ютери (КПК) мають вбудовані АД, які сумісні з багатьма сучасними стандартами.

Для доступу до безпроводової мережі АД може встановлювати зв'язок безпосередньо з іншими АД (рис. 3.1).

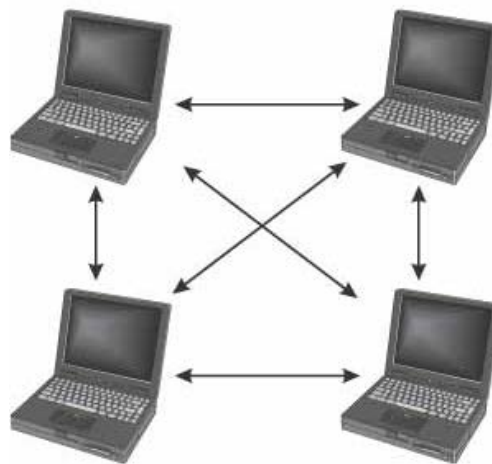


Рисунок 3.1 – Режим Ad Hoc (IBSS)

Така мережа називається безпроводовою одноранговою мережею або Ad Hoc. Їй відповідає найпростіша топологія з набором незалежних базових служб (*Independent Basic Service Set, IBSS*). Service Set, SS – це логічно згруповані пристрої, що забезпечують підключення до безпроводової мережі. SS – це зона обслуговування. Тут мережа є дещо непередбачуваною, оскільки нові станції часто з'являються несподівано.

АД може також встановлювати зв'язок і через ТД (точка доступу дозволяє обслуговувати більшу кількість користувачів і забезпечує більше покриття) (рис. 3.2, а). Такий режим називається інфраструктурою (*Infrastructure*). Група станцій, що зв'язуються між собою безпроводовим зв'язком з використанням однієї ТД називається базовою зоною обслуговування (*Basic Service Set, BSS*). Якщо дві або більше BSS з'єднані через загальну систему розподілення (рис. 3.2, б), маємо так званий розширений сервіс (*Extended Service Set, ESS*).

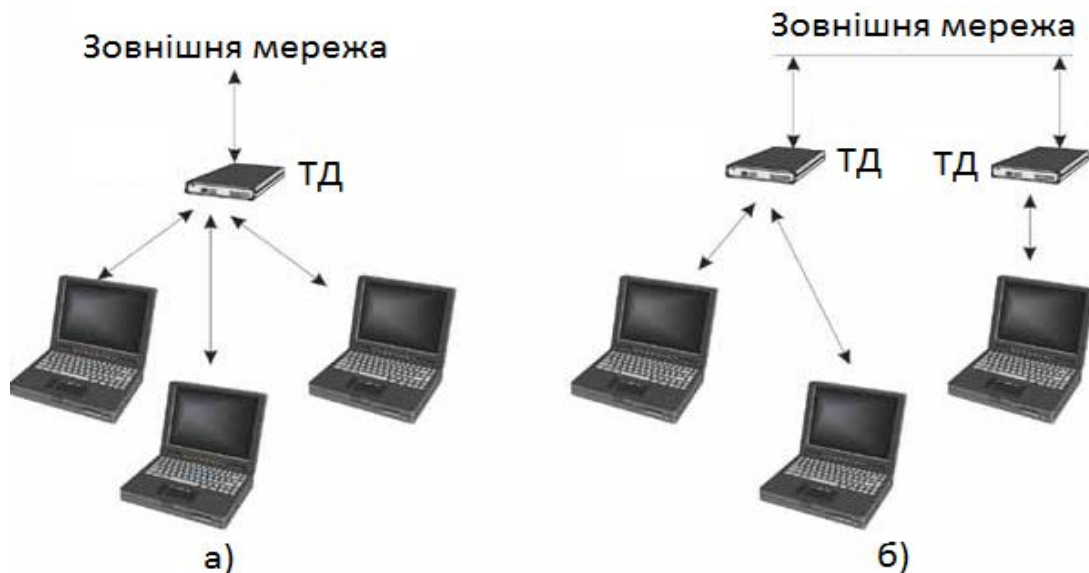


Рисунок 3.2 – Режим Infrastructure: а) BSS; б) ESS

Покриття, що забезпечується IBSS та BSS, називається основною (базовою) зоною обслуговування (*Basic Service Area, BSA*). Відповідно, покриття, що забезпечується ESS, називається розширеною зоною обслуговування (*Extended Service Area, ESA*).

Деякі основні характеристики вищевказаних топологій БЛКМ наведено у табл. 3.1.

Таблиця 3.1 – Деякі основні характеристики топологій БЛКМ

Топологія	IBSS	BSS	ESS
Режим	Ad Hoc	Infrastructure	Infrastructure
Кількість ТД	0	1	≥ 2
З'єднання	Peer-to-Peer	Client to access point	Client to access point
Покриття	BSA	BSA	ESA

Доступ до безпроводової мережі забезпечується шляхом передачі через ефір ширококомовних сигналів. Приймальна станція може отримувати сигнали у діапазоні роботи декількох передавальних станцій. Приймальна станція використовує ідентифікатор зони обслуговування (*Service Set Identifier, SSID*) для фільтрації одержуваних сигналів і виділення того, який їй потрібен.

Асоціація клієнта і точки доступу

Основна частина процесу 802.11 полягає у виявленні WLAN і наступного з'єднання (сполуки) з нею.

Основні компоненти цього процесу:

- Маяки (*Beacons*) – кадри, використовувані мережею WLAN для повідомлення про її присутність. Маяки дозволяють клієнтам WLAN вивчати, які мережі й ТД доступні в даній області, дозволяючи таким чином клієнтам вибрати певну мережу й ТД (рис. 3.3).

- Зонди (*Probes*) – кадри, використовувані клієнтами WLAN для знаходження мережі WLAN.

- Аутентифікація – процес, який є артефактом від вихідного стандарту 802.11, але все ще вимагається стандартом.

- Асоціація – процес встановлення каналу передачі даних між ТД і клієнтом WLAN.

Хоча маяки можуть регулярно ширококомовно передаватися точкою доступу, кадри зондування, аутентифікації й асоціації використовуються лише під час процесу асоціації (або переасоціації).

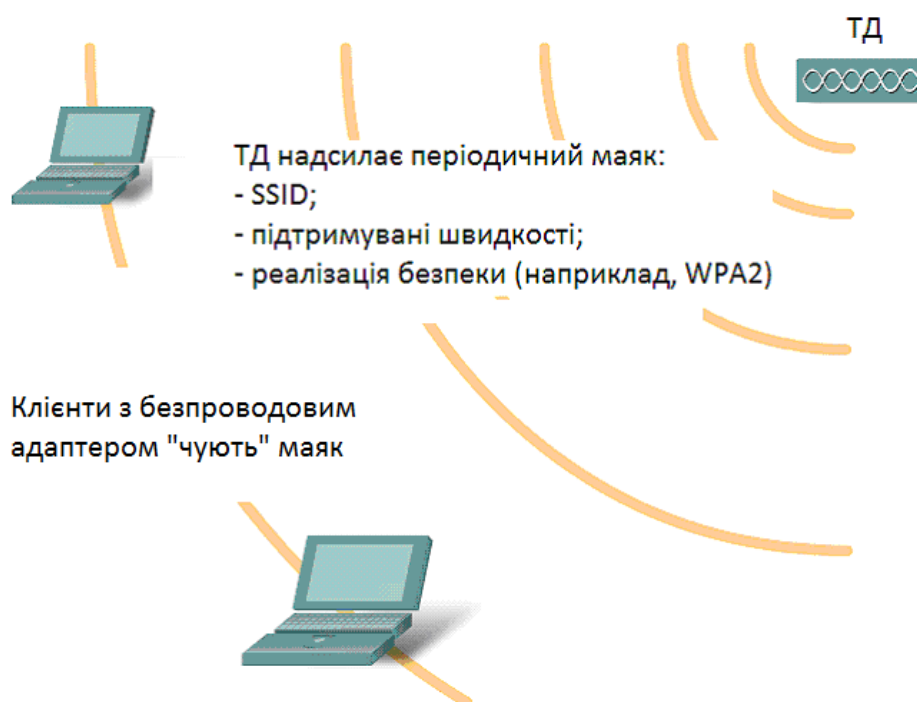


Рисунок 3.3 – Клієнти й ТД мережі WLAN

Перед тим, як клієнт 802.11 зможе надсилати дані мережею WLAN, він повинен пройти через нижченаведений триетапний процес.

1. **Етап зондування** (рис. 3.4). Клієнти шукають певну мережу, надсилаючи тестовий запит на декількох каналах. Тестовий запит визначає мережеве ім'я (SSID) і швидкості передачі. Типовий клієнт WLAN конфігурується з потрібним SSID. Таким чином, тестові запити від клієнта WLAN містять SSID потрібної мережі WLAN.

Якщо ж клієнт просто намагається виявити доступні мережі WLAN, він може надіслати тестовий запит без SSID і всі ТД, які сконфігуровані так, щоб відповідати на цей тип запиту, відповідають. Мережі WLAN з відключеною опцією широкомовної передачі SSID не відповідатимуть.

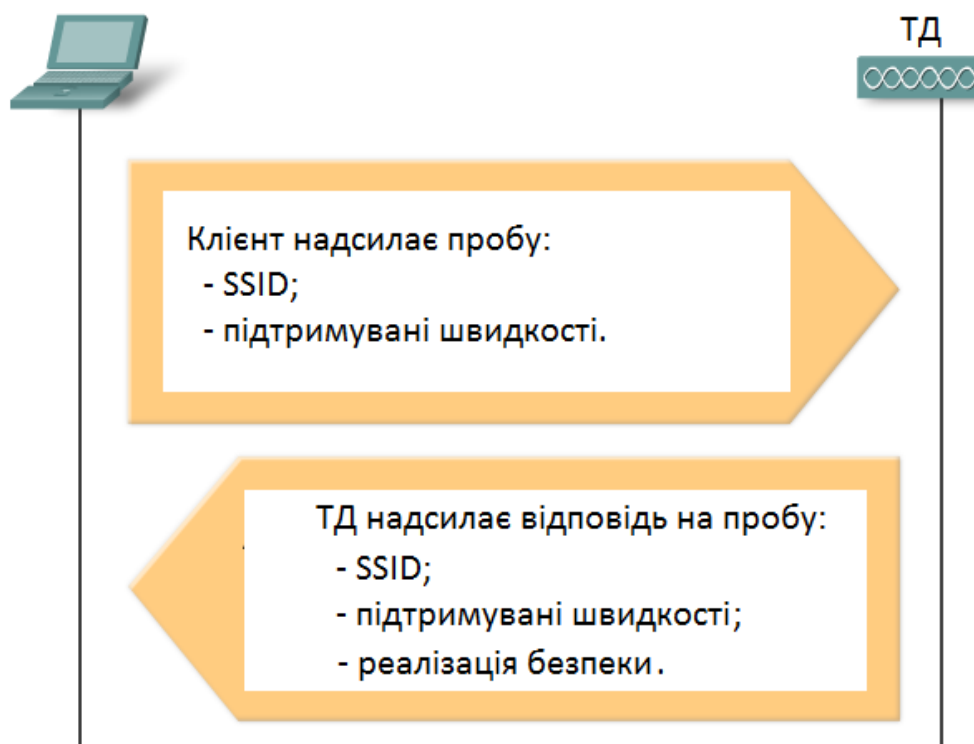


Рисунок 3.4 – Етап зондування

2. **Етап аутентифікації** 802.11 (рис. 3.5) був спочатку розроблений з двома механізмами аутентифікації.

Перший називається відкритою аутентифікацією, (NULL-аутентифікацією), де на запит клієнта щодо його аутентифікації ТД відповідає згодою. Другий називається аутентифікацією із загальним ключем, що спільно використовується клієнтом і ТД, називається безпека, аналогічна захисту провідних мереж (*Wired Equivalent Privacy, WEP*). У цьому методі клієнт надсилає запит аутентифікації до ТД. Далі ТД надсилає текст задачі клієнту, який шифрує повідомлення, використовуючи свій спільно використовуваний ключ і повертає зашифрований текст до ТД.

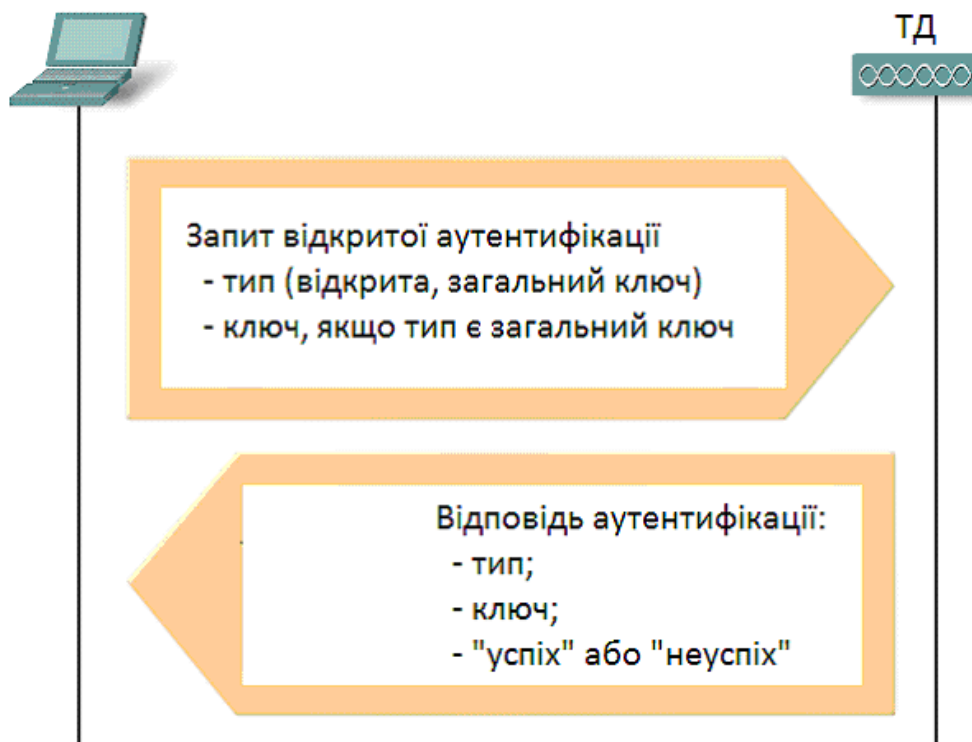


Рисунок 3.5 – Етап аутентифікації

Після цього ТД дешифрує зашифрований текст, використовуючи свій ключ, і якщо дешифрований текст відповідає тексту задачі, це означає, що клієнт і ТД спільно використовують однаковий ключ, і ТД аутентифікує клієнта. Якщо ж дешифрований текст не відповідає тексту задачі – клієнт не аутентифікується.

Хоча аутентифікація загального ключа повинна бути включена у реалізацію клієнта і ТД для повної відповідності стандартів, вона не використовується або не рекомендується. Проблема полягає в тому, що WEP-ключ зазвичай використовується, щоб шифрувати дані під час процесу передачі. Використання цього ж самого WEP-ключа у процесі аутентифікації надає тому, хто атакує, можливість отримати ключ завдяки сніффінгу й порівняти незашифрований текст завдання та повернути зашифроване повідомлення. Як тільки WEP-ключ отримується, будь-яка зашифрована інформація, що надсилається каналом зв'язку, може бути легко дешифрована.

3. **Етап Асоціації** (рис. 3.6) завершує опції безпеки та швидкості передачі та встановлює канал передачі даних між клієнтом WLAN і ТД. Як частина цього етапу клієнт вивчає BSSID, що є MAC-адресою ТД. ТД зіставляє логічний порт, відомий як ідентифікатор асоціації (*Association Identifier, AID*), з клієнтом WLAN. AID є еквівалентом порта на комутаторі. Процес асоціації дозволяє комутатору інфраструктури відстежувати кадри, призначені для клієнта WLAN так, щоб вони могли бути передані. Як тільки клієнт WLAN зв'язався з ТД – вони зможуть обмінюватися трафіком.

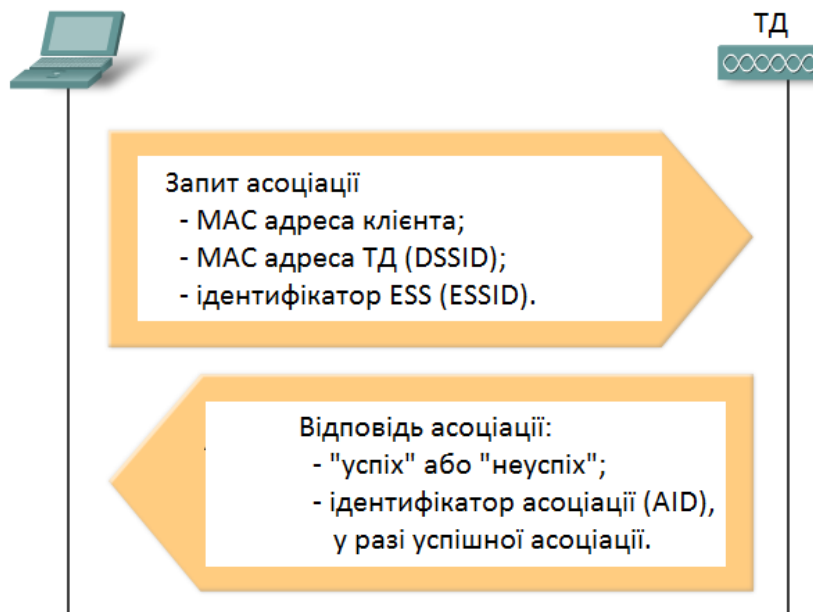


Рисунок 3.6 – Етап асоціації

3.3 Технологія колективного доступу CSMA/CA

Перед тим, як розглядати протокол доступу до середовища передачі даних у безпроводових мережах Wi-Fi, розглянемо основні проблеми, що виникають під час роботи таких мереж. Зауважимо, взаємодія вузлів у безпроводовій ЛКМ має свої особливості, що відрізняють її від взаємодії вузлів у ЛКМ типу Ethernet. Тому для безпроводової ЛКМ потрібні спеціальні протоколи управління доступом до середовища (MAC). До таких особливостей належать [18]:

1. Безпроводові мережі не мають можливості розпізнавати колізії тоді, коли вони відбуваються, оскільки радіопередавачі майже завжди працюють у напівдуплексному режимі, а отже не можуть на одній і тій же частоті одночасно передавати сигнали й прослуховувати сплески шуму. Крім цього, сигнал, що приймається вузлом, може бути у багато разів меншим, ніж сигнал, що надсилається передавачем. Тому для визначення колізій, які вже відбулися, та інших помилок застосовуються підтвердження.

2. На відміну від проводових мереж (якщо один вузол надсилає кадри, усі інші його отримують), у безпроводовій мережі вузол іноді немає можливості надсилати або отримувати кадри від інших вузлів унаслідок обмеженого діапазону радіопередачі.

Розглянемо детальніше другу вищевказану особливість. Припустимо, що кожен передавач працює у деякій фіксованій області покриття, що має форму кола (необхідно розуміти, що практично область покриття буде неправильної форми, оскільки поширення радіосигналів залежить від середовища, у якому можуть бути різні перешкоди й сила сигналу в різних напрямках змінюється. Однак для нашого випадку така модель з колами є цілком прийнятною). У середині цього кола інший вузол може чути й приймати дані від вищевказаного передавача.

Варто зазначити, що використовувати у безпроводових ЛКМ протокол CSMA, який використовується у технології Ethernet (просто прослуховуючи ефір і здійснюючи передачу лише тоді, коли він вільний) неприпустимо. І це пов'язано з тим, що, практично, має значення інтерференція на приймачі, а не на передавачі. Розглянемо таку проблему на прикладі взаємодії чотирьох вузлів (рис. 3.7) [18]. Тут не має значення, який з них є ТД, а який є переносний. Потужність передавачів така, що взаємодіяти можуть лише сусідні вузли, тобто вузол А тільки з В, а вузол С тільки з вузлами В та D, але не з А.

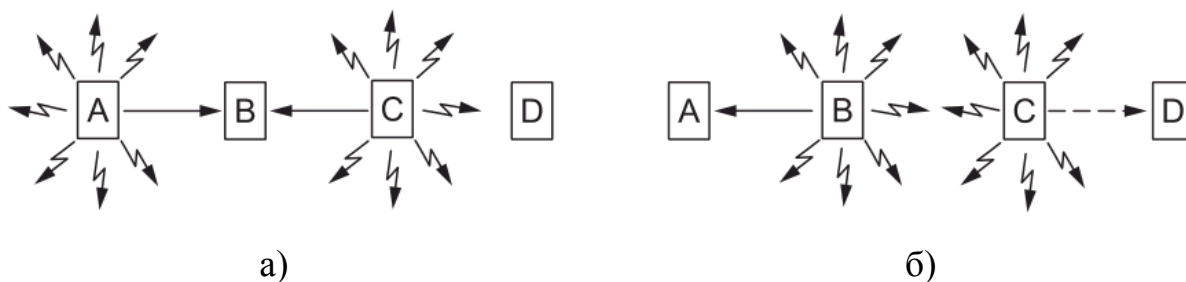


Рисунок 3.7 – Безпроводова ЛКМ:

а – проблема прихованого вузла; б – проблема засвіченого вузла

Розглянемо випадок, коли вузли А і С надсилають дані вузлу В, (див. рис. 3.7, а). Якщо вузол А надсилає дані, а С у той же момент опитує канал, то останній не чутиме вузол А, оскільки він розташований занадто далеко. Як наслідок вузол С може прийти до хибного висновку про те, що канал вільний і можна надсилати дані станції В. І якщо С почне передачу, то виникне конфлікт з вузлом В, а відповідний кадр буде спотворено. Як бачимо, дана проблема полягає в тому, що один вузол не може чути можливого конкурента внаслідок того, що останній розташований занадто далеко від нього. Вищеописана проблема називається **проблемою прихованого вузла** (*Hidden Terminal Problem*).

Тепер розглянемо випадок, коли вузол В надсилає дані до А, і в той же час вузол С хоче надіслати дані до D (див. рис. 3.7, б). Вузол С під час опитування каналу чує передачу і може помилково припустити, що він не має змоги надсилати дані до D. Насправді ж таке передавання створило б перешкоди тільки у зоні від вузла В до С, де у даний момент не відбувається приймання даних. Така ситуація називається **проблемою засвіченого вузла** (*Exposed Terminal Problem*).

Уся складність полягає в тому, що перед тим, як розпочати передачу, вузол має знати, чи наявна будь-яка активність у радіодіпазоні поблизу приймача. Протокол CSMA лише може повідомити про активність навколо передавача шляхом опитування несучої. У разі передачі проводом усі сигнали досягають усіх вузлів, тому такого розходження не спостерігається. Однак у всій системі одночасно тільки один вузол може вести передачу. У системі з використанням радіозв'язку, радіус передачі й прийому якої

обмежений невеликими зонами, одночасно можуть надсилати дані кілька станцій, якщо тільки вони надсилають різним приймальним вузлам, що перебувають досить далеко один від одного.

Одним з перших серйозних протоколів, розроблених для бездротових ЛКМ, що здатен вирішити вищевказані проблеми, є **протокол множинного доступу із запобіганням колізій** (*Multiple Access with Collision Avoidance, MACA*). Його ідея полягає в тому, що відправник змушує отримувача передати короткий кадр, щоб оточуючі вузли могли почути цю передачу і утриматися від дій на час, який потрібен для приймання великого інформаційного кадру. Ця техніка замінює техніку прослуховування несучої [18].

Протокол MACA зображено на рис. 3.8. Розглянемо ситуацію, у якій вузол А надсилає до В. Вузол А починає з того, що надсилає до В кадр запити на передачу (*Request To Send, RTS*) (рис. 3.8, а). Цей короткий кадр (30 байтів) також містить довжину кадру даних, який буде надіслано за ним. Далі вузол В відповідає кадром дозволу передачі (*Clear To Send, CTS*), як це наведено на рис. 3.8, б). Кадр CTS також містить довжину інформаційного кадру (скопійовану з кадру RTS). Приймавши кадр CTS, вузол А починає передачу.

Будь-який вузол, що чує кадр RTS, знаходиться близько до А і тому повинен зберігати мовчання, допоки кадр CTS не буде прийнятий вузлом А. Вузли, які почують кадр CTS, знаходяться поблизу від В, а отже, повинні утриматися від передачі, допоки В не отримає кадр даних, довжину якого вони можуть дізнатися з кадру CTS.

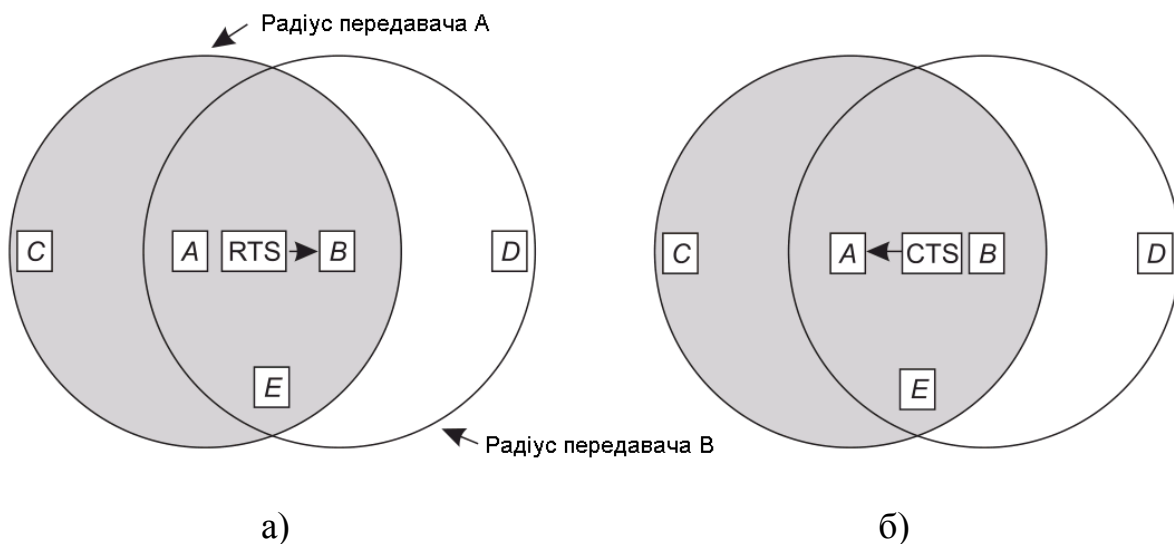


Рисунок 3.8 – Протокол MACA:
а) – вузол А надсилає кадр RTS до В;
б) – вузол В відповідає кадром CTS до А

На рис. 3.8 вузол С знаходиться у зоні вузла А, але не входить у зону В. Тому він чує кадр RTS, надісланий від А, але не чує кадр CTS, яким відповідає В. Оскільки він не інтерферує з кадром CTS, то не повинен утримува-

тися від передачі в той момент, коли надсилається інформаційний кадр. Вузол D, навпаки, знаходиться близько від B, але далеко від A. Він не чує кадру RTS, але чує CTS, а це означає, що він знаходиться поблизу вузла, який збирається прийняти кадр з даними. Тому йому не можна вести передачу, поки цей кадр не буде передано. Вузол E чує обидва керувальних повідомлення і так само, як і D, повинен зберігати мовчання, поки не буде завершено передавання інформаційного кадру.

Незважаючи на усі запобіжні заходи, конфлікти все рівно можуть відбутися. Наприклад, вузли B і C можуть одночасно надіслати кадри RTS до A. При цьому кадри зіштовхнуться і не будуть прийняті. У цьому разі передавачі, не почувши кадр CTS у встановлений термін, чекають випадковий час і після цього повторюють спробу.

Стандарт IEEE 802.11 намагається уникати колізій за рахунок протоколу CSMA/CA (*CSMA with Collision Avoidance*) [18]. Концепція протоколу CSMA/CA подібна до концепції CSMA/CD для Ethernet, де канал прослуховується перед початком відправлення, а період мовчання після колізії обчислюється експоненціально. Та якщо у вузла є кадр для пересилання, то він починає цикл з періоду мовчання випадкової довжини (за винятком випадків, коли він давно не використовував канал, і він нічого не робить). Вузол не очікує колізій. Число слотів, протягом яких він мовчить, обирається у діапазоні від 0 до 15 у випадку фізичного рівня метод ортогонального частотного розділення (*Orthogonal Frequency-Division Multiplexing, OFDM*), який розглядається нижче. Вузол чекає бездіяльності каналу протягом короткого періоду часу (*Distributed InterFrame Space, DIFS*) і відраховує слоти бездіяльності, припиняючи відлік на час відправлення кадрів. Свій кадр він надсилає, коли лічильник досягає нуля. Якщо кадр доставляється успішно, то вузол призначення відразу ж надсилає назад короткий кадр підтвердження. Якщо підтвердження відсутнє – робиться висновок, що сталася помилка (колізія чи інша), і тоді відправник подвоює період мовчання та повторює спробу, продовжуючи експоненціально нарощувати довжину паузи (як у Ethernet) доти, поки кадр не буде успішно переданий або поки не буде досягнуто максимальне число повторів.

Приклад часової шкали наведено на рис. 3.9. Вузол A перший надсилає кадр. Поки він зайнятий надсиленням, вузли B і C переходять у режим готовності виконати надсилення. Вони бачать, що канал зайнятий, і чекають бездіяльності каналу. Незабаром після отримання вузлом A підтвердження канал переходить у режим бездіяльності. Але натомість, щоб відразу ж відправляти кадри (що б привело до колізії), вузли B і C починають свої періоди мовчання. Вузол C вибирає короткий період мовчання, тому йому вдається відправити дані першому. Вузол B призупиняє зворотний відлік, коли бачить, що канал зайнятий вузлом C, і поновлюється тільки після отримання вузлом C підтвердження. Незабаром період мовчання вузла B завершується, і він також надсилає кадр.

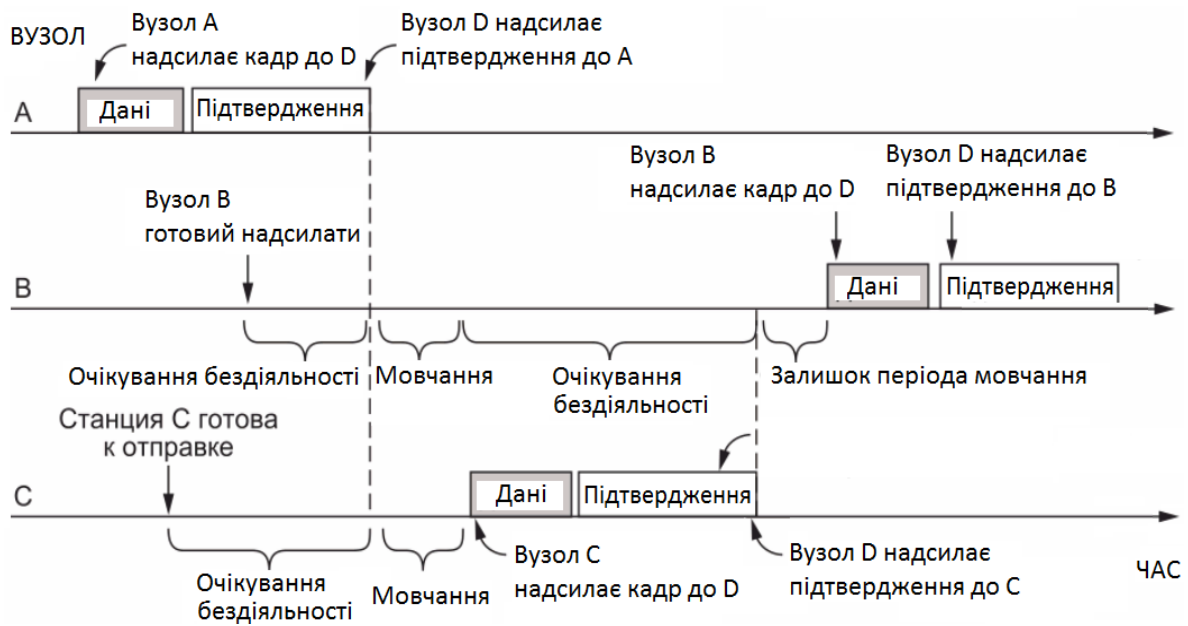


Рисунок 3.9 – Надсилання кадрів за протоколом CSMA/CA

Порівняно з Ethernet, тут є дві основні відмінності [18]:

1. Ранній початок періодів мовчання допомагає уникати колізій. Це важлива перевага, оскільки колізії спричиняють негативні наслідки, адже навіть якщо зіткнення відбувається, кадр все рівно відправляється цілком.

2. Для того, щоб вузли могли «здогадуватися» про колізії, які розпізнати неможливо, застосовується схема з підтвердженнями. Такий режим роботи називається **розподілений координуванням** (*Distributed Coordination Function, DCF*). Усі вузли діють незалежно, централізований контроль не здійснюється.

Стандарт також включає необов'язковий **режим зосередженого координування** (*Point Coordination Function, PCF*), у якому всіма діями у комірці керує ТД – базова станція стільникової мережі. Але PCF на практиці не застосовується, оскільки неможливо заборонити вузлам із сусідньої мережі передавати конкурентний трафік.

У стандарті 802.11 для вирішення, який вузол буде надсилати дані, прослуховування каналу визначається на фізичному й віртуальному рівнях. При фізичному прослуховуванні середовище перевіряється на наявність сигналу. Віртуальне прослуховування полягає у тому, що кожен вузол веде логічний журнал використання каналу, відстежуючи вектор розподілу мережі (*Network Allocation Vector, NAV*). Кожен кадр містить поле NAV, що повідомляє, як довго передаватиметься послідовність, яка утворює даний кадр. Вузли, що почули цей кадр, розуміють, канал буде зайнятий протягом періоду, зазначеного у NAV, навіть якщо фізичний сигнал у каналі відсутній. Наприклад, NAV для кадрів даних містить також час, необхідний для надсилання підтвердження. Усі вузли, які почули цей кадр даних, утримуються від надсилання даних протягом періоду відправлення підтвердження незалежно від того, чи чули вони його в каналі.

Необов'язковий механізм RTS/CTS за допомогою NAV забороняє вузлам надсилати кадри одночасно з прихованими вузлами. Приклад наведено на рис. 3.10. Тут вузол А хоче надіслати дані до В. Вузол С розташований у зоні дії А, а також, можливо, і в зоні дії В (проте це не має значення). Вузол D входить у зону дії В, але не входить у зону дії А. Протокол починає працювати тоді, коли вузол А вирішує, що йому необхідно надіслати дані до В. Вузол А надсилає до В кадр RTS, запитуючи дозвіл на передачу. Якщо В може прийняти дані, він надсилає назад підтвердження (кадр CTS) про те, що канал вільний. Після приймання цього підтвердження вузол А надсилає кадр і запускає таймер. У разі коректного приймання вузол В генерує кадр АСК, який завершує передачу. Якщо інтервал часу таймера на вузлі А закінчується раніше, ніж отримано АСК, то вважається, що сталася колізія, і весь алгоритм роботи протоколу повторюється з самого початку після періоду мовчання.

Тепер розглянемо цей же процес з погляду вузлів С і D. Вузол С знаходиться в зоні дії А, тому він також отримує кадр RTS і розуміє, що скоро каналом будуть надсилатися деякі дані. Виходячи з інформації, що міститься в RTS, вузол С може припустити, скільки часу триватиме передавання послідовності, що містить кінцевий АСК. Тому, щоб не заважати іншим, він утримується від передачі даних, поки обмін не буде завершено. Для цього він оновлює свій запис NAV, вказуючи, що канал зайнятий (рис. 3.10). Вузол D не чує RTS, але чує CTS, і також виставляє NAV. Зверніть увагу, що сигнали NAV не надсилаються, а є лише внутрішніми нагадуваннями вузлів про те, що потрібно зберігати мовчання протягом певного проміжку часу.

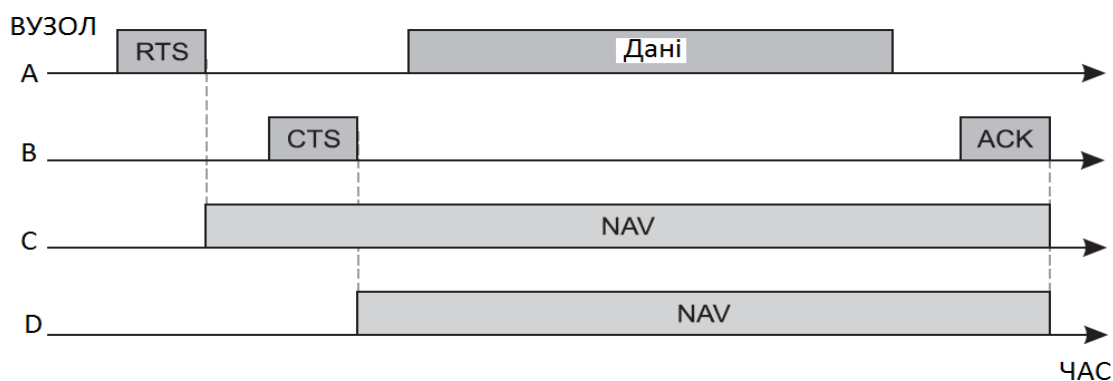


Рисунок 3.10 – Використання прослуховування віртуального каналу в протоколі CSMA/CA

Незважаючи на теоретичну привабливість моделі RTS/CTS, її практична цінність невисока. І цьому є кілька причин. Дана модель не розрахована на короткі кадри (які надсилаються замість RTS) і на присутність ТД (ТД за визначенням мають чути усі). В інших ситуаціях вона також уповільнює роботу. RTS/CTS у стандарті 802.11 дещо відрізняється від протоколу MACA, оскільки кожен, хто отримує RTS або CTS, зберігає мовчання

протягом певного проміжку для того, щоб підтвердження АСК змогло пройти каналом без колізій. Унаслідок цього проблема засвіченої станції не вирішується, як при використанні протоколу МАСА, а усувається лише проблема прихованих станцій. Найчастіше прихованих станцій зовсім небагато, а CSMA/CA і так допомагає їм. Ця технологія уповільнює станції, яким з деякої причини не вдається успішно передати дані для того, щоб підвищити ймовірність вдалого пересилання [18].

CSMA/CA з фізичним і віртуальним прослуховуванням становить основу протоколу 802.11. Однак є й кілька інших механізмів, розроблених для того ж стандарту. Кожен з цих механізмів викликаний певними потребами, пов'язаними з фактичними умовами.

Перша потреба – це надійність. На противагу провідним каналам, безпроводові шумні та ненадійні, у певному ступені внаслідок впливу інших пристроїв, які працюють в тому ж діапазоні радіовипромінювання. Використання підтверджень і повторних передач мало допомагає, якщо ймовірність передачі кадру є малою.

Основна стратегія, використовувана для збільшення числа успішних передач, полягає у тому, щоб знизити швидкість передачі. Повільніші швидкості використовують сильніші методи модуляції сигналу, який з більшою ймовірністю буде правильно отримано для даного відношення сигнал/шум. Якщо втрачено дуже багато кадрів, станція може знизити швидкість. Якщо кадри доставляються з невеликою втратою, станція може іноді використовувати вищу швидкість, щоб побачити, чи може вона використовуватися.

Інша стратегія поліпшити шанс кадру дійти неушкодженим полягає у тому, щоб надсилати коротші кадри. Якщо ймовірність помилки в одному біті дорівнює p , то ймовірність того, що n -бітний кадр буде прийнятий коректно, дорівнює $(1 - p)^n$. Наприклад, для $p = 10^{-4}$ ймовірність коректної передачі повного Ethernet-кадру довжиною 12144 біт становить менше 30%. Велику частину кадрів буде втрачено. Але якщо довжина кадрів становитиме одну третину (4048 біт), то дві третини їх будуть отримані правильно. Тепер більшість кадрів пройде, і повторних передач стане менше.

З одного боку, використання коротших кадрів може бути реалізовано скороченням максимального розміру повідомлення, яке приймається від мережевого рівня. З іншого – 802.11 дозволяє розділяти кадри на дрібніші частини, названі фрагментами (*fragments*), кожен зі своєю контрольною сумою. Розмір фрагмента не фіксований, а є параметром, що може бути скоригований ТД. Фрагменти нумеруються і підтверджуються індивідуально з використанням протоколу з очікуванням (тобто відправник не може передати фрагмент з номером $k+1$, поки не отримає підтвердження про доставлення фрагмента з номером k). Вони йдуть один за одним з підтвердженнями (і можливо повторною передачею) між ними доти, доки або увесь кадр не буде надісланий успішно, або час передачі не досягне дозволеного максимуму. Механізм NAV утримує станції від передачі

тільки до приходу першого підтвердження про доставлення. Але є й інший механізм (він описаний нижче), що дозволяє отримувачеві прийняти всю пачку фрагментів, без кадрів від інших вузлів між ними.

Друга потреба – це економія енергії, яка була завжди дуже актуальною, оскільки час роботи від акумулятора для мобільних безпроводових прис-троїв завжди є проблемою. Стандарт 802.11 передбачає таке управління електроживленням, щоб клієнти не витрачали енергію даремно, коли у них немає інформації, яка надсилається або повинна бути отримана.

Основний механізм для економії енергії ґрунтується на кадрах-маяках. Це періодичні ширококомвні повідомлення ТД, які повідомляють клієнтам про присутність ТД і несуть системні параметри такі, як: ідентифікатор, час, інтервал до наступного маяка і налаштування безпеки.

Клієнти можуть встановити біт управління електроживленням у кадрах, які вони надсилають до ТД, щоб повідомити їй, що вони входять у режим енергозберігання (*power-save mode*). У цьому режимі клієнт може «дрімати», і ТД буде буферизувати призначений для нього трафік. Щоб перевірити наявність вхідного трафіку, клієнт «прокидається» для кожного маяка і перевіряє карту трафіка, що йому надсилають як частину маяка. Ця карта говорить клієнту про наявність буферизованого трафіку. Якщо він є, клієнт надсилає повідомлення опитування до ТД, і вона надсилає буферизований трафік. Потім клієнт може повернутися у сплячий режим до наступного маяка.

У 2005 році до 802.11 було додано другий механізм енергозбереження, який називається автоматичний перехід у режим збереження енергії (*Automatic Power Save Delivery, APSD*). З цим новим механізмом ТД буферизує кадри й надсилає їх клієнтові одразу після того, як клієнт надсилає кадри до ТД. Клієнт може заснути, поки у нього немає більшої кількості трафіку для відправлення (і отримання). Цей механізм добре працює на такому додатку, як IP-телефонія, у якому часто є трафік в обох напрямках. Наприклад, безпроводовий IP-телефон міг би використовувати цей механізм, щоб надсилати й отримувати кадри кожні 20 мс, що набагато частіше, ніж інтервал маяка (100 мс), і знаходиться у режимі сну в проміжках.

Третя й остання потреба – це якість обслуговування. Коли трафік IP-телефонії у попередньому прикладі конкурує з трафіком з'єднання рівноправних вузлів ЛКМ, постраждає трафік IP-телефонії. Він буде відкладений у змаганні з трафіком рівноправних вузлів ЛКМ високої пропускної здатності, навіть при тому, що пропускна здатність IP-телефонії низька. Ці затримки, ймовірно, погіршать голосові виклики. Щоб запобігти цьому погіршенню, необхідно дозволити трафіку IP-телефонії йти перед трафіком вищевказаних рівноправних вузлів, як такому, що має вищий пріоритет. В IEEE 802.11 є розумний механізм, що забезпечує цей вид якості обслуговування, і який був уведений у 2005 році як набір розширень під ім'ям 802.11e. Він працює (розширюючи CSMA/CA) з ретельно визначеними інтервалами між кадрами. Після того,

як кадр надіслано, перш ніж будь-яка станція може надіслати кадр, потрібен певний час простою, щоб перевірити, чи канал більше не зайнятий. Це дозволяє визначити різні часові інтервали для різних видів кадрів.

На рис. 3.11 зображено п'ять інтервалів [18]. Інтервал між регулярними кадрами даних називається міжкадровий інтервал DCF (*DCF InterFrame Spacing DIFS*). Будь-яка станція може спробувати захопити канал, щоб надіслати новий кадр після того, як середовище було неактивне для DIFS. При цьому застосовуються звичайні правила боротьби, включаючи двійкову експонентну витримку, у випадку виникнення колізії.

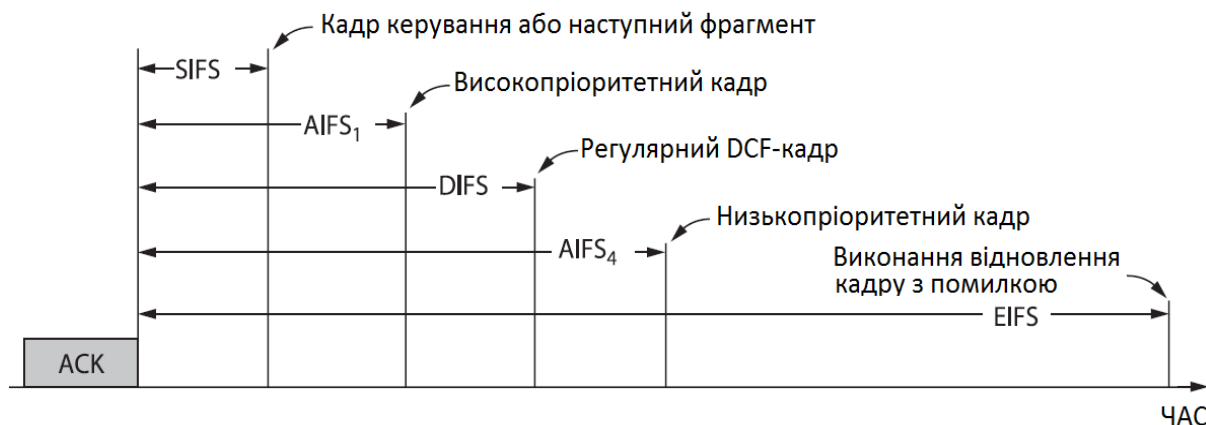


Рисунок 3.11 – Міжкадрові інтервали у стандарті 802.11

Найкоротший інтервал – це SIFS (*Short InterFrame Interval* – короткий міжкадровий інтервал). Він використовується для того, щоб одна зі сторін у діалозі могла отримати шанс почати першою. Приклади включають дозвіл отримувачу надіслати ACK, інші послідовності кадрів управління такі, як RTS і CTS, або дозвіл відправнику надіслати пакет фрагментів. Надсилання наступного фрагмента після очікування тільки SIFS перешкоджає тому, щоб інша станція втрутилася з кадром у середині обміну.

Два інтервали AIFS (*Arbitration InterFrame Space* – міжкадровий арбітражний інтервал) показують приклади двох різних рівнів пріоритету. Короткий інтервал AIFS₁ коротший, ніж DIFS, але довший, ніж SIFS. Він може використовуватися ТД, щоб перемістити голос або інший пріоритетний трафік у початок черги. ТД чекатиме коротшого інтервалу, перш ніж надішле голосовий трафік, і, таким чином, надішле його раніше регулярного трафіку. Довгий інтервал AIFS₄ є довшим, ніж DIFS. Він використовується для фонових трафіку, який може бути затриманий до закінчення регулярного трафіку. Перш ніж надіслати цей трафік, ТД буде чекати протягом довшого інтервалу, надаючи можливість спочатку передати регулярний трафік. Повний механізм якості обслуговування визначає чотири різних пріоритетних рівня, у яких є різні параметри витримки, а також різні параметри часу очікування.

Останній часовий інтервал називається розширений міжкадровий інтервал (*Extended InterFrame Spacing, EIFS*). Він використовується тільки тим вузлом, який щойно отримав зіпсований або нерозпізнаний кадр і хоче повідомити про проблему. Ідея полягає в тому, що приймач може відразу не збагнути, що відбувається, і йому потрібно «вичекати» протягом деякого інтервалу, щоб не перервати своїм вигуком діалог між станціями, який відбувається в цей момент.

Подальша частина розширень, що забезпечують якість обслуговування, – поняття можливості передачі (*Transmission Opportunity*) або ТХОР. Первісний механізм CSMA/CA дозволяв станціям надсилати один кадр за один раз. Ця схема була гарною, допоки діапазон швидкостей не збільшився. У 802.11a/g один вузол міг би надсилати кадри зі швидкістю 6 Мбіт/с, а інший – 54 Мбіт/с. Кожному з них треба надіслати один кадр, але першому вузлу потрібно для надсилання свого кадру в 9 разів більше часу (не рахуючи фіксованих накладних витрат), ніж другому. У цій нерівності є неприємний побічний ефект уповільнення швидкого відправника, який конкурує з повільним відправником, приблизно до швидкості повільного відправника. Наприклад, знову ігноруючи фіксовані накладні витрати, працюючи окремо, відправники реалізовували б свої власні швидкості 6 Мбіт/с і 54 Мбіт/с, а працюючи разом, вони обидва отримують у середньому швидкість 5,4 Мбіт/с. Найбільше при цьому постраждає швидший відправник. Ця проблема відома як аномалія швидкості (*rate anomaly*).

При використанні ТХОР кожна станція отримує однакову кількість ефірного часу, а не однакову кількість кадрів. Станції, які надсилають на вищій швидкості, отримують протягом свого ефірного часу більш високу пропускну здатність. У нашому прикладі відправники, які спільно працюють зі швидкостями 6 і 54 Мбіт/с, тепер відповідно досягнуть швидкостей 3 і 27 Мбіт/с.

3.4 Формати кадрів стандарту IEEE 802.11

Стандарт 802.11 використовує три класи кадрів, що надсилаються каналом [18]:

1. Інформаційні (*Data*) – містять дані;
2. Службові (*Management*) – використовуються для входу й виходу з мережі, включаючи *association request*, *association response* і *reassociation request* тощо;
3. Керувальні (*Control*) – використовуються для підтвердження отримання кадрів даних.

Далі розглянемо структуру кадру на прикладі інформаційного кадру. Формат інформаційного кадру наведено на рис. 3.12, а).

Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Data	CRC
(2 байти)	(2)	(6)	(6)	(6)	(2)	(6)	(0 – 2312)	(4)

а)

Protocol	Type	Subtype	To DS	From DS	MF	Retry	Power	More Data	WEP	Order
(2 біти)	(2)	(4)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)

б)

Рисунок 3.12 – Формат інформаційного кадру IEEE 802.11

1. **Поле управління кадру (Frame Control)** має 11 субполів (рис. 3.12, б):

– *версія протоколу (Protocol)* містить версію протоколу;

– *тип (Type)* задає різновид кадру:

- інформаційний (*Data*) (значення 02) слугує для передавання корисної інформації;

- службовий (*Management*) (значення 00) – для передавання службової інформації (*Beacon, Probe Request, Authentication*);

- керувальний (*Control*) (значення 01) – для контролю доступу до середовища передачі (наприклад, RTS, CTS, ACK);

– кожен тип кадру ділиться на підтипи, які визначаються значенням поля *підтип (Subtype)*;

– *до DS (To DS)* та *від DS (From DS)* вказують на напрямок руху кадру: відповідно в мережу (тоді To DS = 1) або від мережі (тоді From DS = 1), яка з'єднана з ТД і називається системою розподілу (*Distribution system, DS*);

– *MF (More Fragments)* встановлено в одиницю, якщо кадр розбитий на фрагменти й даний фрагмент не останній;

– *повтор (Retry)* вказує на те, що даний кадр є повторною передачею попереднього кадру, що дозволяє вузлу-приймачу розпізнавати повторювані кадри, які виникають через втрату підтверджень;

– *живлення (Power)* означає, що після передавання даного кадру вузол переходить у режим енергозбереження з активного режиму або навпаки;

– *продовженість (More Data)* використовується ТД для того, щоб повідомити станцію, що для неї є дані (у буфері в ТД);

– *WEP* вказує на те, що кадр зашифрований за протоколом WEP;

– *порядок (Order)* повідомляє приймачеві, що кадри з цим бітом повинні оброблятися суворо по порядку (якщо цей біт = 1).

2. **Поле тривалість (Duration/ID)** містить значення часу (у мікросекундах), який буде витрачено на передавання кадру й підтвердження. Це поле присутнє у всіх типах кадрів, у тому числі й службових, і відповідно до нього станції виставляють ознаки NAV. Якщо ж передається кадр функції енергозбереження (*Power Save, PS – Poll*), то у даному полі надсилається ідентифікатор станції.

3. Залежно від структури мережі й напрямку передачі пакета поля адресів (*Address 1*) – (*Address 4*) можуть містити різні значення:

– *Поле Address 1* завжди вказує MAC-адресу безпосереднього отримувача пакета. Якщо біт To DS у поле Frame Control має значення одиниця, то в цьому полі вказана адреса ТД. У цьому випадку він називається ідентифікатором базового набору обслуговування (BSSID). У всіх інших випадках – це адреса станції-отримувача;

– *Поле Address 2* завжди вказує адресу безпосереднього відправника. Якщо біт From DS встановлено в одиницю, то в цьому полі задається адреса ТД (BSSID), у протилежному випадку – це адреса абонента.

– *Поле Address 3* вказує адресу отримувача (розташованого у DS), якщо біт To DS має одиничне значення або адресу відправника; якщо в одиницю встановлений біт From DS. У разі використання однорангової мережі або передачі службових кадрів від ТД, це поле містить значення BSSID;

– *Поле Address 4* використовується тільки у випадку, якщо DS є безпроводовою мережею.

Можливі варіанти використання полів адресації наведено у табл. 3.2, при цьому застосовуються такі скорочення: DA (*Destination Address*) – адреса отримувача кадру; SA (*Source Address*) – адреса відправника кадру; BSSID (*Basic Service Set ID*) – MAC-адреса ТД в інфраструктурному режимі або ідентифікатор мережі в одноранговому режимі; RA (*Recipient Address*) – адреса ТД, що приймає кадр; TA (*Transmitter Address*) – адреса ТД, яка передала кадр.

Таблиця 3.2 – Використання полів адресації

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	TA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	DA

4. **Поле послідовність** (*Sequence control*) складається з двох частин:

– Sequence Number (12 бітів) вказує порядковий номер кожного кадру;
 – Fragment Number (4 біти) вказує кількість надісланих фрагментів (спочатку Fragment Number дорівнює 0, а потім інкрементується з надсиланням кожного наступного фрагмента).

5. **Поле даних** (*Data*) містить інформацію, яка, власне, і має бути надіслана каналом.

6. **Поле контрольна послідовність кадру** (*CRC*) визначає його контрольну суму і призначене для перевірки його цілісності.

Керувальні кадри мають такий же формат, як й інформаційні, та додатково формат для частини даних, яка змінюється залежно від підтипу (наприклад, параметри у кадрах-маяках).

Службові кадри короткі та, як і всі кадри, містять поля Frame Control, Duration та CRC. При цьому вони можуть мати лише одну адресу й не мати поля Data. Ключовою тут є інформація, що міститься у полі Subtype (RTS, CTS або ACK).

3.5 Основні різновиди стандарту IEEE 802.11

Сьогодні виділяють низку різновидів стандарту сімейства IEEE 802.11. Специфікації, що стосуються фізичного рівня середовища передачі, є такі: 802.11, 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac. IEEE 802.11 належать до першого покоління; 802.11b – до другого; 802.11g та 802.11a – до третього; 802.11n – до четвертого; 802.11ac – до п'ятого.

Специфікації 802.11d, 802.11e, 802.11i, 802.11j, 802.11h, 802.11r належать до рівня MAC, а 802.11f та 802.11c – до вищих рівнів моделі OSI.

Сутність та деякі особливості основних стандартів розглянуто нижче.

Стандарт IEEE 802.11

Стандарт 802.11 був прийнятий у 1997 році. Він є батьком усіх інших стандартів безпроводового зв'язку для мереж WLAN і в наш час, фактично, не використовується [17]. 802.11 використовує частотний діапазон шириною 83,5 МГц (від 2400 до 2483,5 МГц), розбитий на декілька частотних підканалів. В основу цього стандарту покладено технологію розширення спектра (*Spread Spectrum, SS*), яка передбачає, що спектр вузькополосного вихідного корисного інформаційного сигналу під час передачі значно розширюється та відбувається перерозподіл спектральної енергетичної щільності сигналу, енергія якого «розмазується» спектром. Для розширення спектра використовується метод прямої послідовності (*Direct Sequence Spread Spectrum, DSSS*), що передбачає вбудовування чіпової послідовності (є послідовністю прямокутних імпульсів) у кожен інформаційний біт вихідної послідовності. Якщо тривалість одного чіпового імпульсу в n разів менша, ніж тривалість інформаційного біта, то ширина спектра перетвореного сигналу буде в n разів більшою, ніж ширина спектра вихідного сигналу. При цьому амплітуда сигналу, що передаватиметься, зменшиться в n разів.

Чіпові послідовності, які вбудовуються в інформаційні біти, називають шумоподібними кодами (PN-послідовностями), оскільки перетворений сигнал стає шумоподібним і його важко відрізнити від природного шуму.

Для того, щоб можна було прийняти та виділити з такого шумоподібного сигналу інформаційний, необхідно так підібрати чіпові послідовності, щоб вони задовольняли певні вимоги автокореляції (автокореляція тут означає ступінь подібності функції самій собі в різні моменти часу). Якщо чіпову послідовність підібрати так, щоб для неї функція автокореляції мала різко виражений пік лише для одного моменту часу, то такий інформаційний сигнал можна виділити на рівні шуму. Для

цього в приймачеві отриманий сигнал множиться на чіпову послідовність (тим самим обчислюється його автокореляційна функція) – і сигнал знову стає вузькосмуговим, тому його фільтрують у вузькій смузі частот, яка дорівнює подвоєній швидкості передачі. Будь-яка перешкода, що потрапляє у смугу вихідного широкосмугового сигналу, після множення на чіпову послідовність навпаки стає широкосмуговою та обрізається фільтрами, а у вузьку інформаційну смугу потрапляє лише частина цієї завади, за потужністю значно менша, ніж завада, яка знаходиться на вході приймача.

У протоколі 802.11 як чіпові послідовності використовуються коди Баркера (оскільки вони мають найкращі серед відомих псевдовипадкових послідовностей шумоподібні властивості) довжиною в 11 чіпів.

Для того, щоб передати сигнал, інформаційна послідовність біт у приймачі складається за модулем 2 ($\text{mod } 2$) з 11-чіповим кодом Баркера за допомогою логічного елемента виключне АБО (XOR). Таким чином, логічна одиниця передається прямою послідовністю Баркера, а логічний нуль – інверсною.

У стандарті 802.11 передбачено два швидкісних режими: обов'язковий – 1 Мбіт/с (*Basic Access Rate*) і опціональний – 2 Мбіт/с (*Enhanced Access Rate*). У першому режимі швидкість проходження окремих чіпів послідовності Баркера становить $11 \cdot 10^6$ чіпів за секунду, а ширина спектра такого сигналу – 22 МГц. Враховуючи, що ширина частотного діапазону дорівнює 83,5 МГц, отримуємо, що в даному діапазоні частот можна розташувати всього три частотних канали, які не перекриваються. Однак, прийнято увесь частотний діапазон ділити на 11 частотних каналів по 22 МГц, які не перекриваються і віддалені один від одного на 5 МГц (рис. 3.13). Наприклад, перший канал займає частотний діапазон від 2400 до 2423 МГц і відцентрований відносно частоти 2412 МГц. Другий канал – відносно частоти 2417 МГц, а останній, 11-й – відносно частоти 2462 МГц. У даному випадку 1-й, 6-й та 11-й канали не перекриваються і мають зазори один між одним у 3 МГц. Тому саме ці три канали можуть застосовуватися незалежно один від одного. Варто наголосити, що 11 каналів використовуються у Північній Америці, а для Європи використовується вже не 11, а 13 таких каналів.

Для модуляції синусоїдального несучого сигналу з інформаційною швидкістю 1 Мбіт/с використовується відносна двійкова фазова модуляція (*Differential Binary Phase Shift Key, DBPSK*). Тут кодування інформації відбувається за рахунок зсуву фази синусоїдального сигналу відносно попереднього стану сигналу. Двійкова фазова модуляція передбачає два можливих значення зсуву фази: 0 та p . Логічний нуль може передаватися синфазним сигналом (зсув по фазі дорівнює 0), а одиниця – сигналом, зсунутим по фазі на p .

Для передачі даних на швидкості 2 Мбіт/с використовується технологія DSSS з 11-чіповими кодами Баркера, але для модуляції несучого коливання застосовується відносна квадратурна фазова модуляція (*Differential Quadrature Phase Shift Key, DQPSK*). Швидкість передачі окремих чіпів послідовності Баркера тут залишається (як і для швидкості 1 Мбіт/с), $11 \cdot 10^6$ чіпів за секунду, а отже, не змінюється й ширина спектра сигналу.

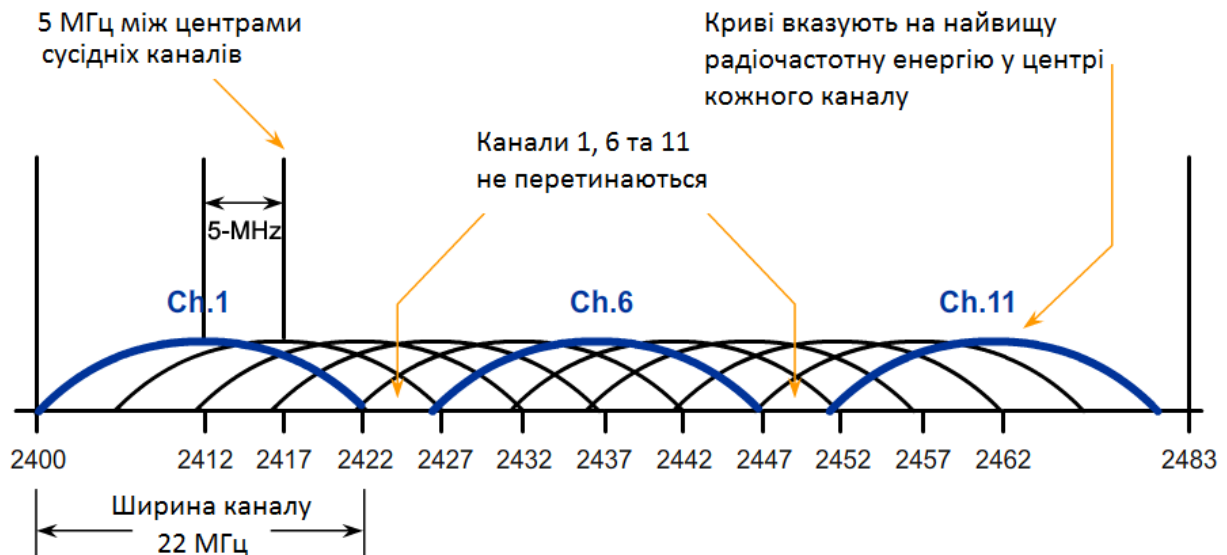


Рисунок 3.13 – Розподіл каналів для діапазону 2,4 ГГц

Стандарт IEEE 802.11b

У липні 1999 року було розроблено та прийнято стандарт IEEE 802.11b, який є розширенням базового протоколу 802.11 [17]. Він, крім швидкостей 1 і 2 Мбіт/с, передбачає ще 5,5 і 11 Мбіт/с, для роботи на яких використовуються комплементарні коди (*Complementary Code Keying, CCK*). Сума автокореляційних функцій комплементарних кодів (КК), як і кодів Баркера для будь-якого відмінного від нуля циклічного зсуву, завжди дорівнює нулю, тому вони можуть використовуватися для розпізнавання сигналу на тлі шуму. Проте, на відміну від кодів Баркера, кодувати логічний нуль або одиницю можна не однією конкретною послідовністю, а цілим набором таких послідовностей. Тому в одному символі, що передається, можна кодувати декілька інформаційних бітів, підвищуючи інформаційну швидкість передачі.

У стандарті IEEE 802.11b використовуються 8-чіпові комплексні комплементарні послідовності, визначені на множині комплексних елементів, які набувають значення $\{1, -1, +j, -j\}$. При цьому значення послідовності 1 та -1 відповідають сигналу, що є синфазним та протифазним до сигналу генератора, а значення j та $-j$ – сигналу, що зміщений по фазі на $p/2$ та $-p/2$ відповідно.

Кожен елемент КК – це комплексне число, яке визначається за досить складним алгоритмом. Усього є 64 набори можливих КК, вибір кожного

з них визначається послідовністю вхідних біт. Під час кодування кожного символу використовується один з 64 можливих восьмирозрядних КК. Для однозначного вибору одного КК потрібно знати шість вхідних біт.

При швидкості 5,5 Мбіт/с в одному символі одночасно кодується 4 біти даних, а при швидкості 11 Мбіт/с – 8. В обох випадках символна швидкість передавача становить $11/8 = 5,5/4 = 1,385 \cdot 10^6$ символів за секунду, а враховуючи, що кожен символ задається 8-чіповою послідовністю, отримуємо, що в обох випадках швидкість прямування окремих чіпів становить $11 \cdot 10^6$ чіпів у секунду. Відповідно, ширина спектра сигналу при швидкості як 11, так і 5,5 Мбіт/с становить 22 МГц.

Стандарт IEEE 802.11g

Стандарт IEEE 802.11g прийнято у 2003 році [17]. Він є логічним розвитком стандарту 802.11b і передбачає передачу даних у тому ж частотному діапазоні, але з вищими швидкостями, і повністю сумісний з 802.11b (тобто будь-який пристрій 802.11g має підтримувати роботу з пристроями 802.11b). Максимальна швидкість передачі даних у стандарті 802.11g становить 54 Мбіт/с.

Під час розробки стандарту 802.11g розглядалися дві конкуруючі технології: метод ортогонального частотного розділення (*Orthogonal Frequency-Division Multiplexing, OFDM*), запозичений зі стандарту 802.11a і запропонований компанією Intersil, та метод двійкового пакетного згортального кодування (*Packet Binary Convolutional Coding, PBCC*), запропонований компанією Texas Instruments. У результаті стандарт 802.11g містить компромісне рішення: як базові застосовуються технології OFDM і ССК, а опціонально передбачено використання технології PBCC.

Ідея згортального кодування полягає в тому, що вхідна послідовність інформаційних бітів перетворюється у загортальному кодері так, щоб кожному вхідному біту відповідало більше одного вихідного. Тобто, до вихідної послідовності додається деяка надлишкова інформація. Якщо, наприклад, кожному вхідному біту відповідають два вихідних, то маємо загортальне кодування зі швидкістю $r = 1/2$.

Загортальний кодер будується на основі декількох послідовно з'єднаних комірок пам'яті та логічних елементів XOR. Кількість комірок пам'яті визначає кількість можливих станів кодера. Якщо, наприклад, використовується 6 комірок пам'яті, то в кодері зберігається інформація про 6 попередніх станів сигналу, а з урахуванням значення вхідного біта отримуємо, що у кодері використовується 7 бітів вхідної послідовності. Такий загортальний кодер називається кодером на 7 станів.

Вихідні біти, що формуються у загортальному кодері, визначаються операціями XOR між значеннями вхідного біта й бітами, що зберігаються в комірках пам'яті. У технології PBCC використовуються згортальні кодери на 7 станів зі швидкістю $r = 1/2$.

Головна перевага загортальних кодерів є завадостійкість сформованої ними послідовності, оскільки при надмірності кодування навіть у випадку виникнення помилок прийому початкова послідовність бітів може бути відновлена. Для такого відновлення на стороні приймача застосовується декодер Вітербі.

Дибіт (два біти), що формується у загортальному кодері, використовується як символ, що надсилається, але попередньо піддається фазовій модуляції. Залежно від швидкості передачі можлива двійкова, квадратурна або восьмипозиційна фазова модуляція.

На відміну від технології DSSS, у технології згортального кодування розширення спектра до стандартних 22 МГц відбувається за рахунок використання варіації можливих сигнальних сузір'їв квадратурної фазової маніпуляції (*Quantitude Phase Shift Keying, QPSK*) і двійкової фазової маніпуляції (*Binary Phase Shift Keying, BPSK*).

Метод РВСС-кодування опціонально використовується у протоколі 802.11b на швидкостях 5,5 і 11 Мбіт/с. Аналогічно у протоколі 802.11g для швидкостей передачі 5,5 і 11 Мбіт/с цей спосіб теж застосовується опціонально. Унаслідок сумісності протоколів 802.11b і 802.11g технології кодування й швидкості, передбачені протоколом 802.11b, підтримуються і в протоколі 802.11g, однак у протоколі 802.11g передбачені такі швидкості, яких немає в протоколі 802.11b.

Стандарт IEEE 802.11a

Стандарт IEEE 802.11a було прийнято в 1999 році. На відміну від стандартів IEEE 802.11b та IEEE 802.11g, які використовують частотний діапазон 2,4 ГГц (від 2,4 до 2,4835 ГГц), даний стандарт передбачає використання частотного діапазону 5 ГГц (від 5,15 до 5,350 ГГц та від 5,725 до 5,825 ГГц). У США цей діапазон називають діапазоном неліцензійної національної інформаційної інфраструктури (*Unlicensed National Information Infrastructure, UNII*) [17].

Відповідно до правил федеральної комісії зі зв'язку (*Federal Communications Commission, FCC*), частотний діапазон UNII розділено на три 100-мегагерцевих піддіапазони, які відрізняються обмеженнями за максимальною потужністю випромінювання. Нижній діапазон (від 5,15 до 5,25 ГГц) передбачає потужність 50 мВт, середній (від 5,25 до 5,35 ГГц) – 250 мВт, а верхній (від 5,725 до 5,825 ГГц) – 1 Вт. Загальна ширина цих трьох частотних піддіапазонів становить 300 МГц, тому стандарт IEEE 802.11a є найширококутовішим із сімейства стандартів 802.11 і дозволяє розділити увесь частотний діапазон на 12 каналів шириною 20 МГц кожен (рис. 3.14). При цьому чотири верхні частотні канали, які передбачають найбільшу потужність передачі, використовують переважно для передачі сигналів поза приміщеннями.

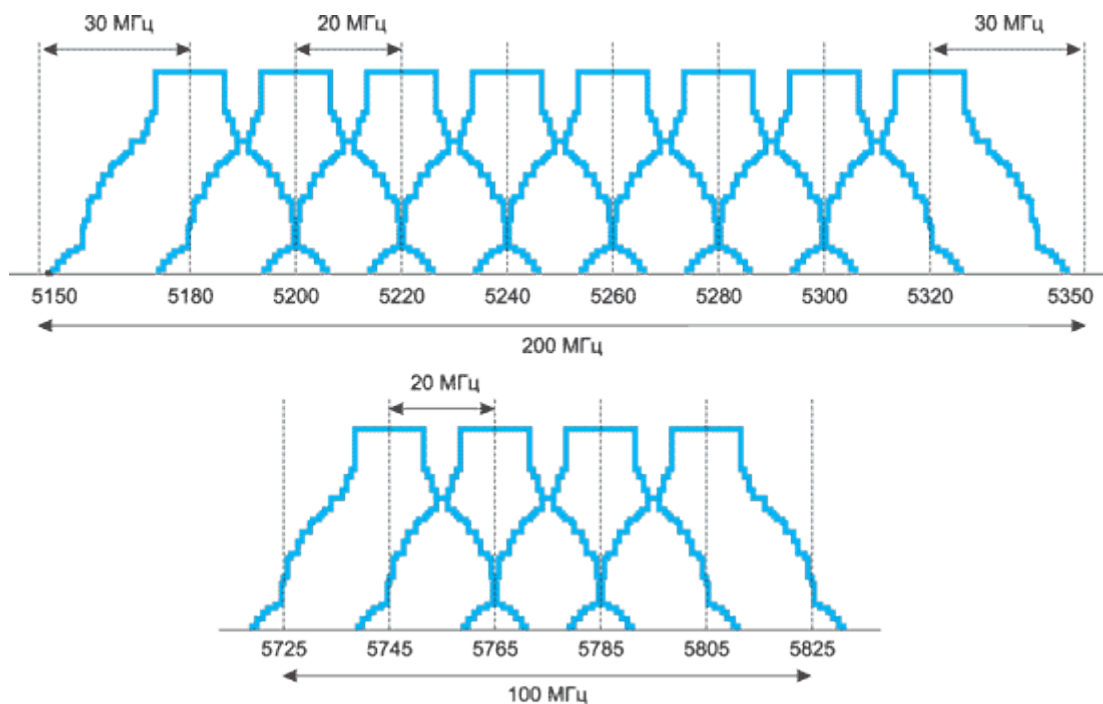


Рисунок 3.14 – Розділення діапазону UNII на 12 частотних піддіапазонів

Стандарт IEEE 802.11a заснований на техніці OFDM. Для розділення каналів застосовується зворотне перетворення Фур'є з вікном у 64 частотних підканали. Оскільки ширина кожного з 12 каналів становить 20 МГц, то кожен ортогональний частотний підканал (піднесуча) має ширину 312,5 кГц. Однак із 64 ортогональних підканалів задіюються лише 52, і лише 48 з них застосовуються для передачі даних (*Data Tones*), а решта – для передачі службової інформації (*Pilot Tones*).

За технікою модуляції протокол 802.11a є аналогічним до 802.11g. На низьких швидкостях передачі для модуляції піднесучих частот використовується двійкова й квадратурна фазові модуляції BPSK і QPSK. BPSK використовується для передачі даних на швидкостях 6 і 9 Мбіт/с, а модуляція QPSK – на швидкостях 12 і 18 Мбіт/с. Для передачі на вищих швидкостях використовується квадратурна амплітудна модуляція 16-QAM (16 різних станів сигналу, що дозволяє закодувати 4 біти в одному символі) і 64-QAM (64 можливих стани сигналу, що дозволяє закодувати 6 бітів в одному символі). Модуляція 16-QAM застосовується на швидкостях 24 і 36 Мбіт/с, а модуляція 64-QAM – на швидкостях 48 і 54 Мбіт/с.

Інформаційна ємність OFDM-символу визначається типом модуляції і числом піднесучих. Оскільки для передавання даних використовуються 48 піднесучих, ємність OFDM-символу становить $48 \cdot K$ (K – кількість бітів, що кодуються в одному символі в одному підканалі). Відповідно ємність OFDM-символу становить від $1 \cdot 48 = 48$ до $6 \cdot 48 = 288$ бітів.

Послідовність обробки вхідних даних (бітів) у стандарті IEEE 802.11a така: спочатку вхідний потік даних скремблюється, а потім надходить на згортальний кодер. Швидкість згортального кодування (у поєднанні з пунктурним кодуванням) може становити 1/2, 2/3 або 3/4. Варто зауважи-

ти, що пунктурне кодування дозволяє знизити надмірну надлишковість даних, збільшивши при цьому швидкість передавання. Нагадаємо, що надмірність загортального кодера дорівнює 2 (на кожен вхідний біт припадає два вихідних) досить висока і за певних умов рівня завад є зайвою, тому її можна зменшити так, щоб кожним двом вхідним бітам відповідали три вихідних. Для цього в схему додали пунктурний кодер, який і знищуватиме зайві біти. Якщо пунктурний кодер вилучає один біт з кожних чотирьох вхідних бітів, тоді кожним чотирьом вхідним бітам відповідатимуть три вихідні. Швидкість такого кодера становить 4:3. Якщо ж пунктурний кодер використовується в парі зі згортальним кодером зі швидкістю 1/2, то загальна швидкість кодування становитиме 2/3, де кожним двом вхідним бітам відповідатимуть три вихідних.

Оскільки швидкість згортального кодування може бути різною, то при використанні одного й того ж типу модуляції швидкість передавання даних також буде неоднаковою.

Розглянемо, наприклад, модуляцію BPSK, при якій швидкість передавання даних становить 6 або 9 Мбіт/с. Тривалість одного символу разом з охоронним інтервалом дорівнює 4 мкс (частота проходження імпульсів 250 КГц). Враховуючи, що у кожному підканалі кодується по одному біту, а всього таких підканалів 48, отримуємо, що загальна швидкість передавання даних становитиме $250 \text{ кГц} \times 48 \text{ каналів} = 12 \text{ МГц}$. Якщо при цьому швидкість згортального кодування дорівнює 1/2 (на кожний інформаційний біт додається один службовий), то інформаційна швидкість буде удвічі меншою, ніж повна швидкість, – тобто 6 Мбіт/с. При швидкості згортального кодування 3/4 на кожні три інформаційних біти додається один службовий, тому в даному випадку корисна (інформаційна) швидкість становить 3/4 від повної швидкості, тобто 9 Мбіт/с.

Аналогічно кожному типу модуляції відповідають дві різні швидкості передавання (табл. 3.3).

Таблиця 3.3 – Співвідношення між швидкостями передачі й типом модуляції у стандарті 802.11a

Швидкість передачі, Мбіт/с	Тип модуляції	Швидкість згортального кодування	Кількість бітів в одному символі в одному підканалі	Загальна кількість бітів у символі (48 підканалів)	Кількість інформаційних бітів у символі	Тип модуляції
6	BPSK	1/2	1	48	24	BPSK
9	BPSK	3/4	1	48	36	BPSK
12	QPSK	1/2	2	96	48	QPSK
18	QPSK	3/4	2	96	72	QPSK
24	16-QAM	1/2	4	192	96	16-QAM
36	16-QAM	3/4	4	192	144	16-QAM
48	64-QAM	2/3	6	288	192	64-QAM
54	64-QAM	3/4	6	288	216	64-QAM

Після згортального кодування потік біт піддається операції перемежування, або інтерлівінга. Її властивість полягає у зміні порядку проходження бітів у межах одного OFDM-символу. Для цього послідовність вхідних бітів розбивається на блоки, довжина яких дорівнює кількості бітів у OFDM-символі (NCBPS). Далі за певним алгоритмом виконується двоетапне переставлення бітів у кожному блоці. На першому етапі біти переставляються так, щоб суміжні біти при передачі OFDM-символу надсилалися на несуміжні піднесучі. Алгоритм переставлення бітів на цьому етапі еквівалентний такій процедурі. Спочатку блок бітів довжиною NCBPS рядком за рядком записується в матрицю, яка містить 16 рядків і NCBPS/16 рядів. Далі біти зчитуються з цієї матриці, але вже по рядах (або так само, як записувалися, але з транспонованої матриці). У результаті такої операції спочатку сусідні біти будуть передаватися на несуміжні піднесучі.

Потім виконується етап другого перестановлення бітів, мета якого полягає в тому, щоб сусідні біти не опинилися одночасно у молодших розрядах груп, які визначають модуляційний символ у сигнальному сузір'ї. Тобто після другого етапу перестановлення, з метою поліпшення завадостійкості переданого сигналу, сусідні біти виявляються поперемінно в старших і молодших розрядах груп.

Після інтерлівінгу послідовність біт розбивається на групи за числом позицій обраного типу модуляції, і формуються OFDM-символи, які надалі піддаються швидкому перетворенню Фур'є. У результаті цього формуються вихідні синфазний і квадратурний сигнали, які потім піддаються модуляції.

Стандарт IEEE 802.11 n

Розробка стандарту IEEE 802.11n офіційно почалася 11 вересня 2002 року (за рік до остаточного прийняття стандарту IEEE 802.11g). У другій половині 2003 року була створена цільова група (*Task Group*) IEEE 802.11n (802.11 TGn), у завдання якої входила розробка нового стандарту бездротового зв'язку на швидкості понад 100 Мбіт/с. Цим же завданням займалась й інша цільова група – 802.15.3a. До 2005 року процеси вироблення єдиного рішення в кожній з груп зайшли в глухий кут. У групі 802.15.3a було протистояння компанії Motorola та усіх інших членів групи, а члени групи IEEE 802.11n розбились на два приблизно однакових табори: WWiSE (*World Wide Spectrum Efficiency*) і TGn Sync. Групу WWiSE очолювала компанія Aigro Networks, а групу TGn Sync – компанія Intel. У кожній з груп довгий час жоден з альтернативних варіантів не міг набрати необхідні для його затвердження 75% голосів.

Після майже трьох років безуспішного протистояння й спроб виробити компромісне рішення, яке влаштовувало б усіх, учасники групи 802.15.3a майже одногосно проголосували за ліквідацію проекту 802.15.3a. Члени проекту IEEE 802.11n виявилися більш гнучкими – вони домовились і створили об'єднану пропозицію, яка б усіх влаштовувала. У результаті 19 січня 2006 року на черговій конференції було схвалено попередню (*draft*)

специфікацію стандарту IEEE 802.11n. Зі 188 членів робочої групи 184 виступили за прийняття стандарту, а четверо утрималось. Головні положення схваленого документа лягли в основу остаточної специфікації нового стандарту.

Стандарт IEEE 802.11n заснований на технології OFDM-MIMO. Багато реалізованих у ньому технічних деталей запозичені зі стандарту 802.11a, проте у стандарті IEEE 802.11n передбачається використання як частотного діапазону, прийнятого для стандарту IEEE 802.11a, так і частотного діапазону, прийнятого для стандартів IEEE 802.11b/g. Тобто пристрої, що підтримують стандарт IEEE 802.11n, можуть працювати в частотному діапазоні або 5 ГГц, або 2,4 ГГц, причому конкретна реалізація залежить від країни.

Збільшення швидкості передачі в стандарті IEEE 802.11n досягається, по-перше, завдяки подвоєнню ширини каналу з 20 до 40 МГц, а по-друге, за рахунок реалізації технології MIMO.

Технологія MIMO (*Multiple Input Multiple Output*) передбачає застосування декількох передавальних і приймальних антен (за аналогією традиційні системи, тобто системи з однією передавальною й однією приймальною антеною, називаються *Single Input Single Output, SISO*). У стандарті IEEE 802.11n передбачено реалізацію до чотирьох просторових потоків.

Теоретично MIMO-система з n -передавальними і n -приймальними антенами здатна забезпечити пікову пропускну здатність в n раз більшу, ніж системи SISO. Це досягається за рахунок того, що передавач розбиває потік даних на незалежні послідовності бітів і надсилає їх одночасно, використовуючи масив антен. Така техніка передачі називається просторовим мультиплексуванням. Усі антени передають дані незалежно одна від одної в одному і тому ж частотному діапазоні.

У стандарті IEEE 802.11n передбачені як стандартні канали зв'язку шириною 20 МГц, так і канали з подвоєною шириною. Однак застосування 40-мегагерцевих каналів є опціональною можливістю стандарту, оскільки використання таких каналів може суперечити законодавству деяких країн.

У стандарті 802.11n передбачено два режими передачі: стандартний (L) і режим з високою пропускну здатністю (*High Throughput, HT*). У традиційних режимах передачі використовуються 52 частотних OFDM-підканали (піднесучих частот), з яких 48 задіюються для передачі даних, а решта – для передачі службової інформації.

У режимах з підвищеною пропускну здатністю із шириною каналу 20 МГц застосовуються 56 частотних підканалів, з яких 52 задіюються для передачі даних, а 4 канали є пілотними. Таким чином, навіть при використанні каналу шириною 20 МГц збільшення частотних підканалів з 48 до 52 дозволяє підвищити швидкість передачі на 8%.

При застосуванні каналу подвоєної ширини (40 МГц), у стандартному режимі передачі віщання ведеться на здвоєному каналі. Відповідно кількість піднесучих частот збільшується удвічі (104 підканали, 96 з яких є інформаційними). Завдяки цьому швидкість передачі збільшується на 100%.

Під час використання 40-мегагерцевого каналу та режиму з високою пропускною здатністю застосовуються 114 частотних підканали, 108 з яких – інформаційні, а 6 – пілотні. Відповідно, це дозволяє збільшити швидкість передачі на 125%.

Стандарт IEEE 802.11ac

Технологія IEEE 802.11ac є розвитком технології IEEE 802.11n і групи стандартів 802.11 загалом. У січні 2011 року було прийнято першу чорнову редакцію стандарту версії 0.1.

До технології IEEE 802.11ac було висунено такі основні вимоги:

1) забезпечення зворотної сумісності з пристроями стандартів IEEE 802.11a та IEEE 802.11n, що працюють у діапазоні частот 5 ГГц;

2) пристрої, що приймають рівні PHY (фізичний) і MAC (доступу до середовища передачі) стандарту IEEE 802.11ac, повинні підтримувати пропускну здатність, яка визначається у ТД до послуги на рівні MAC понад 500 Мбіт/с для одиночної станції та 1 Гбіт/с для кількох станцій, при використанні каналу не більше 80 МГц;

3) на фізичному рівні стандарту IEEE 802.11ac планується повторне використання більшої частини існуючих специфікацій IEEE 802.11a, п скрізь, де це можливо, модифікуючи їх для досягнення поставлених цілей. Такий підхід дає деякі переваги, з погляду зворотної сумісності. IEEE 802.11ac використовує ортогональний частотний поділ каналів (OFDM) так само, як і IEEE 802.11a, п та підтримує таку ж архітектуру модуляції й кодування;

4) пристрої стандарту IEEE 802.11ac повинні підтримувати застосування захисних інтервалів в 800 нс, RBCC і передачі окремих просторових потоків даних; для режиму IEEE 802.11ac обов'язкова підтримка каналів шириною 80 МГц. Як відомо, серед опцій, передбачених у режимі IEEE 802.11n, була підтримка від 2 до 4 просторових потоків, застосування коду з малою щільністю перевірок на парність (*Low-Density Paritycheck Code, LDPC*) і просторово-часового блочного кодування («*Alamouti*» *Space-Time Block Coding, STBC*), формування діаграми спрямованості антени під час передачі та захисного інтервалу 400 нс. Опції 802.11ac передбачають вже підтримку передачі від 5 до 8 просторових потоків, ширину каналу 160 МГц, (суцільна ширина 80 + 80 МГц), з'єднання каналів («*channel bonding*») для несуміжних каналів 80 + 80 МГц, застосування швидкості кодування MCS 8/9 (256-QAM).

Усі пристрої IEEE 802.11ac, що підтримують тільки стандартні параметри (канал 80 МГц, один просторовий потік, модуляцію 64QAM зі швидкістю кодування 5/6), забезпечуватимуть швидкість передачі даних на рівні приблизно 293 Мбіт/с, а системи, здатні підтримувати опціональні параметри (8 просторових потоків і 256-QAM зі швидкістю кодування 5/6 і коротким захисним інтервалом) будуть здатні досягати швидкості передачі до 3,5 Гбіт/с.

Застосування модуляції 256-QAM і зменшення тривалості захисного інтервалу дозволить збільшити пропускну здатність обладнання IEEE 802.11ac на 61% (до 86,7 Мбіт/с) у каналі 20 МГц порівняно з IEEE 802.11a, і на 20%, порівняно з IEEE 802.11n.

Максимальна теоретична пропускну здатність в IEEE 802.11ac становить 6933,3 Мбіт/с, забезпечується при ширині каналу 160 МГц і за умови використання восьми антен, які працюють у режимі просторового мультиплексування, що еквівалентно розділенню потоку даних на кілька просторових потоків і передачі їх одночасно за допомогою кількох антен.

Вищі значення пропускну здатності й швидкості передачі даних у IEEE 802.11ac застосовуються для забезпечення роботи для низки додатків таких, як: бездротові дисплеї; поширення контенту (наприклад, телебачення високої чіткості) у домашньому середовищі; швидкий обмін даними із сервером (скачування/завантаження великих файлів); транзитне передавання даних (мережа, точка–точка і т. д.); різні додатки в аудиторіях та університетських містечках; автоматизація на виробничій ділянці.

Очікується, що найбільш затребуваними на ринку моделями використання з високою пропускну здатністю стануть ігрові додатки, трансляція на телевизор або проектор у конференц-залах, а також забезпечення швидкої синхронізації передачі даних.

Основні відмінності стандарту 802.11ac від 802.11n

У початкових версіях Wi-Fi (до специфікації IEEE 802.11n) усі дані передавалися в одному потоці, версія «n» дозволяє передавати дані в чотирьох потоках, але зазвичай на практиці передавання здійснюється у двох потоках. Нагадаємо, що у стандарті 802.11n, порівняно з попередніми версіями, вдалося підвищити швидкість передачі з 54 до майже 75 Мбіт/с за допомогою оптимізації механізмів передачі пакетів і модуляції. Шляхом з'єднання каналів («*channel bonding*») досягалися нарощування ширини каналу з 20 до 40 МГц, і, відповідно, подвоєння швидкості передачі до 150 Мбіт/с в одному просторовому потоці даних. Мультиплексування чотирьох стандартизованих просторових потоків дозволяло вийти на теоретичну швидкість передачі $4 \cdot 150 = 600$ Мбіт/с, оскільки сумарна максимальна швидкість передачі дорівнює добутку кількості каналів на максимальну швидкість передачі кожного каналу.

В IEEE 802.11ac кількість каналів збільшено до восьми, а максимально можлива швидкість передачі залежить від ширини каналів. Наприклад, для ширини 160 (80 + 80) МГц виходить 866 Мбіт/с, а теоретична максимальна швидкість становитиме майже 7 Гб/с (8·866 Мбіт/с), що значно перевищує можливості IEEE 802.11n.

Під час робіт над IEEE 802.11ac вдалося ще краще оптимізувати механізми передачі пакетів і модуляції: 256-QAM, швидкість кодування 3/4 та 5/6 також додана як опція (в IEEE 802.11n застосовувалася модуляція 64-QAM, максимальна швидкість кодування 5/6). Ця нова версія, як наступний логічний крок збільшення швидкості передачі, передбачає подальше збільшення ширини каналів до значень 80 МГц та 160 МГц, число просторових потоків в 802.11ac збільшилося з 4 до 8.

Нові канали вже не вписуються у діапазон 2,4 ГГц, тому обладнання IEEE 802.11ac – дводіапазонне, працює у діапазоні 5 ГГц, підтримуючи роботу функції IEEE 802.11n у діапазоні 2,4 ГГц. Крім збільшення швидкостей передачі, в IEEE 802.11ac реалізовані такі поліпшення, як: MU-MIMO й динамічна зміна діаграми спрямованості антен – «Beamforming».

Відображення сигналу від різних поверхонь і предметів призводять до падіння його потужності, а на приймач відбиті сигнали надходять із зсувом фази, що зменшує сумарну амплітуду сигналу. Призначення beamforming полягає у формуванні спрямованого сигналу, тобто в оптимальному підлаштуванні зони покриття ТД відповідно до поточного розташування користувачів. Іншими словами, передавач визначає зразкове місце розташування приймача й формує діаграму спрямованості декількох антен в цьому напрямку замість рівномірного випромінювання сигналу в усі сторони від приймача.

У результаті можна не тільки домогтися поліпшення показників поширення сигналу на відкритому просторі, а й долати такі перешкоди, як стіни. Замість нестабільного, часто низькошвидкісного зв'язку, а то й повної відсутності зв'язку домашнього маршрутизатора з пристроями у сусідній кімнаті, пристрої IEEE 802.11ac зможуть підтримувати стійкий і якісний зв'язок з вищою швидкістю.

Цей метод вже був раніше стандартизований як опція стандарту IEEE 802.11n, але ефективність beamforming виявилася недостатньою через відсутність у різних постачальників єдиного підходу та єдиних вимог, що призводило до слабкої взаємної сумісності їхньої продукції. Саме тому даний параметр є обов'язковим у IEEE 802.11ac, усі характеристики цієї опції вже уніфіковані, і на практиці вона буде застосовуватися все частіше.

Для підтримки beamforming були проведені зміни на рівні управління доступом до середовища передачі MAC і розроблені механізми забезпечення сумісності для каналів шириною 20/40/80/160 МГц, а також пристроїв, що підтримують стандарти як IEEE 802.11ac, так і IEEE 802.11a/n.

У Wi-Fi-мережах використовується напівдуплексне передавання даних («один веде передачу – інші слухають»), у кожен момент часу послідовно передається один пакет. Для IEEE 802.11n (наприклад, MIMO 3×3:3) повністю потенціал у 450 Мбіт/с використовувати неможливо: наприклад, якщо передається потік даних у 3 Мбіт/с, то 447/450 смуги пропускання не можна використовувати для передачі даних іншого користувача. Це, насамперед, не дозволяє повною мірою задіяти потенціал швидкостей IEEE 802.11n, особливо у корпоративних мережах, де число користувачів значне, а трафік порівняно низькошвидкісний.

Застосування методу MU-MIMO (Multi-User MIMO, або багато-користувацьке MIMO) дозволяє вирішити цю проблему шляхом поділу великого «поток» на кілька менших, і передавати по них дані паралельно. У MU-MIMO множина станцій Wi-Fi, оснащених однією або декількома антенами, одночасно передає або приймає потоки даних незалежно один від одного.

Варіанти реалізації MU-MIMO у IEEE 802.11ac такі:

– множинний доступ з просторовим поділом (*Space Division Multiple Access, SDMA*). Він характеризується тим, що потоки розділені не за частотою, а просторово, аналогічно MIMO в IEEE 802.11n, і дозволяє передавати дані різним користувачам різними просторовими потоками за допомогою динамічної зміни діаграми спрямованості антен;

– MIMO з поділом піднесучих OFDM – «Downlink MIMO». Він включений у нову версію стандарту як опція, діє за принципом «один передавальний пристрій – багато приймальних пристроїв» та передбачає поділ несучих OFDM на групи з динамічним розподілом потрібного числа піднесучих кожному користувачеві.

Ці методи дозволяють використовувати весь потенціал високої швидкості передачі для мереж домашніх і корпоративних (з великим числом користувачів).

У змішаних мережах усі пристрої будуть взаємодіяти незалежно від своєї базової версії IEEE 802.11, оскільки забезпечення сумісності з усіма ранніми версіями стандарту спочатку було більш пріоритетним порівняно із завданням перевищення гигабітної швидкості будь-якими способами.

У ранніх версіях IEEE 802.11n використовувався спочатку тільки діапазон 2,4 ГГц (у ньому сигнал ефективніше оминає перешкоди і краще поширюється на великі відстані), а в більш пізніх версіях – і 5 ГГц. Вибір робочого діапазону 5 ГГц для IEEE 802.11ac пояснюється саме міркуваннями сумісності та ефективності передачі даних, оскільки діапазон 2,4 ГГц вже переповнений великою множиною пристроїв (від мікрохвильових печей та іншої побутової електроніки до пристроїв Bluetooth і Wi-Fi). На практиці його застосування тільки погіршує результат, крім того, у цьому діапазоні недостатньо спектрального ресурсу для розміщення достатньої кількості каналів з необхідною шириною у 80/160 МГц кожен.

Основні характеристики деяких стандартів БЛКМ наведено у табл. 3.4.

Таблиця 3.4 – Основні характеристики деяких стандартів БЛЮМ

Стандарт	Модуляція	Швидкість передачі (Мбіт/с)	Застосування MIMO (кількість просторових потоків)	Частотний діапазон (МГц)	Дальність дії (м)
802.11	BPSK	До 1	–	2,4	До 35
	DSSS	До 2			
802.11b	DSSS	До 11	–	2,4	До 35
802.11g	DSSS	До 11	–	2,4	До 35
	OFDM	До 54			
802.11a	OFDM	До 54	–	5,7	До 35
802.11n	OFDM	До 600	+ (до 4)	2,4; 5,7	До 70
802.11ac	OFDM	До 6933	+ (до 8)	2,4; 5,7	До 70

Стандарт IEEE 802.11d

Прагнучи розширити географію розповсюдження мереж стандарту 802.11, IEEE розробляє універсальні вимоги до фізичного рівня 802.11 (наприклад, процедури формування каналів, псевдовипадкові послідовності частот тощо). Стандарт визначає вимоги до фізичних параметрів каналів (потужність випромінювання й діапазони частот) та пристроїв безпроводових мереж з метою забезпечення їх відповідності законодавчим нормам різних країн.

Стандарт IEEE 802.11e

Дозволяє створювати мультисервісні бездротові лінії зв'язку, що орієнтовані на різні категорії користувачів як корпоративних, так й індивідуальних, а також дозволяє розширювати їх функціональність за рахунок підтримки потокових мультимедіаданих та гарантованої якості послуг (QoS). Стандарт дбає про застосування, що є чутливими до затримок передачі.

Стандарт IEEE 802.11h

Робоча група IEEE 802.11h розглядає можливість доповнення існуючих специфікацій 802.11 MAC і фізичний рівень у мережах 802.11a алгоритмами ефективного вибору частот для офісних і вуличних безпроводових мереж, а також засобами керування використанням спектра, контролю за випромінюваною потужністю й генерацією відповідних звітів.

Розв'язання цих задач базується на використанні протоколів Dynamic Frequency Selection (DFS) і Transmit Power Control (TPC), запропонованих Європейським інститутом стандартів з телекомунікацій (ETSI). Зазначені протоколи передбачають динамічне реагування клієнтів бездротової мережі на інтерференцію радіосигналів шляхом переходу на інший канал, зниження потужності або обома способами.

Розробка даного стандарту пов'язана з проблемами при використанні 802.11a у Європі, де у діапазоні 5 ГГц працюють деякі системи супутникового зв'язку. Для запобігання взаємних перешкод стандарт 802.11h має механізм «квазіінтелектуального» керування потужністю випромінювання і вибором несучої частоти передачі.

Стандарт IEEE 802.11i

Стандарт було створено з метою підвищення рівня безпеки безпроводових мереж. У ньому реалізовано набір захисних функцій при обміні інформацією через бездротові мережі, зокрема, технологія AES (*Advanced Encryption Standard*) – алгоритм шифрування, що підтримує ключі довжиною 128 бітів, 192 біти і 256 бітів.

Стандарт IEEE 802.11r

Передбачає створення універсальної та сумісної системи роумінгу для можливості переходу користувача із зони дії однієї мережі в зону дії іншої.

Стандарт IEEE 802.11f

Описує протокол обміну службовою інформацією між ТД, що необхідно для побудови розподілених безпроводових мереж передачі даних.

Стандарт IEEE 802.11c

Регламентує роботу безпроводових мостів і використовується розробниками безпроводових пристроїв під час розробки ТД.

Контрольні запитання

1. Поясніть, що означає аббревіатура Wi-Fi. Який номер стандарту вона визначає?
2. Наведіть основні переваги застосування безпроводових ЛКМ порівняно з проводовими.
3. Наведіть основні елементи мережі Wi-Fi.
4. Поясніть, у чому сутність режиму роботи безпроводової мережі Ad Hoc.
5. Поясніть, у чому сутність інфраструктурного режиму роботи безпроводової мережі.
6. Поясніть, що означають аббревіатури IBSS, BSS, ESS, BSA, ESA, SSID.
7. Наведіть порівняння відомих вам топологій, що використовуються у безпроводових ЛКМ.
8. Поясніть, що таке асоціація клієнта й ТД, і для чого потрібна така асоціація.
9. Наведіть та стисло охарактеризуйте основні етапи процесу «асоціація клієнта і ТД».
10. Поясніть сутність проблем прихованого вузла та засвіченого вузла.
11. Поясніть сутність протоколу MACA.
12. Поясніть сутність методу доступу до середовища передачі даних, що використовується в мережах Wi-Fi.
13. Наведіть часову діаграму взаємодії вузлів за протоколом CSMA/CA.
14. Поясніть сутність механізму енергозбереження (*Automatic Power Save Delivery, APSD*).
15. Наведіть міжкадрові інтервали для стандарту IEEE 802.11 та поясніть їх сутність.
16. Поясніть сутність механізму множинності передачі (TXOP).
17. Наведіть назви трьох класів кадрів, що використовує стандарт IEEE 802.11, та поясніть їх загальне призначення.
18. Наведіть структуру інформаційного кадру 802.11 та поясніть призначення його полів.
19. Наведіть основні різновиди стандарту IEEE 802.11
20. Охарактеризуйте стандарт IEEE 802.11.
21. Наведіть стислу характеристику стандарту IEEE 802.11b.
22. Охарактеризуйте стандарт IEEE 802.11g.
23. Наведіть стислу характеристику стандарту IEEE 802.11a.
24. Охарактеризуйте стандарт IEEE 802.11n.
25. Охарактеризуйте стандарт IEEE 802.11ac.
26. Наведіть основні відмінності між стандартами IEEE 802.11n та IEEE 802.11ac.
27. Наведіть призначення стандартів IEEE 802.11d, IEEE 802.11e, IEEE 802.11h, IEEE 802.11i, IEEE 802.11r, IEEE 802.11f та IEEE 802.11c.

4 ІНШІ ТЕХНОЛОГІЇ ПРОВОДОВИХ ЛОКАЛЬНИХ МЕРЕЖ

4.1 Технологія Token Ring

4.1.1 Загальні відомості

Технологія Token Ring була розроблена компанією IBM у 1984 році, а потім передана як проект стандарту в комітет IEEE 802, що на її основі у 1985 році прийняв стандарт 802.5. Компанія IBM довгий час використовувала технологію Token Ring як свою основну для побудови локальних мереж на основі комп'ютерів різних класів (мейнфреймів, мінікомп'ютерів і персональних комп'ютерів). Але потім почала поступово переходити на технології сімейства Ethernet. Доцільно зауважити, що на даний час технологія Token Ring є застарілою.

Технологія Token Ring функціонально є набагато складнішою, ніж Ethernet. Вона має деякі властивості відмовостійкості. Тут визначено процедури контролю роботи мережі, які використовують зворотний зв'язок, притаманний кільцю, де надісланий кадр завжди повертається до вузла-джерела. У деяких випадках виявлення та усунення помилки в роботі мережі відбувається автоматично (наприклад, відновлюється токен, що загубився), а у деяких – лише фіксується й передбачає усунення вручну.

Для контролю мережі один з вузлів виконує роль *активного монітора*. Цей вузол вибирається під час ініціалізації кільця, і ним стає той, який має максимальне значення MAC-адреси. Якщо активний монітор виходить з ладу, процедура ініціалізації кільця повторюється і вибирається новий активний монітор. Щоб мережа могла ідентифікувати відмову активного монітора, останній у працездатному стані кожні три секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється у мережі більше семи секунд, то інші станції мережі починають процедуру вибору нового активного монітора.

4.1.2 Метод доступу до розділюваного середовища

У мережі Token Ring використовується кільцева логічна топологія. Кільце утворюється відрізками кабелю, що з'єднують сусідні вузли, де кожен вузол з'єднується зі своїми попереднім та наступним вузлами і може лише з ними безпосередньо обмінюватися даними. Для забезпечення доступу вузлів до фізичного середовища кільцем циркулює маркер – кадр спеціального формату та призначення. У мережі Token Ring будь-який вузол завжди безпосередньо отримує дані тільки від одного вузла – від того, що є попереднім у кільці. Він називається найближчим активним сусідом, розташованим вище за потоком даних (*Nearest Active Upstream Neighbor, NAUN*). Надсилання даних вузол завжди здійснює своєму найближчому сусіду вниз за потоком даних.

Отримавши маркер, вузол аналізує його і за відсутності в ньому даних для передачі, надсилає його до наступного вузла. Вузол, що має дані для передачі, при отриманні маркера вилучає його з кільця. Це дає йому право доступу до фізичного середовища і передачі власних даних. Потім цей вузол надсилає в кільце кадр даних установленого формату послідовно побітно. Надіслані дані проходять кільцем завжди в одному напрямку від одного вузла до іншого.

Усі вузли кільця ретранслюють кадр побітно як повторювачі. Якщо кадр проходить через вузол призначення, то, розпізнавши свою адресу (у кадрі є адреса джерела й приймача), він копіює кадр у свій внутрішній буфер і додає до кадру ознаку підтвердження прийому. Вузол, що надіслав кадр даних у кільце, при його зворотному отриманні з підтвердженням прийому, вилучає цей кадр з кільця та передає в мережу новий маркер для забезпечення можливості іншим станціям мережі надсилати дані. Такий алгоритм доступу застосовується в мережах Token Ring зі швидкістю роботи 4 Мбіт/с, описаних у стандарті 802.5.

Час володіння розділюваним середовищем у мережі Token Ring обмежується часом утримання маркера (*Token Holding Time*), після закінчення якого вузол зобов'язаний припинити надсилання власних даних (поточний кадр дозволяється завершити) і надіслати маркер далі кільцем. Вузол може встигнути передати за час утримання маркера один або кілька кадрів залежно від їх розміру та значення часу утримання маркера. Переважно час утримання маркера за замовчуванням дорівнює 10 мс, а максимальний розмір кадру в стандарті 802.5 не визначено. Для мереж 4 Мбіт/с він зазвичай дорівнює 4 Кбайт, а для мереж 16 Мбіт/с – 16 Кбайт. Це пов'язано з тим, що за час утримання маркера станція повинна встигнути передати хоча б один кадр. При швидкості 4 Мбіт/с за час 10 мс можна передати 5 000 байтів, а при швидкості 16 Мбіт/с – 20 000 байтів. Максимальні розміри кадру обрані з деяким запасом.

У мережах Token Ring 16 Мбіт/с використовується також дещо інший алгоритм доступу до кільця, який має назву алгоритму раннього звільнення маркера (*Early Token Release*). Відповідно до нього, вузол передає маркер до наступного вузла відразу після закінчення надсилання останнього біта кадру, не чекаючи повернення кільцем цього кадру з бітом підтвердження прийому. У такому разі пропускна здатність кільця використовується ефективніше, оскільки кільцем одночасно передаються кадри декількох вузлів. Проте власні кадри в кожен момент часу може надсилати лише один вузол, який в даний момент володіє маркером доступу. Решта вузлів у цей час тільки ретранслюють чужі кадри, а отже, принцип поділу кільця у часі зберігається. Прискорюється лише процедура передачі володіння кільцем.

Для різних видів повідомлень, кадрам, що надсилаються, можуть призначатися різні пріоритети: від 0 (нижчий) до 7 (вищий). Рішення про пріоритет конкретного кадру (протокол Token Ring отримує цей параметр

через міжрівневі інтерфейси від протоколів верхнього рівня, наприклад, рівня застосувань) приймає вузол, який надсилає. Маркер також завжди має деякий рівень поточного пріоритету. Вузол має право захопити надісланий йому маркер лише за умови, що пріоритет кадру, який він хоче надіслати, вищий або дорівнює пріоритету маркера. Інакше він зобов'язаний надіслати маркер кільцем до наступної станції.

За наявності у мережі маркера та його існування лише в одному екземплярі відповідає активний монітор. Якщо цей монітор не отримує маркер протягом тривалого часу (наприклад, 2,6 с), то він породжує новий маркер.

Пріоритетний доступ до кільця

Кожен кадр даних або маркер має пріоритет, встановлюваний бітами пріоритету (значення від 0 до 7, де 7 – найвищий пріоритет). Вузол може скористатися маркером лише у випадку, коли має для передачі кадри з пріоритетом, що більший, або такий, як пріоритет маркера. Мережевий адаптер вузла з кадрами, у яких пріоритет нижче, ніж пріоритет маркера, не може захопити маркер, але може помістити найбільший пріоритет своїх кадрів, що очікують передачі, у резервні біти маркера лише в тому випадку, якщо записаний у резервних бітах пріоритет нижче його власного. Як наслідок, у резервних бітах пріоритету встановлюється найвищий пріоритет вузла, який намагається отримати доступ до кільця, але не може цього зробити внаслідок високого пріоритету маркера.

Вузол, що захопив маркер, надсилає свої кадри з пріоритетом маркера, а потім надсилає маркер наступному сусіду. При цьому він переписує значення резервного пріоритету в поле пріоритету маркера, а резервний пріоритет зводиться до нуля. Тому при наступному проході маркера кільцем його захопить вузол, що має найвищий пріоритет. При ініціалізації кільця основний і резервний пріоритети маркера встановлюються в нуль.

Хоча механізм пріоритетів у технології Token Ring є, він починає працювати тільки тоді, коли додаток чи прикладний протокол вирішують його використовувати. Інакше усі вузли матимуть рівні права доступу до кільця, що в основному й відбувається на практиці, оскільки велика частина додатків таким механізмом не користується. Це пов'язано з тим, що пріоритети кадрів підтримуються не в усіх технологіях. Наприклад, у мережах Ethernet вони відсутні, тому додаток буде поводитися по-різному залежно від технології нижнього рівня, що небажано. У сучасних мережах пріоритетність обробки кадрів звичайно забезпечується комутаторами або маршрутизаторами, які підтримують їх незалежно від використовуваних протоколів каналного рівня.

4.1.3 Фізичний рівень технології Token Ring

Стандарт Token Ring фірми IBM передбачав побудову зв'язків у мережі за допомогою концентраторів MAU (*Multistation Access Unit*) або MSAU (*Multi-Station Access Unit*), тобто пристроїв багатостанційного доступу. Мережа Token Ring може містити до 260 вузлів [1].

Концентратор Token Ring може бути активним або пасивним. Пасивний просто з'єднує порти внутрішніми зв'язками так, щоб вузли, які під'єднуються до цих портів, утворили кільце. Ні посилення сигналів, ні їх ресинхронізації пасивний MSAU не виконує, а лише забезпечує обхід будь-якого порту, коли приєднаний до останнього комп'ютер вимкнено (роль підсилювача сигналів тут бере на себе кожен мережевий адаптер, а роль ресинхронізувального блоку виконує мережевий адаптер активного монітора кільця). Така функція потрібна для забезпечення зв'язності кільця незалежно від стану підключених комп'ютерів (зазвичай обхід порту виконується за рахунок релейних схем, які живляться постійним струмом від мережевого адаптера, а при вимиканні мережного адаптера нормально замкнені контакти реле з'єднують вхід порту з його виходом).

Активний концентратор виконує функції регенерації сигналів і тому іноді називається повторювачем, як у стандарті Ethernet.

Кожен мережевий адаптер Token Ring має блок повторення, який вмiє регенерувати й ресинхронізувати сигнали, однак останню функцію виконує у кільці тільки блок повторення активного монітора.

Блок ресинхронізації складається з 30-бітового буфера, який приймає манчестерські сигнали з дещо спотвореними (за час обороту кільцем) інтервалами проходження. За максимальної кількості станцій у кільці (260) варіація затримки циркуляції біта кільцем може досягати трьох бітових інтервалів. Активний монітор «вставляє» свій буфер у кільце і синхронізує бітові сигнали, надсилаючи їх на вихід з потрібною частотою.

У загальному випадку мережа Token Ring має комбіновану зірково-кільцеву конфігурацію. Кінцеві вузли під'єднуються до MSAU за топологією зірки, а MSAU об'єднуються через спеціальні порти *Ring In (RI)* і *Ring Out (RO)* для утворення магістрального фізичного кільця.

Усі вузли у кільці повинні працювати на одній швидкості – або 4 Мбіт/с, або 16 Мбіт/с. Кабелі, що з'єднують вузол з концентратором, називаються відгалужувальними (*lobe cable*), а кабелі, що з'єднують концентратори – магістральними (*trunk cable*).

Технологія Token Ring дозволяє використовувати для з'єднання кінцевих станцій і концентраторів різні типи кабелів: скручена пара STP Type 1, UTP Type 3, UTP Type 6 та волоконно-оптичний кабель.

При використанні STP Type 1 з номенклатури кабельної системи IBM у кільце допускається об'єднувати до 260 станцій довжиною відгалужувальних кабелів до 100 м, а при використанні UTP максимальна кількість вузлів скорочується до 72 довжиною відгалужувальних кабелів до 45 м.

Відстань між пасивними MSAU може досягати 100 м при використанні кабелю STP Type 1 і 45 м при використанні кабелю UTP Type 3. Між активними MSAU максимальна відстань збільшується відповідно до 730 м або 365 м залежно від типу кабелю.

Максимальна довжина кільця Token Ring становить 4000 м. Обмеження на максимальну довжину кільця і кількість станцій у кільці в технології Token Ring не є такими жорсткими, як у технології Ethernet. Тут ці обмеження здебільшого пов'язані з часом обороту маркера кільцем (та не лише –

є й інші міркування, що диктують вибір обмежень). Так, якщо кільце складається з 260 станцій, то при часі утримання маркера в 10 мс маркер повернеться до активного монітору в гіршому випадку через 2,6 с, а саме цей час складає тайм-аут контролю обороту маркера. Загалом усі значення тайм-аутів у мережевих адаптерах вузлів мережі Token Ring можна налаштувати, тому можна побудувати мережу Token Ring з більшою кількістю станцій і довжиною кільця.

Для мереж Token Ring є апаратура, яка дозволяє покращити деякі стандартні характеристики цих мереж, наприклад, максимальну довжину мережі, відстань між концентраторами, надійність (шляхом використання подвійних кілець). Крім того, компанія IBM запропонувала модернізований варіант технології Token Ring – High-Speed Token Ring (HSTR), яка підтримує бітові швидкості 100 і 155 Мбіт/с, зберігаючи основні особливості технології Token Ring 16 Мбіт/с. Проте, як вже зазначалося раніше, технологія Token Ring на сьогодні не використовується.

4.2 Технологія FDDI

4.2.1 Загальні відомості та основні характеристики технології

Технологія FDDI (*Fiber Distributed Data Interface* – оптоволоконний інтерфейс розподілених даних) була першою технологією локальних мереж, у якій середовищем передачі даних є волоконно-оптичний кабель. На даний момент вона, як і технологія Token Ring, вважається застарілою.

Роботи зі створення технології та пристроїв для використання волоконно-оптичних каналів у локальних мережах почалися у 80-ті роки, згодом після початку промислової експлуатації подібних каналів у територіальних мережах. Проблемна група X3T9.5 інституту ANSI у період з 1986 по 1988 роки розробила початкові версії стандарту FDDI, що забезпечує передачу кадрів зі швидкістю 100 Мбіт/с подвійним волоконно-оптичним кільцем довжиною до 100 км [1, 7, 8, 13].

Технологія FDDI ґрунтується на технології Token Ring і розвиває та удосконалює її основні ідеї. Розробники технології FDDI прагнули, зокрема:

- підвищити бітову швидкість передачі даних до 100 Мбіт/с;
- підвищити відмовостійкість мережі за рахунок стандартних процедур відновлення її після відмов різного роду (пошкодження кабелю, некоректної роботи вузла, концентратора, виникнення на лінії перешкод високого рівня тощо);
- максимально ефективно використовувати потенційну пропускну здатність мережі як для асинхронного, так і синхронного (чуттєвого до затримок) трафіків.

Мережа FDDI будується на основі двох оптоволоконних кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі. Наявність двох кілець – це основний спосіб підвищення відмовостійкості мережі FDDI, і вузли, що хочуть скористатися цим підвищеним потенціалом надійності, мають бути підключені до обох кілець.

У нормальному режимі роботи мережі дані проходять через усі вузли й усі ділянки кабелю тільки первинного (*Primary*) кільця. Такий режим названий режимом *Thru* – «транзитним». Вторинне кільце (*Secondary*) у цьому режимі не використовується.

У випадку виникнення будь-якої відмови, коли частина первинного кільця не може передавати дані (наприклад, обрив кабелю чи відмова вузла), первинне кільце поєднується із вторинним (рис. 4.1), знову утворюючи єдине кільце. Такий режим роботи мережі називається *Wrap*, тобто «згортання» кілець. Операція згортання здійснюється засобами концентраторів або мережевих адаптерів FDDI. Для спрощення цієї процедури дані первинним кільцем завжди передаються в одному напрямку (на діаграмах цей напрямок зображується проти годинникової стрілки), а вторинним – у зворотному (зображується за годинниковою стрілкою). Тому при утворенні загального кільця з двох кілець передавачі станцій, як і раніше, залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати й приймати інформацію сусідніми станціями.

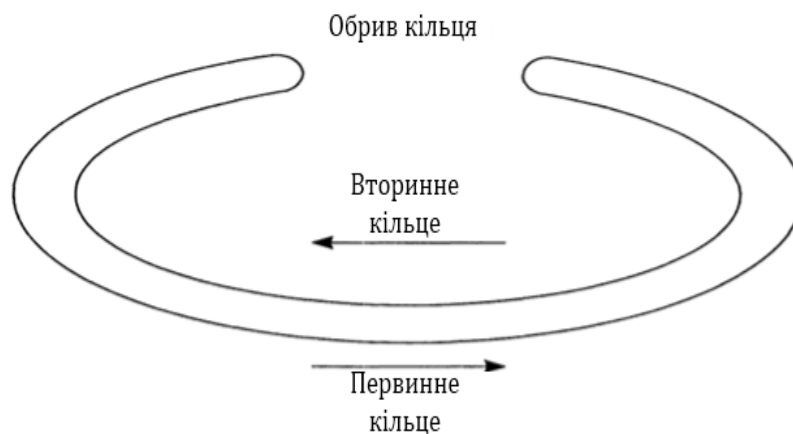


Рисунок 4.1 – Реконфігурація кілець FDDI під час відмови

У стандартах FDDI багато уваги приділяється різним процедурам, які дозволяють спочатку визначити наявність відмов у мережі, а потім зробити необхідну реконфігурацію. Мережа FDDI може цілком відновлювати свою працездатність у випадку одиничних відмов її елементів. При множинних відмовах мережа розпадається на декілька незв'язаних мереж [13].

Технологія FDDI доповнює механізми виявлення відмов технології Token Ring механізмами реконфігурації шляху передачі даних у мережі, заснованими на наявності резервних зв'язків, які забезпечуються другим кільцем.

Кільця у мережах FDDI розглядаються як загальне розділюване середовище передачі даних, тому для нього визначено спеціальний метод доступу. Цей метод дуже близький до методу доступу мереж Token Ring. Вузли FDDI застосовують алгоритм раннього вивільнення токена, як і мережі Token Ring 16 Мбіт/с.

Відмінності у методах доступу полягають у тому, що час утримання маркера у мережі FDDI не є постійною величиною, як у мережі Token Ring. Цей час залежить від завантаження кільця: при невеликому завантаженні воно збільшується, а при великих перевантаженнях може зменшуватися до нуля. Ці зміни у методі доступу стосуються тільки асинхронного трафіка, що є некритичним до невеликих затримок передачі кадрів. Для синхронного трафіка час утримання маркера, як і раніше, залишається фіксованою величиною. Механізм пріоритетів кадрів, прийнятих у технології Token Ring, у технології FDDI відсутній. Розробники технології вирішили, що розподіл трафіка на 8 рівнів пріоритетів надлишковий, і достатньо розділити трафік на два класи – асинхронний і синхронний, останній з яких обслуговується завжди, навіть при перевантаженні кільця.

В іншому випадку, пересилання кадрів між вузлами кільця на рівні MAC повністю відповідає технології Token Ring. Вузли FDDI використовують алгоритм раннього звільнення маркера, як і у мережі Token Ring зі швидкістю 16 Мбіт/с [13].

Адреси рівня MAC мають стандартний для технологій IEEE 802 формат. Формат кадру FDDI близький до формату кадру Token Ring, основні відмінності полягають у відсутності полів пріоритетів. Ознаки розпізнавання адреси, копіювання кадру й помилки дозволяють зберегти наявні в мережах Token Ring процедури обробки кадрів станцією-відправником, проміжними станціями і станцією-одержувачем.

На рис. 4.2 наведено відповідність структури протоколів технології FDDI семирівневій моделі OSI. FDDI визначає протокол фізичного рівня і протокол підрівня доступу до середовища (MAC) каналного рівня. Як і в багатьох інших технологіях локальних мереж, у технології FDDI використовується протокол підрівня керування каналом даних LLC, визначений у стандарті IEEE 802.2. Таким чином, незважаючи на те, що технологія FDDI була розроблена й стандартизована інститутом ANSI, а не комітетом IEEE, вона цілком вписується в структуру стандартів 802.

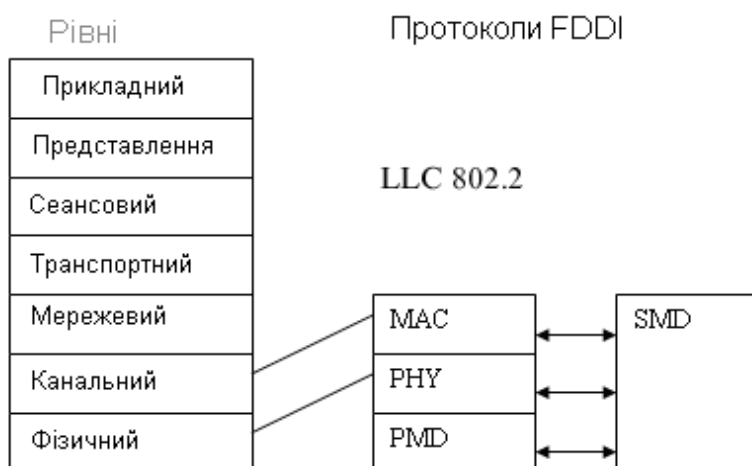


Рисунок 4.2 – Структура протоколів технології FDDI

4.2.2 Метод доступу у FDDI

Для передачі синхронних кадрів вузол завжди має право захопити маркер при його надходженні. При цьому час утримання маркера має заздалегідь задане фіксоване значення. Якщо ж вузлу кільця FDDI потрібно передати асинхронний кадр (тип кадру визначається протоколами верхніх рівнів), то для з'ясування можливості захоплення маркера при його черговому надходженні вузол повинен виміряти інтервал часу, що минув з моменту попереднього надходження маркера. Цей інтервал називається часом обороту маркера (*Token Rotation Time, TRT*). Інтервал TRT порівнюється з іншою величиною – максимально допустимим часом обороту маркера кільцем T_{Org} . Якщо у технології Token Ring максимально допустимий час обороту маркера є фіксованою величиною (2,6 с з розрахунку, що у кільці 260 вузлів), то у технології FDDI вузли домовляються про величину T_{Org} під час ініціалізації кільця. Кожен вузол може запропонувати своє значення T_{Org} , як наслідок, для кільця встановлюється мінімальний, із запропонованих вузлами, час. Це дозволяє враховувати потреби додатків, які працюють на вузлах. Зазвичай синхронним додаткам (додаткам реального часу) потрібно частіше передавати дані в мережу невеликими порціями, тому асинхронним – краще отримувати доступ до мережі рідше, але великими порціями. Перевага надається вузлам, що надсилають синхронний трафік [13].

Таким чином, при черговому надходженні маркера для передачі асинхронного кадру порівнюється фактичний час обертання маркера TRT з максимально можливим T_{Org} . Якщо кільце не перевантажено, то маркер приходить раніше, ніж закінчується інтервал $T_{Org} - TRT < T_{Org}$, і вузлу дозволяється захопити маркер та передати свій кадр (кадри) у кільце. Час утримання маркера TRT дорівнює різниці $T_{Org} - TRT$, і протягом цього часу вузол передає у кільце стільки асинхронних кадрів, скільки встигне.

Якщо ж кільце перевантажено і маркер запізнився, то $TRT > T_{Org}$, і вузол не має права захопити маркер для асинхронного кадру. Якщо всі вузли у мережі хочуть передавати тільки асинхронні кадри, а маркер зробив оберт кільцем занадто повільно, то усі вузли надсилають маркер у режимі повторення, маркер швидко робить черговий оберт і на наступному циклі роботи вузли вже мають право захопити маркер та надсилати свої кадри.

Метод доступу FDDI для асинхронного трафіку є адаптивним і добре регулює тимчасові перевантаження мережі.

4.2.3 Відмовостійкість технології FDDI

Для забезпечення відмовостійкості у стандарті FDDI передбачено створення двох оптоволоконних кілець – первинного та вторинного. У стандарті FDDI допускаються два види під'єднання вузлів до мережі. Одночасне під'єднання до первинного та вторинного кілець називається подвійним під'єднанням (*Dual Attachment, DA*). Під'єднання тільки до первинного кільця називається одиничним під'єднанням (*Single Attachment, SA*).

У стандарті FDDI передбачено наявність у мережі кінцевих вузлів – станцій (*Station*) та концентраторів (*Concentrator*). Для перших і других допустимо як одиничний, так і подвійний вид підключення до мережі. Звичайно, концентратори мають подвійне під'єднання, а станції – одинарне.

У разі одноразового обриву кабелю між пристроями з подвійним під'єднанням мережа FDDI зможе продовжити нормальну роботу за рахунок автоматичної реконфігурації внутрішніх шляхів передачі кадрів між портами концентратора. Двократний обрив кабелю призведе до утворення двох ізольованих мереж FDDI. При обриві кабелю, що проведений до станції з одиничним підключенням, вона стає відрізаною від мережі, а кільце продовжує працювати за рахунок реконфігурації внутрішнього шляху в концентраторі.

Відмовостійкість технології підтримується за рахунок постійного стеження за рівнем керування станцією (*Station Management, SMT*) концентраторів і станцій за тимчасовими інтервалами циркуляції маркера і кадрів, а також за наявністю фізичного з'єднання між сусідніми портами у мережі. У мережі FDDI немає виділеного активного монітора – усі станції та концентратори рівноправні, і при виявленні відхилень від норми вони починають процес повторної ініціалізації мережі, а потім і її реконфігурування [13].

Реконфігурування внутрішніх шляхів у концентраторах і мережевих адаптерах виконується спеціальними оптичними перемикачами, які перенаправляють світловий промінь і мають досить складну конструкцію.

4.2.4 Фізичний рівень технології FDDI

У технології FDDI для передачі світлових сигналів оптичними волокнами реалізовано логічне кодування 4В/5В у поєднанні з фізичним кодуванням NRZI. Ця схема призводить до передачі по ЛЗ сигналів з тактовою частотою 125 МГц.

Оскільки з 32 комбінацій 5-бітових символів для кодування вихідних 4-бітових символів потрібно лише 16 комбінацій, то з решти 16 вибрано кілька кодів, які використовуються як службові. До найважливіших службових символів належить символ Idle, який постійно передається між портами протягом пауз між передачею кадрів даних. За рахунок цього станції та концентратори мережі FDDI мають постійну інформацію про стан фізичних з'єднань своїх портів. У разі відсутності потоку символів Idle фіксується відмова фізичного зв'язку та виконується реконфігурація внутрішнього шляху концентратора або станції, якщо це можливо [13].

При первинному з'єднанні кабелем двох вузлів їх порти спочатку виконують процедуру встановлення фізичного з'єднання. У цій процедурі використовуються послідовності службових символів коду 4В/5В, за допомогою яких створюється певна мова команд фізичного рівня. Ці команди дозволяють, зокрема, вирішити, чи є коректним дане з'єднання, і якщо так – то виконується тестування якості каналу при передачі символів кодів 4В/5В, а потім перевіряється працездатність рівня MAC

з'єднаних пристроїв шляхом передачі декількох кадрів MAC. Якщо усі тести виконано успішно, то фізичне з'єднання вважається встановленим. Роботу зі встановлення фізичного з'єднання контролює протокол управління станцією SMT.

Фізичний рівень розділений на два підрівня: незалежний від середовища підрівень PHY (*Physical*) і залежний від середовища – підрівень PMD (*Physical Media Dependent*) (див. рис. 4.2).

Технологія FDDI підтримує два підрівня PMD: для волоконно-оптичного кабелю і для скрученої пари категорії 5. Останній стандарт з'явився пізніше оптичного та називається TP-PMD.

Оптоволоконний підрівень PMD забезпечує необхідні засоби для передачі даних від одного вузла до іншого через оптичне волокно. Його специфікація визначає:

- використання як основного фізичного середовища багатомодового волоконно-оптичного кабелю 62,5/125 мкм;
- вимоги до потужності оптичних сигналів і максимального загасання між вузлами мережі. Для стандартного багатомодового кабелю ці вимоги призводять до обмеження граничної відстані між вузлами до 2 км, а для одномодового кабелю відстань збільшується до 10–40 км, залежно від якості кабелю;
- вимоги до оптичних обхідних перемикачів (*optical bypass switches*) та оптичного прийомопередавача;
- параметри оптичних конекторів MIC (*Media Interface Connector*), їх маркування;
- подання сигналів в оптичних волокнах, згідно з методом NRZI.

Підрівень TP-PMD визначає можливість передачі даних між вузлами скрученою парою відповідно до методу фізичного кодування MLT-3, що використовує два рівні потенціалу: +V та -V для представлення даних у кабелі. Для отримання рівномірного за потужністю спектра сигналу дані до фізичного кодування проходять через скремблер. Максимальна відстань між вузлами, згідно зі стандартом TP-PMD, дорівнює 100 м [13].

Максимальна загальна довжина кільця FDDI становить 100 км, максимальна кількість станцій з подвійним підключенням у кільці – 500.

4.3 Технологія 100VG-AnyLAN

Технологія 100VG-AnyLAN була розроблена та отримала статус стандарту IEEE 802.12 у 1995 році як альтернатива технології Fast Ethernet. Вона передбачає вдосконалення методу доступу з урахуванням потреби мультимедійних додатків, при збереженні сумісності формату пакета з форматом пакета мереж 802.3. При цьому дана технологія підтримує кадри не лише формату Ethernet, а й Token Ring. Це відображено у назві «технологія для будь-яких мереж» (*Any LAN* перекладається з англійської як «будь-які мережі»), маючи на увазі, що у ЛКМ технології Ethernet і Token Ring використовувалися у переважній кількості вузлів [13].

Не дивлячись на досить високі (на той час) характеристики, технологія 100VG-AnyLAN не знайшла великої кількості прихильників і за популярністю значно поступалася технології Fast Ethernet. Можливо, це відбулося через те, що технічні можливості підтримки різних типів трафіка в технології АТМ значно ширші, ніж у 100VG-AnyLAN. Тому за необхідності тонкого забезпечення якості обслуговування більше застосовували технологію АТМ. А для мереж, у яких немає необхідності підтримувати якість обслуговування на рівні поділюваних сегментів, більш звичною виявилася технологія Fast Ethernet. Тим паче, що для підтримки дуже вимогливих до швидкості передачі даних додатків було розроблено технологію Gigabit Ethernet, яка забезпечує швидкість передачі даних 1000 Мбіт/с.

Варто зазначити, що технологія 100VG-AnyLAN відрізняється від класичного Ethernet у значно більшому ступені, ніж Fast Ethernet. Основні відмінності технології 100VG-AnyLAN наведено нижче. Зокрема, у 100VG-AnyLAN:

- використовується метод доступу Demand Priority (метод доступу за пріоритетом запиту), що забезпечує справедливіший розподіл пропускної здатності мережі та підтримує пріоритетний доступ для синхронних додатків, на відміну від методу CSMA/CD, який використовується в Ethernet;
- кадри надсилаються не усім вузлам мережі, а тільки вузлу призначення;
- є виділений арбітр доступу – концентратор, що відрізняє дану технологію від інших, у яких застосовується розподілений між вузлами мережі алгоритм доступу;
- підтримуються кадри двох технологій: Ethernet і Token Ring;
- дані надсилаються одночасно чотирма парами кабелю UTP категорії 3. Кожною парою дані надсилаються зі швидкістю 25 Мбіт/с, що в сумі дає 100 Мбіт/с. На відміну від Fast Ethernet, у мережах 100VG-AnyLAN немає колізій, тому вдалося використовувати для передачі всі чотири пари стандартного кабелю категорії 3. Для кодування даних застосовується код 5В/6В, який забезпечує спектр сигналу в діапазоні до 16 МГц (смуга пропускання UTP категорії 3) зі швидкістю передачі даних 25 Мбіт/с.

Метод доступу Demand Priority заснований на передачі концентратору функції арбітра, що вирішує проблему доступу до поділюваного середовища. Мережа 100VG-AnyLAN складається із центрального (кореневого) концентратора та з'єднаних з ним кінцевих вузлів, а також інших концентраторів (рис. 4.3). У мережі опускаються три рівні каскадування. Кожен концентратор і мережний адаптер повинні бути настроєні або на роботу з кадрами Ethernet, або з кадрами Token Ring. Циркулювання обох типів кадрів одночасно не допускається.

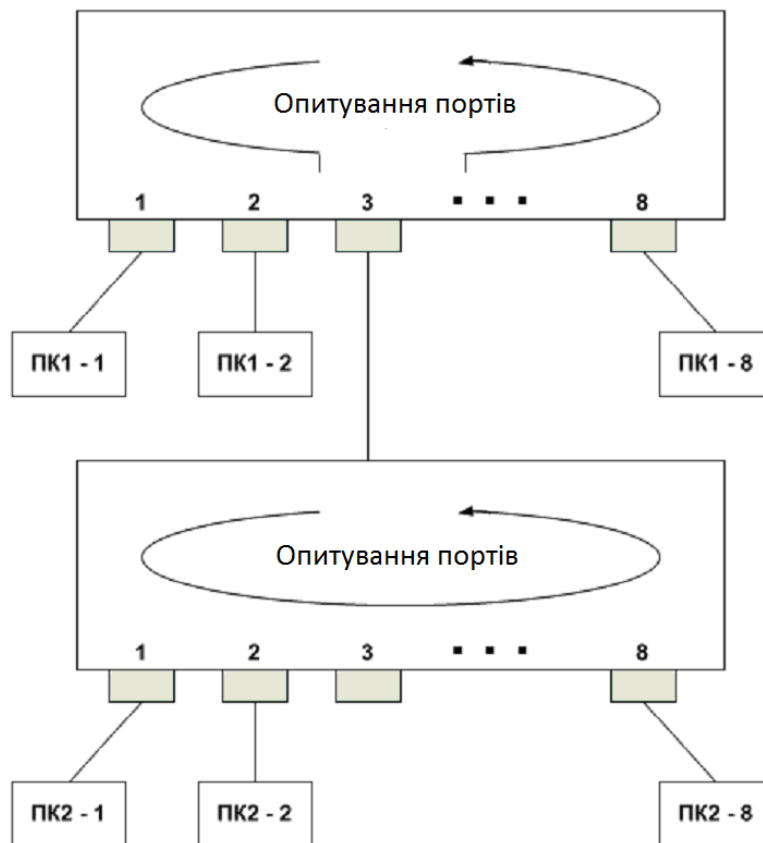


Рисунок 4.3 – Мережа 100VG-AnyLAN

Концентратор циклічно виконує опитування портів. Вузол, що бажає надіслати пакет, надсилає спеціальний низькочастотний сигнал концентратору, запитуючи передачу кадру й указуючи його пріоритет. У мережі 100VG-AnyLAN використовуються два рівні пріоритетів: низький і високий. Низький рівень пріоритету відповідає звичайним даним (файлова служба, служба друку), а високий пріоритет відповідає даним, чутливим до часових затримок (наприклад, мультимедіа). Пріоритети запитів мають статичну й динамічну складові – вузол з низьким рівнем пріоритету, що довго не має доступу до мережі, отримує високий пріоритет.

Якщо мережа вільна, то концентратор дозволяє передачу пакета. Після аналізу адреси отримувача у прийнятому пакеті концентратор автоматично надсилає пакет вузлу призначення. Якщо мережа зайнята, концентратор ставить отриманий запит у чергу, що обробляється відповідно до порядку надходження запитів і з урахуванням пріоритетів. Якщо до порту підключений інший концентратор, то опитування припиняється до завершення опитування концентратором нижнього рівня. Вузли, підключені до концентраторів різного рівня ієрархії, не мають переваг щодо доступу до поділюваного середовища, оскільки рішення про надання доступу приймається після проведення усіма концентраторами опитування всіх своїх портів.

Варто зауважити, що у технології 100VG-AnyLAN визначення MAC-адреси вузла концентратором (для визначення, на який порт потрібно пересилати певний кадр) відбувається в момент його фізичного приєднання до

мережі. Ця MAC-адреса запам'ятовується у таблиці MAC адресів, аналогічній таблиці комутатора. Відмінність концентратора 100VG-AnyLAN від комутатора полягає у тому, що в нього немає внутрішнього буфера для збереження кадрів. Тому він приймає від вузлів тільки один кадр, надсилає його на порт призначення і не приймає нові кадри, допоки цей кадр не буде повністю прийнятий вузлом призначення. Тобто ефект поділюваного середовища зберігається, але кадри не попадають на чужі порти, і їх неможливо перехопити.

Технологія 100VG-AnyLAN підтримує декілька специфікацій фізичного рівня: перший варіант був розрахований на неекрановану скручену пару категорій 3, 4, 5; пізніше з'явилися варіанти фізичного рівня, розраховані на дві неекрановані скручені пари категорії 5; дві екрановані скручені пари типу 1 або два оптичних багатомодових оптоволоконна.

Контрольні запитання

1. Коли і чому було запропоновано технологію Token Ring?
2. Поясніть сутність методу доступу до розділюваного середовища для технології Token Ring. Порівняйте його з аналогічним методом, що використовується в технології Ethernet.
3. Наведіть сутність пріоритетного доступу до кільця для технології Token Ring.
4. Поясніть, з яких міркувань вибирається максимальний час обертання маркера кільцем.
5. Охарактеризуйте фізичний рівень технології Token Ring.
6. Наведіть загальні відомості щодо технології FDDI.
7. Поясніть сутність методу доступу до розділюваного середовища для технології FDDI. Порівняйте його з аналогічним методом, що використовується в технологіях Token Ring та Ethernet.
8. Охарактеризуйте відмовостійкість технології FDDI. Які елементи мережі FDDI забезпечують відмовостійкість?
9. Охарактеризуйте фізичний рівень технології FDDI.
10. Наведіть й охарактеризуйте фізичне та логічне кодування, яке використовується у мережах FDDI.
11. Поясніть, коли та з якою метою було розроблено технологію 100VG-AnyLAN. Поясніть сутність назви даної технології.
12. Наведіть основні відмінності технології 100VG-AnyLAN від технології Ethernet.
13. Як називається метод доступу, що використовується в технології 100VG-AnyLAN? Чим даний метод доступу відрізняється від методу доступу, який використовується в технології Ethernet?
14. Укажіть, які специфікації фізичного рівня підтримує технологія 100VG-AnyLAN.
15. Укажіть максимально допустимі значення MTU для мереж Token Ring, FDDI та 100VG-AnyLAN.

СЛОВНИК ТЕРМІНІВ

Access Control (AC) – керування доступом.

Access Point (AP) – точка доступу.

Arbitration InterFrame Space (AIFS) – міжкадровий арбітражний інтервал.

Association Identifier (AID) – ідентифікатор асоціації.

Association of Radio Industries and Business (ARIB) – Асоціація радіо-промисловості та бізнесу.

Auto-Negotiation – автопереговори.

Baseband Network – мережа з немодульованою передачею (повідомлення надсилаються у цифровій формі єдиним каналом і без частотного поділу).

Beacon – маяк.

Basic Service Area (BSA) – базова зона обслуговування.

Basic Service Set (BSS) – базовий сервіс.

Binary Phase Shift Keying (BPSK) – двійкова фазова маніпуляція.

Bit time (bt) – час передачі одного біту.

Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) – це метод колективного доступу з розпізнавання несучої частоти й запобігання колізій.

Carrier Sense Multiple Access With Collision Detection (CSMA/CD) – це метод колективного доступу з розпізнавання несучої частоти і виявлення колізій.

Clear To Send (CTS) – дозвіл на передачу.

Complementary Code Keying (CCK) – комплементарні коди.

Collision – колізія.

Demand Priority – метод доступу за пріоритетом запиту.

Destination Address (DA) – адреса пункту призначення.

Differential Binary Phase Shift Key (DBPSK) – відносна двійкова фазова модуляція.

Differential Quadrature Phase Shift Key (DQPSK) – відносна двійкова фазова модуляція.

Distributed Coordination Function (DCF) – це режим розподіленого координування.

Dual Attachment Station (DAS) – вузол подвійного під'єднання.

Dual Attachment (DA) – подвійне під'єднання.

End Delimeter (ED) – кінцевий обмежувач.

Exposed Terminal Problem – проблема засвіченого вузла.

European Telecommunications Standards Institute (ETSI) – Європейський інститут стандартів електрозв'язку.

Extended InterFrame Spacing (EIFS) – розширений міжкадровий інтервал.

Extended Service Set (ESS) – розширений сервіс.

Extended Service Area (TSA) – розширена зона обслуговування.

Federal Communications Commission (FCC) – федеральна комісія зі зв'язку.

Fiber Distributed Data Interface (FDDI) – оптоволоконний інтерфейс розподілених даних.

Frame Check Sequence (FCS) – контроль послідовності кадру.

Frame Status (FS) – статус кадру.

Frames-per-second (FPS) – кількість фреймів за секунду.

Full-duplex system (FDX) – дуплексна система.

Independent Basic Service Set (IBSS) – набір незалежних базових служб.

Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів електротехніки й електроніки.

Inter Packet Gap (IPG) – міжкадровий інтервал.

Half-duplex system (HDX) – напівдуплексна система.

Hidden Terminal Problem – проблема прихованого вузла.

Logical Link Control (LLC) – керування логічним каналом.

Media Access Control (MAC) – керування доступом до середовища.

Multiple Access with Collision Avoidance (MACA) – протокол множинного доступу із запобігання колізій.

Multiple Input Multiple Output (MIMO) – технологія, яка передбачає з астосування декількох передавальних і приймальних антен одночасно.

Multistation Access Unit (MSAU) – пристрій багатостанційного доступу.

Nearest Active Upstream Neighbor (NAUN) – найближчий активний сусід, що розташований вище за потоком даних.

Network Allocation Vector (NAV) – вектор розподілу мережі.

Network Utilization (NU) – коефіцієнт використання мережі.

Optical Fiber – оптичне волокно.

Orthogonal Frequency-Division Multiplexing (OFDM) – метод ортогонального частотного розділення.

Packet Binary Convolutional Coding (PBCC) – метод двійкового пакетного згортального кодування.

Packets-per-second (PPS) – кількість пакетів за секунду.

Path Delay Value (PDV) – час подвійного обертання.

Point Coordination Function (PCF) – режим зосередженого координування.

Probe – зонд.

Physical Media Dependent (PMD) – залежний від середовища фізичний рівень.

Physical Medium Attachment (PMA) – підрівень фізичного приєднання.

Quantitude Phase Shift Keying (QPSK) – квадратурна фазова маніпуляція.

Request To Send (RTS) – запит на передавання.

Service Set Identifier (SSID) – ідентифікатор зони обслуговування.

Single Attachment Station (SAS) – вузол одиничного під'єднання.

Shielded Twisted Pair (STP) – екранована скручена пара.

Short InterFrame Interval (SIFS) – короткий міжкадровий інтервал.

Source Address (SA) – адреса джерела.

Space Division Multiple Access (SDMA) – множинний доступ з просторовим поділом.

Start Delimiter (SD) – початковий обмежувач.

Ternary Symbol – трійкова цифра.

Token Holding Time (THT) – час утримання маркера.

Token Rotation Time (TRT) – час обертання маркера.

Unlicensed National Information Infrastructure (UNII) – діапазон неліцензійної національної інформаційної інфраструктури.

Unshielded Twisted Pair (UTP) – неекранована скручена пара.

Wireless Distributed System (WDS) – розподілена мережа.

Wireless Fidelity (Wi-Fi) – безпроводова точність.

Wireless Local Area Network (WLAN) – безпроводова локальна комп'ютерна мережа.

ЛІТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, М. А. Олифер. – [4-е изд., перераб. и доп.]. – СПб. : Питер, 2010. – 944 с.
2. Олифер Н. А. Средства анализа и оптимизации локальных сетей [Электронный ресурс] / Н. А. Олифер, В. Г. Олифер. – Режим доступа : <http://citforum.ru/nets/optimize>.
3. Марченко В. Л. Продуктивність мереж зіркоподібної топології / В. Л. Марченко, О. Д. Войтюк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2011. – № 1. – С. 130–133.
4. Гулиус В. А. Модель оценки производительности сети Fast Ethernet / В. А. Гулиус, А. А. Янковский // Системний аналіз та інформаційні технології : X міжнародна науково-технічна конференція, 2008. – К : 2008.
5. Рональд Б. В. Программа сетевой академии Cisco CCNA 1 и 2 / Б. В. Рональд, К. Р. Киркендаль. – [3-е изд.]. – М. : Изд. дом «Вильямс», 2005. – 1186 с.
6. Буров Є. Комп'ютерні мережі / Буров Є. – [2-ге вид., оновлене і доп.]. – Львів : «Магнолія 2006», 2010. – 262 с.
7. Закер К. Компьютерные сети. Модернизация и поиск неисправностей / Закер К. ; пер. с англ. – СПб. : Питер, 2003. – 1008 с.
8. Спортак М. Компьютерные сети и сетевые технологии / М. Спортак, Ф. Панас. – М. ; СПб. ; К. : 000 «ТНД ДС», 2002. – 736 с.
9. Шиндер Д. Основы компьютерных сетей / Шиндер Д. ; пер. с англ. – М. : Изд. дом «Вильямс», 2002. – 656 с.
10. Кульгин М. В. Компьютерные сети. Практика построения. Для профессионалов / Кульгин М. В. – [2-е изд.]. – СПб. : Питер, 2003. – 462 с.
11. Столлингс В. Современные компьютерные сети / Столлингс В. – [2-е изд.]. – СПб. : Питер, 2003. – 783 с.
12. Арсенюк І. Р. Комп'ютерні мережі : навч. посіб. / Арсенюк І. Р., Яровий А. А., Івасюк І. Д. – Вінниця : ВНТУ, 2013. – 272 с.
13. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер. – [2-е изд., перераб. и доп.]. – СПб. : Питер, 2003. – 864 с.
14. Современные беспроводные сети: состояние и перспективы развития / [Гепко И. А., Олейник В. Ф., Чайка Ю. Д., Бондаренко А. В.] ; под ред. В. Ф. Олейника. – К. : «Экмо», 2009. – 672 с.
15. Росс Д. Wi-Fi. Беспроводная сеть / Росс Д. ; пер. с англ. – М. : ИТ «Пресс», 2007. – 320 с.
16. Гейер Д. Беспроводные сети. Первый шаг / Гейер Д. ; пер. с англ. – М. : Изд. дом «Вильямс», 2005. – 192 с.
17. Пахомов С. Стандарты беспроводной связи IEEE 802.11 / С. Пахомов // КомпьютерПресс. – М. : «КомпьютерПресс», 2008. – № 2. – С. 36–44.
18. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – [5-е изд., перераб. и доп.]. – СПб. : Питер, 2012. – 960 с.
19. Зайченко О. Ю. Комп'ютерні мережі : навч. посіб. для студ. / О. Ю. Зайченко, Ю. П. Зайченко. – К. : Вид. дім «Слово», 2010. – 520 с.

Навчальне видання

**Арсенюк Ігор Ростиславович
Яровий Андрій Анатолійович**

КОМП'ЮТЕРНІ МЕРЕЖІ Частина 3

Навчальний посібник

Редактори: І. Городенська
О. Ткачук

Оригінал-макет підготовлено І. Арсенюком

Підписано до друку 06.02.2017 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різнографічний. Ум. друк. арк. 5,7.
Наклад 50 пр. Зам. № 2017-022.

Вінницький національний технічний університет,
навчально-методичний відділ ВНТУ.
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, к. 2201.
Тел. (0432) 59-87-36.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному
університеті в комп'ютерному інформаційно-видавничому центрі
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-87-38.
publish.vntu.edu.ua; email: kivc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.