О. І. Суприган

ОСНОВИ ПРОЕКТУВАННЯ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Міністерство освіти і науки України
Вінницький національний технічний університет

О. І. Суприган

ОСНОВИ ПРОЕКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів спеціальності «Інтелектуальні системи прийняття рішень». Протокол № 7 від «27» грудня 2007 року.

Вінниця ВНТУ 2008

УДК 681.3.004.7 (075)
С89

Рецензенти:

А. М. Пстух, доктор технічних наук, професор
О. В. Нахайчук, доктор технічних наук, професор
С. М. Захарченко, кандидат технічних наук, доцент

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

Суприган О. І.

С89 **Основи проектування корпоративних комп'ютерних мереж.** Навчальний посібник. – Вінниця: ВНТУ, 2008.- 137 с.

В даному навчальному посібнику розглядаються основні принципи проектування комп'ютерних мереж.

Перша частина посібника містить опис архітектури стандартних комп'ютерних мереж. Друга частина описує основні принципи проектування та розроблення апаратної частини корпоративних мереж. В останній частині описуються основні протоколи, які потрібні для забезпечення коректної роботи мережі, що була розроблена.

Навчальний посібник призначений для студентів спеціальності "Інтелектуальні системи прийняття рішень" курсів "Системне адміністрування", "Захист комп'ютерних мереж", "Корпоративні та глобальні комп'ютерні мережі" і може бути рекомендований для студентів денної та заочної форм навчання.

УДК 681.3.004.7 (075)

ЗМІСТ

ВСТУП

За час, що пройшов з моменту появи перших мереж, був розроблено декілька сотень різних мережевих технологій, однак помітного розповсюдження набули лише деякі з них. Це пов'язано, насамперед, з високим рівнем стандартизації принципів організації мереж і з підтримкою їх відомими компаніями. Проте, не завжди стандартні мережі мають рекордні характеристики, забезпечують найоптимальніші режими обміну.

В даний час зменшення кількості типів використовуваних мереж стало тенденцією. Справа в тому, що збільшення швидкості передавання в локальних мережах до 100 і навіть до 1000 Мбіт/с вимагає застосування найпередовіших технологій, проведення дорогих наукових досліджень. Очевидно, що це можуть дозволити собі тільки найбільші фірми, що підтримують свої стандартні мережі і їх досконаліші різновиди. До того ж більшість споживачів вже встановили в себе якісь мережі і не бажають відразу і цілком заміняти мережеве устаткування. У найближчому майбутньому навряд чи варто очікувати того, що будуть прийняті принципово нові стандарти.

Зв'язок на невеликі відстані в комп'ютерній техніці існував ще задовго до появи перших персональних комп'ютерів. До великих комп'ютерів (mainframes), приєднувалися багаточисельні термінали (або "інтелектуальні дисплеї"). Правда, інтелекту в цих терміналах було дуже мало, практично ніякої обробки інформації вони не здійснювали, і основна мета організації зв'язку полягала в тому, щоб розділити інтелект ("машинний час") великого і дорогого комп'ютера між користувачами, що працюють за цими терміналами. Таке явище називалося режимом поділу часу, тому що великий комп'ютер послідовно в часі вирішував задачі великої кількості користувачів.

Потім були створені мікропроцесори і перші мікрокомп'ютери. З'явилася можливість розмістити комп'ютер на столі у кожного користувача, тому що обчислювальні, інтелектуальні ресурси стали дешевшими. Але зате всі інші ресурси залишалися ще досить дорогими. А що означає голий інтелект без засобів збереження інформації і її документування? Не будеш же кожного разу після включення живлення набирати виконувану програму спочатку або зберігати її в маломісткій постійній пам'яті. На допомогу знову прийшли засоби зв'язку. Об'єднавши кілька мікрокомп'ютерів, можна було організувати спільне використання ними комп'ютерної периферії (магнітних дисків, магнітної стрічки, принтерів). При цьому вся обробка інформації проводилася на місці, але її результати передавалися на централізовані ресурси. Тут знову ж спільно використовувалося найдорожче, що є в системі, але вже зовсім новим способом. Такий режим одержав назву режиму зворотного поділу часу. Як і в першому випадку, засоби зв'язку знижували вартість комп'ютерної системи в цілому.

Потім з'явилися персональні комп'ютери, що відрізнялися від перших мікрокомп'ютерів тим, що мали повний комплект достатньо розвинутої для

цілком автономної роботи периферії: магнітні диски, принтери, не говорячи вже про досконаліші засоби інтерфейсу користувача (монітори, клавіатури, миші і т.д.). Периферія стала дешевшою і за ціною цілком порівняною з комп'ютером.

Без мережі також неможливо обійтися в тому випадку, коли необхідно забезпечити погоджену роботу декількох комп'ютерів. Ця ситуація найчастіше зустрічається, коли ці комп'ютери використовуються не для обчислень і роботи з базами даних, а в задачах керування, вимірювання, контролю, там, де комп'ютер сполучається з тими або іншими зовнішніми пристроями. Прикладами можуть служити різні виробничі технологічні системи, а також системи керування науковими комплексами. Тут мережа дозволяє синхронізувати дії комп'ютерів, розкласти паралельно і відповідно прискорити процес оброблення даних, тобто скласти вже не тільки периферійні ресурси, але й інтелектуальну міць.

Розділ 1
ТОПОЛОГІЯ МЕРЕЖ

1.1 Основні можливості та характеристик мережі

Особливе значення має така характеристика мережі, як можливість роботи з великими навантаженнями, тобто з високою інтенсивністю обміну (або, як ще говорять, з великим трафіком). Адже якщо механізм управління обміном, що використовується у мережі, не занадто ефективний, то комп'ютери можуть тривалий час чекати своєї черги на передавання. І навіть якщо це передавання буде здійснюватися потім на найвищій швидкості і безпомилково, для користувача мережі така затримка доступу до всіх мережевих ресурсів неприйнятна. Адже йому не важливо для чого потрібно чекати.

Механізм керування обміном може гарантовано успішно працювати тільки в тому випадку, коли заздалегідь відомо, скільки комп'ютерів (або, як ще говорять, абонентів, вузлів), можливо підключити до мережі. Інакше завжди можна підключити стільки абонентів, що внаслідок перевантаження перестане працювати будь-який механізм керування. Нарешті, мережею можна назвати тільки таку систему передавання даних, що дозволяє поєднувати до декількох десятків комп'ютерів, але ніяк не два, як у випадку зв'язку через стандартні порти.

Таким чином, сформулювати основні ознаки мережі можна так:

- висока швидкість передачі інформації, велика пропускна здатність мережі. Прийнятна швидкість зараз – не менше 100 Мбіт/с;
- низький рівень помилок передавання (або, що те ж саме, високоякісні канали зв'язку). Припустима імовірність помилок передавання даних повинна бути порядку $10^{-8} – 10^{-12}$;
- ефективний, швидкодіючий механізм керування обміном по мережі;
- заздалегідь чітко обмежена кількість комп'ютерів, що підключаються до мережі.

При такому означенні зрозуміло, що глобальні мережі відрізняються від локальних насамперед тим, що вони розраховані на необмежене число абонентів. Крім того, вони використовують (або можуть використовувати) не занадто якісні канали зв'язку і порівняно низьку швидкість передавання. А механізм керування обміном у них не може бути гарантовано швидким. У глобальних мережах набагато важливіше не якість зв'язку, а сам факт її існування.

Однак мережі мають і досить істотні недоліки, про які завжди варто пам'ятати:

- мережа вимагає додаткових, іноді значних матеріальних витрат на придбання мережевого устаткування, програмного забезпечення, на прокладення сполучних кабелів і навчання персоналу;

• мережа вимагає прийому на роботу фахівця (адміністратора мережі), що буде займатися контролем роботи мережі, її модернізацією, керуванням доступу до ресурсів, усуненням можливих несправностей, захистом інформації і резервним копіюванням. Для великих мереж може знадобитися ціла бригада адміністраторів;

• мережа обмежує можливості переміщення комп'ютерів, підключених до неї, тому що при цьому може бути необхідним перекладання сполучних кабелів;

• мережі являють собою прекрасне середовище для поширення комп'ютерних вірусів, тому питанням захисту від них доведеться приділяти набагато більше уваги, ніж у випадку автономного використання комп'ютерів. Адже досить інфікувати один – і всі комп'ютери мережі будуть уражені;

• мережа різко підвищує небезпеку несанкціонованого доступу до інформації з метою її крадіжки або знищення. Інформаційний захист вимагає проведення цілого комплексу технічних і організаційних заходів.

Необхідно визначити, чи варто підключати до мережі всі комп'ютери компанії або частину з них краще залишити автономними. Можливо мережа взагалі не потрібна, тому що викличе набагато більше проблем, ніж дозволить вирішити.

Тут же варто згадати про такі найважливіші поняття теорії мереж, як абонент, сервер, клієнт.

Абонент (вузол, хост, станція) – це пристрій, підключений до мережі, що активно приймає участь в інформаційному обміні. Найчастіше абонентом (вузлом) мережі є комп'ютер, але абонентом також може бути, наприклад, мережевий принтер або інший периферійний пристрій, що має можливість прямо підключатися до мережі.

Сервером називається абонент (вузол) мережі, що надає свої ресурси іншим абонентам, але сам не використовує їхні ресурси. Таким чином він обслуговує мережу. Серверів у мережі може бути декілька, і зовсім не обов'язково, що сервер – самий потужний комп'ютер. Виділений (dedicated) сервер – це сервер, що займається тільки мережевими задачами. Невиділений сервер може крім обслуговування мережі виконувати й інші задачі. Специфічний тип сервера – це мережевий принтер.

Клієнтом називається абонент мережі, що тільки використовує мережеві ресурси, але свої ресурси в мережу не віддає, тобто мережа його обслуговує, а він нею тільки користується. Комп'ютер-клієнт також часто називають робочою станцією. В принципі кожен комп'ютер може бути одночасно як клієнтом, так і сервером.

Під сервером і клієнтом часто розуміють також не самі комп'ютери, а працюючі на них програмні додатки. У цьому випадку той додаток, що тільки віддає ресурс у мережу, є сервером, а той додаток, що тільки користується мережевими ресурсами – клієнтом.

1.2 Види топології мережі

Під топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі звичайно розуміється фізичне розташування комп'ютерів мережі один щодо іншого і спосіб з'єднання їхніми лініями зв'язку. Важливо відзначити, що поняття топології відноситься, насамперед, до локальних мереж, у яких структуру зв'язків можна легко простежити. У глобальних мережах структура зв'язків звичайно прихована від користувачів і не занадто важлива, тому що кожен сеанс зв'язку може проходити по власному шляху.

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, припустимі і найзручніші методи керування обміном, надійність роботи, можливості розширення мережі. І хоча вибирати топологію користувачеві мережі доводиться нечасто, знати про особливості основних топологій, їхні переваги і недоліки потрібно.

Є три базові топології мережі:

- "Шина" (bus) – усі комп'ютери паралельно підключаються до однієї лінії зв'язку. Інформація від кожного комп'ютера одночасно передається всім іншим комп'ютерам (рис. 1.1).

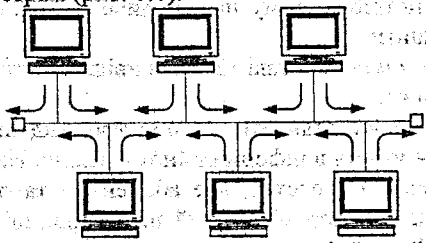

Рисунок 1.1 – Мережева топологія "шина"

- "Зірка" (star) – до одного центрального комп'ютера приєднуються інші периферійні комп'ютери, причому кожний з них використовує окрему лінію зв'язку (рис. 1.2.). Інформація від периферійного комп'ютера передається тільки центральному комп'ютеру, від центрального – одному або декільком периферійним.

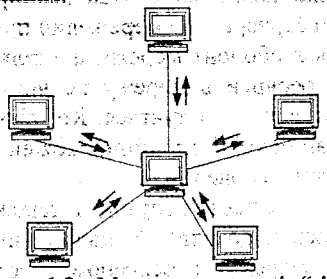

Рисунок 1.2 – Мережева топологія "зірка"

• "Кільце" (ring) – комп'ютери послідовно об'єднані в кільце. Передавання інформації в "кільці" завжди здійснюється тільки в одному напрямку. Кожний з комп'ютерів передає інформацію тільки одному комп'ютеру, що йде в ланцюжку за ним, а одержує інформацію тільки від попереднього у ланцюжку комп'ютера (рис. 1.3).

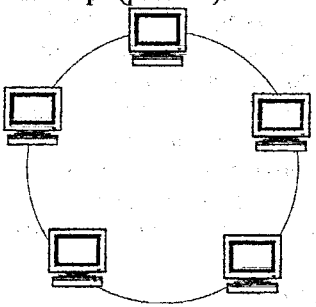

Рисунок 1.3 – Мережева топологія "кільце"

На практиці нерідко використовують і інші топології локальних мереж, однак більшість мереж орієнтована саме на три базові топології.

1.2.1 Топологія "шина"

Топологія "шина" (або, як її ще називають, "загальна шина") своєю структурою припускає ідентичність мережевого устаткування комп'ютерів, а також рівноправність всіх абонентів при доступі до мережі. Комп'ютери в "шині" можуть передавати інформацію тільки по черзі, тому що лінія зв'язку в даному випадку єдина. Якщо кілька комп'ютерів будуть передавати інформацію одночасно, вона спотвориться в результаті накладення (конфлікту, колізії). У шині завжди реалізується режим так званого півдуплексного (half duplex) обміну (в обох напрямках, але по черзі, а не одночасно).

У топології "шина" відсутній явно виражений центральний абонент, через який передається вся інформація, це збільшує її надійність (адже при відмові центра перестає функціонувати вся керована ним система). Додання нових абонентів у шину досить просте і звичайно можливе навіть під час роботи мережі. У більшості випадків при використанні шини необхідна мінімальна кількість сполучного кабелю порівняно з іншими топологіями.

Оскільки центральний абонент відсутній, розв'язання можливих конфліктів у даному випадку покладено на мережеве устаткування кожного окремого абонента. У зв'язку з цим мережева апаратура при топології "шина" складніша, ніж при інших топологіях. Проте через значне поширення мереж з топологією "шина" (насамперед найпопулярнішої мережі Ethernet) вартість мережевого устаткування не занадто висока.

Важлива перевага шини полягає в тому, що при відмові кожного з комп'ютерів мережі, справні машини зможуть нормально продовжувати роботу.

Якщо вважати, що сигнал у кабелі мережі послабляється до гранично припустимого рівня на довжині $L_{пр}$, то повна довжина шини не може перевищувати величини $L_{пр}$. У цьому сенсі "шина" забезпечує найменшу довжину порівняно з іншими базовими топологіями.

Для збільшення довжини мережі з топологією "шина" часто вико ристовують кілька сегментів (частин мережі, кожна з яких є шиною), з'єднаних між собою за допомогою спеціальних підсилювачів і відновлювачів сигналів – репітерів або повторювачів. Однак таке нарощування довжини мережі не може продовжуватися нескінченно. Обмеження на довжину пов'язані з кінцевою швидкістю поширення сигналів по лініях зв'язку.

1.2.2 Топологія "зірка"

"Зірка" – це єдина топологія мережі з явно виділеним центром, до якого підключаються всі інші абоненти. Обмін інформацією йде винятково через центральний комп'ютер, на який покладено велике навантаження, тому нічим іншим, крім мережі, він, як правило, займатися не може. Зрозуміло, що мережеве устаткування центрального абонента повинне бути істотно складнішим, ніж устаткування периферійних абонентів. Про рівноправність всіх абонентів (як у шині) у даному випадку говорити не доводиться. Звичайно центральний комп'ютер самий потужний, саме на нього покладаються усі функції з управління обміном. Ніякі конфлікти в мережі з топологією "зірка" в принципі неможливі, тому що управління цілком централізоване.

Якщо говорити про стійкість "зірки" до відмови комп'ютерів, то вихід з ладу периферійного комп'ютера або його мережевого устаткування ніяк не відбивається на функціонуванні частини мережі, що залишилася, зате будь-яка відмова центрального комп'ютера робить мережу цілком непрацездатною. У зв'язку з цим повинні вживатися спеціальні заходи для підвищення надійності центрального комп'ютера і його мережевої апаратури.

На відміну від "шини", у "зірці" на кожній лінії зв'язку знаходяться тільки два абоненти: центральний і один з периферійних. Найчастіше для їхнього з'єднання використовується дві лінії зв'язку, кожна з яких передає інформацію в одному напрямку, тобто на кожній лінії зв'язку є тільки один приймач і один передавач. Це так зване передавання "точка-точка". Усе це істотно спрощує мережеве устаткування порівняно із шиною і рятує від необхідності застосування додаткових, зовнішніх термінаторів.

Проблема затухання сигналів у лінії зв'язку також вирішується в "зірці" простіше, ніж у випадку "шини", адже кожен приймач завжди одержує сигнал одного рівня. Гранична довжина мережі з топологією "зірка" може

бути вдвічі більшою, ніж у шині (тобто $2L_{пр}$), тому що кожний з кабелів, що з'єднує центр із периферійним абонентом, може мати довжину $L_{пр}$.

"Зірка", показана на рис. 1.2, називається активною або активною зіркою. Існує також топологія, що називається "пасивною зіркою", що тільки зовні схожа на зірку (рис. 1.4). В даний час вона поширена набагато більше, ніж "активна зірка". Досить сказати, що вона використовується в найпопулярнішій сьогодні мережі Ethernet.

У центрі мережі з даною топологією міститься не комп'ютер, а спеціальний пристрій – концентратор або, як його ще називають, хаб (hub), що виконує ту ж функцію, що і репітер, тобто відновлює вхідні сигнали і пересилає їх в усі інші лінії зв'язку.

Велика перевага "зірки" (як активної, так і пасивної) полягає в тому, що всі точки підключення зібрані в одному місці. Це дозволяє легко контролювати роботу мережі, локалізувати несправності шляхом простого відключення від центра тих або інших абонентів (що неможливо, наприклад, у випадку шинної топології), а також обмежувати доступ сторонніх осіб до життєво важливих для мережі точок підключення. До периферійного абонента у випадку "зірки" може підходити як один кабель (по якому йде передавання в обох напрямках), так і два (кожний кабель передає в одному з двох зустрічних напрямків), причому останнє зустрічається набагато частіше.

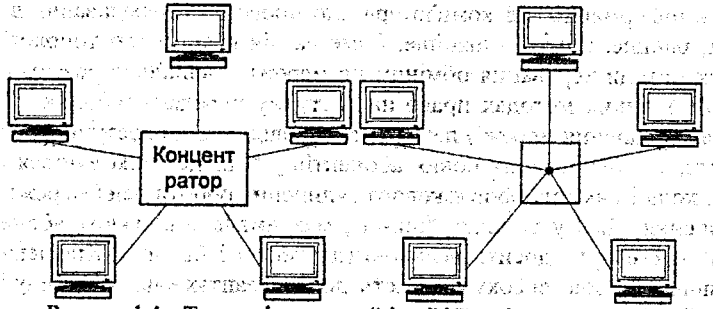

Рисунок 1.4 – Топологія пасивна "зірка" і її еквівалентна схема

Загальним недоліком для всіх топологій типу "зірка" (як активної, так і пасивної) є значно більша, ніж при інших топологіях, витрата кабелю. Наприклад, якщо комп'ютери розташовані в одну лінію, то при виборі топології "зірка" знадобиться в кілька разів більше кабелю, ніж при топології "шина". Це істотно впливає на вартість мережі в цілому і помітно ускладнює прокладання кабелю.

1.2.3 Топологія "кільце"

"Кільце" – це топологія, у якій кожен комп'ютер з'єднаний лініями зв'язку з двома іншими: від одного він одержує інформацію, а іншому

передає. На кожній лінії зв'язку, як і у випадку "зірки", працює тільки один передавач і один приймач (зв'язок типу "точка-точка"). Це дозволяє відмовитися від застосування зовнішніх терміналів.

Важлива особливість "кільця" полягає в тому, що кожен комп'ютер ретранслює (відновлює, підсилює) сигнал, що приходить до нього, тобто виступає в ролі репітера. Затухання сигналу у всьому кільці не має ніякого значення, важливо тільки затухання між сусідніми комп'ютерами кільця. Якщо гранична довжина кабелю, обмежена затуханням, складає $L_{пр}$, то сумарна довжина кільця може досягати $NL_{пр}$, де N – кількість комп'ютерів у кільці. Повний розмір мережі в межах буде $NL_{пр}/2$, тому що кільце доведеться скласти вдвічі. На практиці розміри кільцевих мереж досягають десятків кілометрів (наприклад, у мережі FDDI). Кільце в цьому відношенні істотно перевершує будь-які інші топології.

Чітко виділеного центра при кільцевій топології немає, усі комп'ютери можуть бути однаковими і рівноправними. Однак досить часто в кільці виділяється спеціальний абонент, який керує обміном або контролює його. Зрозуміло, що наявність такого єдиного керуючого абонента знижує надійність мережі, тому що вихід його з ладу відразу ж паралізує весь обмін.

Слід відмітити, що комп'ютери в "кільці" не є цілком рівноправними (на відміну, наприклад, від шинної топології). Адже один з них обов'язково одержує інформацію від комп'ютера, що проводить передавання в даний момент, раніше, а інші – пізніше. Саме на цій властивості топології і будуються методи керування обміном по мережі, спеціально розраховані на "кільце". У таких методах право на наступну передачу (або, як ще говорять, на захоплення мережі) переходить послідовно до наступного по колу комп'ютера. Підключення нових абонентів у "кільце" виконується досить просто, хоча і вимагає обов'язкового зупинення роботи всієї мережі на час підключення. Як і у випадку "шини", максимальна кількість абонентів у "кільці" може бути досить великою (до тисячі і більше). Кільцева топологія звичайно має високу стійкість до перевантажень, забезпечує впевнену роботу з великими потоками переданої по мережі інформації, тому що в ній, як правило, немає конфліктів (на відміну від "шини"), а також відсутній центральний абонент (на відміну від "зірки"), що може бути перевантажений великими потоками інформації.

Сигнал у "кільці" проходить послідовно через усі комп'ютери мережі, тому вихід з ладу хоча б одного з них (або ж його мережевого устаткування) порушує роботу мережі в цілому. Це суттєвий недолік "кільця".

Точно так само обрив або коротке замикання в кожному з кабелів "кільця" робить роботу всієї мережі неможливою. З трьох розглянутих топологій "кільце" найбільш вразливе до ушкоджень кабелю, тому у випадку топології "кільця" звичайно передбачають прокладання двох (або більше) паралельних ліній зв'язку, одна з яких знаходиться в резерві.

Іноді мережа з топологією "кільце" виконується на основі двох паралельних кільцевих ліній зв'язку, що передають інформацію в протилежних напрямках (рис. 1.5). Ціль подібного рішення – збільшення (в ідеалі – вдвічі) швидкості передавання інформації в мережі. До того ж при ушкодженні одного з кабелів мережа може працювати з іншим кабелем (правда, гранична швидкість зменшиться).

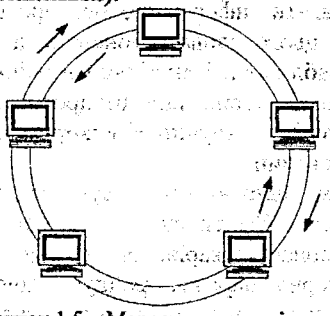

Рисунок 1.5 – Мережа з двома кільцями

Коли говорять про топологію мережі, автори можуть мати на увазі чотири зовсім різні поняття, що відносяться до різних рівнів мережевої архітектури:

- фізична топологія (географічна схема розташування комп'ютерів і прокладення кабелів). У цьому сенсі, наприклад, пасивна "зірка" нічим не відрізняється від активної, тому її нерідко називають просто "зіркою";
- логічна топологія (структура зв'язків, характер поширення сигналів в мережі). Це найправильніше означення топології;
- топологія керування обміном (принцип і послідовність передавання права на захоплення мережі між окремими комп'ютерами);
- інформаційна топологія (напрямок потоків інформації, що передається по мережі).

Наприклад, мережа з фізичною і логічною топологією "шина" може як метод керування використовувати естафетне передавання права захоплення мережі (бути в цьому сенсі "кільцем") і одночасно передавати всю інформацію через виділений комп'ютер (бути в цьому сенсі "зіркою"). Або мережа з логічною топологією "шина" може мати фізичну топологію "зірка" (пасивна) або "дерево" (пасивне).

Мережа з будь-якою фізичною топологією, логічною топологією, топологією управління обміном може вважатися "зіркою" як інформаційна топологія, якщо вона побудована на основі одного сервера і декількох клієнтів, що спілкуються тільки з цим сервером. У даному випадку справедливі всі міркування про низьку відмовостійкість мережі до відмов центра (сервера). Так само будь-яка мережа може бути названа "шиною" в інформаційному сенсі, якщо вона побудована з комп'ютерів, що є одночасно як

серверами, так і клієнтами. Така мережа буде мало чуттєва до відмов окремих комп'ютерів.

1.3 Бездротове середовище передавання

1.3.1 Переваги бездротових комунікацій

Можливість передавати інформацію без дротів, що прив'язують (в буквальному розумінні цього слова) абонентів до певного приміщення, завжди була дуже привабливою. І як тільки технічні можливості ставали достатніми для того, щоб новий вид бездротових послуг набув обох необхідних складових успіху – зручності використання і низької вартості, – успіх йому був гарантований.

Бездротовий зв'язок давно використовується для передавання даних. Велика частина застосувань бездротового зв'язку в комп'ютерних мережах була пов'язана з її фіксованим варіантом. Це може відбуватися у тому випадку, коли комп'ютерна мережа орендує лінію зв'язку у оператора первинної мережі, і окремий канал такої лінії є супутниковим або наземним НВЧ-каналом.

З появою стандарту IEEE 802.11 з'явилася можливість будувати мобільні мережі Ethernet, що забезпечують взаємодію користувачів не залежно від того, в якій країні вони знаходяться і устаткуванням якого виробника вони користуються.

Бездротові мережі часто пов'язують з радіосигналами, проте це не завжди вірно. Бездротовий зв'язок використовує широкий діапазон електромагнітного спектра, від радіохвиль низької частоти в декілька кілогерц до видимого світла, частота якого складає приблизно 8×10^{14} Гц.

1.3.2 Бездротова лінія зв'язку

Бездротова лінія зв'язку будується відповідно до простої схеми. Кожен вузол оснащується антеною, яка одночасно є передавачем і приймачем електромагнітних хвиль. Електромагнітні хвилі поширюються в атмосфері або вакуумі із швидкістю 3×10^8 м/с у всіх напрямках чи ж в межах певного сектора.

Спрямованість або неспрямованість поширення залежить від типу антени. Як спрямовані антени використовують параболічні. Інший тип антен – ізотронні антени, які виконані як вертикальний провідник за вдовжки в чверть хвилі випромінювання, є неспрямованими. Вони широко використовуються в автомобілях і портативних пристроях. Поширення випромінювання на всіх напрямках можна також забезпечити декількома направленими антенами.

Оскільки при неспрямованому поширенні електромагнітні хвилі заповнюють весь простір (в межах певного радіусу, визначеного згасанням потужності сигналу), той цей простір може служити середовищем, що

розділяється. Розділення середовища передавання породжує ті ж проблеми, що і в локальних мережах, проте тут вони посилюються тим, що простір на відміну від кабелю є загальнодоступним, а не належить одній організації. Крім того, дротове середовище строго визначає напрям поширення сигналу в просторі, а бездротове середовище є неспрямованим.

Для передавання дискретної інформації за допомогою бездротової лінії зв'язку необхідно модулювати електромагнітні коливання передавача відповідно до потоку передаваних бітів. Цю функцію здійснює DCE-пристрій, що розташовується між антеною і DTE-пристроєм, яким може бути комп'ютер, комутатор або маршрутизатор комп'ютерної мережі.

1.3.3 Діапазони електромагнітного спектра

Характеристики бездротової лінії зв'язку – відстань між вузлами, територія покриття, швидкість передавання інформації і т.п. – багато в чому залежать від частоти використовуваного електромагнітного спектра.

Діапазон до 300 ГГц має загальну стандартну назву – радіодіапазон. Союз ITU розділив його на декілька піддіапазонів, починаючи від наднизьких частот (Extremely Low Frequency, ELF) і закінчуючи надвисокими (Extra High Frequency, EHF). Звичні для нас радіостанції працюють в діапазоні від 20 кГц до 300 Мгц, і для цих діапазонів існує хоч і не визначена в стандартах, проте часто використовувана назва "широкомовне радіо". Сюди потрапляють низькошвидкісні системи AM- і FM-діапазонів, призначені для передавання даних з швидкостями від декількох десятків до сотень кілобітів в секунду. Прикладом можуть служити радіомодеми, які сполучають два сегменти локальної мережі на швидкостях 2400, 9600 або 19200 Кбіт/с.

1.3.4 Поширення електромагнітних хвиль

Потреба в швидкісному передаванні інформації є переважаючою, тому всі сучасні системи бездротового передавання інформації працюють у високочастотних діапазонах, починаючи з 800 Мгц, не дивлячись на переваги, які обіцяють низькочастотні діапазони завдяки поширенню сигналу уздовж поверхні землі або віддзеркалення від іоносфери.

Для успішного використання мікрохвильового діапазону необхідно також враховувати додаткові проблеми, пов'язані з поведінкою сигналів, що поширюються в режимі прямої видимості і зустрічають на своєму шляху перешкоди.

На рис. 1.6 показано, що сигнал, зустрівшись з перешкодою, може поширюватися відповідно до трьох механізмів: віддзеркалення, дифракція і розсіювання.

Коли сигнал зустрічається з перешкодою, яка частково прозора для даної довжини хвилі і в той самий час розміри якої набагато перевищують довжину хвилі, то частина енергії сигналу відбивається від такої перешко-

ди. Хвилі мікрохвильового діапазону мають довжину декілька сантиметрів, тому вони частково відбиваються від стін будинків при передаванні сигналів в місті. Якщо сигнал зустрічає непроникну для нього перешкоду (наприклад, металеву пластину) також набагато більшого розміру, ніж довжина хвилі, то відбувається дифракція – сигнал ніби огинає перешкоду так, що такий сигнал можна одержати навіть не знаходячись в зоні прямої видимості. При зустрічі з перешкодою, розміри якої майже такі як довжина хвилі, сигнал розсіюється, поширюючись під різними кутами.

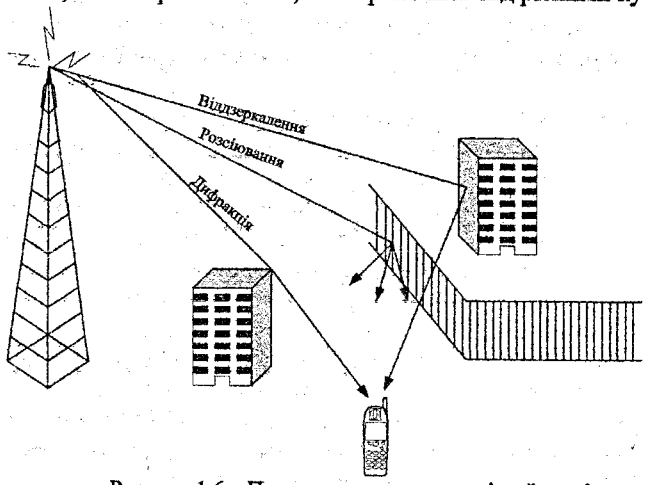

Рисунок 1.6 – Поширення електромагнітної хвилі

В результаті подібних явищ, які всюди зустрічаються при бездротовому зв'язку в місті, приймач може одержати декілька копій одного і того ж сигналу. Такий ефект називається багатопроменевим поширенням сигналу. Результат багатопроменевого поширення сигналу часто виявляється негативним, оскільки один з сигналів може прийти із зворотною фазою і подавити основний сигнал.

Оскільки час поширення сигналу уздовж різних шляхів буде в загальному випадку різним, то може також спостерігатися і міжсимвольна інтерференція, ситуація, коли в результаті затримки сигнали, що кодують сусідні біти даних, доходять до приймача одночасно.

Проблема високого рівня перешкод бездротових каналів вирішується різними способами. Важливу роль відіграють спеціальні методи кодування, які розподіляють енергію сигналу в широкому діапазоні частот. Крім того, передавачі сигналу (і приймачі, якщо це можливо) прагнуть розмістити на високих баштах, щоб уникнути багаторазового відбиття. Ще одним способом є застосування протоколів зі встановленням з'єднань і повторним передаванням кадрів вже на канальному рівні стека протоколів. Ці протоколи дозволяють швидше коректувати помилки, оскільки працюють з мен-

шими значеннями таймаутів, ніж ті що коректують протоколи транспортного рівня, такі як TCP.

1.4 Бездротові системи

1.4.1 Двоточковий зв'язок

Типова схема дротового двоточкового каналу є популярною і для бездротового зв'язку. За двоточковою схемою можуть працювати бездротові канали різного призначення, що використовують різні діапазони частот.

У телекомунікаційних первинних мережах така схема вже довгий час використовується для створення так званих радіорелейних ліній зв'язку. Таку лінію утворюють декілька башт, на яких встановлено параболічні направлені антени. Кожна така лінія працює в мікрохвильовому діапазоні на частотах в декілька гігагерц. Направлена антена концентрує енергію у вузькому пучку, що дозволяє передавати інформацію на значні відстані, звичайно до 50 км. Високі башти забезпечують пряму видимість антен.

Пропускна спроможність лінії може бути досить високою, звичайно вона знаходиться в межах від декількох бітів до сотень мегабітів в секунду. Такі лінії можуть бути як магістральними, так і лініями доступу (у останньому випадку вони найчастіше мають лише один канал). Оператори зв'язку часто використовують такі лінії, коли прокладання оптичного волокна або неможливе (через природні умови), або економічно невигідне.

Радіорелейна лінія зв'язку може використовуватися в місті для з'єднання двох будівель. Оскільки висока швидкість у такому разі не завжди потрібна (наприклад, потрібно з'єднати невеликий сегмент локальної мережі з основною локальною мережею підприємства), то тут можуть застосовуватися радіомодеми, що працюють в АМ-діапазоні. Для зв'язку двох будівель може також використовуватися лазер, забезпечуючи високу інформаційну швидкість (до 155 Мбіт/с), але тільки при відповідному стані атмосфери.

Для відстаней в межах одного приміщення може використовуватися як діапазон інфрачервоних хвиль, так і мікрохвильовий діапазон. Більшість сучасних ноутбуків оснащена вбудованим інфрачервоним портом, тому таке з'єднання може бути утворено автоматично, як тільки порти двох комп'ютерів опиняться в межах прямої видимості (або видимості відбитого променя).

Мікрохвильовий варіант працює в межах декількох десятків або сотень метрів – граничну відстань передбачити неможливо, оскільки при поширенні мікрохвильового сигналу в приміщенні відбуваються численні відбиття, дифракція і розсіювання, до яких додаються ефекти проникнення.

1.4.2 Зв'язок одного джерела і декількох приймачів

Схема бездротового каналу з одним джерелом і декількома приймачами характерна для такої організації доступу, при якій численні призначе-

ні для користувача термінали з'єднуються з базовою станцією (Base Station, BS).

Бездротові лінії зв'язку для схеми одного джерела і декількох приймачів використовуються як для фіксованого доступу, так і для мобільного.

Оператор зв'язку використовує високу вишку (можливо, телевізійну), щоб забезпечити пряму видимість з антенами, встановленими на дахах будівель своїх клієнтів. Фактично такий варіант може бути набором двоточкових ліній зв'язку – за кількістю будівель, які необхідно з'єднати з базовою станцією. Проте це досить марнотратний варіант, оскільки для кожного нового клієнта потрібно встановлювати нову антену на вищці. Тому для економії звичайно застосовують антени, захоплюючі певний сектор, наприклад, 45°. Тоді за рахунок декількох антен оператор може забезпечити зв'язок в межах повного сектора в 360°, звичайно, на обмеженій відстані (звичайно, декілька кілометрів).

Користувачі ліній доступу можуть обмінюватися інформацією тільки з базовою станцією, а вона, у свою чергу, транзитом забезпечує взаємодію між окремими користувачами.

Базова станція звичайно з'єднується дротовим зв'язком з дротовою частиною мережі, забезпечуючи взаємодію з користувачами інших базових станцій або користувачами дротових мереж. Тому базова станція також називається точкою доступу (Access Point, AP). Точка доступу включає не тільки DCE-обладнання, необхідне для утворення лінії зв'язку, але і найчастіше є комутатором мережі, доступ до якої вона забезпечує телефонним комутатором або комутатором пакетів.

У більшості схем мобільного доступу використовується сьогодні принцип стільників, які є невеликими за площею територіями, що обслуговуються однією базовою станцією.

Принцип розбиття всієї області обхвату мережі на невеликі стільники доповнюється ідеєю багаторазового використання частоти. На рис. 1.7 показаний варіант організації стільників за наявності всього трьох частот, при цьому жодна з сусідніх пар стільників не задіює одну і ту саму частоту. Багаторазове використання частот дозволяє оператору економно витрачати виділений йому частотний діапазон, при цьому абоненти і базові станції сусідніх стільників не відчувають проблем через інтерференцію сигналів. Звичайно, базова станція повинна контролювати потужність випромінюваного сигналу, щоб два стільники (несуміжні), що працюють на одній і тій самій частоті, не створювали один одному перешкод.

При гексагональній формі стільників кількість повторюваних частот може бути більшою, ніж 3, наприклад 4, 7, 9, 12, 13 і т.д.

Якщо відома мінімальна відстань D між центрами стільників, що працюють на одній і тій самій частоті, то число стільників (N) можна вибрати за формулою:

$$N = \frac{D^2}{3R^2},$$

де R – радіус стільника.

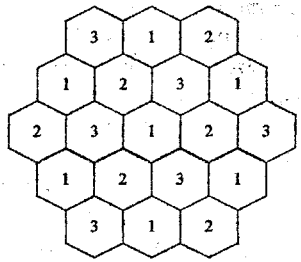

Рисунок 1.7 – Багаторазове використання частот в стільниковій мережі

Невеликі за величиною стільники забезпечують невеликі габарити і потужність термінального пристрою користувача. Саме ця обставина (а також загальний технологічний прогрес) дозволяє сучасним мобільним телефонам бути такими компактними.

Мобільні комп'ютерні мережі поки не набули такого поширення, як телефонні, але принципи організації бездротових ліній зв'язку в них залишаються тими ж.

Важливою проблемою мобільної лінії зв'язку є перехід термінального пристрою з одного стільника до іншого. Ця процедура, яка називається естафетним передаванням, відсутня при фіксованому доступі і відноситься до протоколів вищих рівнів, ніж фізичний.

1.4.3 Зв'язок декількох джерел і декількох приймачів

У випадку схеми з декількома джерелами і декількома приймачами бездротова лінія зв'язку є загальним електромагнітним середовищем, що розділяється декількома вузлами. Кожен вузол може використовувати це середовище для взаємодії з будь-яким іншим вузлом без звернення до базової станції. Оскільки базова станція відсутня, то необхідний де централізований алгоритм доступу до середовища.

Найчастіше такий варіант бездротового каналу застосовується для з'єднання комп'ютерів. Для телефонного трафіка невизначеність в частці пропускної спроможності, що одержується при розділенні середовища, може різко погіршити якість передавання голосу. Тому вони будуються за раніше розглянутою схемою з одним джерелом (базовою станцією) для розподілення смуги пропускання і декількома приймачами.

Сьогодні такі мережі передають дані з швидкістю до 52 Мбіт/с в мікрохвильовому або інфрачервоному діапазоні. Для зв'язку одного з одним використовуються ненапрямлені антени. Для того, щоб інфрачер-

воне світло поширювалося у різних напрямах, застосовуються дифузні передавачі, які розсіюють промені за допомогою системи лінз.

1.4.3.1 Типи супутникових систем

Супутниковий зв'язок використовується для організації високошвидкісних мікрохвильових протяжних ліній. Оскільки для таких ліній зв'язку потрібна пряма видимість, яку через кривизну Землі неможливо за безпечити на великих відстанях, то супутник як відбивач сигналу є природним рішенням цієї проблеми.

Сьогодні супутник може грати роль вузла первинної мережі, а також телефонного комутатора і комутатора/маршрутизатора комп'ютерної мережі. Для цього апаратура супутників може взаємодіяти не тільки з наземними станціями, але і між собою, утворюючи прямі космічні бездротові лінії зв'язку. Принципово техніка передавання мікрохвильових сигналів в космосі і на Землі не відрізняється, проте у супутникових ліній зв'язку є і очевидна специфіка – один з вузлів такої лінії постійно знаходиться у польоті, причому на великій відстані від інших вузлів.

Для супутникового зв'язку союз ITU виділив декілька частотних діапазонів (табл. 1.1.).

Таблиця 1.1 – Частотні діапазони для супутникового зв'язку

Діапазон	Низхідна частота, ГГц	Висхідна частота, ГГц
L	1,5	1,6
S	1,9	2,2
C	3,7-4,2	5,925-6,425
Ku	11,7-12,2	14,0-14,5
Ka	17,7-21,7	27,5-30,5

Історично першим використовувався діапазон С, в якому для кожного з дуплексних потоків Земля-Супутник (висхідна частота) і Супутник-Земля (низхідна частота) виділяється по 500 МГц – достатньо для великого числа каналів. Діапазони L і S призначаються для організації мобільних послуг за допомогою супутників. Вони також часто використовуються наземними системами. Діапазони Ku і Ka поки мало "населені" на Землі, їх застосуванню перешкоджає висока вартість устаткування, особливо для діапазону Ka.

Штучні супутники Землі обертаються навколо неї відповідно до законів, відкритих Йоханесом Кеплером (Johannes Kepler). Орбіта обертання спутника в загальному випадку є еліптичною, але для збереження постійної висоти над Землею супутники можуть переходити на майже кругову орбіту.

Сьогодні використовується три групи кругових орбіт, що відрізняються висотою над Землею:

- геостаціонарна орбіта (Geostationary Orbit, GEO) – 35 863 км;
- середньовисотна орбіта (Medium Earth Orbit, MEO) – 5000-15000 км;
- маловисотна орбіта (Low Earth Orbit, LEO) – 100-1000 км.

1.4.4 Технологія широкосмугового сигналу

Техніка розширеного спектра розроблена спеціально для бездротового передавання. Вона дозволяє поліпшити перешкодостійкість коду для сигналів малої потужності, що дуже важливо для мобільних застосувань. Проте потрібно підкреслити, що техніка розширеного спектра – не єдина техніка кодування, яка застосовується для бездротових ліній зв'язку мікрохвильового діапазону. Тут також застосовуються частотна (FSK) і фазова (PSK) маніпуляції. Амплітудна маніпуляція (ASK) не використовується з тієї причини, що канали мікрохвильового діапазону мають широку смугу пропускання, а підсилювачі, які забезпечують однаковий коефіцієнт посилення для широкого діапазону частот, дуже дорогі.

Широка смуга пропускання дозволяє також застосовувати модуляцію з декількома несучими, в цьому випадку смуга ділиться на декілька підканалів, кожний з яких використовує свою несучу частоту. Відповідно бітовий потік ділиться на декілька підпотоків з нижчою швидкістю. Потім кожен підпотік модулюється за допомогою певної несучої частоти, яка звичайно кратна основній несучій частоті, тобто f_0, $2f_0$, $3f_0$ і т.д. Модуляція виконується за допомогою звичайних методів FSK або PSK. Така техніка називається ортогональним частотним мультиплексуванням (Orthogonal Frequency Division Multiplexing, OFDM).

Перед передаванням всі несучі об'єднуються в загальний сигнал шляхом швидкого перетворення Фур'є. Після передання із загального сигналу шляхом зворотного перетворення Фур'є виділяються несучі підканали, а потім з кожного каналу виділяється бітовий потік. Виграш в розділенні початкового високошвидкісного бітового потоку на декілька низькошвидкісних підпотоків виявляється в тому, що збільшується інтервал між окремими символами коду. Це означає, що знижується ефект міжсимвольної інтерференції, яка з'являється через багатопроменеве поширення електромагнітних хвиль.

1.4.4.1 Розширення спектра стрибкоподібною перебудовою частоти

Ідея методу розширення спектра стрибкоподібною перебудовою частоти (Frequency Hopping Spread Spectrum, FHSS) виникла під час Другої світової війни, коли радіо широко використовувалося для секретних переговорів і для керування військовими об'єктами. Для того, щоб радіообмін не можна було перехопити або заглушити вузькосмуговим шумом, було запропоновано вести передавання з постійною зміною в межах широкого діапазону частот. В результаті потужність сигналу розподілялася по всьо-

му діапазону, і прослуховування якоїсь певної частоти давало тільки невеликий шум. Послідовність несучих частот вибиралася псевдовипадковою, відомою тільки передавачу і приймачу. Спроба заглушення сигналу в якомусь вузькому діапазоні також не дуже погіршувала сигнал, оскільки пригнічувалася тільки невелика частина інформації.

Протягом певного фіксованого інтервалу часу передавання ведеться на незмінній несучій частоті. На кожній несучій частоті для передавання дискретної інформації застосовуються стандартні методи модуляції, такі як FSK або PSK. Для того, щоб приймач синхронізувався з передавачем, для позначення початку кожного періоду передавання протягом деякого часу передаються синхробіти. Отже корисна швидкість цього методу кодування виявляється меншою через постійні накладні витрати на синхронізацію.

Несуча частота змінюється відповідно до номерів частотних підканалів, псевдовипадкових чисел, що виробляються алгоритмом. Псевдовипадкова послідовність залежить від деякого параметра, який називають початковим числом. Якщо приймачу і передавачу відомі алгоритм і значення початкового числа, то вони змінюють частоти в однаковій послідовності, так званій послідовності псевдовипадкової перебудови частоти.

Метод швидкого розширення спектра стійкіший до перешкод, оскільки вузькосмугова перешкода, яка пригнічує сигнал в певному підканалі, не приводить до втрати біта, оскільки його значення повторюється кілька разів в різних частотних підканалах. У цьому режимі не виявляється ефект міжсимвольної інтерференції, тому що до часу надходження затриманого уздовж одного з шляхів сигналу система встигає перейти на іншу частоту.

Метод повільного розширення спектра такої властивості не має, але він простіший в реалізації і має менші накладні витрати.

У методах FHSS підхід до використання частотного діапазону не такий, як в інших методах кодування – замість економного витрачання вузької смуги робиться спроба зайняти весь доступний діапазон. На перший погляд це здається не дуже ефективним – адже в кожен момент часу в діапазоні працює тільки один канал. Проте останнє твердження не завжди справедливе – коди розширеного спектра можна використовувати також і для мультиплексування декількох каналів в широкому діапазоні. Зокрема, методи FHSS дозволяють організувати одночасну роботу декількох каналів шляхом вибору для кожного каналу таких псевдовипадкових послідовностей, щоб в кожен момент часу кожен канал працював на своїй частоті (звичайно, це можна зробити, тільки якщо число каналів не перевищує числа частотних підканалів).

1.4.4.2 Пряме послідовне розширення спектра

У методі прямого послідовного розширення спектра (Direct Sequence Spread Spectrum, DSSS) також використовується весь частотний діапазон, виділений для однієї бездротової лінії зв'язку. На відміну від методу FHSS

весь частотний діапазон займається не за рахунок постійних перемикань з частоти на частоту, а за рахунок того, що кожен біт інформації замінюється N бітами, тобто тактова швидкість передачі сигналів збільшується в N раз. А це, у свою чергу, означає, що спектр сигналу також розширюється в N раз. Достатньо відповідним чином вибрати швидкість передавання даних і значення N, щоб спектр сигналу заповнив весь діапазон.

Мета кодування методом DSSS та ж, що й методом FHSS – підвищення стійкості до перешкод. Вузькосмугова перешкода спотворюватиме тільки певні частоти спектра сигналу, тобто приймач з великим ступенем вірогідності зможе правильно розпізнати передавану інформацію.

Код, яким замінюється двійкова одиниця початкової інформації, називається послідовністю, що розширюється, а кожен біт такої послідовності – чіпом. Відповідно швидкість передавання результуючого коду називають чіповою швидкістю. Двійковий нуль кодується інверсним значенням розширювальної послідовності. Приймачі повинні знати розширювальну послідовність, яку використовує передавач, щоб зрозуміти передавану інформацію.

Кількість бітів в розширювальній послідовності визначає коефіцієнт розширення початкового коду. Як і у разі FHSS, для кодування бітів результуючого коду може використовуватися будь-який вид модуляції, наприклад BFSK.

Чим більший коефіцієнт розширювальної послідовності, тим ширший спектр результуючого сигналу і тим більше ступінь придушення перешкод. Але при цьому росте займаний каналом діапазон спектру. Звичайно коефіцієнт розширення має значення від 10 до 100. Прикладом значення розширювальної послідовності є послідовність Баркера (Barker), яка складається з 11 бітів: 10110111000. Якщо передавач використовує цю послідовність, то передавання трьох бітів АЛЕ веде до передавання таких бітів:

10110111000 10110111000 01001000111.

Послідовність Баркера дозволяє приймачу швидко синхронізуватися з передавачем, тобто надійно виявляти початок послідовності. Приймач визначає таку подію, по черзі порівнюючи одержувані біти із зразком послідовності. Якщо порівняти послідовність Баркера з такою ж послідовністю, але зсунутою на один біт вліво або управо, то матимемо менше половини збігів значень бітів. Це означає, що навіть при спотворенні декількох бітів з великою часткою ймовірності приймач правильно визначить початок послідовності, а значить, зможе правильно інтерпретувати одержувану інформацію.

Метод DSSS у меншій мірі захищений від перешкод, ніж метод швидкого розширення спектра, оскільки могутня вузькосмугова перешкода впливає на частину спектра, а значить, і на результат розпізнавання одиниць або нулів.

1.4.4.3 Множинний доступ з кодовим розділенням

Як і у разі FHSS, кодування методом DSSS дозволяє мультиплексировать декілька каналів в одному діапазоні. Техніка такого мультиплексування називається множинним доступом з кодовим розділенням (Code Division Multiple Access, CDMA). Вона широко використовується в стільникових мережах.

Техніка CDMA може використовуватися спільно з кодуванням методом FHSS, проте на практиці вона частіше застосовується в бездротовій мережі з методом DSSS.

Кожен вузол мережі, що працює за методом CDMA, посилає дані в середовище, що розділяється, в ті моменти часу, коли це йому потрібно, тобто синхронізація між вузлами відсутня. Ідея CDMA полягає в тому, що кожен вузол мережі використовує власне значення розширювальної послідовності. Ці значення вибираються так, щоб приймальний вузол, який знає значення розширювальної послідовності передавального вузла, міг виділити дані передавального вузла з сумарного сигналу, що утворюється в результаті одночасного передавання інформації декількома вузлами.

Для того, щоб таку операцію демультиплексування можна було виконати, значення розширювальної послідовності вибираються певним чином. Розглянемо ідею CDMA на прикладі.

Нехай в мережі працює чотири вузли: A, B, C і D. Кожен вузол використовує такі значення розширювальної послідовності:

A:	0	0	0	0
B:	0	1	0	1
C:	0	0	1	1
D:	0	1	1	0

При передаванні одиниць і нулів розширювальної послідовності (тобто вже перетвореного початкового коду) використовуються сигнали, які є адитивними і інверсними. Інверсивність означає, що двійкова одиниця кодується, наприклад, синусоїдою з амплітудою +A, а двійковий нуль – синусоїдою з амплітудою -A. З умови адитивності виходить, що якщо фази цих амплітуд збігатимуться, то при одночасному передаванні одиниці і нуля отримується нульовий рівень сигналу. Для спрощення запису розширювальної послідовності позначимо синусоїду з додатною амплітудою значенням +1, а синусоїду з від'ємною амплітудою – значенням -1. Для простоти допустимий також, що всі вузли CDMA-мережі синхронізовані.

Таким чином, при передаванні одиниці початкового коду 4 вузли передають в середовище такі послідовності:

A:	-1	-1	-1	-1
B:	-1	+1	-1	+1
C:	-1	-1	+1	+1
D:	-1	+1	+1	-1

При передаванні нуля початкового коду сигнали розширювальної послідовності інвертуються. Нехай тепер кожний з 4 вузлів незалежно від інших передає в мережу один біт початкової інформації: вузол А – 1, вузол В – 0, вузол С – 0, вузол D – 1.

У середовищі S мережі спостерігається така послідовність сигналів:

A: -1 -1 -1 -1
B: +1 -1 +1 -1
C: +1 +1 -1 -1
D: -1 +1 +1 -1

Відповідно до властивості адитивності одержуємо: S: 0 0 0 -4

Якщо, наприклад, деякий вузол Е хоче приймати інформацію від вузла А, то він повинен використовувати свій демодулятор CDMA, задавши йому як параметр значення розширювальної послідовності вузла А.

Демодулятор CDMA працює таким чином. Він послідовно додає всі чотири сумарні сигнали S_j, прийняті протягом кожного такту роботи.

При цьому сигнал S_j прийнятий в такті, на якому код розширення станції А рівний +1, враховується в сумі зі своїм знаком, а сигнал, прийнятий в такті, на якому код розширення станції А рівний -1, додається в суму з протилежним знаком. Іншими словами, демодулятор виконує операцію скалярного множення вектора прийнятих сигналів на вектор значення розширювальної послідовності потрібної станції:

$$S \times A = (0\ 0\ 0\ -4) \times (-1\ -1\ -1\ -1) = 4.$$

Для того, щоб дізнатися, який біт відправила станція А, залишилося нормалізувати результат, тобто розділити його на кількість станцій мережі: 4/4 = 1.

Якби станція була здатна приймати інформацію від станції В, то їй потрібно було б при демодуляції використовувати код розширення станції (-1+1-1+1):

$$S \times B = (0\ 0\ 0\ -4) \times (-1\ +1\ -1\ +1) = -4.$$

Після нормалізації отримується сигнал -1, який відповідає двійковому нулю початкової інформації станції В.

Особливість розширювальних послідовностей, використовуваних в CDMA, полягає в тому, що вони є взаємно ортогональними. Це означає, що якщо їх розглядати як вектори, то при попарному множенні вони дають нульовий результат, наприклад, взаємно ортогональними є вектори координат простору: (1 0 0), (0 1 0) і (0 0 1). Проте крім взаємної ортогональності потрібно, щоб такі вектори були ортогональні з інверсіями членів набору векторів (оскільки інверсії застосовуються для кодування нулів початкової інформації).

На практиці CDMA є вельми складною технологією, яка оперує не умовними значеннями +1 і -1, а модульованими сигналами, наприклад, сигналами BPSK. Крім того, вузли мережі не синхронізовані між собою, а сигнали, які приходять від віддалених на різні відстані від приймача вуз-

лів, мають різну потужність. Проблема синхронізації приймача і передавача вирішується за рахунок передавання довгої послідовності певного коду (пілотним сигналом). Для того ж, щоб потужності всіх передавачів були приблизно рівні для базової станції, в CDMA застосовуються спеціальні процедури керування потужністю.

1.5 Модель OSI

У мережі здійснюється безліч операцій, що забезпечують передавання даних від комп'ютера до комп'ютера. Користувача не цікавить, як саме це відбувається, йому необхідно мати доступ до додатку або комп'ютерного ресурсу, що розташований на іншому комп'ютері мережі. У дійсності вся передана інформація проходить багато етапів обробки.

Насамперед, вона розбивається на блоки, кожний з яких забезпечується керувальною інформацією. Отримані блоки оформляються у вигляді мережевих пакетів, потім ці пакети кодуються, передаються за допомогою електричних або світлових сигналів по мережі відповідно до обраного методу доступу, потім із прийнятих пакетів знову відновлюються поміщені в них блоки даних, блоки з'єднуються в дані і стають доступні іншому додаткові. Це, звичайно, спрощений опис процесів, що відбуваються. Частина з зазначених процедур реалізується тільки програмно, інша частина – апаратно, а якісь операції можуть виконуватися як програмами, так і апаратурою.

Для того, щоб упорядкувати всі виконувані процедури, розділити їх на рівні і підрівні, взаємодіючі між собою, і використовуються моделі мереж. Ці моделі дозволяють правильно організовувати взаємодію як абонентам усередині однієї мережі, так і самим різним мережам на різних рівнях. В даний час найбільшого поширення набула так звана еталонна модель обміну інформацією відкритої системи OSI (Open System Interchange). Під терміном "відкрита система" розуміється незамкнута в собі система, що має можливість взаємодії з іншими системами (на відміну від закритої системи).

1.5.1 Еталонна модель OSI

Модель OSI була запропонована Міжнародною організацією стандартів ISO (International Standards Organization) у 1984 році. З того часу її використовують (більш-менш строго) усі виробники мережевих продуктів. Як і будь-яка універсальна модель, OSI досить громіздка, надлишкова, і не занадто гнучка. Тому реальні мережеві засоби, які пропонуються різними фірмами, не обов'язково дотримуються прийнятого поділу функцій. Однак знайомство з моделлю OSI дозволяє краще зрозуміти, що ж відбувається в мережі.

Усі мережеві функції в моделі розділені на 7 рівнів (рис. 1.8). При цьому вищерозташовані рівні виконують складніші, глобальніші задачі,

для чого використовують у своїх цілях нижчерозташовані рівні, а також керують ними. Ціль нижчерозташованого рівня – надання послуг вищерозташованому рівню, причому вищерозташованому рівню не важливі деталі виконання цих послуг. Нижчерозташовані рівні виконують простіші і конкретніші функції. В ідеалі кожен рівень взаємодіє тільки з тими, котрі знаходяться поруч з ним (вище і нижче нього). Верхній рівень відповідає прикладній задачі, працюючому в даний момент додатку, нижній – безпосередньому передаванню сигналів по каналу зв'язку.

Модель OSI відноситься не тільки до локальних мереж, але і до будь-яких мереж зв'язку між комп'ютерами або іншими абонентами. Зокрема, функції мережі Інтернет також можна поділити на рівні відповідно до моделі OSI. Принципові відмінності локальних мереж від глобальних, з погляду моделі OSI, спостерігаються тільки на нижніх рівнях моделі.

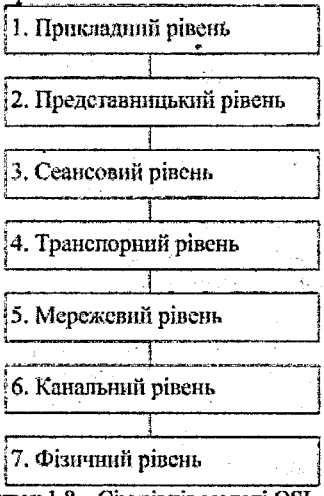

Рисунок 1.8 – Сім рівнів моделі OSI

Функції, що входять в показані на рис. 1.8 рівні, реалізуються кожним абонентом мережі. При цьому кожен рівень для одного абонента працює так, начебто він має прямий зв'язок з відповідним рівнем іншого абонента. Між однойменними рівнями абонентів мережі існує віртуальний (логічний) зв'язок, наприклад, між прикладними рівнями взаємодіючих по мережі абонентів. Реально ж фізичний зв'язок (кабель, радіоканал) абоненти однієї мережі мають тільки на самому нижньому, першому, фізичному рівні. В абонента, що передає, інформація проходить усі рівні, починаючи з верхнього і закінчуючи нижнім. У абонента, що приймає, отримана інформація проходить зворотний шлях: від нижнього рівня до верхнього (рис. 1.9).

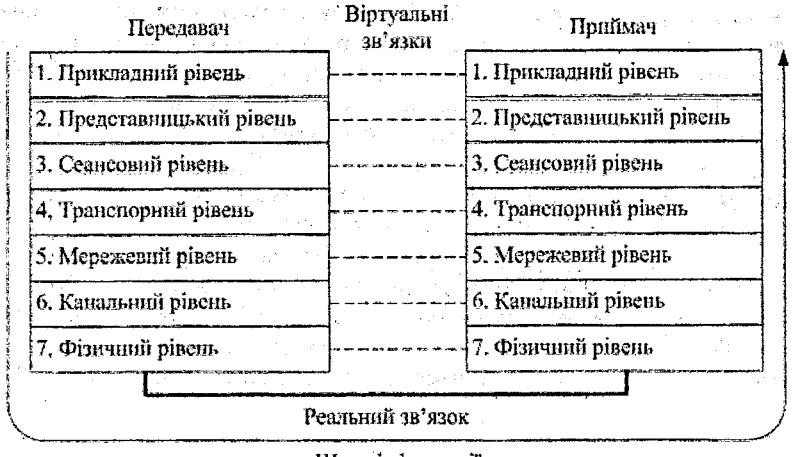

Рисунок 1.9 – Шлях інформації від абонента до абонента

1.5.2 Потоки даних у моделі OSI

Модель OSI надає архітектуру стандартних потоків даних так визначаючи протоколи, що приймальний рівень на комп'ютері-адресаті одержує саме той об'єкт, що був переданий відповідним рівнем на комп'ютері-відправнику.

Передавальний процес посилає дані прикладному рівневі, а той вставляє в них свій заголовок і передає сформований кадр представницькому рівневі. При необхідності представницький рівень може перетворювати дані різними спробами, після чого додає заголовок і передає сеансовому рівневі. Представницькому рівневі не відомо, яка частина даних, отриманих від прикладного рівня, відповідає заголовкові прикладного рівня, а яка частина – власне даним, оскільки це не має ніякого значення для виконання його функцій.

Кожен рівень вставляє свій заголовок, і в кінцевому рахунку кадр потрапляє на канальний рівень, що додає не тільки заголовок, але і кінцеву частину канального рівня (data-link trailer). Останній містить контрольну суму і символи, що доповнюють кадр до потрібного розміру (це допомагає синхронізувати кадри). Далі кадр передається на фізичний рівень, звідки він пересилається приймальному комп'ютерові.

На приймальному комп'ютері від кадру в міру його просування з одного рівня на інший – послідовно відокремлюються заголовки і кінцева частина, і в кінцевому рахунку він потрапляє до процеса-одержувача.

Хоча реальне передавання даних здійснюється вертикально, кожен рівень програмується так, начебто дані передаються горизонтально. Наприклад, транспортний рівень відправника, одержавши повідомлення від сеансового рівня, додає свій заголовок і передає повідомлення транспорт-

ному рівневі одержувача. Той факт, що повідомлення насправді передається через мережевий рівень, для нього не важливий.

Модель OSI не тільки визначає мережеві функції, що закріплюються за кожним рівнем, і ідеальну мережеву архітектуру, але й описує стандартний набір правил, яким повинні відповідати міжмережеві інтерфейси.

Протоколи кожного рівня називаються елементами (entities) і, як правило, реалізуються як процеси. Елементи одного рівня на різних комп'ютерах є рівноправними (peer entities). Так, TCP/IP на своєму транспортному рівні містить два елементи: TCP (Transmission Control Protocol) і UDP (User Datagram Protocol). При цьому рівень n – / завжди реалізує сервиси, використовувані рівнем n.

У випадку сервісів передавання даних OSI визначає термінологію, що використовується для позначення окремих компонентів даних, переданих по інтерфейсу і між рівноправними елементами.

Дані, які необхідно передати по мережі, на шляху від верхнього (сьомого) рівня до нижнього (першого) проходять процес інкапсуляції. Кожен нижчерозташований рівень не тільки виконує оброблення даних, що приходять з вищого рівня, але і постачає їх своїм заголовком, а також службовою інформацією. Такий процес додання службової інформації продовжується до останнього (фізичного) рівня. На фізичному рівні вся ця багатоповерхнева конструкція передається по кабелю приймачеві. Там вона проходить зворотну процедуру декапсуляції, тобто при передаванні на вищерозташований рівень забирається одна з оболонок. Верхнього сьомого рівня досягають дані, звільнені від всіх поверхонь(оболонок), тобто від усієї службової інформації нижчерозташованих рівнів. При цьому кожен рівень приймального абонента виконує оброблення даних, отриманих з нижчерозташованого рівня відповідно до службової інформації, що забирається ним.

Якщо на шляху між абонентами в мережі включаються якісь проміжні пристрої (наприклад, трансівери, репітери, концентратори, комутатори, маршрутизатори), то і вони теж можуть виконувати функції, що входять у нижні рівні моделі OSI. Чим вища складність проміжного пристрою, тим більше рівнів він захоплює. Але будь-який проміжний пристрій повинен приймати і повертати інформацію на нижньому, фізичному рівні. Усі внутрішні перетворення даних повинні виконуватись двічі і у зворотних напрямках (рис. 1.10.). Проміжні мережеві пристрої на відміну від повноцінних абонентів (наприклад, комп'ютерів) працюють тільки на нижніх рівнях і до того ж виконують двостороннє перетворення.

Розглянемо докладніше функції різних рівнів.

• Прикладний (7) рівень (Application Layer) або рівень додатків за безпечує послуги, безпосередньо підтримуючи додатки користувача, наприклад, програмні засоби передавання файлів, доступу до баз даних, засоби електронної пошти, службу реєстрації на сервері. Цей рівень керує всіма іншими шістьма рівнями. Наприклад, якщо користувач працює з електрон-

ними таблицями Excel і вирішує зберегти робочий файл у своїй директорії на мережевому файлі-сервері, то прикладний рівень забезпечує переміщення файлу з робочого комп'ютера на мережевий диск.

Рисунок 1.10 – Включення проміжних пристроїв між абонентами мережі

• Представницький (6) рівень (Presentation Layer) або рівень подання даних визначає і перетворює формати даних і їхній синтаксис у форму, зручну для мережі, тобто виконує функцію перекладача. Тут же виконується шифрування і дешифрування даних, а при необхідності – і їхній стиск. Стандартні формати існують для текстових файлів (ASCII, EBCDIC, HTML), звукових файлів (MIDI, MPEG, WAV), малюнків (JPEG, GIF, TIFF), відео (AVI). Усі перетворення форматів здійснюються на представницькому рівні. Якщо дані передаються у вигляді двійкового коду, то перетворення формату не потрібно.

• Сеансовий (5) рівень (Session Layer) керує проведенням сеансів зв'язку (тобто встановлює, підтримує і припиняє зв'язок). Цей рівень передбачає три режими встановлення сеансів: симплексний (передача даних в одному напрямку), півдуплексний (передача даних по черзі в двох напрямках) і повнодуплексний (передача даних одночасно в двох напрямках). Сеансовий рівень може також вставляти в потік даних спеціальні контрольні точки, що дозволяють контролювати процес передавання при розривi зв'язку. Цей рівень розпізнає логічні імена абонентів, контролює надані їм права доступу.

• Транспортний (4) рівень (Transport Layer) забезпечує доставку пакетів без помилок і втрат, а також у потрібній послідовності. Тут здійснюється розбиття на блоки переданих даних, що поміщаються в пакети, і відновлення прийнятих даних з пакетів. Доставка пакетів можлива як із установленням з'єднання (віртуального каналу), так і без цього. Транспорт-

ний рівень є прикордонним і сполучним між верхніми трьома, які залежать від додатків, і трьох нижніх рівнів, які "прив'язані" до конкретної мережі.

• Мережевий (3) рівень (Network Layer) відповідає за адресацію пакетів і переклад логічних імен (логічних адрес, наприклад, IP-адрес або IPX-адрес) у фізичні мережеві MAC-адреси (і навпаки). На цьому ж рівні розв'язується задача вибору маршруту (шляху), по якому пакет доставляється за призначенням (якщо в мережі є кілька маршрутів). На мережевому рівні працюють такі складні проміжні мережеві пристрої як маршрутизатори.

• Канальний (2) рівень або рівень керування лінією передачі (Data link Layer) відповідає за формування пакетів (кадрів) стандартного для даної мережі (Ethernet, Token-Ring, FDDI) виду, що включають початкове і кінцеве керувальні поля. Тут же здійснюється керування доступом до мережі, виявляються помилки передавання шляхом підрахунку контрольних сум, і здійснюється повторне пересилання приймачеві помилкових пакетів. Канальний рівень поділяється на два підрівні: верхній LLC і нижній MAC.

• Фізичний (1) рівень (Physical Layer) – це найнижчий рівень моделі, що відповідає за кодування переданої інформації в рівні сигналів, прийнятих у середовищі передавання, що використовується, і зворотне декодування. Тут же визначаються вимоги до з'єднувачів, роз'ємів, електричного узгодження, заземлення, захисту від завад і т.д. На фізичному рівні працюють такі мережеві пристрої, як трансівери, репітери і репітерні концентратори.

Більшість функцій двох нижніх рівнів моделі (1 і 2) звичайно реалізуються апаратно (частина функцій рівня 2 – програмним драйвером мережевого адаптера). Саме на цих рівнях визначається швидкість передавання і топологія мережі, метод управління обміном і формат пакета, тобто те, що має безпосереднє відношення до типу мережі, наприклад, Ethernet, Token-Ring, FDDI, 100VG-AnyLAN. Вищі рівні, як правило, не працюють безпосередньо з конкретною апаратурою, хоча рівні 3, 4 і 5 ще можуть враховувати її особливості. Рівні 6 і 7 ніяк не пов'язані з апаратурою, заміни одного типу апаратури на інший вони не помічають.

Контрольні питання до розділу 1

1. Перелічити основні ознаки мережі.
2. Види топології мережі.
3. Порівняти переваги та недоліки мережевих топологій.
4. Основні характеристики бездротових мереж.
5. Принципи поширення електромагнітних хвиль.
6. Основні види бездротових систем.
7. Методи передавання широкосмугового сигналу.
8. Еталонна модель OSI.
9. Призначення кожного з рівнів моделі OSI.

Розділ 2
АПАРАТУРА МЕРЕЖ

Апаратура мереж забезпечує реальний зв'язок між абонентами. Вибір апаратури має найважливіше значення на етапі проектування мережі, тому що вартість апаратури складає найбільшу частину від вартості мережі в цілому, а заміна апаратури пов'язана не тільки з додатковими витратами, але найчастіше і з трудомісткою роботою. До апаратури локальних мереж відносяться:

- кабелі для передачі інформації;
- роз'єми для приєднання кабелів;
- погоджувальні термінатори;
- мережеві адаптери;
- повторювачі;
- трансівери;
- концентратори;
- мости;
- маршрутизатори;
- шлюзи.

2.1 Кабелі

Кабелі є найпоширенішим фізичним середовищем передавання інформації в мережах. Використовуються кілька типів кабелів. Вони відрізняються товщиною, швидкістю передавання даних, складністю установки, ціною й т.д. У різних ситуаціях можуть знадобитися різні типи кабелів. При виборі конкретного кабелю для даної мережі варто враховувати необхідний тип кабелю й додатки, які будуть функціонувати в створюваній мережі. Вимоги існуючих додатків можна звести в п'ять класів:

- клас А. Передавання голосу й низькошвидкісне передавання даних у діапазоні частот до 100 КГц;
- клас В. Передавання даних у діапазоні до 1 МГц;
- клас С. Передавання даних з високою швидкістю – до 16 МГц;
- клас D. Передавання даних з надвисокою швидкістю – до 100 МГц.

Оптичний. Оптичний кабель використовується, як правило, для передавання даних з високою й надвисокою швидкістю; можна вважати, що ширина смуги практично необмежена.

Аналіз роботи локальних мереж показує, що більша частка виникаючих збоїв і відмов припадає на кабельні системи. Згідно з даними, що наводяться багатьма фахівцями, через ушкодження кабелів відбувається приблизно 70 % аварій у мережах. У цьому зв'язку питанням прокладання кабелю, вибору типу кабелю, тестування, керування кабельною системою й т.д. варто приділяти (і приділяється) надзвичайно велику увагу.

2.1.1 Кручена пара

Зазвичай кручена пара використовувалася в телефонних лініях. У такому кабелі звичайно використовуються декілька пар ізольованих проводів, скручених один із одним. Взаємне скручення забезпечує захист від власних і зовнішніх наведень. Кабель із крученою парою буває двох типів: неекранованим і екранованим. Стандарт EIA/TIA 568 Commercial Building Wiring Standard (стандарт проводки в офісах) визначив п'ять категорій кабелів на неекранованій крученій парі (Unshielded Twisted Pair, UTP).

Кабель UTP 1 не підтримує передавання цифрових даних.

Кабель UTP 2 застарів; він підтримує швидкість передавання до 4 Мбіт/с.

Кабель UTP 3 здатний підтримувати швидкість передавання до 10 Мбіт/с і відповідає лише мінімальним вимогам до середовища передавання. Ця категорія відповідає класу С.

Кабель UTP 4 не набагато випереджає кабель категорії 3 по швидкості передавання. Він здатний передавати дані зі швидкістю 16 Мбіт/с. Цей кабель був розроблений для стандарту IEEE 802.5.

Більш сучасним є кабель UTP 5, що відповідає класу D. Він здатний працювати зі швидкістю 100 Мбіт/с. Цей кабель був розроблений для мереж IEEE 802.5 і TPFDDI (специфікація мережі FDDI на електричному кабелі),

Згідно зі стандартом хвильовий опір кабелів UTP 4 і 5 повинен становити 100 Ом у діапазоні частот від 1 МГц до граничної. Для кабелю UTP 5 встановлене мінімальне число взаємних скручувань на одиницю довжини (8 на 1 фут, або, приблизно, 26 на 1 м).

З'єднання кабелю з адаптером і концентратором виконується за допомогою 8-контактних з'єднувачів RJ-45. До переваг кабелю на крученій парі відносять його дешевину й простоту установлення. Його недоліками є: взаємне накладення сигналів між суміжними проводами (crosstalk), чутливість до зовнішніх електромагнітних полів, можливість несанкціонованого перехоплення інформації, більший ступінь загасання сигналу по шляху, ніж у кабелів інших типів.

Об'єднання комп'ютерів у мережу зі специфікацією 100BASE-TX практично нічим не відрізняється від схеми 10BASE-T. Використовуються 8-контактні рознімання RJ-45 і дві виті пари в кабелі, але різних категорій (5 і 3). Довжина сегмента мережі на такому кабелі не може перевищувати 100 м.

Топологія "пасивна зірка" вимагає обов'язкового використання концентратора. Між адаптерами й мережевими кабелями можуть бути підключені трансівери. При підвищенні якості кабелю для специфікації 10BASE-T може бути збільшена його гранична довжина. У специфікації 100BASE-TX гранична довжина визначається подвійним часом проходження сигналу й із цієї причини не може бути збільшена. Для специфікації 100BASE-T4, що використовує чотири кручені пари, вимоги до кабелю

трохи знижені. Можуть бути використані UTP 3, 4 або 5. Обмін даними проводиться по одній передавальній парі, по одній приймаючій парі й по двох двонаправлених парах.

Підвищення швидкостей передавання даних висуває нові, жорсткіші вимоги до сучасної кабельної інфраструктури. Із цієї причини неекранована кручена пара категорії 5 у цей час є найпоширенішим типом кабелів. Цей кабель добре підходить для технології Fast Ethernet.

У зв'язку зі збільшенням швидкості передачі до гігабітної робоча група по Gigabit Ethernet інституту IEEE розробляє спеціальну версію зазначеного стандарту для кабелів UTP 5.

Кабелі UTP 5 традиційно містять чотири пари проводів, з яких у мережах Ethernet і Fast Ethernet використовуються тільки дві. У зв'язку з тим, що в мережах Gigabit Ethernet і ATM зі швидкістю передачі 622 Мбіт/с і вище задіються всі чотири пари, зростає інтенсивність перехресних завад. Зараз зусилля багатьох організацій спрямовані саме на їхнє ослаблення. Є "розширений" варіант кабельної системи категорії 5.

2.1.1.1 Екранована і неекранована кручена пара

Крученою парою називається скручена пара дротів. Цей вид середовища передавання даних дуже популярний і складає основу великої кількості як внутрішніх, так і зовнішніх кабелів. Кабель може складатися з декількох кручених пар (зовнішні кабелі іноді містять до декількох десятків таких пар).

Скручування дротів знижує вплив зовнішніх і взаємних перешкод на корисні сигнали, що передаються по кабелю. Основні особливості конструкції кабелів схематично показані на рис. 2.1.

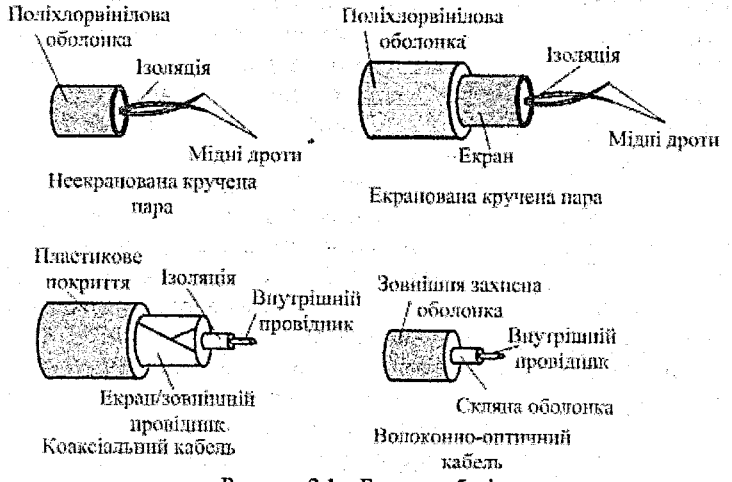

Рисунок 2.1 – Будова кабелів

Кабелі на основі крученої пари є симетричними, тобто вони складаються з двох однакових в конструктивному відношенні провідників. Симетричний кабель на основі крученої пари може бути як екранованим, так і неекранованим.

Потрібно відрізняти електричну ізоляцію провідних жил, яка є в будь-якому кабелі, від електромагнітної ізоляції. Перша складається з непровідного діелектричного шару – паперу або полімеру, наприклад хлориду полівінілу або полістиролу. У другому випадку крім електричної ізоляції провідні жили розміщуються також всередину електромагнітного екрану із провідного мідного обплетення.

Кабель на основі неекранованої крученої пари використовується для проводки усередині будівлі, класифікується в міжнародних стандартах на категорії (від 1 до 7).

Кабелі категорії 1 застосовуються там, де вимоги до швидкості передавання мінімальні. Зазвичай це кабель для цифрового і аналогового передавання голосу і низькошвидкісного (до 20 Кбіт/с) передавання даних. До 1983 року це був основний тип кабелю для телефонного розведення.

Кабелі категорії 2 були вперше застосовані фірмою IBM при побудові власної кабельної системи. Головна вимога до кабелів цієї категорії – здатність передавати сигнали із спектром до 1 МГц.

Кабелі категорії 3 були стандартизовані в 1991 році. Стандарт EIA-568 визначив електричні характеристики кабелів для частот в діапазоні до 16 МГц. Кабелі категорії 3, призначені як для передавання даних, так і для передавання голосу, складають зараз основу багатьох кабельних систем будівель.

Кабелі категорії 4 є дещо покращеним варіантом кабелів категорії 3. Кабелі категорії 4 зобов'язані витримувати тести на частоті передавання сигналу 20 МГц і забезпечувати підвищену завадостійкість і низькі втрати сигналу. На практиці використовуються рідко.

Кабелі категорії 5 були спеціально розроблені для підтримки високошвидкісних протоколів. Їх характеристики визначаються в діапазоні до 100 МГц. Більшість високошвидкісних технологій (FDDI, Fast Ethernet, ATM і Gigabit Ethernet) орієнтуються на використання крученої пари категорії 5. Кабель категорії 5 прийшов на заміну кабелю категорії 3, і сьогодні все нові кабельні системи будуються саме на цьому типі кабелю (у поєднанні з волоконно-оптичним).

Особливе місце займають кабелі категорій 6 і 7. Для кабелю категорії 6 характеристики визначаються до частоти 250 МГц, а для кабелів категорії 7 – до 600 МГц. Кабелі категорії 7 обов'язково екрануються, причому як кожна пара, так і весь кабель в цілому. Кабель категорії 6 може бути як екранованим, так і неекранованим. Основне призначення цих кабелів – підтримка високошвидкісних протоколів на відрізках кабелю більшої довжини, ніж кабель UTP категорії 5.

Всі кабелі UTP незалежно від їх категорії випускаються в 4-парному виконанні. Кожна з чотирьох пар кабелю має певний колір і крок скручування. Зазвичай дві пари призначені для передавання даних, а дві – для передавання голосу.

Екранована кручена пара добре захищає сигнали від зовнішніх перешкод, а також менше випромінює електромагнітні коливання назовні, що, у свою чергу, захищає користувачів мереж від шкідливого для здоров'я випромінювання. Наявність екрану, що заземляється, здорожує кабель і ускладнює його прокладання.

Основним стандартом, що визначає параметри екранованої крученої пари для застосування усередині будівель, є фірмовий стандарт IBM. У цьому стандарті кабелі діляться не на категорії, а на типи від 1 до 9 включно.

Розглянемо для прикладу кабель типу 1 стандарту IBM. Він складається з двох пар скручених дротів, екранованих проводовим обплетенням, яке заземляється. Електричні параметри кабелю типу 1 приблизно відповідають параметрам кабелю UTP категорії 5. Проте хвилевий опір кабелю типу 1, рівний 150 Ом, значно більший хвилевого опору UTP категорії 5 (100 Ом), тому неможливе "поліпшення" кабельної проводки мережі шляхом простої заміни неекранованої пари екранованою парою типу 1. Передавачі, розраховані на роботу з кабелем, що має хвилевий опір 100 Ом, погано працюватимуть на хвилевому опорі 150 Ом.

2.1.2 Коаксіальний кабель

Найпершим знайшов застосування в мережах коаксіальний кабель (або, як його іноді називають, просто коаксіал). Такий кабель здатний передавати дані зі швидкістю 10 Мбіт/с на відстань до 500 м. Основними типами коаксіальних кабелів для ЛВМ є "товстий" Ethernet (Thick Ethernet, Thicknet) і "тонкий" Ethernet (Thin Ethernet, Thinnet).

Кабель "тонкого" Ethernet маркується як RG-58 і найбільше поширений. Товщина цього кабелю дорівнює 6 міліметрам. Для з'єднання комп'ютерів у мережі на базі коаксіального кабелю застосовуються Т-конектори або циліндричні з'єднувачі типу BNC (British Naval Connector) і п'ятидесятиомні заглушки (термінатори, Terminator). Заглушки встановлюють на обох кінцях мережевого сегмента. Мінімальна відстань між абонентами повинна бути не менша півметра. Трансіверний кабель не потрібний. У цьому випадку Т-конектори вставляються безпосередньо в BNC-роз'ємів мережевого адаптера. При реалізації мережі на тонкому кабелі можна зробити максимум 5 сегментів по 185 м, тобто максимальна довжина може скласти 925 м. Зменшуючи довжину сегмента, можна підключити більше комп'ютерів, але при цьому загальне число комп'ютерів не повинно перевищувати 150.

"Товстий" Ethernet використовує більш товстий і дорогий кабель. Він застосовується як основа специфікації 10BASE5. Такі кабелі маркуються як

RJ-8 або RJ-11. Товщина кабелю становить близько 12 міліметрів. Для приєднання мережевого адаптера до основного кабелю використовується трансіверний кабель і трансівер AUI (Attachment Unit Interface, інтерфейсний пристрій з'єднання). Трансіверний кабель має декілька провідників і може мати довжину до 50 м у звичайному виконанні (до 12,5 м у так званому офісному варіанті). "Товстий" Ethernet забезпечує надійне передавання даних на відстань до 500 м. До його недоліків можна віднести складність установки (що пов'язана з його товщиною й твердістю) і більшу вартість.

2.1.3 Оптоволоконний кабель

Оптоволоконний кабель складається з вільно покладених або певним чином скручених волоконних світловодів і захисного покриття. Передавання даних виконується за допомогою лазерного або світловодного передавача, що генерує світлові імпульси, що проходять через світловоди. Перед тим як потрапити у світловод, сигнал від передавача (випромінювача) проходить через оптичний погоджувальний пристрій і через оптичний рознімний з'єднувач (конектор). На приймальному кінці сигнал сприймається фотодіодом, що перетворить його в електричний струм. Оптоволоконний кабель має ряд переваг. До них можна віднести:

- мале загасання й незалежність загасання від частоти переданого сигналу;
- високий ступінь захисту від зовнішніх електромагнітних полів;
- виключення несанкціонованого доступу до даних;
- малу вартість і постійну тенденцію до її зниження.

Основний недолік проявляється при установленні мережі на такому кабелі. Потрібно дороге устаткування й висока кваліфікація персоналу.

Залежно від умов поширення світлової хвилі в центральному світловоді, оптичні кабелі діляться на одномодові (single mode – SM) і багатомодові (multi mode – MM).

Схема підключення пристроїв для специфікації 100BASE-FX дуже схожа на схему 10BASE-FL. В обох цих специфікаціях використовується топологія "пасивна зірка". Комп'ютери підключаються до концентратора за допомогою двох оптоволоконних кабелів (один відповідає за прийом, інший – за передавання). Між адаптером і мережевим кабелем можливе включення трансівера. Максимальна довжина кабелю (412 м) визначається тимчасовими параметрами. Застосування оптоволоконного кабелю дозволяє значно збільшити довжину сегмента й підвищити ступінь захисту мережі.

2.2 Адаптери

Мережеві адаптери (вони ж контролери, карти, плати, інтерфейси, NIC – Network Interface Card) – це основна частина апаратури локальної мережі. Призначення мережевого адаптера – сполучення комп'ютера (або

іншого абонента) з мережею, тобто забезпечення обміну інформацією між комп'ютером і каналом зв'язку відповідно до прийнятих правил обміну. Саме вони реалізують функції двох нижніх рівнів моделі OSI.

Функції мережевого адаптера поділяються на магістральні і мережеві. До магістральних відносяться ті функції, що здійснюють взаємодію адаптера з магістраллю (системною шиною) комп'ютера (тобто розпізнання своєї магістральної адреси, пересилання даних у комп'ютер і з комп'ютера, створення сигналу переривання комп'ютера і т.д.). Мережеві функції забезпечують спілкування адаптера з мережею.

До основних мережевих функцій адаптерів відносяться:

- гальванічна розв'язка комп'ютера і кабелю локальної мережі (для цього звичайно використовується передача сигналів через імпульсні трансформатори);
- перетворення логічних сигналів у мережеві (електричні або світлові) і навпаки;
- кодування і декодування мережевих сигналів, тобто пряме і обернене перетворення мережевих кодів передавання інформації (наприклад, манчестерський код);
- розпізнання прийнятих пакетів (вибір із усіх пакетів, що надійшли, тих, котрі адресовані даному абонентові або всім абонентам мережі одночасно);
- перетворення рівнобіжного коду в послідовний при передаванні і обернене перетворення при прийомі;
- буферизація переданої і прийнятої інформації в буферній пам'яті адаптера;
- організація доступу до мережі відповідно до прийнятого методу керування обміном;
- підрахунок контрольної суми пакетів при передачі і прийомі.

Типовий алгоритм взаємодії комп'ютера з мережевим адаптером виглядає таким чином.

Якщо комп'ютер хоче передати пакет, то він спочатку формує цей пакет у своїй пам'яті, потім пересилає його в буферну пам'ять мережевого адаптера і дає команду адаптерові на передавання. Адаптер аналізує поточний стан мережі і з першою ж нагодою видає пакет у мережу (виконує керування доступом до мережі). При цьому він виконує перетворення інформації з буферної пам'яті в послідовний вид для побітового передавання по мережі, підраховує контрольну суму, кодує біти пакета в мережевий код і через вузол гальванічної розв'язки видає пакет у кабель мережі. Буферна пам'ять у даному випадку дозволяє звільнити комп'ютер від контролю стану мережі, а також забезпечити необхідний для мережі темп видачі інформації.

Якщо по мережі приходить пакет, то мережевий адаптер через вузол гальванічної розв'язки приймає біти пакета, виконує їхнє декодування з

мережевого коду і порівнює мережеву адресу приймача з пакета із своєю власною адресою. Адреса мережевого адаптера, як правило, встановлюється виробником адаптера. Якщо адреси збігаються, то мережевий адаптер записує пакет, що прийшов, у свою буферну пам'ять і повідомляє комп'ютеру (звичайно – сигналом апаратного переривання) про те, що прийшов пакет і його потрібно прочитати. Одночасно з записуванням пакета здійснюється підрахунок контрольної суми, що дозволяє до кінця прийому зробити висновок, чи є помилки в цьому пакеті. Буферна пам'ять у даному випадку знову ж дозволяє звільнити комп'ютер від контролю мережі, а також забезпечити високий ступінь готовності мережевого адаптера до приймання пакетів.

Найчастіше мережеві функції виконуються спеціальними мікросхемами високого ступеня інтеграції, що дає можливість знизити вартість адаптера і зменшити площу його плати.

Деякі адаптери дозволяють реалізувати функцію віддаленого завантаження, тобто підтримувати роботу в мережі бездискових комп'ютерів, що завантажують свою операційну систему прямо з мережі. Для цього до складу таких адаптерів включається постійна пам'ять з відповідною програмою завантаження. Правда, не всі мережеві програмні засоби підтримують даний режим роботи. Мережевий адаптер виконує функції першого і другого рівнів моделі OSI.

Всі інші апаратні засоби локальних мереж (крім адаптерів) мають допоміжний характер, і без них часто можна обійтися. Це мережеві проміжні пристрої.

2.3. Трансівери та повторювачі

Трансівери або прийомопередавачі (від англійського TRANsmitter + reCEIVER) служать для передачі інформації між адаптером і кабелем мережі або між двома сегментами (частинами) мережі. Трансівери підсилюють сигнали, перетворюють їхні рівні або перетворюють сигнали в іншу форму (наприклад, з електричної у світлову і навпаки). Трансіверами також часто називають вбудовані в адаптер прийомопередавачі.

Репітери або повторювачі (repeater) виконують простішу функцію, ніж трансівери. Вони не перетворюють ні рівні сигналів, ні їхню фізичну природу, а тільки відновлюють ослаблені сигнали (їхню амплітуду і форму), приводячи їх до вихідного вигляду. Ціль такої ретрансляції сигналів полягає винятково в збільшенні довжини мережі (рис. 2.2).

Однак часто репітери виконують і деякі інші, допоміжні функції, наприклад, гальванічну розв'язку сегментів, що з'єднуються, і кінцеве узгодження. Репітери так само як і трансівери не виконують ніякого інформаційного оброблення сигналів, що проходять через них.

Рисунок 2.2 – З'єднання репітером двох сегментів мережі

2.4 Концентратори

Концентратори (хаби, hub), як випливає з їхньої назви, служать для об'єднання в мережу декількох сегментів. Концентратори (або репітерні концентратори) являють собою декілька зібраних в одному конструктиві репітерів, вони виконують ті ж функції, що і репітери (рис. 2.3).

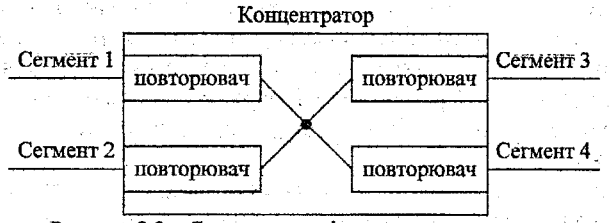

Рисунок 2.3 – Структура репітерного концентратора

Перевага подібних концентраторів порівняно з окремими репітерами в тому, що всі точки підключення зібрані в одному місці, це спрощує реконфігурацію мережі, контроль і пошук несправностей. До того ж всі репітери в даному випадку живляться від одного якісного джерела живлення.

Концентратори іноді втручаються в обмін, допомагаючи усувати деякі очевидні помилки обміну. У будь-якому випадку вони працюють на першому рівні моделі OSI, тому що мають справу тільки з фізичними сигналами, з бітами пакета і не аналізують вміст пакета, розглядаючи пакет як єдине ціле. На першому ж рівні працюють і трансівери, і репітери.

У мережах знайшли застосування топології різних типів. Поряд із поширеною "шиною" застосовуються топології "пасивна зірка" і "дерево". Всі типи топологій можуть використовувати повторювачі й пасивні концентратори для об'єднання різних сегментів мережі. Основна вимога до даних топологій – відсутність петель (замкнутих контурів).

Для підключення до мережі віддалених груп можуть бути використані концентратори з додатковим волоконно-оптичним портом. Існують три різновиди реалізації такого порту: такий, що вставляє в гніздо розширення slide-in-мікротрансівер, що вставляє в гніздо роз'єму AUI навісний мікро-

трансівер і постійний оптичний порт. Оптичні концентратори застосовуються як центральний пристрій розподіленої мережі з більшою кількістю окремих вилучених робочих станцій і невеликих робочих груп. Порти такого концентратора виконують функції підсилювачів і здійснюють повну регенерацію пакетів. Існують концентратори з фіксованою кількістю сегментів, що підключаються, але деякі типи концентраторів мають модульну конструкцію, що дозволяє гнучко підлаштовуватися до існуючих умов. Найчастіше концентратори й повторювачі є автономними блоками з окремим живленням.

Для технології Fast Ethernet визначені два класи концентраторів.

Концентратори першого класу перетворюють надані із сегментів сигнали в цифрову форму і тільки після цього передають їх в усі інші сегменти. Це дозволяє підключати до таких концентраторів сегменти, виконані за різними специфікаціями: 100BASE-TX, 100BASE-T4 або 100BASE-FX.

Концентратори другого класу виконують просте повторення сигналів без перетворення. До такого концентратора можна підключати сегменти тільки одного типу.

2.5 Комутатори

Комутатори (комутувальні концентратори, switch), як і концентратори, служать для з'єднання сегментів у мережу. Вони також виконують складніші функції, здійснюючи сортування пакетів, що надходять.

Комутатори передають з одного сегмента мережі в інший не всі пакети, що надходять на них, а тільки ті, котрі адресовані комп'ютерам з іншого сегмента. Пакети, передані між абонентами одного сегмента, через комутатор не проходять. При цьому сам пакет комутатором не приймається, а тільки пересилається. Інтенсивність обміну в мережі знижується внаслідок поділу навантаження, оскільки кожен сегмент працює не тільки зі своїми пакетами, але і з пакетами, що прийшли з інших сегментів.

Комутатор працює на другому рівні моделі OSI (підрівень MAC), тому що аналізує MAC-адресу всередині пакета. Очевидно, що він виконує і функції першого рівня.

Популярність комутаторів обумовлена насамперед тим, що вони дозволяють за рахунок сегментації підвищити продуктивність мережі. Крім поділу мережі на дрібні сегменти, комутатори дають можливість створювати логічні мережі й легко перегруповувати пристрої в них. Іншими словами, комутатори дозволяють створювати віртуальні мережі.

Уперше комутатори з'явилися наприкінці 80-х років. Перші комутатори використовувалися для перерозподілення пропускної здатності й, відповідно, підвищення продуктивності мережі. Можна сказати, що комутатори спочатку застосовувалися винятково для сегментації мережі. У наш

час відбулася переорієнтація, і тепер у більшості випадків комутатори використовуються для прямого підключення до кінцевих станцій.

Загальний термін "комутація" застосовується для чотирьох різних технологій:

- конфігураційної комутації;
- комутації кадрів;
- комутації комірок;
- перетворення між кадрами й комірками.

В основі конфігураційної комутації лежить знаходження відповідності між конкретним портом комутатора й певним сегментом мережі. Ця відповідність може програмно налаштовуватися при підключенні або переміщенні користувачів у мережі.

При комутації кадрів використовуються стандартні формати кадрів мереж Ethernet, Token Ring і т.д. Кадр при надходженні в мережу обробляється першим комутатором на його шляху. Під терміном обробка розуміється вся сукупність дій, вироблених комутатором для визначення свого вихідного порту, на який необхідно направити даний кадр. Після оброблення він передається далі по мережі наступному комутатору або безпосередньо одержувачеві.

В технології ATM також застосовується комутація, але в ній одиниці комутації звуться комірками. Перетворення між кадрами й комірками дозволяє станціям у мережі Ethernet, Token Ring і т.д. безпосередньо взаємодіяти із пристроями ATM. Ця технологія застосовується при емуляції локальної мережі.

Комутатори поділяються на чотири категорії.

1. Прості автономні комутатори мереж робочих груп дозволяють деяким мережевим пристроям або сегментам обмінюватися інформацією з максимальною для даної кабельної системи швидкістю. Вони можуть виконувати роль мостів для зв'язку з іншими мережевими сегментами, але не транслюють протоколи й не забезпечують підвищеної пропускної здатності із окремими виділеними пристроями, такими як сервери.

2. Комутатори робочих груп другої категорії забезпечують високошвидкісний зв'язок одного або декількох портів із сервером або базовою мережею.

3. Третю категорію становлять комутатори мережі відділу підприємства, які часто використовуються для взаємодії мереж робочих груп. Вони надають більш широкі можливості адміністрування й підвищення продуктивності мережі. Такі пристрої підтримують деревоподібну архітектуру зв'язків, що використовується для передавання інформації з резервних каналів і фільтрації пакетів. Фізично такі комутатори підтримують резервні джерела живлення й дозволяють оперативно змінювати модулі.

4. Остання категорія – це комутатори мережі масштабу підприємства, що виконують диспетчеризацію трафіка, визначаючи найефективніший

маршрут. Вони можуть підтримувати велику кількість логічних з'єднань локальної мережі. Багато виробників корпоративних комутаторів пропонують у складі своїх виробів модулі АТМ. Ці комутатори здійснюють трансляцію протоколів Ethernet у протоколи АТМ.

Технологія конфігураційної комутації сегментів Ethernet була запропонована фірмою Kalpana в 1990 році. Ця технологія заснована на відмові від використання поділюваних ліній зв'язку між всіма вузлами сегмента й застосуванні комутаторів, що дозволяють передавати пакети одночасно між всіма парами портів. Нововведення полягало в паралельному обробленні кадрів, що надходять.

Найчастіше використовуються три типи функціональної структури комутаторів:

- з комутаційною матрицею;
- із загальною шиною;
- з поділюваною багатовходовою пам'яттю.

Комутатори з комунікаційною матрицею за рахунок паралельного оброблення здійснюють взаємодію портів швидше. Однак число портів у таких комутаторах обмежене, тому що складність реалізації комутатора зростає пропорційно квадрату числа портів.

Якщо комутатору необхідно передати кадр із порту 1 у порт 5, будуть відбуватись такі дії. Процесор комутатора дає команду комутаційній матриці на установлення шляху, що зв'язує ці два порти. Комутаційна матриця може це зробити тільки в тому випадку, коли вихідний порт 5 у цей момент вільний. Якщо він зайнятий, кадр буферизується процесором порту 1, після чого процесор комутатора очікує звільнення порту 5 і утворення комутаційною матрицею потрібного шляху. Після встановлення комутаційного шляху по ньому направляються буферизовані портом 1 кадри, які після одержання доступу до середовища передаються в мережу через порт 5.

Ситуація, коли вихідний порт зайнятий, зустрічається досить часто – вона називається колізією вихідного порту. У більшості комутаторів передбачене реагування на колізію вихідного порту. Щоб уберегти дані від втрати, у комутаторах передбачена буферна область пам'яті, де й зберігаються вже прийняті кадри. Буферна пам'ять здатна згладжувати випадкові сплески трафіка, не допускаючи втрати інформації. На думку виробників комутаторів, кращою схемою буферизації є буферизація на вхідному порту. При буферизації на вході дані можуть надходити в комутатор практично з будь-якою швидкістю. Як тільки з'являється можливість відправити дані в порт призначення, комутатор бере їх з буфера й пересилає.

Велика буферна пам'ять може призводити до деякої затримки передавання. Це входить у суперечність із основною метою комутаторів, тому що вони застосовуються саме для усунення уповільнення. Для вирішення цього протиріччя комутатори для локальних мереж і мереж АТМ мають буфери різних розмірів. У технології АТМ комутатори утворюють магістраль із

обмеженою смугою пропускання. У комутаторах АТМ часто встановлюється більша буферна пам'ять. Для комутаторів у локальних мережах, особливо на рівні робочих груп, можна підібрати досить швидкий віртуальний носій, що не дозволить виникати заторам, тому буфери комутаторів для локальних мереж часто невеликі за розмірами.

У комутаторах із загальною шиною використовується високошвидкісна шина, призначена для зв'язку процесорів портів. Зв'язок портів через шину здійснюється в режимі поділу часу. У цьому випадку високошвидкісна шина відіграє пасивну роль. Активними є спеціалізовані процесори портів. Для того щоб шина не була вузьким місцем комутатора, її продуктивність повинна бути в кілька разів вищою швидкості надходження даних на вхідні порти. Для зменшення затримок при передаванні кадр повинен передаватися по шині невеликими частинами. Розмір цих частин визначається виробником комутатора. Шина, так само як і комутаційна матриця, не може здійснювати проміжну буферизацію.

Третій тип комутаторів – комутатори з поділюваною багатовходовою пам'яттю.

Виробники комутаторів застосовують у своїх виробах різні алгоритми керування потоком кадрів для запобігання втрат кадрів при перевантаженнях у мережі. Втрата навіть невеликої кількості кадрів звичайно різко знижує корисну продуктивність мережі. Тому при виникненні перевантаження розумно було б знизити інтенсивність надходження кадрів від кінцевих вузлів до комутатора. Для уповільнення потоку в розпорядженні комутатора повинен бути механізм зниження інтенсивності трафіка підключених до його портів вузлів. Існують два таких механізми:

- агресивна поведінка порту;
- метод зворотного тиску.

Порт комутатора для захоплення середовища повинен "поводитися агресивно" і при передаванні, і при колізії в мережі (для мережі Ethernet).

У першому випадку комутатор закінчує передавання чергового кадру й робить технологічну паузу в 9,1 мкс замість покладеної паузи в 9,6 мкс. При цьому комп'ютер, витримавши паузу в 9,6 мкс, не може захопити середовище передавання даних. Після колізії, коли кадри комутатора й комп'ютера зіштовхуються, комп'ютер робить стандартну паузу в 51,2 мкс, а комутатор – в 50 мкс. І в цьому випадку середовище передавання залишається за комутатором.

В основі другого методу – методу зворотного тиску – лежить передавання фіктивних кадрів комп'ютеру при відсутності в буфері комутатора кадрів для передавання через даний порт. У цьому випадку комутатор може не порушувати алгоритм доступу, однак інтенсивність передавання кадрів у комутатор у середньому зменшується вдвічі. Метод зворотного тиску використовується або для розвантаження загального буфера, або для роз-

вантаження буфера процесора іншого порту, у який передає свої кадри даний порт.

2.5.1 Додаткові функції комутаторів

Комутатор – це складний пристрій, що має один або кілька процесорних модулів і, природно, може виконувати, крім основного завдання із передавання кадрів з порту на порт, деякі додаткові функції. До них відносяться:

- трансляція протоколів канального рівня;
- підтримка протоколу Spanning Tree;
- фільтрація кадрів;
- використання різних класів сервісу;
- підтримка віртуальних мереж.

Комутатори можуть виконувати трансляцію одного протоколу канального рівня в інший, наприклад, Ethernet в FDDI, Fast Ethernet в Token Ring і т.д. При цьому вони працюють за тим самим алгоритмом, що й мости, які транслюють, тобто згідно зі специфікаціями перетворення полів кадрів різних протоколів (RFC 1042, IEEE 802.1H).

Багато комутаторів поряд зі стандартною фільтрацією відповідно до адресної таблиці дозволяють адміністраторам задавати додаткові умови фільтрації кадрів. Користувацькі фільтри призначені для створення додаткових "бар'єрів", які обмежують доступ певних користувачів до деяких сервісів мережі.

Використання класів сервісу дозволяє адміністраторові призначити різним типам кадрів пріоритети їхнього оброблення. При цьому комутатор підтримує кілька черг неопрацьованих кадрів, а самі черги можуть мати різні пріоритети. Оскільки не всі протоколи канального рівня підтримують механізм визначення пріоритету кадру, розроблено метод приписування пріоритетів портам комутатора. При такому підході комутатор поміщає кадр у чергу з певним пріоритетом залежно від того, через який порт надійшов цей кадр. Більш гнучким є призначення пріоритетів Мас-адресам вузлів.

Комутатор дозволяє локалізувати потоки інформації в мережі й керувати ними, тобто створювати й підтримувати особливі умови фільтрації. Одним з дуже популярних видів спеціальних фільтрів є фільтри, що створюють віртуальні мережі. Віртуальною мережею (у цьому контексті) називається група вузлів у мережі, трафік якої, у тому числі й широкомовний, повністю ізольований від інших вузлів мережі.

Всередині віртуальної мережі кадри передаються за технологією комутації, а для передавання кадрів між віртуальними мережами можуть застосовуватися маршрутизатори. При використанні віртуальних мереж з комутаторами одночасно вирішуються два завдання:

• підвищення продуктивності віртуальної мережі, тому що комутатор передає кадри тільки вузлу призначення (це можливо, якщо вузли підключаються безпосередньо до портів комутатора);

• ізоляція віртуальних мереж одна від одної для керування правами доступу користувачів і створення захисних бар'єрів на шляху широкомовних "штормів".

При всій розмаїтості структурних схем мереж, побудованих на комутаторах, у них використовуються всього дві базові схеми: стягнута в точку магістраль і розподілена магістраль.

Стягнута в точку магістраль одержала свою назву через те, що внутрішня магістраль комутатора поєднує всі компоненти такої мережі. Перевага такої схеми – висока продуктивність внутрішньої магістралі (до декількох Гбіт/с). Ще однією перевагою такої схеми є її незалежність від протоколів мережевого рівня еталонної моделі OSI.

При необхідності поширення мережі по великій території можна скористатися іншою базовою схемою – мережею з розподіленою магістраллю. Прикладом мережі з розподіленою магістраллю служить подвійне кільце FDDI, до якого підключені комутатори мереж робочих груп. Мережа з розподіленою магістраллю спрощує зв'язок між робочими групами, скорочує вартість кабельної системи й допускає рознесення вузлів на більші відстані. Недоліком є значно менша швидкість порівняно з мережею зі стягнутою в точку магістраллю.

За конструктивним виконанням комутатори діляться на три групи:

• автономні комутатори з фіксованою кількістю портів;

• модульні комутатори на основі шасі;

• комутатори з фіксованою кількістю портів, що збирають у стек.

Комутатори першої групи звичайно призначені для невеликих робочих груп.

Модульні комутатори на основі шасі найчастіше використовуються на магістралі мережі. Модулі такого комутатора допускають заміну блоків без вимикання комутатора.

Стекові комутатори являють собою безліч комутаторів, які можуть працювати автономно, тому що виконані в окремих корпусах, але мають спеціальний інтерфейс (високошвидкісну шину), що дозволяє об'єднати їх в одну систему – єдиний комутатор.

Мости (bridge), маршрутизатори (router) і шлюзи (gateway) служать для об'єднання в одну мережу кількох різнорідних мереж з різними протоколами обміну нижнього рівня, зокрема, з різними форматами пакетів, методами кодування, швидкістю передавання і т.д. У результаті їхнього застосування складна і неоднорідна мережа, що містить у собі різні сегменти, з погляду користувача виглядає самою звичайною мережею. Забезпечується прозорість мережі для протоколів високого рівня. Усі вони набагато дорожчі, ніж концентратори, тому що вони здійснюють досить

складну обробка інформації. Реалізуються вони звичайно на базі комп'ютерів, підключених до мережі за допомогою мережевих адаптерів. По суті це спеціалізовані абоненти (вузли) мережі.

2.6 Мости

Мости – найбільш прості пристрої, що служать для об'єднання мереж з різними стандартами обміну, наприклад, Ethernet і Arcnet, або декількох сегментів (частин) однієї і тієї ж мережі, наприклад, Ethernet (рис. 2.4). В останньому випадку міст, як і комутатор, тільки розділяє навантаження сегментів, підвищуючи тим самим продуктивність мережі в цілому. На відміну від комутаторів мости приймають пакети, що надходять, повністю і в разі потреби виконують їхнє найпростіше оброблення. Мости, як і комутатори, працюють на другому рівні моделі OSI, але на відміну від них можуть захоплювати також і верхній підрівень LLC другого рівня (для зв'язку різнорідних мереж). Останнім часом мости швидко витісняються комутаторами, що стають функціональнішими.

Мости досить інтелектуальні, так що не повторюють шуми мережі, помилки або зіпсовані кадри. Для кожної з'єднуваної мережі міст є вузлом (абонентом мережі). Вузлом мережі може бути комп'ютер, спеціальна робоча станція або інший пристрій. При цьому міст приймає кадр, запам'ятовує його у своїй буферній пам'яті, аналізує адресу призначення кадру. Якщо кадр належить до мережі, з якої він отриманий, міст не повинен на цей кадр реагувати. Якщо кадр потрібно переслати в іншу мережу, він туди й відправляється. Доступ до середовища здійснюється відповідно до тих самих правил, що й для звичайного вузла.

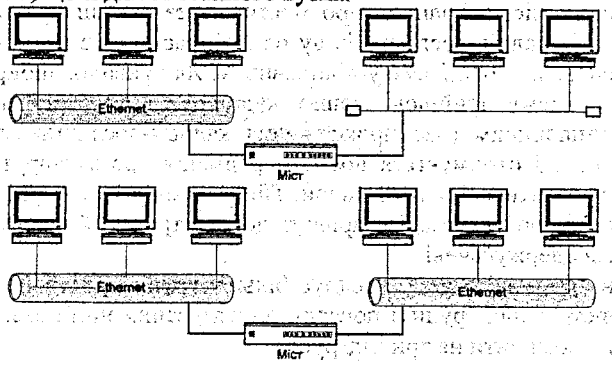

Рисунок 2.4 – Включення моста

За приналежністю до різних типів мереж розрізняють локальні й глобальні (віддалені) мости. Ці мости відрізняються за типами своїх мережевих портів.

Локальні мости постачаються з портами. Як правило, для з'єднання пристроїв у мережах використовуються коаксіальний і волоконно-оптичний кабель або кручена пара. Однією з найважливіших переваг локальних мостів є їхня здатність з'єднувати локальні мережі, що використовують різні середовища. Наприклад, мости здатні об'єднати мережі на коаксіальному кабелі з мережею, побудованою на волоконно-оптичному кабелі.

Глобальні мости встановлюються в мережах передачі інформації на великі відстані. При цьому глобальні мости можуть бути обладнані локальними портами.

За алгоритмом роботи мости поділяються на мости з "маршрути зацією від джерела" (Source Routing) і на "прозорі" (transparent) мости.

Алгоритм "маршрутизації від джерела" призначений для опису проходження кадрів через мости в мережах Token Ring. У цих мережах мости можуть не містити адресну базу даних. Вони обчислюють маршрут проходження кадру виходячи з інформації, яка зберігається в полях самого кадру. Вузол мережі, якому необхідний зв'язок з іншим вузлом, надсилає йому спеціальний кадр-дослідник (Explorer Frame). Цей кадр містить спеціальний ідентифікатор, призначений для мостів з алгоритмом "маршрутизація від джерела". Після одержання цього кадру такий міст записує інформацію про напрямок, з якого був отриманий кадр, і своє власне ім'я в спеціальне поле в кадрі, що називається розділом запису про маршрут (Routing Information Field). Після цього міст передає кадр по всіх доступних йому напрямках, за винятком того, по якому кадр був прийнятий. У результаті в мережі виникає безліч копій того самого кадру-дослідника. До вузла, що повинен одержати пакет, надходять відразу кілька копій кадру – по одній з кожного можливого маршруту. При цьому кожний отриманий кадр-дослідник містить записи про мости, через які він проходив. Після одержання всіх кадрів-дослідників вузол вибирає один з можливих маршрутів і надсилає відповідь вузлу-відправнику. Як правило, вибирається той маршрут, по якому прийшов перший кадр-дослідник, тому що він, імовірно, є найшвидшим (час проходження кадром-дослідником мінімальний). У відповіді отримується повна інформація про маршрут, по якому повинні направлятися всі інші кадри. Після визначення маршруту вузол-відправник використовує цей маршрут досить тривалий час при відправленні пакетів одержувачеві.

Термін "прозорі" мости поєднує більшу групу пристроїв. Якщо розглядати пристрої цієї групи з погляду розв'язуваних ними завдань, то цю групу можна розділити на три підгрупи:

- прозорі мости (transparent bridges) поєднують мережі з єдиними протоколами канального й фізичного рівнів моделі OSI (Ethernet-Ethernet, Token Ring-Token Ring і т.д.);
- транслювальні мости (translating bridges) поєднують мережі з різними протоколами канального й фізичного рівнів;

• Q інкапсулювальні мости (encapsulating bridges) з'єднують мережі з єдиними протоколами канального й фізичного рівня (наприклад, Ethernet) через мережі з іншими протоколами (наприклад, FDDI).

Прозорі мости найбільше поширені. Для цих мостів локальна мережа подається як набір MAC-адрес пристроїв, що працюють у мережі. Мости переглядають ці адреси для ухвалення рішення про подальший шлях передавання кадру. Для аналізу адреси кадр записується у внутрішній буфер мосту. Мости не працюють із інформацією, що відноситься до мережевого рівня. Вони нічого не знають про топологію зв'язків сегментів або мереж між собою. Тому мости зовсім прозорі для протоколів, починаючи з мережевого й вище. Мости дозволяють об'єднати кілька локальних мереж у єдину логічну мережу. З'єднувальні локальні мережі утворюють мережеві сегменти такої логічної мережі.

Порівняно із прозорою маршрутизацією (тією, котру складають прозорі мости) "маршрутизація від джерела" може викликати додаткові витрати, які призводять до незначного зменшення продуктивності мережі. Але в останньої є також багато переваг. Наприклад, робоча станція сама вибирає маршрут. Вибір оптимального маршруту неможливий при прозорій маршрутизації. Маршрутизація від джерела також надає ширші можливості керування передаванням інформації, тому що вся інформація про маршрут утримується в самому переданому пакеті.

Крім адреси відправника міст аналізує й адреси одержувачів. Цей аналіз необхідний для ухвалення рішення про подальший шлях передавання кадру. Міст порівнює адресу одержувача кадру з адресами, що зберігаються в базі даних.

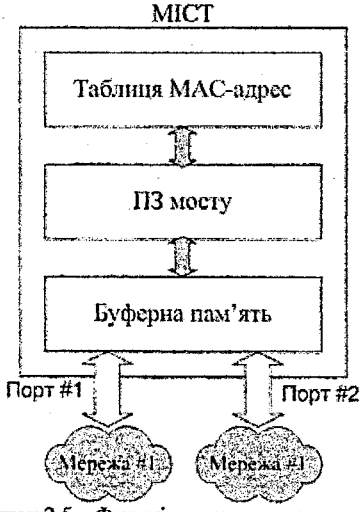

Рисунок 2.5 – Функціональна структура мосту

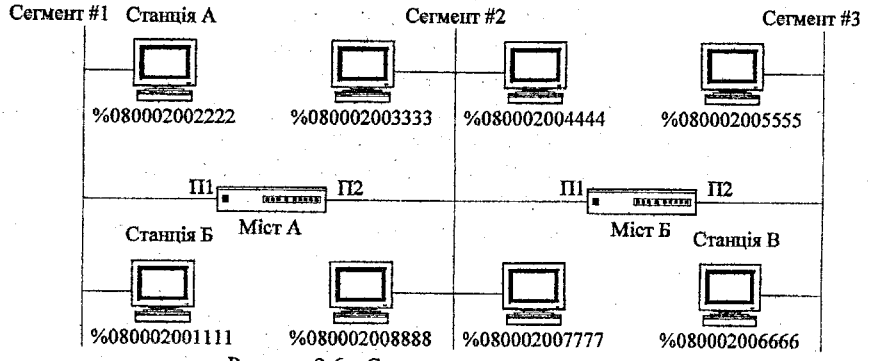

Рисунок 2.6 – Схема з прозорими мостами

На рис. 2.6 показана мережа, що складається із трьох сегментів, зв'язаних двома мостами. Знак % указує на шістнадцяткове подання фізичної (MAC) адреси. З початком роботи мости А і Б перевіряють весь трафік на кожному з підключених сегментів. У процесі перевірки трафіка кожний міст формує свою базу даних адрес станцій. Припустимо, що станція А посилає кадр станції Б. Міст А одержує цей кадр на свій порт 1 (П1). Оскільки станції А і Б належать до одного сегмента мережі, міст відкидає (не реагує) цей кадр. Якщо станція А посилає кадр станції В, що перебуває в третьому сегменті мережі, міст А просуває цей кадр у другий сегмент через свій порт 2 (П2). Міст Б отримає кадр на порт 1 і перешле його через порт 2 у третій сегмент мережі, де й розташована станція В.

Так як робочі станції можуть переноситися з одного сегмента в інший, мости повинні періодично обновляти вміст своїх адресних баз. У зв'язку з чим записи в адресній базі діляться на два типи – статичні й динамічні. З кожним динамічним записом пов'язаний таймер неактивності. При одержанні кадру з адресою відправника, що відповідає певному запису в адресній базі, відповідний таймер неактивності скидається у вихідний стан. Якщо яка-небудь станція довгий час не відсилає кадри, таймер неактивності після закінчення певного проміжку часу видаляє цю адресу з бази даних.

На рис. 2.7 структура мосту аналізується з погляду еталонної моделі OSI.

Мости, як прозорі, так і з маршрутизацією від джерела, працюють на MAC-підрівні канального рівня еталонної моделі OSI. Необхідно відзначити, що маршрутизація від джерела означає в загальному значенні спосіб (алгоритм) пошуку абонента в мережі. Для мостів цей алгоритм застосовується тільки для мереж Token Ring.

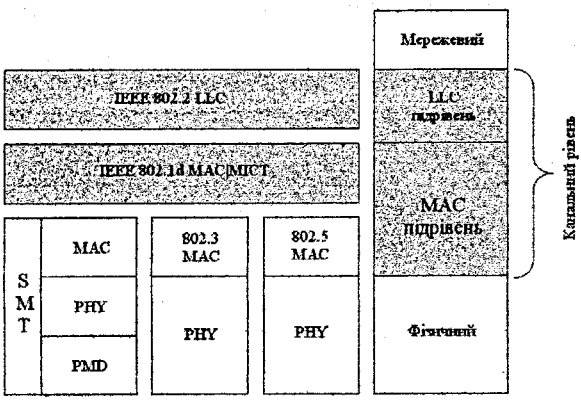

Рисунок 2.7 – Еталонна модель OSI і структура мосту

2.7 Маршрутизатори

Дуже часто в комп'ютерній літературі можна зустріти таке означення маршрутизатора (англійська назва – rouier): "маршрутизатор – це пристрій мережевого рівня еталонної моделі OSI, що використовує одну або більше метрик для визначення оптимального шляху передачі мережевого трафіка на підставі інформації мережевого рівня". З цього випливає, що маршрутизатор насамперед необхідний для вибору подальшого шляху даних, що відсилаються в розподілену мережу.

Користувачі для відправлення своїх даних у мережу вказують лише адресу абонента. Ці дані йдуть в мережу й у місцях з розгалуженням маршрутів надходять на маршрутизатори, які як раз і служать для вибору подальшого шляху. При цьому маршрутизатор вибирає оптимальний шлях. Оптимальність шляху визначається кількісними характеристиками, що називаються метриками. Кращий шлях – це шлях з метрикою, яка в даному конкретному випадку є найбільш прийнятною. В метриці можуть враховуватися кілька показників, наприклад довжина шляху, час проходження і т.д.

За означенням, основне призначення маршрутизаторів – це вибір оптимального шляху проходження трафіка мережі. Процес маршрутизації можна розділити на два ієрархічно пов'язаних рівні.

1. Рівень маршрутизації. На цьому рівні відбувається робота з таблицею маршрутизації. Таблиця маршрутизації служить для визначення адреси мережевого рівня наступного маршрутизатора або безпосередньо одержувача. Після визначення адреси вибирається інтерфейс маршрутизатора, через який будуть передаватися пакети. Цей процес називається визначен-

ням маршруту. Керування таблицею маршрутизації виконується протоколами маршрутизації.

2. Рівень передавання пакетів. Перед тим як передати пакет, необхідно: перевірити контрольну суму заголовка пакета, визначити адресу (канальний рівень) одержувача пакета і виконати безпосередньо відправлення пакета з урахуванням черговості, фрагментації, фільтрації і т.д. Ці дії виконуються на підставі команд, що надходять з рівня маршрутизації.

Маршрутизатори ділять на пристрої вищого, середнього й нижнього класів.

Високопродуктивні маршрутизатори вищого класу служать для об'єднання мереж підприємства. Вони підтримують безліч протоколів і інтерфейсів, причому не тільки стандартних, але, часом, і досить екзотичних. Пристрої даного типу можуть мати до 50 портів локальних або глобальних мереж.

За допомогою маршрутизаторів середнього, проміжного, класу формуються менші мережеві об'єднання масштабу підприємства. Стандартна конфігурація включає два-три порти локальних мереж і від чотирьох до восьми портів глобальної мережі. Такі маршрутизатори підтримують найпоширеніші протоколи маршрутизації й транспортні протоколи.

Маршрутизатори нижнього класу призначаються для локальних мереж підрозділів; вони зв'язують невеликі офіси з мережею підприємства. Типова конфігурація: один порт локальної мережі (Ethernet або Token Ring) і два порти глобальної мережі, розраховані на низькошвидкісні виділені лінії або здатні до комутації з'єднання. Проте подібні маршрутизатори користуються більшим попитом в адміністраторів, яким необхідно розширити наявні міжмережеві об'єднання.

Маршрутизатори для базових мереж і віддалених офісів мають різну архітектуру, оскільки до них висуваються різні функціональні й операційні вимоги. Маршрутизатори базових мереж обов'язково повинні бути розширюваними. Маршрутизатори локальних мереж підрозділу, для яких, як правило, заздалегідь встановлюється фіксована конфігурація портів, містять тільки один процесор, керуючий роботою трьох або чотирьох інтерфейсів. У них використовуються приблизно ті ж протоколи, що й у маршрутизаторах базових мереж, однак програмне забезпечення більше спрямоване на полегшення інсталяції й експлуатації, оскільки в більшості вилучених офісів відсутні достатньо кваліфіковані фахівці з мережевого обслуговування.

Маршрутизатор базової мережі складається з таких основних компонентів: мережевих адаптерів, що залежать від протоколів і служать інтерфейсами з локальними й глобальними мережами; керувального процесора,

що визначає маршрут і обновляє інформацію про топологію; основної магістралі. Після надходження пакета на інтерфейсний модуль він аналізує адресу призначення й приймає команди керувального процесора для визначення вихідного порту. Потім пакет по основній магістралі маршрутизатора передається в інтерфейсний модуль, що служить для зв'язку з адресованим сегментом локальної мережі або портом глобальної мережі.

Як маршрутизатор може виступати робоча станція або сервер, що мають кілька мережевих інтерфейсів і мають спеціальне програмне забезпечення. Маршрутизатори вищого класу – це, як правило, спеціалізовані пристрої, що поєднують в окремому корпусі безліч маршрутизувальних модулів. Узагальнена функціональна схема маршрутизації зображена на рис. 2.8.

Рисунок 2.8 – Узагальнена функціональна схема маршрутизації

Визначення маршруту передавання даних відбувається програмно. Відповідні програмні засоби носять назви протоколів маршрутизації. Логіка їхньої роботи заснована на алгоритмах маршрутизації. Алгоритми маршрутизації обчислюють вартість доставки й вибирають шлях з меншою вартістю. Найпростіші алгоритми маршрутизації визначають маршрут на підставі найменшого числа проміжних (транзитних) вузлів на шляху до адресата. Складніші алгоритми в поняття "вартість" закладають кілька показників, наприклад, затримку при передаванні пакетів, пропускну здатність каналів зв'язку або грошову вартість зв'язку. Основним результатом роботи алгоритму маршрутизації є створення й підтримка таблиці маршрутизації, у яку записується вся маршрутна інформація. Зміст таблиці маршрутизації

залежить від використовуваного протоколу маршрутизації. У загальному випадку таблиця маршрутизації містить таку інформацію:

- дійсні адреси пристроїв у мережі;
- службову інформацію протоколу маршрутизації;
- адреси найближчих маршрутизаторів.

Основними вимогами, пропонованими до алгоритму маршрутизації, є:

- оптимальність вибору маршруту;
- простота реалізації;
- стійкість;
- швидка збіжність;
- гнучкість реалізації.

Оптимальність вибору маршруту є основним параметром алгоритму, що не вимагає пояснень.

Алгоритми маршрутизації повинні бути прості в реалізації й використовувати якнайменше ресурсів; стійкими до відмов устаткування на спочатку обраному маршруті, високих навантажень і помилок у побудові мережі.

Збіжність – це процес узгодження між маршрутизаторами інформації про топологію мережі. Якщо певна подія в мережі призводить до того, що певні маршрути стають недоступні або виникають нові маршрути, маршрутизатори розсилають повідомлення про це один одному по всій мережі. Після одержання цих повідомлень маршрутизатори роблять перепризначення оптимальних маршрутів, що у свою чергу може породити новий потік повідомлень. Цей процес повинен завершитися, причому досить швидко, інакше в мережевій топології можуть з'явитися петлі або мережа взагалі може перестати функціонувати. Алгоритми маршрутизації повинні швидко й правильно враховувати зміни в стані мережі (наприклад, відмова вузла або сегмента мережі).

Переваги гнучкої реалізації не вимагають коментарів.

Алгоритми маршрутизації можуть бути:

- статичними або динамічними;
- одномаршрутними або багатомаршрутними;
- однорівневими або ієрархічними;
- внутрішньодоменними або міждоменними;
- одноадресними або груповими.

Для статичних (неадаптивних) алгоритмів маршрути вибираються заздалегідь і заносяться вручну в таблицю маршрутизації, де зберігається інформація про те, на який порт відправити пакет з відповідною адресою. Протоколи, розроблені на базі статичних алгоритмів, називають не здатними до маршрутизації протоколами. Прикладами не здатних до маршру-

тизації протоколів можуть служити LAT (Local Area Transport, транспортний протокол для локальних областей) фірми DEC, протокол підключення термінала й NetBIOS. Зазвичай із цими протоколами працюють мости, тому що вони не розрізняють протоколів мережевого рівня.

При використанні динамічних алгоритмів таблиця маршрутизації автоматично обновляється при зміні топології мережі або трафіка. Динамічні алгоритми розрізняються за способом одержання інформації про стан мережі, час зміни маршрутів і використовуваних показників оцінки маршруту.

2.7.1 Апаратна архітектура маршрутизаторів

Маршрутизатор можна розглядати як спеціалізований комп'ютер, що призначений для виконання конкретних задач. І як усякий комп'ютер, маршрутизатор має власний центральний процесор (Central Processing Unit – CPU), тип якого може розрізнятися залежно від класу маршрутизатора, фірми-виготовлювача, серії маршрутизатора усередині класу (наприклад, це може бути Motorola 68030 або Опоп/ДО4600). Основна задача процесора маршрутизатора (поряд з багатьма другорядними) полягає в обробці вхідних пакетів для прийняття рішень про їхнє подальше перенаправлення. При цьому швидкість, з якою маршрутизатор здатен обробляти пакети, що надходять, прямо залежить від типу використовуваного процесора.

Іншою важливою частиною маршрутизатора, крім процесора, є його пам'ять, що поділена за функціональним принципом. Маршрутизатори підтримують чотири основних типи пам'яті: постійний запам'ятовувальний пристрій (Read-Only Memory – ROM), флеш-пам'ять (flash memory), пам'ять з довільним доступом (Random-Access Memory – RAM) і енергонезалежну пам'ять (Non-Volatile RAM – NVRAM). З перерахованих типів пам'яті тільки RAM є енергозалежною, тобто її вміст стирається після вимикання живлення маршрутизатора. Тому пам'ять RAM може використовуватися тільки для збереження тимчасових даних при роботі маршрутизатора.

Важливою складовою частиною маршрутизатора, крім його апаратних компонентів, є конфігураційні файли (configuration files). Є два типи конфігурації операційної системи: робоча (running configuration) і завантажувальна (startup configuration). Часто конфігурацію першого типу також називають активною (active), тому що вона розташовується в оперативній пам'яті маршрутизатора (RAM) і визначає його поточні налаштування. Коли адміністратор виконує команди конфігурування, на маршрутизаторі змінюється вміст саме цієї конфігурації. На противагу робочій, завантажувальна конфігурація розміщається в пам'яті NVRAM маршрутизатора і містить команди операційної системи, які виконуються в момент його завантаження.

Робоча і завантажувальна конфігурації в якійсь мірі самостійні. Звичайно адміністратор мережі, виконавши початкові етапи налаштування маршрутизатора і перевіривши його роботоздатність, копіює робочу конфігурацію в пам'ять NVRAM, формуючи в такий спосіб завантажувальну конфігурацію. Основною причиною такої послідовності дій є необхідність збереження зроблених змін при перезавантаженні маршрутизатора.

Маршрутизатори здійснюють вибір оптимального маршруту для кожного пакета з метою запобігання надмірного навантаження окремих ділянок мережі і обходу ушкоджених ділянок. Вони застосовуються, як правило, у складних розгалужених мережах, що мають кілька маршрутів між окремими абонентами. Маршрутизатори не перетворюють протоколи нижніх рівнів, тому вони з'єднують тільки сегменти однойменних мереж.

Маршрутизатори працюють на третьому рівні моделі OSI, тому що вони аналізують не тільки MAC-адреси пакета, але і IP-адреси, тобто глибше проникають у інкапсульований пакет.

Є також гібридні маршрутизатори (brouter) – гібрид моста і маршрутизатора. Вони виділяють пакети, яким потрібна маршрутизація, та обробляють їх як маршрутизатор, а для інших пакетів служать звичайним мостом.

2.8 Шлюзи

Шлюзи – це пристрої для з'єднання мереж із різними протокольними стеками, наприклад, для з'єднання локальних мереж з великими комп'ютерами або з глобальними мережами. Це найдорожчі мережеві пристрої і вони рідко застосовуються. Шлюзи реалізують зв'язок між абонентами на верхніх рівнях моделі OSI (з четвертого по сьомий). Тобто вони повинні виконувати і всі функції нижчерозташованих рівнів.

Контрольні питання до розділу 2

1. Основні типи середовища передаванні мережі.
2. Описати категорії кабелів.
3. Перелічити функції мережевих адаптерів.
4. Основне призначення повторювачів.
5. На якому рівні мережі працює комутатор. Описати його основні переваги та недоліки.
6. Функції та категорії комутаторів.
7. Основні алгоритми маршрутизації мережі.
8. Переваги маршрутизаторів та принцип їх роботи.
9. Апаратна архітектура маршрутизаторів.

Розділ 3
ТЕХНОЛОГІЇ КОРПОРАТИВНИХ МЕРЕЖ

3.1 Стандарти локальних мереж

Стандартні мережі забезпечують широкий діапазон припустимих розмірів мережі, кількості абонентів і, що не менш важливо, цін на апаратуру. Але зробити вибір все ж таки непросто. Адже на відміну від програмних засобів, замінити які неважко, апаратура звичайно служить багато кому протягом років, її заміна веде не тільки до значних витрат, до необхідності перекладання кабелів, але і до перегляду системи комп'ютерних засобів організації. У зв'язку з цим помилки у виборі апаратури звичайно обходяться набагато дорожче помилок у виборі програмних засобів.

У таблиці 3.1 наведено характеристики класичних варіантів стандартних мереж. Усі стандартні мережі мають кілька варіантів, що відрізняються типом кабелю, що використовується, швидкостями передачі, припустимими розмірами мережі.

Таблиця 3.1 – Параметри базових варіантів стандартних мереж

Параметр мережі	Fast Ethernet	Token-Ring	FDDI	Gigabit Ethernet
Стандарт	IEEE 802.3	IEEE 802.5	ISO 9314	IEEE 802.3ab IEEE 802.3z
Топологія	"Зірка"	"Кільце"	"Кільце"	"Зірка"
Швидкість передачі	100 Мбіт/с	(16) Мбіт/с	100 Мбіт/с	10 Гбіт/с
Довжина	5 км	120 м	20 км	1 км
Середовище	КП	КП	ОВ	КП, ОВ
Метод керування	CSMA/CD	Маркер	Маркер	CSMA/CD
Код	4B/5B	Біфазний	4B/5B	PAM5, 8B/10B
Кількість	До 1024	До 260	До 1000	До 1024
КП – кабель на кручених парах, ОВ – оптоволоконний кабель				

3.1.1 Мережі Fast Ethernet

Найбільше поширення серед стандартних мереж одержала мережа Ethernet. Вперше вона з'явилася в 1972 році (розроблювачем виступила відома фірма Xerox). Мережа виявилася досить вдалою, і внаслідок цього її в 1980 році підтримали такі найбільші компанії, як DEC і Intel (об'єднання цих компаній назвали DIX по перших буквах їхніх назв). Їхніми стараннями в 1985 році мережа Ethernet стала міжнародним стандартом, її прийняли найбільші міжнародні організації по стандартах: комітет 802 IEEE (Institute of Electrical and Electronic Engineers) і ECMA (European Computer Manufacturers Association).

Стандарт одержав назву IEEE 802.3 (англійською читається як "eight oh two dot three"). Він визначає множинний доступ до багатоканального типу "шина" з виявленням конфліктів і контролем передавання, тобто з уже

згадуваним методом доступу CSMA/CD. Цьому стандартові задовольняли і деякі інші мережі, тому що рівень його деталізації невисокий. У результаті мережі стандарту IEEE 802.3 нерідко були несумісні між собою як за конструктивними, так і за електричними характеристиками. Однак останнім часом стандарт IEEE 802.3 вважається стандартом саме мережі Ethernet.

Основні характеристики початкового стандарту IEEE 802.3:

- топологія – "шина";
- середовище передавання – коаксіальний кабель;
- швидкість передачі – 10 Мбіт/с;
- максимальна довжина мережі – 5 км;
- максимальна кількість абонентів – до 1024;
- довжина сегмента мережі – до 500 м;
- кількість абонентів на одному сегменті – до 100;
- метод доступу – CSMA/CD;
- передавання без модуляції (моноканал).

У класичній мережі Ethernet застосовувався 50-омний коаксіальний кабель двох видів (товстий і тонкий). Однак останнім часом (з початку 90-х років) найбільше поширення одержала версія Ethernet, що використовує як середовище передавання кручені пари. Визначений також стандарт для застосування в мережі оптоволоконного кабелю. Для обліку цих змін у споконвічний стандарт IEEE 802.3 минулого зроблені відповідні доробки. У 1995 році з'явився додатковий стандарт на більш швидкісну версію Ethernet, що працює на швидкості 100 Мбіт/с (так званий Fast Ethernet, стандарт IEEE 802.3u), що використовує як середовище передавання "кручену" пару або оптоволоконний кабель. У 1997 році з'явилася і версія на швидкість 1000 Мбіт/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Крім стандартної топології "шина" усе ширше застосовуються топології типу "пасивна зірка" і "пасивне дерево". При цьому передбачається використання репітерів і репітерних концентраторів, що з'єднують між собою різні частини (сегменти) мережі. У результаті може сформуватися деревоподібна структура на сегментах різних типів.

Як сегмент (частина мережі) може виступати класична "шина" або одиничний абонент. Для шинних сегментів використовується коаксіальний кабель, а для променів пасивної зірки (для приєднання до концентратора одиночних комп'ютерів) – кручена пара та оптоволоконний кабель. Головна вимога до отриманої в результаті топології – щоб у ній не було замкнутих шляхів (петель). Фактично виходить, що всі абоненти з'єднані у фізичну шину, тому що сигнал від кожного з них поширюється відразу в усі сторони і не повертається назад (як у кільці).

Максимальна довжина кабелю мережі в цілому (максимальний шлях сигналу) теоретично може досягати 6,5 кілометра, але практично не перевищує 3,5 кілометра.

У мережі Fast Ethernet не передбачена фізична топологія "шина", використовується тільки "пасивна зірка" або "пасивне дерево". До того ж у Fast Ethernet більш жорсткі вимоги до граничної довжини мережі. Адже при збільшенні в 10 разів швидкості передавання і збереженні формату пакета його мінімальна довжина стає в десять разів коротшою. У такий спосіб у 10 разів зменшується припустима величина подвійного часу проходження сигналу мережею (5,12 мкс проти 51,2 мкс у Ethernet).

Для передавання інформації в мережі Ethernet застосовується стандартний манчестерський код.

3.1.1.1 Доступ до середовища і передавання даних

Припускаючи для простоти викладення, що кожен вузол (станція) має тільки один мережевий інтерфейс, розглянемо, як на основі алгоритму CSMA/CD відбувається передавання даних в мережі Ethernet.

Всі комп'ютери в мережі з середовищем, що розділяється, мають можливість негайно (з урахуванням затримки поширення сигналу у фізичному середовищі) одержати дані, які будь-який з комп'ютерів почав передавати в загальне середовище. Говорять, що середовище, до якого підключені всі станції, працює в режимі колективного доступу (Multiply Access, MA).

Щоб дістати можливість передавати кадр, інтерфейс-відправник повинен переконатися, що середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, яка також називається несучою частотою (Carrier Sense, CS).

Ознакою "незайнятості" середовища є відсутність на ній частоти, яка при манчестерському способі кодування, прийнятому для всіх варіантів Ethernet 10 Мбіт/с, рівна 5-10 МГц залежно від послідовності одиниць і нулів, передаваних в даний момент.

Якщо середовище вільне, то вузол має право почати передавання кадру. У прикладі, показаному на рис. 3.1, вузол 1 виявив, що середовище вільне, і почав передавати свій кадр. У класичній мережі Ethernet на коаксіальному кабелі сигнали передавача вузла 1 поширюються в обидві сторони, так що їх одержують всі вузли мережі. Кадр даних завжди супроводжується преамбулою, яка складається з 7 байтів, кожний з яких має значення 10101010, і 8-го байта, рівного 10101011. Останній байт носить назву обмежувача початка кадру. Преамбула потрібна для входження приймача в побітову і побайтову синхронізацію з передавачем. Наявність двох одиниць, що йдуть підряд, говорить приймачу про те, що преамбула закінчилася і наступний біт є початком кадру.

Всі станції, підключені до кабелю, починають записувати байти переданого кадру в свої внутрішні буфери. Перші 6 байтів кадру містять адресу призначення. Та станція, яка розпізнає власну адресу в заголовку кадру, продовжує записувати його вміст в свій внутрішній буфер, а решта станцій на цьому прийом кадру припиняють. Станція призначення опра-

цьовує одержані дані, передає їх вгору по своєму стеку. Кадр Ethernet містить не тільки адресу призначення, але і адресу джерела даних, тому станція-одержувач знає, кому потрібно надіслати відповідь.

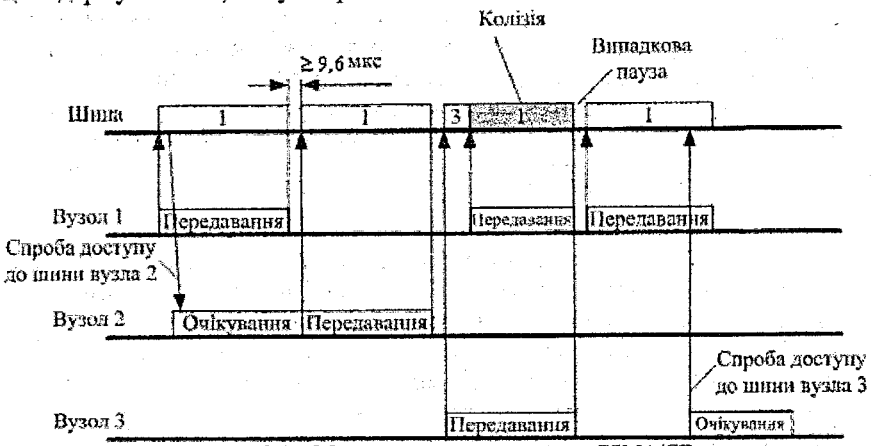

Рисунок 3.1 – Метод випадкового доступу CSMA/CD

Вузол 2 під час передавання кадру вузлом 1 також намагався почати передавання свого кадру, проте виявляє, що середовище зайняте –у ньому наявна несуча частота, – тому вузол 2 вимушений чекати, поки вузол 1 не припинить передавання кадру.

Після закінчення передавання кадру всі вузли мережі зобов'язані витримати технологічну паузу, рівну міжпакетному інтервалу (Inter Packet Gap, IPG) в 9,6 мкс. Ця пауза потрібна для повернення мережевих адаптерів до початкового стану, а також для запобігання монопольному захопленню середовища однією станцією. Після закінчення технологічної паузи вузли мають право почати передавання свого кадру, оскільки середовище вільне. У наведеному прикладі вузол 2 дочекався закінчення передавання кадру вузлом 1, зробив паузу в 9,6 мкс і почав передавання свого кадру.

3.1.1.2 Формати кадрів технології Ethernet

Стандарт технології Ethernet, визначений в документі IEEE 802.3, дає опис єдиного формату кадру рівня MAC. Оскільки в кадр рівня MAC повинен вкладатися кадр рівня LLC, описаний в документі IEEE 802.2, то за стандартами IEEE в мережі Ethernet може використовуватися тільки єдиний варіант кадру канального рівня, заголовок якого є комбінацією заголовків підрівнів MAC і LLC.

Проте на практиці в мережах Ethernet на канальному рівні використовуються кадри 4-х різних форматів (типів). Один і той же тип кадру може мати різні назви, тому далі для кожного типу кадрів наведено декілька найвикористовуваніших назв.

Кадр Ethernet DIX, або Ethernet II, з'явився в результаті роботи консорціуму трьох фірм Digital, Intel і Xerox в 1980 році, який подав на розгляд комітету 802.3 свою фірмову версію стандарту Ethernet як проект міжнародного стандарту.

Проте комітет 802.3 прийняв стандарт, що відрізняється в деяких деталях від пропозиції DIX, причому відмінності стосувалися і формату кадру. Так виник формат кадру 802.3/LLC, 802.3/802.2, або Novell 802.2. Кадр Raw 802.3, або Novell 802.3, з'явився в результаті зусиль компанії Novell щодо прискорення роботи свого стека протоколів в мережах Ethernet.

Кадр Ethernet SNAP став результатом діяльності комітету 802.2 із приведення попередніх форматів кадрів до деякого загального стандарту і додання кадру необхідної гнучкості для обліку в майбутньому можливостей додання полів або зміни їх призначення.

Відмінності у форматах кадрів можуть призводити до несумісності в роботі апаратури і мережевого програмного забезпечення, розрахованого на функціонування тільки з одним стандартом кадру Ethernet. Проте сьогодні практично всі мережеві адаптери, драйвери мережевих адаптерів, мости/комутатори і маршрутизатори уміють працювати зі всіма використовуваними на практиці форматами кадрів технології Ethernet, причому розпізнавання типу кадру виконується автоматично.

Формати всіх цих чотирьох типів кадрів Ethernet наведені на рис. 3.2.

Кадр 802.3/LLC

6	6	2	1	1	1(2)	46-1497(1496)	4
DA	SA	L	DSAP	SSAP	Керувальне поле	Дані	FCS
			Заголовок LLC				

Кадр Raw 802.3/Novell 802.3

6	6	2	46-1500	4
DA	SA	L	Дані	FCS

Кадр Ethernet DIX (II)

6	6	2	46-1500	4
DA	SA	L	Дані	FCS

Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	46-1492	4
DA	SA	L	DSAP	SSAP	Керувальне поле	OUI	T	Дані	FCS
			AA	AA	03	000000			
			Заголовок LLC			Заголовок SNAP			

Рисунок 3.2 – Формати кадрів Ethernet

3.1.1.2.1 Кадр 802.3/LLC

Заголовок кадру 802.3/LLC є результатом об'єднання полів заголовків кадрів, визначених в стандартах IEEE 802.3 і 802.2.

Стандарт 802.3 визначає вісім полів заголовка.

Поле преамбули складається з семи синхронізувальних байтів – 10101010. При манчестерському кодуванні ця комбінація подається у фізичному середовищі періодичним хвилевим сигналом з частотою 5 Мгц.

Початковий обмежувач кадру (Start-of-Frame-Delimiter, SFD) складається з одного байта 10101011. Поява цієї комбінації бітів є вказанням на те, що наступний байт – це перший байт заголовка кадру.

Адреса призначення (Destination Address, DA) може бути завдовжки 2 або 6 байтів. На практиці завжди використовуються MAC-адреси з 6 байтів.

Адреса джерела (Source Address, SA) – це дво- або шестибайтове поле, що містить MAC-адресу вузла – відправника кадру. Перший біт адреси завжди має значення 0.

Довжина (Length, L) – двобайтове поле, яке визначає довжину поля даних в кадрі.

Поле даних може містити від 0 до 1500 байтів. Але якщо довжина поля менше 46 байтів, то використовується наступне поле – поле заповнювача, доповнюючe кадр до мінімально допустимого значення в 46 байтів.

Поле заповнювача складається з такої кількості байтів заповнювача, яка забезпечує мінімальну довжину поля даних 46 байтів. Це дозволяє коректно працювати механізму виявлення колізій. Якщо довжина поля даних більша або рівна мінімальній, то поле заповнювача в кадрі не з'являється.

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

Кадр 802.3/LLC є кадром підрівня MAC, тому відповідно до стандарту IEEE 802.2 в його полі даних вкладається кадр підрівня LLC з видаленими прапорцями початку і кінця кадру. Формат кадру LLC був описаний вище. Оскільки кадр LLC має заголовок завдовжки 3 (у режимі LLC1) або 4 байти (у режимі LLC2), то максимальний розмір поля даних зменшується до 1497 або 1496 байтів.

3.1.1.2.2 Кадр Raw 802.3/Novell 802.3

Кадр Raw 8023, званий ще кадром Novell 802.3, є кадром підрівня MAC стандарту 802.3, але без вкладеного кадру підрівня LLC. Компанія Novell довгий час не використовувала службові поля кадру LLC в своїй операційній системі NetWare завдяки відсутності необхідності ідентифікувати тип інформації, вкладеної в полі даних, – там завжди знаходився пакет протоколу IPX мережевого рівня, що довгий час був єдиним протоколом в ОС NetWare.

Тепер, коли необхідність ідентифікації протоколу верхнього рівня з'явилася, компанія Novell стала використовувати можливість інкапсуляції в кадр підрівня MAC кадру LLC, тобто можливість застосовувати стандартні кадри 802.3/LLC. Такий кадр компанія позначає тепер в своїх операційних системах як кадр 802.2, хоча він є комбінацією заголовків 802.3 і 802.2.

3.1.1.2.3 Кадр Ethernet DIX/Ethernet II

Кадр Ethernet DIX, званий також кадром Ethernet II, має структуру, яка збігається із структурою кадру Raw 802.3. Проте двобайтове поле довжини (L) кадру Raw 802.3 в кадрі Ethernet DIX використовується як поле типу (T) протоколу. Це поле призначене для тих самих цілей, що і поля DSAP і SSAP кадру LLC – для вказання типу протоколу вищого рівня, що вклав свій пакет в полі даних цього кадру.

Тоді як коди протоколів в полях SAP мають довжину один байт, в полі типу для коду протоколу відводяться 2 байти. Тому один і той самий протокол в полі SAP і в полі типу кодуватиметься в загальному випадку різними числовими значеннями. Наприклад, протокол IP має код 204810 (0×0800) для поля типу і значення 6 для поля SAP. Значення кодів протоколів для поля типу з'явилися раніше значень для поля SAP, оскільки фірмова версія Ethernet DIX існувала до появи стандарту 802.3, і до часу поширення устаткування 802.3 ці значення вже стали стандартами де-факто для багатьох апаратних і програмних продуктів. Оскільки структури кадрів Ethernet DIX і Raw 802.3 збігаються, то поле довжини/типу часто в документації позначають як поле L/T. При цьому числове значення цього поля визначає його сенс: якщо значення менше 1500, то це поле довжини, а якщо більше – то типу.

3.1.1.2.4 Кадр Ethernet SNAP

Для усунення розходжень в кодуваннях типів протоколів, повідомлення яких вкладені в полі даних кадрів Ethernet, комітетом 802.2 була проведена робота з подальшої стандартизації кадрів Ethernet. В результаті з'явився кадр Ethernet SNAP (SubNetwork Access Protocol – протокол доступу до підмереж). Кадр Ethernet SNAP є розширенням кадру 802.3/ LLC за рахунок введення додаткового заголовка протоколу SNAP, що складається з двох полів: OUI і типу. Поле типу складається з 2 байтів і повторює за форматом і призначенням поле типу кадру Ethernet II (тобто в ньому використовуються ті ж значення кодів протоколів). Поле OUI визначає вже знайомий нам організаційно унікальний ідентифікатор – тобто ідентифікатор організації, яка контролює коди протоколів в полі типу. За допомогою заголовка SNAP досягнуто сумісності з кодами протоколів в кадрах Ethernet II, а також створено універсальну схему кодування протоколів. Коди протоколів для технологій 802 контролює організація IEEE, ідентифікатор OUI якої рівний 000000. Якщо в майбутньому буде потрібно інші коди протоколів для якої-небудь нової технології, для цього досить буде вказати інший ідентифікатор органі-

зації, що призначає ці коди, а старі значення кодів залишаться у силі (у поєднанні з іншим ідентифікатором OUI).

Оскільки SNAP є протоколом, вкладеним в протокол LLC, то в полях DSAP і SSAP записується код OXAA, відведений для протоколу SNAP. У полі керувального заголовка LLC встановлюється значення 0×03, що відповідає використанню ненумерованих кадрів.

Заголовок SNAP є доповненням до заголовка LLC, тому він допустимий не тільки в кадрах Ethernet, але і в кадрах протоколів інших технологій комітету 802. Наприклад, протокол IP завжди використовує структуру заголовків LLC/SNAP при інкапсуляції в кадри всіх протоколів локальних мереж: FDDI, Token Ring, 100VG-AnyLAN, Ethernet, Fast Ethernet, Gigabit Ethernet. Правда, при передаванні IP-пакетів через мережі Ethernet, Fast Ethernet і Gigabit Ethernet протокол IP використовує кадри Ethernet DIX.

3.1.1.3 Використання різних типів кадрів Ethernet

Через те, що існує чотири типи кадрів Ethernet, для протоколів мережевого рівня виникає проблема –користуватися завжди одним типом кадру, застосовувати всі чотири чи ж надавати перевагу тільки деяким з них.

Протокол IP може використовувати два типи кадрів: оригінальний кадр Ethernet II і структурно найскладніший кадр Ethernet SNAP. Переважним типом кадру для протоколу IP є кадр Ethernet II.

Сучасні мережеві адаптери автоматично розпізнають тип кадру Ethernet, використовуючи значення полів кадрів. Наприклад, кадри Ethernet II легко відрізнити від інших типів кадрів за значенням поля L/T: якщо воно більше 1500, це означає, що поле є полем типу протоколу (T), оскільки значення кодів протоколів вибрані так, що вони завжди більше 1500. У свою чергу, наявність поля T говорить про те, що це кадр Ethernet II, який єдиний використовує це поле в даній позиції кадру.

Протокол IPX "є максималістом", він може працювати зі всіма чотирма типами кадрів Ethernet. Він розпізнає кадри Ethernet II описаним вище способом, а якщо кадр належить до іншого типу (поле L/T має значення менше або рівне 1500), то виконується подальша перевірка за наявністю або відсутністю полів LLC. Поля LLC можуть бути відсутніми тільки в тому випадку, коли за полем довжини йде початок пакету IPX, а саме двобайтове поле, яке завжди заповнюється одиницями, що дає значення 0×FFFF, або два байти по 255. Ситуація, коли поля DSAP і SSAP одночасно містять такі значення, виникнути не може, тому наявність двох байтів 255 говорить про те, що це кадр Raw 802.3.

У решті випадків подальший аналіз проводиться залежно від значень полів DSAP і SSAP. Якщо вони рівні OXAA, то це кадр Ethernet SNAP, а якщо ні, то 802.3/LLC.

Точно так само для мережі Ethernet, що працює на швидкості 100 Мбіт/с (Fast Ethernet), стандарт визначає три типи сегментів, що відрізняються типами середовища передавання:

- 100BASE-T4 (зчетверена "кручена" пара);
- 100BASE-TX (подвоєна "кручена" пара);
- 100BASE-FX (оптоволоконний кабель).

Тут число "100" означає швидкість передачі 100 Мбіт/с, буква "T" – "кручена" пара, буква "F" – оптоволоконний кабель. Типи 100BASE-TX і 100BASE-FX іноді поєднуються під ім'ям 100BASE-X, а 100BASE-T4 і 100BASE-TX – під ім'ям 100BASE-T.

Розвиток технології Ethernet йде по шляху усе більшого відходу від початкового стандарту. Застосування нових середовищ передавання і комутаторів дозволяє істотно збільшити розмір мережі. Відмова від манчестерського коду (у мережі Fast Ethernet і Gigabit Ethernet) забезпечує збільшення швидкості передавання даних і зниження вимог до кабелю. Відмова від методу управління CSMA/CD (при повнодуплексному режимі обміну) дає можливість різко підвищити ефективність роботи і зняти обмеження з довжини мережі. Проте, всі нові різновиди мережі також називаються мережею Ethernet.

3.1.2 Технологія Gigabit Ethernet

Основна ідея розробників стандарту Gigabit Ethernet полягала в максимальному збереженні ідей класичної технології Ethernet, досягши бітової швидкості в 1000 Мбіт/с.

Оскільки при розробленні нової технології природно очікувати деяких технічних новинок, що йдуть в загальному руслі розвитку мережевих технологій, то важливо відзначити, що стандарт Gigabit Ethernet на рівні протоколу не підтримує:

- якість обслуговування;
- надмірні зв'язки;
- тестування роботоздатності вузлів і устаткування (за винятком тестування зв'язку порт-порт, як це робиться в Ethernet 10Base-T, 10Base-F і Fast Ethernet).

Не дивлячись на те, що в Gigabit Ethernet не стали вбудовувати нові функції, забезпечення навіть досить простих функцій класичного стандарту Ethernet на швидкості 1 Гбіт/с вимагало розв'язання декількох складних задач.

Забезпечення прийнятного діаметру мережі для роботи у середовищі. У зв'язку з обмеженнями, що накладаються методом CSMA/CD на довжину кабелю, версія Gigabit Ethernet для середовища, що розділяється, допускала б довжину сегмента всього 25 м при збереженні розміру кадрів і всіх параметрів методу CSMA/CD незмінними. Оскільки є велика кількість застосувань, що вимагають діаметра мережі хоч би 200 м, необхідно було

якимсь чином вирішити це завдання за рахунок мінімальних змін в технології Fast Ethernet.

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

Використання як кабелю крученої пари. Таке завдання на перший погляд здається нерозв'язним – адже навіть для стомегабітових 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 у фізичний рівень, як це було у разі Fast Ethernet, але і в рівень MAC.

3.1.2.1 Засоби забезпечення діаметра мережі 200 м у середовищі, що розділяється

Для розширення максимального діаметра мережі Gigabit Ethernet до 200 м в півдуплексному режимі розробники технології застосовували заходи, які засновані на співвідношенні часу передачі кадру мінімальної довжини і часу обернення (PDV).

Мінімальний розмір кадру був збільшений (без урахування преамбули) з 64 до 512 байтів або до 4096 бітів. Відповідно, час обороту також можна було збільшити до 4095 бітових інтервалів, що робить допустимим діаметр мережі близько 200 м при використанні одного повторювача.

Для збільшення довжини кадру до потрібної в новій технології величини мережевий адаптер повинен доповнити поле даних до довжини 448 байтів так званим розширенням, що є полем, заповненим нулями. Формально мінімальний розмір кадру не змінився, він як і раніше дорівнює 64 байтам або 512 бітам, але це пояснюється тим, що поле розширення розташовується після поля контрольної суми кадру FCS. Відповідно значення цього поля не включається в контрольну суму і не враховується при вказанні довжини поля даних в полі довжини. Поле розширення є просто розширенням сигналу несучої частоти, необхідним для коректного виявлення колізій.

Для скорочення накладних витрат при використанні дуже довгих кадрів для передачі коротких повідомлень розробники стандарту дозволили кінцевим вузлам передавати декілька кадрів підряд. Такий режим одержав назву режиму пульсацій. Станція може передати підряд декілька кадрів із загальною довжиною не більше 65 536 бітів або 8192 байти. Якщо станції потрібно передати декілька невеликих кадрів, то вона може не доповнювати перший кадр до розміру 512 байтів за рахунок поля розширення, а передавати декілька кадрів підряд до вичерпання межі в 8192 байти (у що межу входять всі байти кадру, зокрема преамбула, заголовок, дані і контрольна сума). Межа 8192 байти називається довжиною пульсації. Якщо станція почала передавати кадр і межу довжини пульсації досягнуто на

середині кадру, то кадр дозволяється передати до кінця. Збільшення "сумі-щеного" кадру до 8192 байтів затримує доступ до середовища інших станцій, але при швидкості 1000 Мбіт/с ця затримка неістотна.

3.1.2.2 Специфікації фізичного середовища стандарту 802.3z

У стандарті 802.3z визначені 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 передачі даних по традиційному для комп'ютерних мереж багатомодовому волоконно-оптичному кабелю стандарт визначає 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, що працюють на довжині хвилі 1300 нм, хоча при цьому максимальна довжина кабелю зменшується, оскільки загасання багатомодового оптоволокна на хвилі 850 м більш ніж в два рази вище, ніж на хвилі 1300 нм. Проте можливість здешевлення надзвичайно важлива для такої в цілому дорогої технології, як Gigabit Ethernet.

Для багатомодового оптоволокна стандарт 802.3z 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 може використовувати тільки багатомодовий кабель, при цьому його максимальна довжина складає близько 500 м.

Для специфікації 1000Base-LX як джерело випромінювання завжди застосовується напівпровідниковий лазерний діод з довжиною хвилі 1300 нм. Специфікація 1000Base-LX може 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 доходити до декількох десятків кілометрів).

Як середовище передавання даних в специфікації 1000-CX визначений екранований збалансований мідний кабель з хвилевим опором 150 Ом. Максимальна довжина сегменту складає всього 25 м, тому це рішення підходить для з'єднання устаткування, розташованого в одній кімнаті.

3.1.2.3 Gigabit Ethernet на крученій парі категорії 5

Як відомо, кожна пара кабелю категорії 5 має гарантовану смугу пропускання до 100 МГц. Для передавання по такому кабелю даних із швидкістю 1000 Мбіт/с було вирішено організувати паралельне передавання одночасно по всіх 4 парах кабелю.

Це відразу знизило швидкість передавання даних по кожній парі до 250 Мбіт/с. Проте і для такої швидкості необхідно було розробити метод

кодування, який мав би спектр не вище 100 МГц. Наприклад, застосування коду 4B/5B не може вирішити поставлене завдання, оскільки основний внесок в спектр сигналу на такій швидкості у нього вносить частота 155 МГц. Крім того, не потрібно забувати, що кожна нова технологія повинна підтримувати не тільки класичний півдуплексний режим, але і дуплексний режим. На перший погляд здається, що одночасне використання чотирьох пар позбавляє мережу можливості роботи в дуплексному режимі, оскільки не залишається вільних пар для одночасного передавання даних в двох напрямах – від вузла і до вузла.

Для кодування даних був застосований код PAM5, в якому 5 рівнів потенціалу: -2, -1, 0, +1, +2. Тому за один такт по одній парі передається 2,322 біт інформації (log25). Отже, для досягнення швидкості 250 Мбіт/с тактову частоту 250 МГц можна зменшити в 2,322 раза. Розробники стандарту вирішили використовувати декілька вищу частоту, а саме 125 МГц. При цій тактовій частоті код PAM5 має спектр вужчий, ніж 100 МГц, тобто він може бути переданий без спотворень по кабелю категорії 5.

У кожному такті передається не 2,322 × 4 = 9,288 бітів інформації, а 8. Це і дає шукану сумарну швидкість 1000 Мбіт/с. Передавання точно 8 бітів в кожному такті досягається за рахунок того, що при кодуванні інформації використовуються не всі 625 комбінацій коду PAM5, а тільки 256. Комбінації, що залишилися, приймач використовує для контролю інформації, що приймається, і виділення правильних комбінацій на фоні шуму.

Для організації дуплексного режиму розробники специфікації 802.3ab застосували техніку виділення сигналу, що приймається, з сумарного. Два передавачі працюють назустріч один одному у кожній з чотирьох пар в одному і тому ж діапазоні частот (рис. 3.3). Н-подібна схема гібридної розв'язки дозволяє приймачу і передавачу одного і того ж вузла використовувати одночасно кручену пару і для прийому, і для передачі (так само, як і в трансіверах Ethernet на коаксіалі).

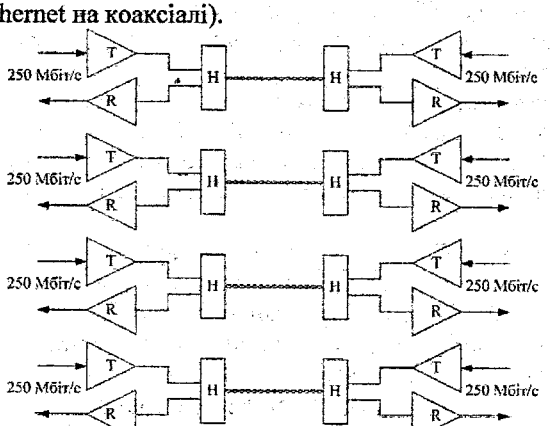

Рисунок 3.3 – Двонаправлена передача по чотирьох парах UTP категорії 5

Для відділення сигналу, що приймається, від власного приймач віднімає з результуючого сигналу відомий йому свій сигнал. Природно, що це непроста операція і для її виконання використовуються спеціальні процесори цифрового сигналу (Digital Signal Processor, DSP).

3.1.3 Мережа Token-Ring

Мережа Token-Ring (маркерне кільце) була запропонована компанією IBM у 1985 році. Вона призначалася для об'єднання в мережу всіх типів комп'ютерів, що випускаються IBM. Уже той факт, що її підтримує компанія IBM, найбільший виробник комп'ютерної техніки, говорить про те, що їй необхідно приділити особливу увагу. Але не менш важливо і те, що Token-Ring є в даний час міжнародним стандартом IEEE 802.5 (хоча між Token-Ring і IEEE 802.5 є незначні відмінності). Це ставить дану мережу на один рівень за статусом з Ethernet.

Мережа Token-Ring має топологію "кільце", хоча зовні вона більше нагадує "зірку". Це пов'язано з тим, що окремі абоненти (комп'ютери) приєднуються до мережі не прямо, а через спеціальні концентратори або багатостанційні пристрої доступу (MSAU або MAU – Multistation Access Unit). Фізично мережа утворить зірково-кільцеву топологію (рис. 3.4).

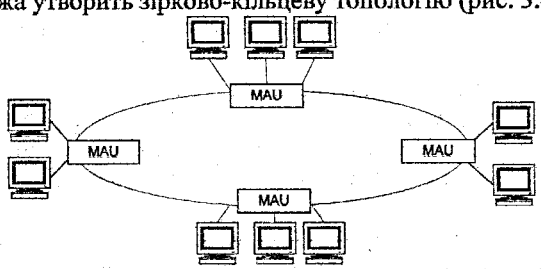

Рисунок 3.4 – Зірково-кільцева топологія мережі Token-Ring

У дійсності ж абоненти поєднуються все-таки в кільце, тобто кожний з них передає інформацію одному сусідньому абоненту, а приймає інформацію від іншого.

Концентратор (MAU) при цьому дозволяє централізувати завдання конфігурації, відключення несправних абонентів, контроль роботи мережі і т.д. Ніякої обробки інформації він не робить.

Для кожного абонента в складі концентратора застосовується спеціальний блок підключення до магістралі (TCU – Trunk Coupling Unit), що забезпечує автоматичне включення абонента в кільце, якщо він підключений до концентратора і справний. Якщо абонент відключається від концентратора або ж він несправний, то блок TCU автоматично відновлює цілісність кільця без участі даного абонента. Спрацьовує TCU за сигналом постійного струму (так званий "фантомний" струм), що приходить від абонента, який бажає включитися в кільце. Абонент може також відключитися від кільця і

провести процедуру самотестування. "Фантомний" струм ніяк не впливає на інформаційний сигнал, тому що сигнал у кільці не має постійної складової.

Концентратор у мережі може бути єдиним, у цьому випадку в кільце замикаються тільки абоненти, підключені до нього. Зовні така топологія виглядає, як "зірка". Якщо ж потрібно підключити до мережі більше восьми абонентів, то кілька концентраторів з'єднуються магістральними кабелями і утворюють зірково-кільцеву топологію.

Кільцева топологія дуже чуттєва до обривів кабелю кільця. Для підвищення живучості мережі у Token-Ring передбачений режим так званого згортання кільця, що дозволяє обійти місце обриву.

У нормальному режимі концентратори з'єднані в кільце двома рівнобіжними кабелями, але передача інформації здійснюється при цьому тільки по одному з них. Основні технічні характеристики класичного варіанта мережі Token-Ring:

- максимальна кількість концентраторів типу IBM 8228 MAU – 12;
- максимальна кількість абонентів у мережі – 96;
- максимальна довжина кабелю між абонентом і концентратором – 45 метрів;
- максимальна довжина кабелю між концентраторами – 45 метрів;
- максимальна довжина кабелю, що з'єднує всі концентратори – 120 метрів;
- швидкість передавання даних – 4 Мбіт/с і 16 Мбіт/с.

Всі наведені характеристики відносяться до випадку використання неекранованої "крученої" пари. Якщо застосовується інше середовище передавання, характеристики мережі можуть відрізнятися. Наприклад, при використанні екранованої "крученої" пари (STP) кількість абонентів може бути збільшена до 260 (замість 96), довжина кабелю – до 100 метрів (замість 45), кількість концентраторів – до 33, а повна довжина кільця, що з'єднує концентратори – до 200 метрів. Якщо використати оптоволоконний кабель, то довжина кільця може бути збільшена до двох кілометрів.

Для передачі інформації в Token-Ring застосовується біфазний код (точніше, його варіант з обов'язковим переходом у центрі бітового інтервалу). Як і в будь-якій зіркоподібній топології, ніяких додаткових заходів із електричного узгодження і зовнішнього заземлення не потрібно. Узгодження виконується апаратурою мережевих адаптерів і концентраторів.

Мережа Token-Ring у класичному варіанті поступається мережі Ethernet як за допустимим розміром, так і за максимальною кількістю абонентів. Що стосується швидкості передавання, то в даний час існують версії Token-Ring з швидкістю 100 Мбіт/с (High Speed Token-Ring, HSTR) і з 1000 Мбіт/с (Gigabit Token-Ring). Однак на відміну від Ethernet мережа Token-Ring значно краще тримає високий рівень навантаження (більш 30–40%) і забезпечує гарантований час доступу. Це необхідно, наприклад, у

мережах виробничого призначення, у яких затримка реакції на зовнішній вплив може призвести до серйозних аварій.

У мережі Token-Ring використовується класичний маркерний метод доступу, тобто по кільцю постійно циркулює маркер, до якого абоненти можуть приєднувати свої пакети даних. Звідси випливає така важлива перевага даної мережі, як відсутність конфліктів, але є і недоліки, зокрема необхідність контролю цілісності маркера і залежність функціонування мережі від кожного абонента (у випадку несправності абонент обов'язково повинен бути виключений з кільця).

Кожен абонент мережі (його мережевий адаптер) повинен виконувати такі функції:

- виявлення помилок передавання;
- контроль конфігурації мережі (відновлення мережі при виході з ладу того абонента, що передує йому в кільці);
- контроль численних тимчасових співвідношень, прийнятих у мережі.

У мережі Token-Ring передбачено також використання мостів і комутаторів. Вони застосовуються для поділу великого кільця на кілька кільцевих сегментів, що мають можливість обміну пакетами між собою. Це дозволяє знизити навантаження на кожен сегмент і збільшити частку часу, надану кожному абонентові.

У результаті можна сформувати розподілене кільце, тобто об'єднання декількох кільцевих сегментів одним великим магістральним кільцем (рис. 3.5) або ж зірково-кільцеву структуру з центральним комутатором, до якого підключені кільцеві сегменти (рис. 3.6).

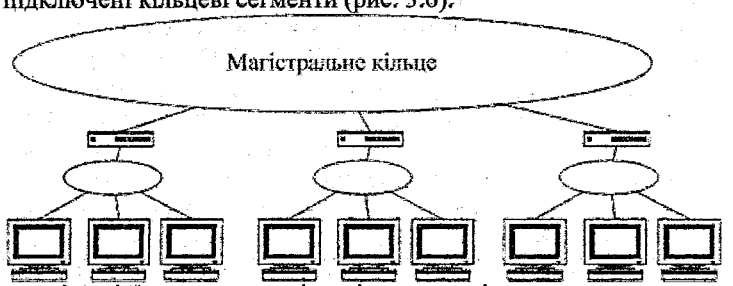

Рисунок 3.5 – Об'єднання сегментів магістральним кільцем за допомогою мостів

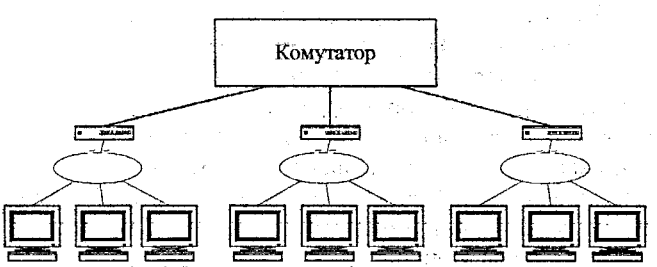

Рисунок 3.6 – Об'єднання сегментів центральним комутатором

3.1.4 Мережа FDDI

Мережа FDDI (від англійського Fiber Distributed Data Interface, оптоволоконний розподілений інтерфейс даних) – це одна з новітніх розробок стандартів локальних мереж. Стандарт FDDI був запропонований Американським національним інститутом стандартів ANSI (специфікація ANSI X3T9.5). Потім був прийнятий стандарт ISO 9314, що відповідає специфікаціям ANSI. Рівень стандартизації мережі досить високий.

На відміну від інших стандартних локальних мереж, стандарт FDDI споконвічно орієнтувався на високу швидкість передачі (100 Мбіт/с) і на застосування найперспективнішого оптоволоконного кабелю. Тому в даному випадку розроблювачі не були обмежені рамками старих стандартів, що орієнтувалися на низькі швидкості й електричний кабель.

Вибір оптоволокна як середовища передавання визначив такі переваги нової мережі, як висока завадозахищеність, максимальна секретність передавання інформації і прекрасна гальванічна розв'язка абонентів. Висока швидкість передачі, що у випадку оптоволоконного кабелю досягається набагато простіше, дозволяє вирішувати багато задач, що є недоступними для менш швидких мереж, наприклад, передавання зображень у реальному масштабі часу. Крім того, оптоволоконний кабель легко вирішує проблему передавання даних на відстань декількох кілометрів без ретрансляції, що дозволяє будувати великі за розмірами мережі, що охоплюють навіть цілі міста і мають при цьому всі переваги локальних мереж (зокрема, низький рівень помилок). Усе це визначило популярність мережі FDDI, хоча вона поширена ще не так широко, як Ethernet і Token-Ring.

За основу стандарту FDDI був узятий метод маркерного доступу, передбачений міжнародним стандартом IEEE 802.5 (Token-Ring). Несуттєві відмінності від цього стандарту визначаються необхідністю забезпечити високу швидкість передавання інформації на великі відстані. Топологія мережі FDDI – це кільце – топологія, що найбільше підходить для оптоволоконного кабелю. У мережі застосовується два різнонаправлених оптоволоконних кабелі, один із яких звичайно знаходиться в резерві, однак таке рішення дозволяє використовувати і повнодуплексне передавання інформації (одночасно в двох напрямках) з подвоєною ефективною швидкістю в 200 Мбіт/с (при цьому кожний із двох каналів працює на швидкості 100 Мбіт/с). Застосовується і зірково-кільцева топологія з концентраторами, включеними в кільце (як у Token-Ring).

Основні технічні характеристики мережі FDDI.

- Максимальна кількість абонентів мережі – 1000.
- Максимальна довжина кільця мережі – 20 кілометрів.
- Максимальна відстань між абонентами мережі – 2 кілометри.
- Середовище передавання – багатомодовий оптоволоконний кабель (можливе застосування електричної крученої пари).
- Метод доступу – маркерний.

• Швидкість передавання інформації – 100 Мбіт/с (200 Мбіт/с для дуплексного режиму передавання).

Стандарт FDDI має значні переваги порівняно з усіма розглянутими раніше мережами. Наприклад, мережа Fast Ethernet, що має таку ж пропускну здатність 100 Мбіт/с, не може зрівнятися з FDDI за допустимими розмірами мережі. До того ж маркерний метод доступу FDDI забезпечує на відміну від CSMA/CD гарантований час доступу і відсутність конфліктів при будь-якому рівні навантаження.

Обмеження на загальну довжину мережі в 20 км пов'язане не з затуханням сигналів у кабелі, а з необхідністю обмеження часу повного проходження сигналу по кільцю для забезпечення гранично допустимого часу доступу. А от максимальна відстань між абонентами (2 км при багатомодовому кабелі) визначається саме затуханням сигналів у кабелі (воно не повинно перевищувати 11 дБ). Передбачена також можливість застосування одномодового кабелю, і в цьому випадку відстань між абонентами може досягати 45 кілометрів, а повна довжина кільця – 200 кілометрів.

Стандарт FDDI для досягнення високої гнучкості мережі передбачає включення в кільце абонентів двох типів:

• абоненти (станції) класу А (абоненти подвійного підключення, DAS – Dual-Attachment Stations) підключаються до обох (внутрішніх і зовнішніх) кілець мережі. При цьому реалізується можливість обміну зі швидкістю до 200 Мбіт/с або резервування кабелю мережі (при ушкодженні основного кабелю використовується резервний). Апаратура цього класу застосовується в найкритичніших з погляду швидкодії частинах мережі.

• абоненти (станції) класу В (абоненти одинарного підключення, SAS – Single-Attachment Stations) підключаються тільки до одному (зовнішньому) кільцю мережі. Вони простіші і дешевші, порівняно з адаптерами класу А, але не мають їхніх можливостей. В мережу вони можуть включатися тільки через концентратор або обхідний комутатор, що відключає їх у випадку аварії.

Приклад конфігурації мережі FDDI поданий на рис. 3.7.

FDDI визначає чотири типи портів абонентів:

• порт А призначений тільки для пристроїв подвійного підключення, його вхід підключається до первинного (зовнішнього) кільця, а вихід – до вторинного (внутрішнього) кільця;

• порт В призначений тільки для пристроїв подвійного підключення, його вхід підключається до вторинного (внутрішнього) кільця, а вихід – до первинного (зовнішнього) кільця. Порт А звичайно з'єднується з портом В, а порт В – з портом А;

• порт М (Master) призначений для концентраторів і з'єднує два концентратори між собою або концентратор з абонентом при одному кільці. Порт М, як правило, з'єднується з портом S;

• порт S (Slave) призначений тільки для пристроїв одинарного підключення (концентраторів і абонентів). Порт S звичайно з'єднується з портом M.

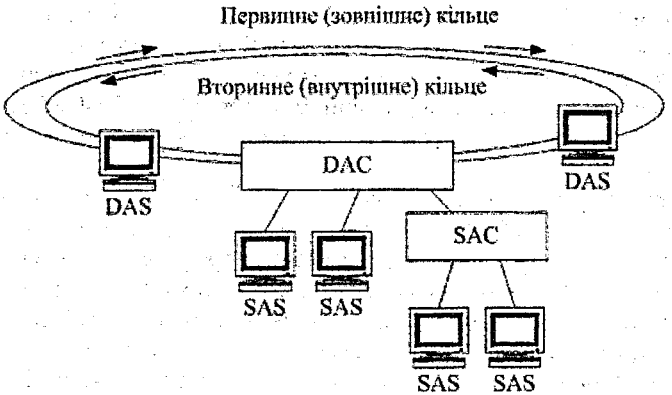

Рисунок 3.7 – Приклад конфігурації мережі FDDI

На відміну від методу доступу, запропонованого стандартом IEEE 802.5, у FDDI застосовується так зване множинне передавання маркера. Якщо у випадку мережі Token-Ring новий (вільний) маркер передається абонентом тільки після повернення до нього його пакета, то в FDDI новий маркер передається абонентом відразу ж після закінчення передавання ним пакета (подібно тому, як це робиться при методі ETR у мережі Token-Ring).

Для правильної роботи мережі затримка проходження сигналу по кільцю повинна бути обмежена. Так, у випадку максимальної довжини кільця 200 км і максимальній кількості абонентів 1000 повний час затримки не повинен перевищувати 1,617 мс.

Формати маркера (рис. 3.8) і пакета (рис. 3.9) мережі FDDI трохи відрізняються від форматів, що використовуються у мережі Token-Ring.

Преамбула (8 байтів)	Початковий розділювач (1 байт)	Керування (1 байт)	Кінцевий розділювач (1 байт)	Статус пакету (1 байт)

Рисунок 3.8 – Формат маркера FDDI

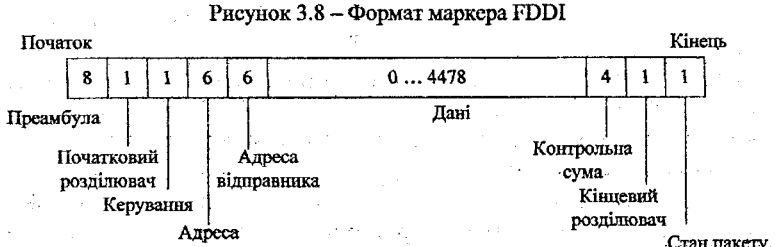

Рисунок 3.9 – Формат пакета FDDI

Призначення полів.

• Преамбула (Preamble) використовується для синхронізації. Спочатку вона містить 64 біти, але абоненти, через які проходить пакет, можуть змінювати її розмір.

• Початковий розділювач (SD – Start Delimiter) виконує функцію ознаки початку кадру.

• Байт управління (FC – Frame Control) містить інформацію про пакет (розмір поля адреси, синхронна/асинхронна передача, тип пакета – службовий або інформаційний, код команди).

• Адреси приймача і джерела (SA – Source Address і DA – Destination Address) можуть бути шестибайтовими (аналогічно Ethernet і Token-Ring) або двобайтовими.

• Поле даних (Info) має змінну довжину (від 0 до 4478 байтів). У службових (командних) пакетах поле даних має нульову довжину.

• Поле контрольної суми (FCS – Frame Check Sequence) містить 32-бітову циклічну контрольну суму пакета (CRC).

• Кінцевий розділювач (ED – End Delimiter) визначає кінець кадру.

• Байт стану пакета (FS – Frame Status) містить у собі біт виявлення помилки, біт розпізнавання адреси і біт копіювання (аналогічно Token-Ring).

Але незважаючи на очевидні переваги FDDI дана мережа не одержала значного поширення, що пов'язано головним чином з високою вартістю її апаратури. Основна область застосування FDDI зараз – це базові, опорні (Backbone) мережі, що поєднують кілька мереж. Застосовується FDDI також для з'єднання могутніх робочих станцій або серверів, що вимагають високошвидкісного обміну. Передбачається, що мережа Fast Ethernet може потіснити FDDI, однак переваги оптоволоконного кабелю, маркерного методу керування і рекордний допустимий розмір мережі ставлять у даний час FDDI поза конкуренцією. А в тих випадках, коли вартість апаратури має вирішальне значення, можна на некритичних ділянках застосовувати версію FDDI на основі крученої пари (TPDDI). До того ж вартість апаратури FDDI може сильно зменшиться з ростом об'єму її випуску.

3.2 Стандарти глобальних мереж

3.2.1 Мережі Frame Relay

Мережі Frame Relay набагато краще підходять для передавання пульсуючого трафіка комп'ютерних мереж порівняно з мережами X.25. Ця перевага виявляється тільки тоді, коли лінії зв'язку наближаються за якістю до ліній зв'язку локальних мереж, а для глобальних ліній така якість звичайно досяжна тільки при використанні волоконно-оптичних кабелів.

Технологія Frame Relay була спочатку стандартизована комітетом CCITT (ITU-T) як одна із служб мереж ISDN. Технологія ISDN є першим

широкомасштабним проектом створення всесвітньої універсальної мережі, що надає всі основні види послуг телефонних мереж і мереж передавання даних. На жаль, цей амбітний проект не досяг поставленої мети, і сьогодні мережі нового покоління будуються вже на основі інших технологій, зокрема IP. В той самий час в ході реалізації проекту були досягнуті декілька хоч і не таких глобальних, але проте дуже важливих цілей. До них можна зарахувати і створення технології Frame Relay, яка сьогодні є вже незалежною від ISDN технологією.

У рекомендаціях I.122, що вийшли в світ в 1988 році, послуги з передавання даних входили до числа додаткових послуг пакетного режиму ISDN. При перегляді цих рекомендацій в 1992-93 рр. з'явилися стандарти на дві нові послуги: Frame Relay і Frame Switching. Різниця між ними полягає в тому, що Frame Switching забезпечує гарантовану доставку кадрів, а Frame Relay – доставку коли можна.

Проста і в той же час ефективна для волоконно-оптичних ліній зв'язку технологія Frame Relay відразу привернула увагу провідних телекомунікаційних компаній і організацій із стандартизації. У її становленні і стандартизації крім CCITT (ITU-T) активну участь брали форум із ретрансляції кадрів (Frame Relay Forum, FRF) і комітет T1S1 інституту ANSI. Технологія ж Frame Switching так і залишилася всього лише стандартом, що ніколи не мав значного поширення.

Стандарти Frame Relay, підготовлені і ITU-T/ANSI, і FRF, визначають два типи віртуальних каналів – постійні (PVC) і комутовані (SVC). Це відповідає потребам користувачів, оскільки для з'єднань, по яких трафік передається майже завжди, більше підходять постійні канали, а для з'єднань, потрібних тільки декілька годин в місяць, – комутовані. Проте виробники устаткування Frame Relay і постачальники послуг мереж Frame Relay почали з підтримки тільки постійних віртуальних каналів. Це значно збіднило технологію. Устаткування, що підтримує комутовані віртуальні канали, з'явилося на ринку з великою затримкою. Саме тому технологія Frame Relay часто асоціюється тільки з постійними віртуальними каналами.

3.2.1.1 Стек протоколів Frame Relay

Стек протоколів Frame Relay влаштований досить просто. Розробники технології Frame Relay, враховуючи високу якість каналів зв'язку на оптичному волокні, що з'явилися в кінці 80-х років, порахували можливим не включати в протоколи стека функції забезпечення надійності. Якщо ж, не дивлячись на малу вірогідність такої події, помилка все ж таки відбувається, то технологія Frame Relay ігнорує цю ситуацію, залишаючи роботу із відновлення загублених або спотворених кадрів протоколам верхніх рівнів, таким як TCP.

На рис. 3.10 показаний стек протоколів технологій Frame Relay і Frame Switching в тому вигляді, в якому вони описані в рекомендаціях

ITU-T. Протоколи шару керування виконують роботу із встановлення віртуального з'єднання, а протоколи шару даних передають кадри по вже встановленому віртуальному з'єднанню.

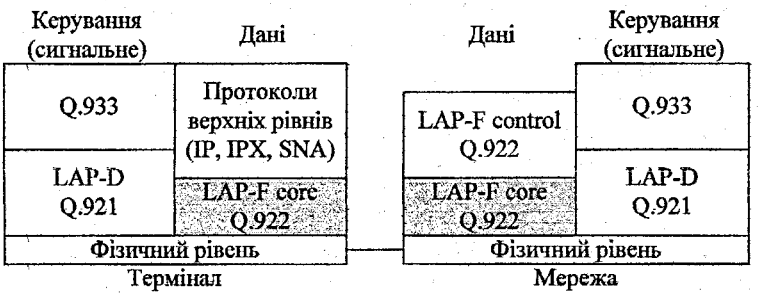

Рисунок 3.10 – Стек протоколів технологій Frame Relay і Frame Switching

На канальному рівні мереж Frame Relay працює протокол LAP-F (Link Access Procedure for Frame mode bearer services), названий в рекомендаціях ITU-T абревіатурою Q.922. Існує дві версії цього протоколу.

Протокол LAP-F core є тією "робочою конячкою", яка трудиться у всіх мережах Frame Relay. Цей протокол забезпечує мінімум засобів, що дозволяють побудувати мережу Frame Relay. В цьому випадку мережа надаватиме тільки послуги постійних віртуальних каналів.

Протокол LAP-F control, що забезпечує відновлення кадрів за алгоритмом ковзного вікна, необхідний для того, щоб мережа надавала послуги Frame Switching (комутації кадрів).

Обидва протоколи (LAP-F core і LAP-F control) відносяться до протоколів канального рівня, забезпечуючи передавання кадрів між двома сусідніми комутаторами.

Комутатори мережі повинні підтримувати два протоколи шару керування – на канальному рівні LAP-D (який називається також Q.921) і Q.933 на мережевому. Протокол LAP-D в мережах Frame Relay забезпечує надійне передавання сигнальних кадрів між сусідніми комутаторами.

Протокол Q.933 використовує адреси кінцевих вузлів, між якими встановлюється віртуальний канал. Ці адреси звичайно задаються у форматі телефонних адрес, відповідних стандарту E.164. Адреса складається з 15 десяткових цифр, які діляться, як і звичайні телефонні номери, на поля коду країни (від 1 до 3 цифр), коду міста і номера абонента. До адреси додається до 40 цифр підадреси, які потрібні для нумерації термінальних пристроїв, якщо у одного абонента їх декілька.

Протокол автоматичного складання таблиць маршрутизації для технології Frame Relay не визначений, тому може використовуватися фірмовий протокол виробника устаткування чи ж таблиці можуть складатися спеціалістом.

Технологію Frame Relay найчастіше відносять до технологій канального рівня, ставлячи як головні процедури передавання призначених для користувача даних і опускаючи процедури встановлення віртуального каналу, які виконуються із залученням протоколу мережевого рівня.

По віртуальних каналах Frame Relay можуть передаватися дані різних протоколів. Специфікація RFC 1490 визначає методи інкапсуляції в кадри Frame Relay пакетів мережевих протоколів, таких як IP і IPX, протоколів локальних мереж, наприклад Ethernet, а також протоколу SNA.

Структура кадру протоколу LAP-F наведена на рис. 3.11.

Поле DLCI (Data Link Connection Identifier – ідентифікатор з'єднання рівня каналу даних) складається з 10 бітів, що дозволяє задіювати до 1024 віртуальних з'єднань. Поле DLCI може займати і більше число розрядів – цим керують ознаки розширення адреси EAO і EA1 (абревіатура EA якраз і означає Extended Address, тобто розширена адреса). Якщо біт розширення адреси встановлений в нуль, то ознака називається EAO і означає, що в наступному байті є продовження поля адреси, а якщо біт розширення адреси рівний 1, то поле називається EA1 і означає закінчення поля адреси. Десятирозрядний формат DLCI є основним, але при використанні трьох байтів для адресації поле DLCI має довжину 16 бітів, а при використанні чотирьох байтів – 23 біти.

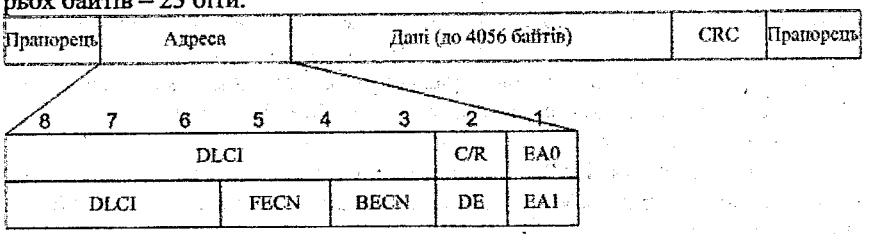

Рисунок 3.11 – Формат кадру LAP-F

Стандарти Frame Relay розподіляють DLCI-адреси між користувачами і мережею таким чином:

0 – використовується для віртуального каналу локального інтерфейсу адміністрування (LMI);

1-15 – зарезервовані;

16-991 – використовуються абонентами для нумерації каналів PVC і SVC;

992-1007 – використовуються мережевою транспортною службою;

1008-1022 – зарезервовані;

1023 – використовується для керування канальним рівнем.

Таким чином, в будь-якому інтерфейсі Frame Relay для кінцевих пристроїв користувача відводиться 976 DLCI-адрес. Поле даних може мати розмір 4056 байтів.

Поле C/R переносить ознаку команди (Command) або відповіді (Response). Ця ознака є успадкованою і використовується в протокольних операціях HDLC.

Поля DE, FECN і BECN використовуються протоколом для керування трафіком і підтримки заданої якості обслуговування віртуального каналу.

3.2.2 Високошвидкісні мережі

Швидкодія мережі Fast Ethernet і інших мереж, що працюють на швидкості в 100 Мбіт/с, у даний час задовольняє вимоги більшості задач, але в ряді випадків навіть її виявляється недостатньо. Особливо в тих ситуаціях, коли необхідно підключати до мережі сучасні високопродуктивні сервери або будувати мережі з великою кількістю абонентів, що вимагають високої інтенсивності обміну. Наприклад, усе ширше застосовується мережеве оброблення тривимірних динамічних зображень. Швидкість комп'ютерів безупинно зростає, вони забезпечують усе вищі темпи обміну з зовнішніми пристроями. У результаті мережа може виявитися найбільш слабким місцем системи, і її пропускна здатність буде основним стримувальним фактором у збільшенні швидкодії.

Роботи з досягнення швидкості передавання в 1 Гбіт/с (1000 Мбіт/с) в останні роки ведуться досить інтенсивно декількома компаніями. Однак, швидше за все, найбільш перспективною виявиться мережа Gigabit Ethernet. Це пов'язано, насамперед, з тим, що перехід на неї виявиться найбезболіснішим, найдешевшим і психологічно прийнятним. Адже мережа Ethernet і її версія Fast Ethernet сьогодні далеко випереджають усіх своїх конкурентів за об'ємом продаж і поширеністю у світі.

Мережа Gigabit Ethernet – це природний, еволюційний шлях розвитку концепції, закладеної в стандартній мережі Ethernet. Безумовно, вона успадковує і всі недоліки своїх прямих попередників, наприклад, негарантований час доступу до мережі. Однак величезна пропускна здатність призводить до того, що завантажити мережу до тих рівнів, коли цей фактор стає визначальним, досить важко. Зате збереження спадковості дозволяє досить просто з'єднувати сегменти Ethernet, Fast Ethernet і Gigabit Ethernet у мережу, і, найголовніше, переходити до нових швидкостей поступово, вводячи гігабітні сегменти тільки на самих напружених ділянках мережі. (До того ж далеко не скрізь така висока пропускна здатність дійсно необхідна).

Номенклатура сегментів мережі Gigabit Ethernet у даний час містить у собі такі типи:

- 1000BASE-SX – сегмент на мультимодовому оптоволоконному кабелі з довжиною хвилі світлового сигналу 850 нм (довжиною до 500 метрів). Використовуються лазерні передавачі.
- 1000BASE-LX – сегмент на мультимодовому (довжиною до 500 метрів) і одномодовому (довжиною до 2000 метрів) оптоволоконному кабелі з

довжиною хвилі світлового сигналу 1300 нм. Використовуються лазерні передавачі.

• 1000BASE-CX – сегмент на екранованій крученій парі (довжиною до 25 метрів).

• 1000BASE-T (стандарт IEEE 802.3ab) – сегмент на зчетвереній неекранованій "скрученій" парі категорії 5 (довжиною до 100 метрів). Використовується п'ятирівневе кодування (PAM-5), причому в повнодуплексному режимі передавання ведеться по кожній парі в двох напрямках.

Спеціально для мережі Gigabit Ethernet запропонований метод кодування переданої інформації 8B/10B, побудований по тому ж принципу, що і код 4B/5B мережі FDDI (крім 1000BASE-T). Таким чином, восьми бітам інформації, яку потрібно передати, ставиться у відповідність 10 бітів, переданих по мережі. Цей код дозволяє зберегти самосинхронізацію, легко виявляти факт передачі, але не вимагає подвоєння смуги пропускання, як у випадку манчестерського коду.

Мережа Gigabit Ethernet, насамперед, знаходить застосування в мережах, що поєднують комп'ютери великих підприємств, які розташовуються в декількох будинках. Вона дозволяє за допомогою відповідних комутаторів, що перетворюють швидкості передавання, забезпечити канали зв'язку з високою пропускною здатністю між окремими частинами складної мережі або лінії зв'язку комутаторів із швидкодіючими серверами.

Імовірно, у ряді випадків Gigabit Ethernet буде витісняти оптоволоконну мережу FDDI, яка в даний час все частіше використовується для об'єднання в мережу декількох локальних мереж, у тому числі і Ethernet. Правда, FDDI може зв'язувати абонентів, що знаходяться на великих відстанях один від одного, але за швидкістю передавання інформації Gigabit Ethernet суттєво перевершує FDDI.

На теперішньому етапі розвитку мережевих технологій постає питання створення більш швидкісних технологій. До таких технологій відносять мережі типу 10 Gigabit Ethernet. Слід відмітити, що найдоцільнішим є використання оптичного волокна як середовища передавання.

Стандарт IEEE 802.3ae 10-Gigabit Ethernet включає послідовний інтерфейс 10GBASE-S (S – short, означає коротку довжину хвилі), а це передбачає використання багатомодового волокна на довжині хвилі 850 нм (довжиною до 300 м). Основними факторами, які говорять на користь такого стандарту, є популярність невеликих розділень та низька вартість інтерфейсів відносно інших.

3.2.3 Мережа ATM

3.2.3.1 Технологія ATM

Технологія ATM (Asynchronous Transfer Mode – асинхронний режим передавання) була розроблена як єдиний універсальний транспорт для

нового покоління мереж з інтегрованим обслуговуванням, які називаються також широкосмуговими мережами ISDN (Broadband ISDN, B-ISDN). Технологія ATM стала другою спробою побудови універсальної мережі після невдачі ISDN. На відміну від технології Frame Relay, яка спочатку призначалася тільки для передавання еластичного комп'ютерного трафіка, цілі розробників ATM були значно ширші.

Необхідно відразу підкреслити, що велика частина цих цілей була досягнута, і з середини 90-х років ATM є працюючою технологією, що забезпечує найповнішу і послідовну підтримку параметрів QoS для користувачів мережі. Крім того, ATM, як і будь-яка технологія на основі техніки віртуальних каналів, надає широкі можливості для розв'язань завдань інжинірингу трафіка.

Розробку стандартів ATM здійснює велика кількість виробників телекомунікаційного устаткування і операторів зв'язку, що входять у форум ATM, а також комітети ITU-T і ANSI.

Не дивлячись на очевидні успіхи технології ATM, яка працює на багатьох магістралях найбільших операторів зв'язку, досвід експлуатації показав і її обмеження. Так, технологія ATM не витіснила всю решту технологій і не стала єдиною транспортною технологією телекомунікаційних мереж, хоча у середині 90-х років здавалося, що завдяки очевидним технологічним достоїнствам ATM це неминуче повинно статися. Теоретично ATM може використовуватися безпосередньо прикладним рівнем протоколів, тобто мережа може працювати без протоколів IP і TCP/UDP. ATM має для цього багато якостей: підтримка всіх видів трафіка, масштабованість і власний складний протокол маршрутизації. Проте це можливо тільки в тому випадку, коли мережа є технологічно однорідною та всі мережі всіх постачальників послуг підтримують ATM. Очевидно, такий підхід суперечить принципу складених мереж, згідно з яким кожна мережа може підтримувати власну транспортну технологію, а загальний мережевий рівень об'єднує ці мережі в єдину мережу.

Тому на практиці протокол IP, що почав домінувати на мережевому рівні у середині 90-х років, як і раніше використовується для об'єднання мереж, а ATM залишається однією з технологій, на основі якої працюють багато мереж, створюючих складену мережу.

3.2.3.2 Основні принципи технології ATM

Мережа ATM має класичну ієрархічну структуру територіальної мережі – кінцеві станції з'єднуються індивідуальними лініями зв'язку з комутаторами нижнього рівня, які, у свою чергу, з'єднуються з комутаторами вищих рівнів. Комутатори ATM з моменту народження цієї технології підтримують як канали PVC, так і канали SVC. Для мереж ATM призначений протокол маршрутизації PNNI (Private NNI – приватний інтерфейс NNI), за допомогою якого комутатори можуть будувати таблиці маршрутизації

автоматично, причому з урахуванням вимог інжинірингу трафіка. У публічних мережах ATM звичайно використовуються адреси в стандарті E.164, що робить простою взаємодію цих мереж з телефонними мережами. Адреси ATM мають ієрархічну структуру, подібну до телефонних номерів або IP-адрес, яка забезпечує масштабованість мереж ATM до будь-якого рівня, навіть загальносвітового.

У великих мережах застосовується поняття агрегованого віртуального шляху, який об'єднує віртуальні канали, що мають в мережі ATM загальний маршрут між початковим і кінцевим вузлами або загальну частину маршруту між деякими двома комутаторами мережі. Ця властивість також забезпечує масштабованість мереж ATM, оскільки дозволяє суттєво скоротити кількість віртуальних з'єднань, які підтримує магістральний комутатор, а значить, підвищити ефективність його роботи.

Стандарт ATM не вводить свої специфікації на реалізацію фізичного рівня. Тут він грунтується на технології SDH/SONET, приймаючи її ієрархію швидкостей. Відповідно до цього початкова швидкість доступу користувача мережі – це швидкість STM-1/OC-3 – 155 Мбіт/с. Магістральне устаткування ATM працює і на вищих швидкостях STM-4 – 622 Мбіт/с і STM-16 – 2,5 Гбіт/с. Існує також устаткування ATM, яке підтримує швидкості PDH, такі як 2 або 34/45 Мбіт/с.

Проте всі перераховані характеристики технології ATM не свідчать про те, що це якась "особлива" технологія, а швидше подають її як достатньо розвинену, але в той самий час достатньо типову технологію глобальних мереж, засновану на техніці віртуальних каналів.

Для досягнення цієї властивості розробники ATM ретельно проаналізували всі типи трафіка і провели його класифікацію. ATM розбиває весь трафік на 5 класів. Перші чотири класи – це трафік типових додатків, які відрізняються стійким набором вимог до затримок і втрат пакетів, а також тим, що генерують трафік з постійною (CBR) або змінною (VBR) бітовою швидкістю. П'ятий клас X зарезервований для унікальних додатків, набір характеристик і вимог яких не відноситься ні до одного з перших чотирьох класів.

Проте на яку кількість класів не розбивається існуючий трафік, принципове завдання від цього не змінюється – потрібно знайти рішення для успішного співіснування в одному каналі і еластичних, і чутливих до затримок класів трафіка. Вимоги цих класів майже завжди суперечать один одному. Однією з таких суперечностей є вимога до розміру комірки.

Еластичний трафік виграє від збільшення розміру комірки, оскільки при цьому зменшуються накладні витрати на службову інформацію. На прикладі Ethernet видно, що швидкість передавання призначеної для користувача інформації може змінюватися майже в два рази при зміненні розміру поля даних від його мінімальної величини 46 байтів до максимальної 1500 байтів. Звичайно, розмір комірки не може збільшуватися до нескінченності, оскільки при цьому втрачається сама ідея комутації паке-

тів. Проте для еластичного трафіка при сучасному рівні швидкостей розмір комірки в декілька тисяч байтів є цілком прийнятним.

Навпаки, чутливий до затримок трафік обслуговується краще при використанні комірок невеликого розміру в декілька десятків байтів. При застосуванні великих комірок починають виявлятися два небажані ефекти:

- очікування низькопріоритетних комірок в чергах;
- затримка пакетизації.

Час очікування комірки в черзі можна зменшити, якщо обслуговувати комірки чутливого до затримок трафіка в пріоритетній черзі. Проте якщо розмір комірки може змінюватися в широкому діапазоні (наприклад, від 29 до 4500 байтів, як в технології FDDI), то навіть при наданні чутливим до затримок комірок вищого пріоритету обслуговування в комутаторах час очікування комп'ютерного пакета може все одно опинитися неприпустимо високим. Наприклад, пакет в 4500 байтів передаватиметься у вихідний порт на швидкості 2 Мбіт/с (максимальна швидкість роботи порту комутатора Frame Relay) 18 мс. При поєднанні трафіка за цей час необхідно через той самий порт передати 144 виміри голосу. Переривати передавання пакета в мережах небажано, оскільки при розподіленому характері мережі накладні витрати на сповіщення сусіднього комутатора про переривання пакета, а потім – про відновлення передавання пакета з перерваного місця виявляються дуже великими.

Затримка пакетизації – це час, протягом якого перший вимір голосу чекає моменту остаточного формування пакета і відправки його по мережі. Важливо відзначити, що затримка пакетизації не залежить від бітової швидкості протоколу, вона залежить тільки від частоти роботи кодека і розміру поля даних комірки. Це відрізняє її від затримки очікування, яка знижується із зростанням бітової швидкості.

Комірка ATM в 53 байти з полем даних 48 байтів є результатом компромісу між вимогами еластичного і чутливого до затримок трафіків. Іншими словами, можна сказати, що компроміс був досягнутий між телефоністами і IT-спеціалістами – перші наполягали на розмірі поля даних 32 байти, а другі – 64 байти. Невеликий і фіксований розмір комірки ATM дав йому спеціальну назву – комірка.

При розмірі поля даних 48 байтів одна комірка ATM звичайно переносить 48 вимірів голосу, які робляться з інтервалом в 125 мкс. Тому перший вимір повинен чекати приблизно 6 мс, перш ніж комірка буде відправлена по мережі. Саме з цієї причини телефоністи боролися за зменшення розміру комірки, оскільки 6 мс – це затримка, близька до межі, за якою починаються порушення якості передавання голосу. При виборі розміру комірки 32 байти затримка пакетизації склала б 4 мс, що гарантувало б якісніше передавання голосу. А прагнення комп'ютерних фахівців збільшити поле даних до 64 байтів цілком зрозуміло – при цьому підвищується корисна швидкість передавання даних. Надмірність службових даних при

використанні 48-байтового поля даних складає 10%, а при використанні 32-байтового поля даних вона відразу підвищується до 16%.

Для пакету, що складається з 53 байтів, при швидкості в 155 Мбіт/с час передачі комірки на вихідний порт складає менше 3 мкс. Отже ця затримка не дуже істотна для трафіка, пакети якого повинні передаватися кожні 125 мкс.

Щоб пакети містили адресу вузла призначення і в той самий час відсоток службової інформації не перевищував розмір поля даних пакета, в технології ATM застосований стандартний для WAN приймання – передавання комірок відповідно до техніки віртуальних каналів. Загальна довжина номера віртуального каналу складає 24 біти, що цілком достатньо для обслуговування великої кількості віртуальних з'єднань кожним портом комутатора глобальної мережі ATM.

Потрібно відзначити, що використання в ATM комірок такого невеликого розміру, що створюють відмінні умови для якісного обслуговування чутливого до затримок трафіка, має і зворотну сторону. Платнею за якість є високий рівень навантаження на ATM-комутатори при роботі на високих швидкостях. Нагадаємо, що об'єм роботи, який виконує комутатор або маршрутизатор будь-якої технології, прямо пропорційний кількості оброблюваних за одиницю часу пакетів або комірок. Очевидно, що використання комірок розмірів з полем даних 48 байтів приводить до колосального зростання об'єму роботи для ATM-комутатора порівняно з, наприклад, комутатором Ethernet, що працює з кадрами 1500 байтів. Через цю обставину ATM-комутатори довго не могли перевершити межу швидкості інтерфейсів в 622 Мбіт/с і порівняно недавно стали підтримувати інтерфейси 2,5 Гбіт/с.

Вибір для передачі даних будь-якого типу невеликого осередку фіксованого розміру ще не вирішує проблему поєднання різнорідних трафіків в одній мережі, а тільки створює передумови для її вирішення. Для повного вирішення цього завдання технологія ATM використовує і розвиває ідеї резервування пропускної спроможності і якості обслуговування, реалізовані в технології Frame Relay.

У технології ATM для кожного класу трафіка визначено набір кількісних параметрів, які в додатку повинні задаватися. Наприклад, для трафіка класу A необхідно вказати постійну швидкість, з якою додаток посилатиме дані в мережу, а для трафіка класу B – максимально можливу швидкість, середню швидкість і максимально можливу пульсацію. Для голосового трафіка можна не тільки вказати на важливість синхронізації між передавачем і приймачем, але і кількісно задати верхні межі затримок і варіації затримок комірок.

У технології ATM підтримується такий набір основних кількісних параметрів для трафіка віртуального з'єднання:

- пікова швидкість передавання комірок (Peak Cell Rate, PCR);
- середня швидкість передавання комірок (Sustained Cell Rate, SCR);

- мінімальна швидкість передавання комірок (Minimum Cell Rate, MCR);
- максимальна величина пульсацій (Maximum Burst Size, MBS);
- частка втрачених комірок (Cell Loss Ratio, CLR);
- затримка передавання комірок (Cell Transfer Delay, CTD);
- варіація затримок комірок (Cell Delay Variation, CDV).

Параметри швидкості вимірюються в осередках за секунду, максимальна величина пульсацій – в комірках, а тимчасові параметри – в секундах. Максимальна величина пульсацій визначає кількість комірок, яка може передати додаток з піковою швидкістю при заданій середній швидкості. Частка втрачених комірок є відношенням втрачених комірок до загальної кількості відправлених комірок по даному віртуальному з'єднанню. Оскільки віртуальні з'єднання є дуплексними, то для кожного напряму з'єднання можуть бути задані різні значення параметрів.

У технології ATM прийнятий не зовсім традиційний підхід до трактування якості обслуговування (QoS). Звичайно якість обслуговування трафіка характеризується параметрами пропускної спроможності (тут це RCR, SCR, MCR, MBS), параметрами затримок пакетів (CTD і CDV) а також параметрами надійності передавання пакетів (CLR). У ATM швидкісні характеристики називають параметрами трафіка, але їх не включають в число параметрів якості обслуговування. Параметрами QoS в ATM є тільки CTD, CDV і CLR. Мережа прагне забезпечити такий рівень обслуговування, щоб підтримувалися необхідні значення і для параметрів трафіка, і для затримок осередків, і для частки втрачених комірок.

Угода між додатком і мережею ATM називається контрактом трафіка. Основною його відмінністю від угод, використовуваних в мережах Frame Relay, є вибір одного з декількох певних класів трафіка, для якого разом з параметрами пропускної спроможності трафіка можуть указуватися параметри затримок комірок, а також параметр надійності доставки комірок. У мережі Frame Relay клас трафіка один, і він характеризується тільки параметрами пропускної спроможності.

Якщо для додатку не критична підтримка параметрів пропускної спроможності і QoS, то він може відмовитися від задання цих параметрів, вказавши в запиті на встановлення з'єднання ознаку обслуговування з максимальними зусиллями. Такий тип трафіка одержав назву трафіка з невизначеною бітовою швидкістю (UBR).

Після визначення необхідного трафіка, який відноситься до певного віртуального з'єднання, в мережі ATM працює декілька протоколів і служб, що забезпечують потрібну якість обслуговування. Для трафіка UBR мережа виділяє такі ресурси, які в даний момент не зайняті віртуальними з'єднаннями, що замовили певні параметри якості обслуговування.

3.2.3.3 Стек протоколів ATM

Стек протоколів ATM показаний на рис. 3.12, а розподіл протоколів між кінцевими вузлами і комутаторами ATM – на рис. 3.13. Стек протоколів ATM відповідає нижнім рівням семирівневої моделі ISO/OSI і включає рівень адаптації ATM, власне рівень ATM і фізичний рівень. Прямої відповідності між рівнями протоколів технології ATM і рівнями моделі OSI немає.

<table>
<tr><td colspan="3">Верхні рівні мережі</td></tr>
<tr><td rowspan="2">Рівні адаптації ATM (AAL1-5)</td><td rowspan="2">Підрівень конвергенції (CS)</td><td>Загальна частина підрівня конвергенції</td></tr>
<tr><td>Специфічна частина для сервісу</td></tr>
<tr><td colspan="2">Підрівень сегментації та реассемблювання (SAR)</td></tr>
<tr><td colspan="3">Рівень ATM
(маршрутизація пакетів, мультиплексування, керування потоком, обробка пріоритетів)</td></tr>
<tr><td rowspan="2">Фізичний рівень</td><td colspan="2">Підрівень узгодження передавання</td></tr>
<tr><td colspan="2">Підрівень, що залежить від фізичного середовища</td></tr>
</table>

Рисунок 3.12 – Структура стека протоколів ATM

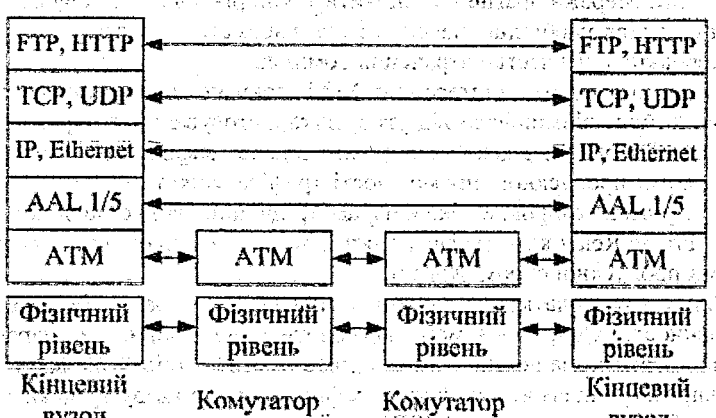

Рисунок 3.13 – Розподіл протоколів між вузлами і комутаторами мережі ATM

3.2.3.4 Протокол ATM

Протокол ATM виконує комутацію за номером віртуального з'єднання, який в технології ATM розбитий на дві частини:

- ідентифікатор віртуального шляху (Virtual Path Identifier, VPI);
- ідентифікатор віртуального каналу (Virtual Channel Identifier, VCI).

Крім розв'язання цієї основної задачі протокол ATM виконує ряд функцій із контролю за дотриманням контракту трафіка з боку користувача мережі, маркування комірок-порушників, відкидання комірок-порушників при перевантаженні мережі, а також керування потоком комірок для підвищення продуктивності мережі (природно, при дотриманні умов передавання трафіка для всіх віртуальних з'єднань).

Формат комірок протоколу ATM поданий на рис. 3.14.

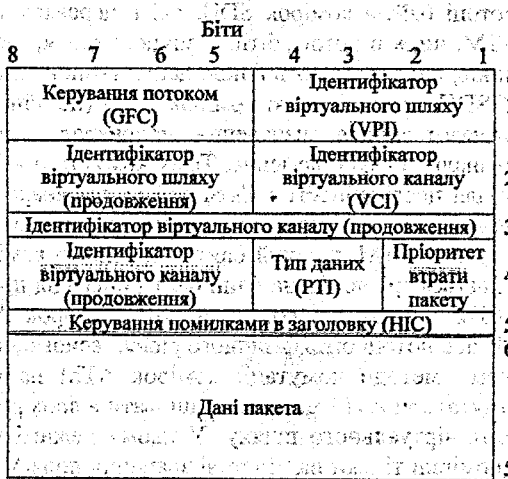

Рисунок 3.14 – Формат ATM-комірки

Поле узагальненого керування потоком (Generic Flow Control, GFC) використовується тільки при взаємодії кінцевого вузла і першого комутатора мережі. В даний час його точні функції не визначені.

Поля ідентифікатора віртуального шляху (VPI) і ідентифікатора віртуального каналу (VCI) займають відповідно 1 і 2 байти. Ці поля задають номер віртуального з'єднання, поділений на старшу (VPI) і молодшу (VCI) частини.

Поле ідентифікатора типу даних (Payload Type Identifier, PTI) складається з 3 бітів і задає тип даних, переносимих коміркою, – призначені для користувача або такі, що керують (наприклад, керівники встановленням віртуального з'єднання). Крім того, один біт цього поля використовується для вказання про перевантаження в мережі. Це біт EFCI (Explicit Forward Congestion Identifier – прямий явний ідентифікатор перевантаження), який відіграє ту ж роль, що і біт FECN в технології Frame Relay, тобто передає інформацію про перевантаження напрямку потоку даних.

Поле пріоритету втрати комірки (Cell Loss Priority, CLP) відіграє в даній технології ту ж роль, що і поле DE в технології Frame Relay – в ньому

комутатори ATM відзначають комірки, які порушують угоди про параметри якості обслуговування, щоб видалити їх при перевантаженнях мережі.

Поле керування помилками в заголовку (Header Error Control, HEC) містить контрольну суму, обчислену для заголовка комірки. Контрольна сума обчислюється за допомогою техніки корегувальних кодів Хеммінга, тому вона дозволяє не тільки виявляти помилки, але і виправляти всі одиночні помилки, а також деякі подвійні. Крім того, поле HEC забезпечує не тільки виявлення і виправлення помилок в заголовку, але і знаходження межі початку комірки в потоці байтів комірок SDH, які є переважним фізичним рівнем технології ATM, чи ж в потоці бітів фізичного рівня, заснованого на комірках. Покажчиків, що дозволяють в полі даних комірки STS-n (STM-n) технології SONET/SDH виявляти межі комірок ATM (подібних тим покажчикам, які використовуються для визначення, наприклад, меж віртуальних контейнерів підканалів T1/E1), не існує. Тому комутатор ATM обчислює контрольну суму для послідовності з п'яти байтів, що знаходяться в полі даних комірки STM-n, і, якщо обчислена контрольна сума говорить про коректність заголовка осередку ATM, перший байт стає межею комірки. Якщо ж це не так, то відбувається зрушення на один байт і операція продовжується. Отже, технологія ATM виділяє асинхронний потік комірок ATM в синхронних комірках SDH або потоці бітів фізичного рівня, заснованого на комірках.

Розглянемо методи комутації комірок ATM на основі пари чисел VPI/VCI. Комутатори ATM можуть працювати в двох режимах.

Комутація віртуального шляху. У цьому режимі комутатор виконує просування комірки тільки на підставі значення поля VPI, а значення поля VCI він ігнорує. Звичайно так працюють магістральні комутатори територіальних мереж. Вони доставляють комірки з однієї призначеної для користувача мережі в іншу на підставі тільки старшої частини номера віртуального каналу, що відповідає ідеї агрегації адрес. В результаті один віртуальний шлях відповідає цілому набору віртуальних каналів, комутованих як єдине ціле.

Комутація віртуального каналу. Після доставки комірки до локальної мережі ATM її комутатори починають комутувати комірки як поля VPI, так і поля VCI, але при цьому їм вистачає для комутації тільки молодшої частини номера віртуального з'єднання, так що фактично вони працюють з VCI, залишаючи VPI без зміни. Цей режим і називається режимом комутації віртуального каналу.

Для створення комутованого віртуального каналу в технології ATM використовується підхід, який є аналогічним підходу в мережі ISDN – для встановлення з'єднання розроблений окремий протокол Q.2931, який умовно можна віднести до мережевого рівня. Цей протокол багато в чому схожий на протоколи Q.931 і Q.933 (навіть номером), але в нього внесені зміни, пов'язані з наявністю декількох класів трафіка і додаткових параметрів якості обслуговування. Протокол Q.2931 опирається на достатньо склад-

ний протокол канального рівня SSCOP, який забезпечує надійне передавання пакетів Q.2931 в своїх комірках. У свою чергу, протокол SSCOP працює поверх протоколу AAL5, який необхідний для розбиття кадрів SSCOP на ATM-комірки і складання цих комірок в кадри при доставці кадру SSCOP в комутатор призначення.

Віртуальні з'єднання, утворені за допомогою протоколу Q.2931, бувають симплексними (однонаправленими) і дуплексними.

Протокол Q.2931 дозволяє також встановлювати двоточкові віртуальні з'єднання і віртуальні з'єднання з одним відправником і декількома одержувачами. Перший випадок підтримується у всіх технологіях, заснованих на віртуальних каналах, а другий характерний для технології ATM і є аналогом групової розсилки з одним провідним (передавальним) вузлом. При встановленні з'єднання з одним відправником і декількома одержувачами провідним вважається вузол, який є ініціатором цього з'єднання. Спочатку цей вузол встановлює віртуальне з'єднання всього з одним вузлом, а потім шляхом спеціального виклику додає до з'єднання по одному новому члену. Провідний вузол стає вершиною дерева з'єднання, а решта вузлів – листям цього дерева. Повідомлення, які посилає провідний вузол, приймають все листя з'єднання, але повідомлення, які посилає який-небудь лист (якщо з'єднання дуплексне), приймає тільки провідний вузол.

Пакети протоколу Q.2931, призначені для встановлення комутованого віртуального каналу, мають ті ж назви і те ж призначення, що і пакети протоколу Q.933, розглянуті при вивченні технології Frame Relay, але структура їхніх полів інша – інша адреса кінцевого вузла в комутаторах ATM 20-байт.

При роботі в публічних мережах використовується адреса стандарту E.164. Адреса має гнучкий формат і може ділитися на частини для забезпечення ієрархічної маршрутизації між мережами і підмережами.

Останні 6 байтів адреси займає поле ідентифікатора кінцевої системи (End System Identifier, ESI), яке має смисл MAC-адреси вузла ATM, причому формат його також відповідає формату MAC-адреси.

ESI-адреса присвоюється кінцевому вузлу на підприємстві-виготівнику відповідно до правил IEEE, тобто три перші байти містять код підприємства, а інші три – порядковий номер, за унікальність якого відповідає дане підприємство.

Кінцевий вузол при підключенні до комутатора ATM виконує так звану процедуру реєстрації. При цьому кінцевий вузол повідомляє комутатору свою ESI-адресу, а комутатор повідомляє кінцевому вузлу старшу частину адреси, тобто номер мережі, в якій працює вузол.

Окрім адресної частини пакет CALL SETUP протоколу Q.2931, за допомогою якого кінцевий вузол запитує встановлення віртуального з'єднання, включає також частини, що описують параметри трафіка і вимоги QoS. Під час надходження такого пакета комутатор повинен проаналізувати ці параметри і вирішити, чи досить у нього вільних ресурсів для об-

слуговування нового віртуального з'єднання. Якщо так, то нове віртуальне з'єднання приймається, і комутатор передає пакет CALL SETUP далі відповідно до адреси призначення і таблиці маршрутизації, а якщо ні, то запит відкидається.

3.2.4 Безпровідні мережі

Стандарт містить такі специфікації:

- 802.11 – початковий стандарт WLAN. Підтримує передавання даних зі швидкостями від 1 до 2 Мбіт/с;
- 802.11a – високошвидкісний стандарт WLAN для частоти 5 ГГц. Підтримує швидкість передавання даних 54 Мбіт/с;
- 802.11b – стандарт WLAN для частоти 2,4 ГГц. Підтримує швидкість передавання даних 11 Мбіт/с;
- 802.11e – встановлює вимоги якості запиту, необхідної для всіх радіоінтерфейсів IEEE WLAN;
- 802.11f – описує порядок зв'язку між рівнозначними точками доступу;
- 802.11g – установлює додаткову техніку модуляції для частоти 2,4 ГГц. Призначений для забезпечення швидкостей передавання даних до 54 Мбіт/с;
- v802.11h – описує керування спектром частоти 5 ГГц для використання в Європі й Азії;
- 802.11i – виправляє існуючі проблеми безпеки в областях аутентифікації і протоколів шифрування.

Устаткування безпровідних мереж містить у собі точки безпровідного доступу (Access Point) і безпровідні адаптери для кожного абонента.

Точки доступу виконують роль концентраторів, що забезпечують зв'язок між абонентами і між собою, а також функцію мостів, що здійснюють зв'язок з кабельною локальною мережею і з Інтернет. Декілька близько розташованих точок доступу утворять зону доступу Wi-Fi, у межах якої всі абоненти, оснащені безпровідними адаптерами, одержують доступ до мережі. Такі зони доступу (Hotsppt) створюються в місцях масового скупчення людей: в аеропортах, студентських містечках, бібліотеках, магазинах, бізнесах-центрах і т.д.

Кожна точка доступу може обслуговувати декількох абонентів, але чим більше абонентів, тим менша ефективна швидкість передавання для кожного з них. Метод доступу до мережі – CSMA/CD. Мережа будується за стільниковим принципом. У мережі передбачений механізм роумінгу, тобто підтримується автоматичне підключення до точки доступу і переключення між точками доступу при переміщенні абонентів, хоча жорстких правил роумінгу стандарт не встановлює.

Оскільки радіоканал не забезпечує високого ступеня захисту від прослуховування, у мережі Wi-Fi використовується спеціальний вбудований механізм захисту інформації. Він включає засоби і процедури аутенти-

фікації для протидії несанкціонованому доступу до мережі і шифрування для запобігання перехопленню інформації.

Стандарт IEEE 802.11b був прийнятий у 1999 р. і завдяки орієнтації на освоєний діапазон 2,4 ГГц завоював найбільшу популярність у виробників устаткування. Як базова радіотехнологія в ньому використовується метод DSSS (Direct Sequence Spread Spectrum), що відрізняється високою стійкістю до спотворення даних, завад, у тому числі навмисних, а також до їх виявлення. Оскільки устаткування 802.11b, що працює на максимальній швидкості 11 Мбіт/с, має менший радіус дії, ніж на нижчих швидкостях, то стандартом 802.11b передбачене автоматичне зниження швидкості при погіршенні якості сигналу. Пропускна здатність (теоретична 11 Мбіт/с, реальна – від 1 до 6 Мбіт/с) відповідає вимогам більшості додатків. Відстані – до 300 метрів, але звичайно – до 160 метрів.

Стандарт IEEE 802.11a розрахований на роботу в частотному діапазоні 5 ГГц. Швидкість передавання даних до 54 Мбіт/с, тобто приблизно в п'ять разів швидше мереж 802.11b. Це найбільший широкосмуговий стандарт із сімейства стандартів 802.11. Визначено три обов'язкові швидкості – 6, 12 і 24 Мбіт/с і п'ять необов'язкових – 9, 18, 36, 48 і 54 Мбіт/с. Як метод модуляції сигналу прийнято ортогональне частотне мультиплексування (OFDM). Його найсуттєвіша відмінність від методів DSSS полягає в тому, що OFDM допускає рівнобіжне передавання корисного сигналу одночасно по декількох частотах діапазону, у той час як технології розширення спектра передають сигнали послідовно. У результаті підвищується пропускна здатність каналу і якість сигналу. До недоліків 802.11a відносяться велика споживана потужність радіопередавачів для частот 5 ГГц, а також менший радіус дії (близько 100 м). Крім того, пристрій для 802.11a дорожчий, але згодом ціновий розрив між продуктами 802.11b і 802.11a буде зменшуватися.

Стандарт IEEE 802.11g є новим стандартом, що регламентує метод побудови WLAN, що функціонує в неліцензованому частотному діапазоні 2,4 ГГц. Завдяки застосуванню технології ортогонального частотного мультиплексування (OFDM) максимальна швидкість передавання даних у безпровідних мережах IEEE 802.11g складає 54 Мбіт/с. Устаткування, що підтримує стандарт IEEE 802.11g, наприклад точки доступу безпровідних мереж, забезпечує одночасне підключення до мережі безпровідних пристроїв стандартів IEEE 802.11g і IEEE 802.11b. Стандарт 802.11g є розвитком 802.11b і обернено сумісний з 802.11b. Теоретично 802.11g має переваги двох своїх попередників. У числі переваг 802.11g треба відзначити низьку споживчу потужність, великі відстані (до 300 м) і високу проникну здатність сигналу.

Специфікація IEEE 802.11d встановлює універсальні вимоги до фізичного рівня (процедури формування каналів, псевдовипадкові послідовності частот і т.д.). Стандарт 802.11d поки що знаходиться в стадії розробки.

Специфікація IEEE 802.11e дозволить створювати мультисервісні безпровідні мережі для корпорацій і індивідуальних споживачів. При збереженні повної сумісності з діючими стандартами 802.11a і b вона розширить їхню функціональність за рахунок обслуговування потокових мультимедіа-даних і гарантованої якості послуг. Поки що затверджено попередній варіант специфікацій 802.11e.

Специфікація IEEE 802.11f описує протокол обміну службовою інформацією між точками доступу (Inter-Access Point Protocol, IAPP), що необхідно для побудови розподілених безпровідних мереж передачі даних. Знаходиться в стадії розробки.

Специфікація IEEE 802.11h передбачає можливість доповнення діючими алгоритмами ефективного вибору частот для всіх можливих безпровідних мереж, а також засобами керування використанням спектра, контролю випромінюваної потужності і генерації відповідних звітів.

Отже, безпровідні мережі досить перспективні. Незважаючи на свої недоліки, головний з яких – незахищеність середовища передавання, вони забезпечують просте підключення абонентів, не потребуюче кабелів, мобільність, гнучкість і масштабуємість мережі. До того ж немаловажливим є те, що користувачам не потрібні знання мережевих технологій.

3.3 Методика і початкові етапи проектування мережі

Будь-яке проектування, як відомо, – це сильно спрощене моделювання дійсності, що ще не настала. Саме тому передбачити всі можливі фактори, врахувати всі потреби, що можуть виникнути в майбутньому, практично неможливо. Отже, навіть найдетальніші посібники з проектування мають не занадто велику цінність.

Однак загальні підходи до проектування корпоративних комп'ютерних мереж усе-таки можуть бути сформульовані, деякі корисні принципи такого проектування пропонуються і з успіхом використовуються. Не варто тільки сприймати їх як щось придатне для будь-яких практичних випадків і враховуюче всі можливі ситуації.

На рис. 3.15 наведено зразкову послідовність етапів і варіанти вибору при проектуванні локальної мережі. Узагалі, проблема вибору одного з численних варіантів при проектуванні локальної мережі (ЛМ) є основною для даного розділу. Вибір затруднює необхідність обліку безлічі вимог, іноді суперечливих (наприклад, забезпечення високих технічних характеристик мережі при доступній вартості), а також наполеглива, часом агресивна реклама окремих рішень. Останнє часто відноситься до новітніх варіантів мережевого устаткування і/або програмного забезпечення, що аж ніяк не єдине доступне за ціною і не завжди має значні переваги по технічними характеристиками перед випробуваними варіантами.

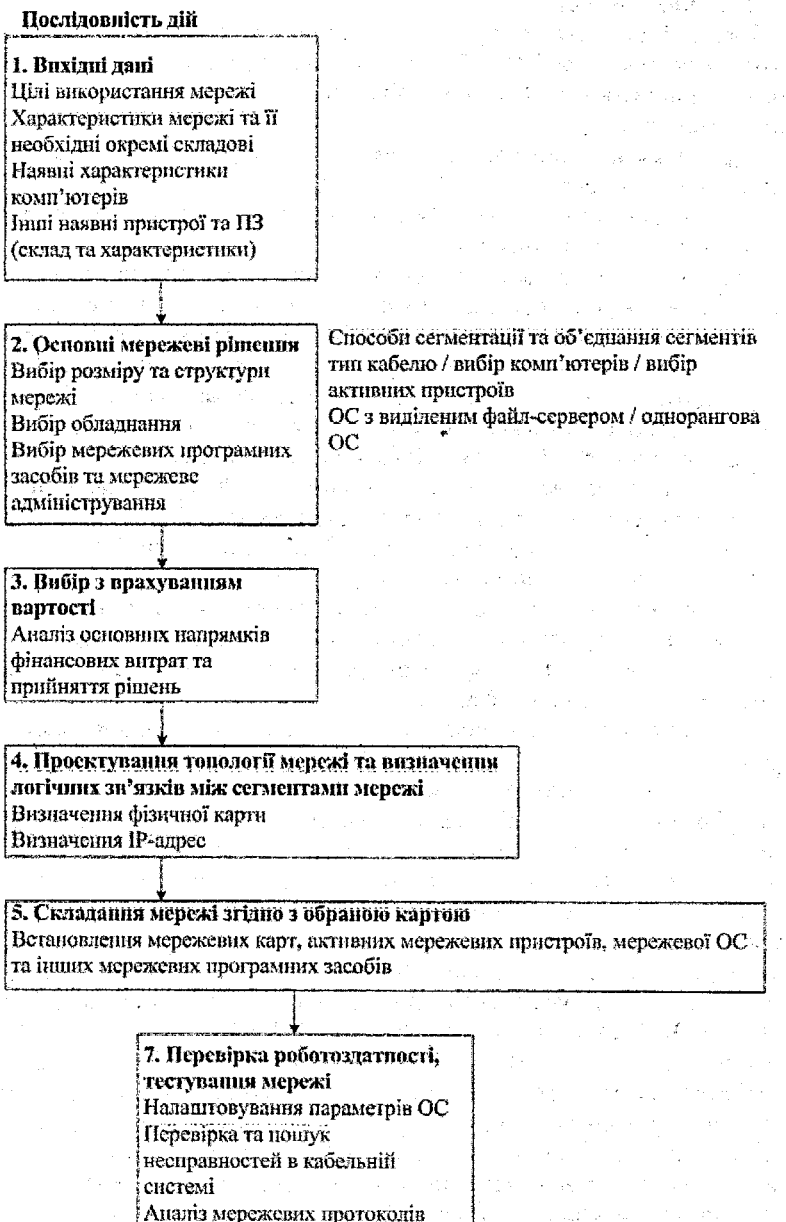

Рисунок 3.15 – Рекомендована послідовність етапів і варіанти вибору при проектуванні локальної мережі

3.3.1 Вихідні дані

Важливість цього етапу пов'язана як з необхідністю упорядкування вимог до створюваної ЛМ і її окремих складових для забезпечення можливості прийняття в майбутньому зважених конкретних рішень, так і з її обґрунтуванням.

При створенні нової мережі для якого-небудь підприємства бажано враховувати такі фактори:

- необхідний розмір мережі (у даний час, у найближчому майбутньому і за прогнозом на перспективу);
- структура, ієрархія й основні частини мережі (по підрозділах підприємства, а також по кімнатах, поверхах і будинках підприємства);
- основні напрямки й інтенсивність інформаційних потоків у мережі (у даний час, у найближчому майбутньому й у далекій перспективі). Характер переданої по мережі інформації (дані, оцифрована мова, зображення), що безпосередньо позначається на необхідній швидкості передавання (до декількох сотень Мбіт/с для телевізійних зображень високої чіткості);
- технічні характеристики устаткування (комп'ютерів, адаптерів, кабелів, репітерів, концентраторів, комутаторів) і його вартість;
- можливості прокладання кабельної системи в приміщеннях і між ними, а також міри забезпечення цілісності кабелю;
- обслуговування мережі і контроль її безвідмовності і безпеки;
- вимоги до програмних засобів щодо допустимих розмірів мережі, швидкості, гнучкості, розмежування прав доступу, вартості, щодо можливостей контролю обміну інформацією і т.д.;
- необхідність підключення до глобальної або до інших локальних мереж.

На початку проектування мережі необхідно провести повну "інвентаризацію" наявних комп'ютерів і їхнього програмного забезпечення, а також периферійних пристроїв (принтерів, сканерів і т.д.). Це дозволить при організації мережі виключити непотрібне дублювання (устаткування і програмне забезпечення тепер можуть бути поділюваними ресурсами), а також поставити задачі модернізації (апгрейда) як апаратних, так і програмних засобів. Для коректного визначення характеристик комп'ютерів доцільно використовувати спеціальні діагностичні програми або вбудовані програми ОС (наприклад, в ОС Windows Millennium це програма "Інформація про систему" з розділу службових програм і програма "Система" з панелі керування). Варто вибирати такі варіанти програм, що забезпечують одержання правильних даних ("старі" діагностичні програми можуть невірно вказати тип процесора і версію ОС), а також збереження даних у файлі (це особливо важливо при великому числі комп'ютерів). Крім того, варто приділити увагу наявності вбудованої мережевої карти або мережевого контролера на системній платі, а також типу підтримуваних ними мережевих стандартів (як правило, підтримується мережа Ethernet на

крученій парі, але принципово знати її різновид – 10/100/1000 Мбіт/с). Не всі характеристики комп'ютерів, що важливі при їхньому об'єднанні в мережу, можуть бути визначені описаними вище способами. Із супровідної документації до комп'ютера або після розкриття системного блоку можна і потрібно визначити число і тип вільних слотів (роз'ємів) розширення, а також максимальну потужність блоку живлення. Це необхідно для оцінки можливості установлення в комп'ютер нових плат.

3.3.2 Вибір розміру і структури мережі

Під розміром мережі в даному випадку розуміється як кількість поєднуваних у мережу комп'ютерів, так і відстані між ними. Треба чітко уявляти собі, скільки комп'ютерів (мінімально і максимально) потрібно підключити до мережі. При цьому необхідно залишати можливість для подальшого збільшення кількості комп'ютерів у мережі, хоча б відсотків на 20–50.

Необхідна довжина ліній зв'язку мережі також відіграє не малу роль у проектуванні мережі. Наприклад, якщо відстані дуже великі, може знадобитися використання додаткового устаткування. До того ж зі збільшенням відстані різко зростає значимість захисту ліній зв'язку від зовнішніх електромагнітних завад. Від відстані залежить і швидкість передавання інформації з мережі (вибір між Ethernet і Fast Ethernet). Доцільно при виборі відстаней закладати невеликий запас (хоча б відсотків 10) для обліку непередбачених обставин. Перебороти обмеження по довжині іноді можна шляхом вибору структури мережі, розбивки її на окремі частини.

3.3.3 Вибір конфігурації мережі

При виборі конфігурації мережі Ethernet, що складається із сегментів різних типів, виникає багато питань, пов'язаних насамперед з максимально допустимим розміром (діаметром) мережі і максимально можливим числом різних елементів. Мережа буде роботоздатною тільки в тому випадку, коли затримка поширення сигналу в ній не перевищуватиме граничного значення. Це визначається обраним методом керування обміном CSMA/CD, заснованим на виявленні і дозволі колізій.

Насамперед слід зазначити, що для одержання складних конфігурацій Ethernet з окремих сегментів застосовуються проміжні пристрої двох основних типів:

- репітерні концентратори (хаби) – це набір репітерів і ніяк логічно не розділяють сегменти, підключені до них;
- комутатори передають інформацію між сегментами, але не передають конфлікти із сегмента на сегмент.

При виборі й оцінці конфігурації Ethernet використовуються дві основні моделі.

Перша модель формулює набір правил, яких необхідно дотримуватись проектувальникові мережі при з'єднанні окремих комп'ютерів і сегментів:

1. Репітер або концентратор, підключений до сегмента, знижує на одиницю максимально допустиме число абонентів, що підключаються до сегмента;
2. Повний шлях між двома будь-якими абонентами повинний містити в собі не більше п'яти сегментів, чотирьох концентраторів (репітерів) і двох трансіверів (MAU);
3. Якщо шлях між абонентами складається з п'яти сегментів і чотирьох концентраторів (репітерів), то кількість сегментів, до яких підключені абоненти, не повинна перевищувати трьох, а інші сегменти повинні просто зв'язувати між собою концентратори (репітери). Це вже згадуване "правило 5-4-3";
4. Якщо шлях між абонентами складається з чотирьох сегментів і трьох концентраторів (репітеров), то повинні виконуватися такі умови:
   - максимальна довжина оптоволоконного кабелю сегмента 10BASE-FL, що з'єднує між собою концентратори (репітери), не повинна перевищувати 1000 метрів;
   - максимальна довжина оптоволоконного кабелю сегмента 10BASE-FL, що з'єднує концентратори (репітери) з комп'ютерами, не повинна перевищувати 400 метрів;
   - до всіх сегментів можуть підключатися комп'ютери.

При виконанні перерахованих правил можна бути упевненим, що мережа буде роботоздатною. Ніяких додаткових розрахунків у даному випадку не потрібно. Вважається, що дотримання даних правил гарантує допустиме значення затримки сигналу в мережі.

Друга модель, застосовувана для оцінки конфігурації Ethernet, заснована на точному розрахунку тимчасових характеристик обраної конфігурації мережі. Ця модель іноді дозволяє вийти за межі твердих обмежень моделі 1. Застосування моделі 2 необхідно в тому випадку, коли розмір проектованої мережі близький до максимально допустимого.

У моделі 2 використовуються дві системи розрахунків:

- перша система припускає обчислення подвійного (кругового) часу проходження сигналу по мережі і порівняння його з максимально допустимим значенням;
- друга система перевіряє допустимість величини одержуваного міжпакетного тимчасового інтервалу, міжпакетної щілини (IPG – InterPacket Gap) у мережі.

При цьому обчислення в обох системах розрахунків ведуться для найгіршого випадку, для шляху максимальної довжини, тобто для такого шляху переданого по мережі пакета, що вимагає для свого проходження максимального часу.

При першій системі розрахунків виділяються три типи сегментів:

- початковий сегмент, відповідає початкові шляху максимальної довжини;

• кінцевий сегмент розташований наприкінці шляху максимальної довжини;

• проміжний сегмент входить у шлях максимальної довжини, але не є ні початковим, ні кінцевим.

Під структурою мережі розуміється спосіб поділу мережі на частині (сегменти), а також спосіб з'єднання цих сегментів між собою. Мережа підприємства може містити в собі робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі можуть використовуватися репітери, репітерні концентратори, комутатори, мости і маршрутизатори. Причому в ряді випадків вартість цього об'єднавчого устаткування може навіть перевищувати вартість комп'ютерів, мережевих адаптерів і кабелю, тому вибір структури мережі винятково важливий.

В ідеалі структура мережі повинна відповідати структурі будинку або комплексу будинків підприємства. Робочі місця групи співробітників, що займаються однією задачею (наприклад, бухгалтерія, відділ продажів, інженерна група), повинні розміщатися в одній або в поруч розташованих кімнатах. Тоді можна комп'ютери цих співробітників об'єднати в один сегмент, у єдину робочу групу й установити поблизу їхніх кімнат сервер, з яким вони будуть працювати, а також концентратор або комутатор, що зв'язує всі їхні машини. Точно так само робочі місця співробітників підрозділу, що займаються комплексом близьких задач, краще розташувати на одному поверсі будинку, що суттєво спростить їхнє об'єднання в сегмент і подальше його адміністрування. На цьому ж поверсі зручно розташувати комутатори, маршрутизатори і сервери, з якими працює даний підрозділ.

Як і в інших випадках, при виборі структури розумно залишати можливості для подальшого розвитку мережі. Наприклад, краще використовувати комутатори або маршрутизатори з кількістю портів, трохи більшою, ніж потрібно в даний момент (хоча б на 10–20 відсотків). Це дозволить при необхідності легко включити в мережу один або кілька сегментів. Адже будь-яке підприємство завжди прагне до зростання (часом зовсім дарма), і це зростання не повинно щораз призводити до необхідності проектувати мережу підприємства заново.

Нехай невелике підприємство займає три поверхи, на кожному по п'ять кімнат, і містить у собі три підрозділи по три групи. У цьому випадку можна побудувати мережу в такий спосіб (рис. 3.16).

• Робочі групи займають по 1–3 кімнати, їхні комп'ютери об'єднані між собою репітерними концентраторами. Концентратор може використовуватися один на кімнату, один на групу або один на весь поверх. Концентратор доцільно розташувати в приміщенні, до якого має доступ мінімальна кількість співробітників.

• Підрозділи займають окремий поверх. Усі три мережі робочих груп кожного підрозділу поєднуються комутатором, а для зв'язку з мережами

інших підрозділів використовується маршрутизатор. Комутатор разом з одним з концентраторів краще розташовувати в окремій кімнаті.

• Загальна мережа підприємства включає три сегменти мереж підрозділів, об'єднаних маршрутизатором. Цей самий маршрутизатор може використовуватися для підключення до глобальної мережі.

• Сервери робочих груп розташовуються в кімнатах робочих груп, сервери підрозділів – на поверхах підрозділів.

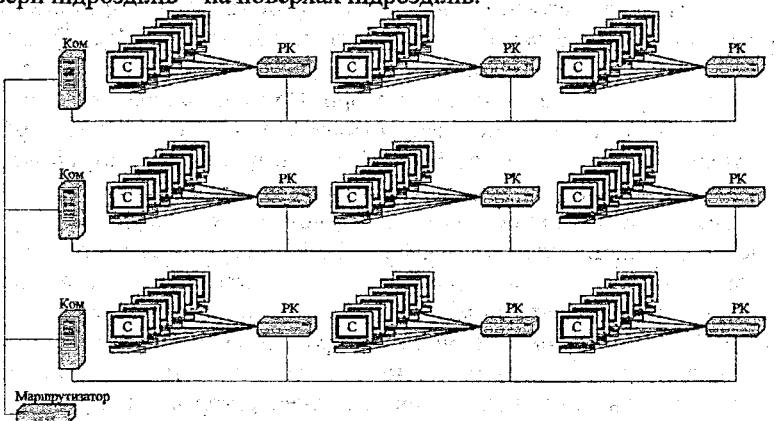

Рисунок 3.16 – Структура мережі підприємства (С – сервери робочих груп, РК – репітерні концентратори, Ком – комутатори)

У розглянутій ситуації області колізій (зони конфлікту) мережі будуть містити в собі сегменти, розташовані в кімнатах кожної робочої групи, плюс сегмент, що зв'язує концентратор робочої групи з комутатором підрозділу. Усього таких областей колізій буде дев'ять. Саме для них необхідно проводити розрахунки роботоздатності мережі відповідно до попередньої глави.

Широкомовні області будуть містити в собі всі сегменти мережі кожного підрозділу плюс сегмент, що зв'язує комутатор підрозділу з маршрутизатором підприємства. Таких широкомовних областей буде всього три.

Якщо передбачувана інтенсивність обміну по проектованій мережі не дуже велика, комп'ютерів не занадто багато, і розміри будинку дозволяють, то цілком можливо обійтися без маршрутизаторів, досить складних і порівняно дорогих пристроїв.

Області колізій у даному випадку будуть містити в собі всі сегменти мережі кожного підрозділу плюс сегмент, що з'єднує концентратор підрозділу і комутатор підприємства. Таких областей колізій всього три. Для них треба проводити розрахунок роботоздатності мережі, як раніше описано. У єдину широкомовну область увійде вся мережа підприємства.

У ситуації, коли комп'ютерів на підприємстві небагато (до 50), має сенс відмовитися не тільки від маршрутизаторів, але і від комутаторів, залишивши тільки репітерні концентратори.

3.3.4 Вибір устаткування

При виборі мережевого устаткування треба враховувати безліч факторів, зокрема:

- рівень стандартизації устаткування і його сумісність з найпоширенішими програмними засобами;
- швидкість передавання інформації і можливість її подальшого збільшення;
- можливі топології мережі і їхньої комбінації ("шина", "пасивна зірка", "пасивне дерево");
- метод керування обміном у мережі (CSMA/CD, повний дуплекс або маркерний метод);
- дозволені типи кабелю мережі, максимальну його довжину, захищеність від завад;
- вартість і технічні характеристики конкретних апаратних засобів (мережевих адаптерів, трансиверів, репітерів, концентраторів, комутаторів).

Основні аргументи на користь того або іншого вибору надані в таблиці 3.1.

Таблиця 3.1 – Аргументи при виборі типу кабелю

Тип кабелю	Аргументи при виборі	
	за	проти
1	2	3
неекранована кручена пара UTP (категорія 3 або вище)	• доступність за ціною; • доступність інструментів для установлення роз'ємів (RJ45); • зручність прокладання кабелю; • відносна простота ремонту; • підтримка перспективних високошвидкісних мереж (Fast і Gigabit Ethernet) при використанні кабелю категорії 5 або вище	• відносно низька стійкість до електромагнітних завад; • порівняно малі припустимі відстані кабельних з'єднань, особливо для високошвидкісних мереж; • неможливість використання в зовнішніх ділянках з'єднань
екранована кручена пара STP (екрануюче обплетення)	• підвищена стійкість до електромагнітних завад	• вища ціна порівняно з кабелем типу UTP.
екранована кручена пара FTP (екран з фольги)	• подібно попередньому типу кабелю	
багатомодовий оптоволоконний кабель	• практична нечутливість до зовнішніх електромагнітних завад і відсутність власного випромінювання; • підтримка перспективних високошвидкісних мереж, у тому числі на відстанях, недоступних при використанні крученої пари	• відносно висока ціна кабелю і мережевого устаткування; • складність установлення; • низька ремонтопридатність; • чутливість до впливів факторів навколишнього середовища (можуть викликати помутніння оптоволокна)

Продовження таблиці 3.1

1	2	3
одномодовий оптоволоконний кабель	• поліпшені технічні характеристики порівняно з багато модовим кабелем (можливість збільшення швидкості передавання або довжини з'єднань)	• вища ціна; • складне установлення і ремонт
безпровідні з'єднання (радіо й інфрачервоні канали)	• усунення необхідності організації кабельної системи; • мобільність робочих станцій; • можливість організації глобальних мереж (з використанням радіоканалів і супутникового зв'язку)	• відносно дороге устаткування; • сильна залежність надійності з'єднання від наявності завад (для радіохвиль) і пилу в приміщенні (для інфрачервоних каналів); • досить низька швидкість передавання (максимум до декількох Мбіт/с) і неможливість її істотного збільшення

Ще одна важлива задача – це вибір комп'ютерів. Якщо для робочих станцій або невиділених серверів звичайно використовують ті комп'ютери, що вже є на підприємстві, то виділений сервер бажано купувати спеціально для мережі. Краще, якщо це буде швидкодіючий спеціалізований комп'ютер-сервер, спроектований з урахуванням специфічних недоліків мережі (такі сервери випускаються всіма найбільшими виробниками комп'ютерів).

3.3.5 Вимоги до сервера

1. Максимально швидкий процесор (компанія Microsoft рекомендує для своєї операційної системи Windows Server 2003 процесор з тактовою частотою не менше 500 МГц). Типова величина тактової частоти процесора для сервера зараз складає 2–3 ГГц. Для великих мереж застосовують і багатопроцесорні сервери (іноді до 32 процесорів).

2. Великий обсяг оперативної пам'яті (фірма Microsoft рекомендує для своєї операційної системи Windows Server 2003 обсяг пам'яті не менше 256 Мбайтів, такі ж вимоги фірми Novell до NetWare 6). Типовий обсяг оперативної пам'яті сервера зараз складає 512 Мбайтів–20 Гбайтів. Великий обсяг пам'яті сервера навіть важливіший швидкодії процесора, тому що дозволяє ефективно використовувати кешування дискової інформації, зберігаючи в пам'яті копії тих областей диска, з якими проводиться найінтенсивніший обмін.

3. Швидкі жорсткі диски великого обсягу. Типова величина обсягу диска сервера зараз складає 150–500 Гбайтів. Дисководи повинні бути сумісні з мережевою операційною системою (тобто їхні драйвери обов'язково повинні входити в набір драйверів, що постачаються з ОС). Широко застосовують SCSI-дисководи, що швидше традиційних IDE-дисководів. У

серверах часто передбачають можливість "гарячої" заміни дисків (без вимикання живлення сервера), що дуже зручно.

4. Спеціалізовані сервери вже містять у своєму складі мережеві адаптери з оптимальними характеристиками. Якщо як сервер використовується звичайний персональний комп'ютер, то мережевий адаптер для нього потрібно вибирати з найбільшою швидкодією.

5. Відеомонітори, клавіатури і миші не є обов'язковим приладдям сервера, тому що сервер, як правило, ніколи не працює в режимі звичайного комп'ютера.

Проектувальникові мережі доводиться розв'язувати задачі, пов'язані з вибором мережевих адаптерів, репітерів, концентраторів, комутаторів і маршрутизаторів, але про це вже достатньо сказано в попередніх главах. Варто відзначити, що продуктивність мережі і її надійність визначаються самим найнизькоякіснішим її компонентом. Тому бажано, щоб усі компоненти устаткування максимально повно відповідали один одному.

3.3.6 Вибір мережевих програмних засобів

На жаль, у процесі проектування мережі зовсім неможливо виділити ті проблеми, що повинні бути вирішені на початку, і ті, котрі можна відкласти на самий кінець. Вибір програмних засобів не варто вважати чимось другорядним, що зовсім не впливає ні на розмір і структуру мережі, ні на характеристики необхідного устаткування. Тому приймати рішення про те, які програмні засоби потрібно використовувати або хоча б до якого класу вони повинні належати, необхідно з самого початку проектування.

При виборі мережевого програмного забезпечення (ПЗ) потрібно, у першу чергу, враховувати такі фактори:

- яку мережу підтримує мережеве ПЗ: однорангову, мережу на основі сервера або обидва ці типи;
- максимальна кількість користувачів (брати з запасом не менше 20%);
- кількість серверів і можливі їхні типи ;
- сумісність з різними операційними системами і комп'ютерами, а також з іншими мережевими засобами;
- рівень продуктивності програмних засобів у різних режимах роботи;
- ступінь надійності роботи, дозволені режими доступу і ступінь захисту даних;
- які мережеві служби підтримуються;
- і головне – вартість програмного забезпечення, його експлуатації і модернізації.

Тільки після всього перерахованого можна переходити до установлення обраного програмного забезпечення, якщо, звичайно, таке потрібно. Варто відмітити, що в більшості випадків безпосередньо установленням програмних засобів займаються працівники спеціалізованих комп'ютерних фірм. Але приймати рішення, про те, що потрібно конкретному підприємству, повинні

все-таки ті, хто буде з цією мережею працювати надалі. Потім необхідно провести конфігурування мережі, тобто задати її логічну конфігурацію, налаштувати на роботу в конкретних умовах. В обов'язки системного адміністратора мережі, що здійснює контроль і керування входить:

- створення груп користувачів різного призначення;
- визначення прав доступу користувачів;
- навчання нових користувачів і оперативна допомога в разі потреби;
- контроль дискового простору всіх серверів мережі;
- захист і резервне копіювання даних, боротьба з комп'ютерними вірусами;
- модернізація програмного забезпечення і мережевої апаратури;
- налаштування мережі для одержання максимальної продуктивності.

Системний адміністратор, як правило, дістає максимальні права доступу до всіх мережевих ресурсів і службових програм. Всі інші користувачі в ідеалі не повинні помічати мережі: просто в них з'являються нові диски, розташовані на файлах-серверах, нові принтери, сканери, модеми, програми, спеціально орієнтовані на мережу, наприклад, електронна пошта.

Бажано, щоб кожною групою керував свій мережевий адміністратор (якщо, звичайно, групи досить великі). Як приклад, мережева ОС Windows Server 2000 дозволяє створювати чотири типи груп:

- локальні групи реєструються на локальному комп'ютері;
- глобальні групи реєструються на головному контролері домену;
- спеціальні групи (звичайно використовуються для внутрішньосистемних недоліків);
- убудовані групи поділяються на три категорії: адміністратори, оператори й інші користувачі.

Свої права доступу можна установити і кожному користувачеві окремо. Користувач повинен мати стільки прав доступу, скільки йому потрібно.

Контрольні питання до розділу 3

1. Різниця між стандартами локальних мереж.
2. Основні принципи стандарту Fast Ethernet.
3. Принципи передавання кадру та його формати в мережі Fast Ethernet.
4. Відмінність технології Fast Ethernet від Gigabit Ethernet.
5. Принципи побудови мережі Token-Ring.
6. Доцільність використання мережі FDDI. Її переваги та недоліки.
7. Формат пакету мережі FDDI.
8. Стандарти глобальних мереж.
9. Принципи побудови мережі технології ATM.
10. Стеки протоколів глобальних мереж.
11. Формат ATM-комірки.
12. Описати стандарти безпровідних технологій.
13. Охарактеризувати етапи проектування мережі.

Розділ 4
ЗАСТОСУВАННЯ СТЕКА ПРОТОКОЛІВ TCP/IP

4.1 Набір протоколів TCP/IP

TCP/IP – це відповідний промисловим стандартам набір протоколів, призначений для підтримки міжмережевих зв'язків між регіональними мережами (WAN). TCP/IP розроблений у 1969 році Управлінням ARPA (Advanced Research Projects Agency) Міністерства оборони США для експериментальної мережі, відомої під назвою ARPANET (ARPA Network). Мета розробки TCP/IP полягала в тому, щоб забезпечити високошвидкісні комунікаційні з'єднання між окремими мережами. Згодом ARPANET перетворилася у всесвітнє співтовариство мереж – Інтернет.

4.1.1 TCP/IP

TCP/IP, реалізований у сучасних ОС, дозволяє комп'ютерам працювати в корпоративних мережах. Установлення TCP/IP на комп'ютері з такою ОС дасть:

- найповніший з існуючих набір стандартних, маршрутизовних протоколів. TCP/IP підтримують усі сучасні мережеві операційні системи, але у більшості великих мереж основний трафік йде по TCP/IP;
- технологію для з'єднання різних систем. Передавання даних між такими системами дозволяють багато стандартних засобів, у тому числі FTP (File Transfer Protocol) і Telnet протокол емуляції термінала;
- відмовостійку, масштабуєму і крос-платформну інфраструктуру "клієнт-сервер". TCP/IP передбачає програмний інтерфейс Windows Sockets, ідеальний для розробки клієнт-серверних додатків, що можуть працювати зі стеками від інших постачальників, сумісними з Windows Sockets;
- доступ в Інтернет. Останній складається з тисяч мереж і з'єднує дослідницькі лабораторії, університети, бібліотеки і приватні компанії по усьому світу.

4.1.2 Стандарти по TCP/IP

Стандарти по TCP/IP публікуються в серії документів Request for Comments (RFC). RFC описують внутрішні механізми Інтернет. Одна частина RFC-документів визначає мережеві служби або протоколи й описує їх реалізації, а інша – політику, яка проводиться в тій або іншій сфері, що має відношення до Інтернет.

RFC-документам може бути присвоєно п'ять видів статусу (табл. 4.1). Якщо документ приймається за стандарт, він проходить процес Internet Standards Process що включає етапи розробки, тестування і затвердження. Ці етапи відповідають рівням готовності документа (табл. 4.2). При пуб-

лікації RFC-документові присвоюється певний номер. Зміст вихідного RFC ніколи не оновлюється. Якщо потрібно внести якісь зміни, публікується новий RFC під новим номером.

Таблиця 4.1 – Види статусу RFC-документів

Статус	опис
Required (обов'язковий)	Реалізація даного RFC обов'язкова на всіх TCP/IP-хостах і шлюзах
Recommended (рекомендований)	Реалізація даного RFC бажана на всіх TCP/IP-хостах і шлюзах (рекомендовані RFC звичайно реалізуються)
Elective (необов'язковий)	Реалізація даного RFC не обов'язкова; згода щодо відповідної специфікації досягнута, але її дотримання не є безумовною вимогою
Limited Use (для обмеженого застосування)	Даний RFC не призначений для широкого застосування
Not recommended (не рекомендований)	Реалізація даного RFC не рекомендується

Таблиця 4.2 – Рівні готовності Інтернет-стандартів

Рівень готовності	Опис
Proposed Standard (запропонований стандарт)	Специфікація рівня Proposed Standard має в цілому закінчений вигляд. Вважається досить зрозумілою, про неї отримані позитивні відгуки, і вона задовольняє інтереси досить великої кількості організацій
Draft Standard (проект стандарту)	Специфікація рівня Draft Standard вважається повністю зрозумілою і має майже остаточний вид, тому на її основі можна створювати відповідну реалізацію
Internet Standard (Інтернет-стандарт)	Специфікація рівня Internet Standard (яку можна називати просто стандартом) відрізняється високим ступенем технічної зрілості і загальним визнанням її як стандарту, що дає істотні вигоди Інтернет-співтовариству

4.1.3 Архітектура TCP/IP

Протоколи TCP/IP відповідають чотирирівневій концептуальній моделі, відомій як модель DARPA (як уже згадувалося, саме Управління ARPA Міністерства оборони США початково розробило TCP/IP). Рівні в цій моделі називаються так: прикладний, транспортний, міжмережевий і мережевий інтерфейс. Кожен рівень у моделі DARPA відповідає одному або більше рівням у семирівневій моделі OSI (Open Systems Interconnection). Архітектура протоколів TCP/IP показана на рис. 4.1.

4.1.3.1 Рівень мережевого інтерфейсу

Рівень мережевого інтерфейсу (network interface layer), також відомий як рівень мережевого доступу (network access layer), відповідає за передавання TCP/IP-пакетів у мережеве середовище і прийом цих пакетів з мережевого середовища. TCP/IP незалежний від способу доступу до мережі,

формату кадрів і мережевого середовища. Завдяки цьому TCP/IP можна використовувати для з'єднання мереж різних типів, побудованих, зокрема, на технологіях LAN (Ethernet, Toking Ring) і WAN (X.25. Frame Relay). Незалежність від мережевої технології дозволяє адаптувати TCP/IP до нових технологій, таких як ATM (Asynchronous Transfer Mode).

Рівень мережевого інтерфейсу надає функціональність канальному і фізичному рівням у моделі OSI. Слід зазначити, що міжмережевий рівень не використовує переваги служб, що забезпечують упорядкування і підтвердження прийому пакетів і підтримуються канальним рівнем. Рівень мережевого інтерфейсу вважається ненадійним – за підтримку надійного комунікаційного зв'язку відповідає транспортний рівень.

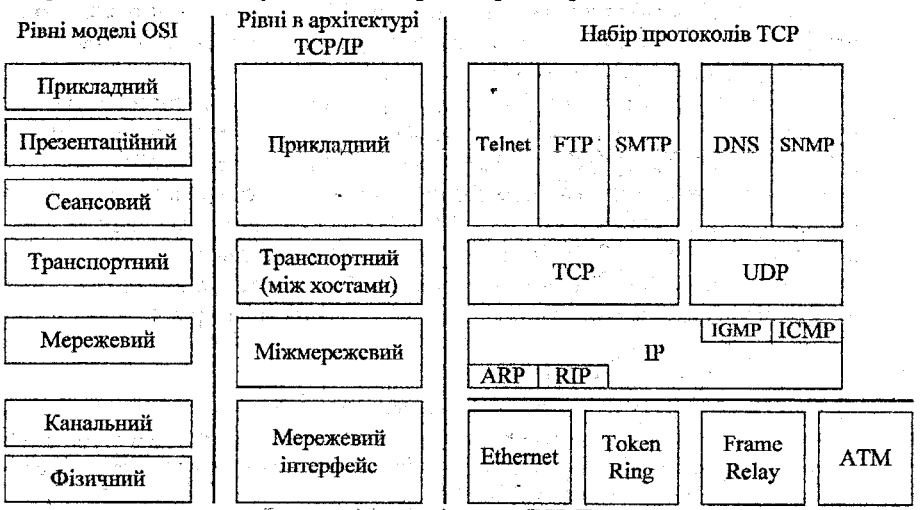

Рисунок 4.1 – Архітектура TCP/IP

4.1.3.2 Міжмережевий рівень

Міжмережевий рівень (internet layer) відповідає за підтримку адресації, пакетів і маршрутизації. Пазові протоколи цього рівня – IP. ARP, ICMP і IGMP.

- IP (Internet Protocol) – маршрутизовний протокол, відповідальний за IP-адресацію, маршрутизацію, а також за фрагментацію і відновлення пакетів.
- ARP (Address Resolution Protocol) – забезпечує перетворення адрес міжмережевого рівня в адреси рівня мережевого інтерфейсу.
- ICMP (Internet Control Message Protocol) – підтримує діагностичні функції і повідомляє про помилки у випадку невдалого доставлення IP-пакетів.

• IGMP (Internet Group Management Protocol) – керує групами IP-розсилання (IP multicast groups).

Міжмережевий рівень аналогічний мережевому рівневі в моделі OSI.

4.1.3.3 Транспортний рівень

Транспортний рівень (transport layer), також відомий як рівень транспорту між хостами (host-to-host transport layer), надає прикладному рівневі сеансові комунікаційні служби і забезпечує підтримку дейтаграм. Базові протоколи цього рівня – TCP і UDP.

• TCP (Transmission Control Protocol) – забезпечує надійний, потребуючий логічного з'єднання комунікаційний зв'язок типу "один-до-одного". TCP відповідає за встановлення TCP-з'єднання, упорядкування пакетів, що відсилаються, підтвердження прийняття пакетів, що надходять, і відновлення пакетів, загублених у процесі передачі.

• UDP (User Datagram Protocol) – забезпечує ненадійний, не потребуючий логічного з'єднання комунікаційний зв'язок типу "один-до-одного" або "один-до-багатьох". UDP використовується, коли обсяг передаваних даних невеликий (наприклад, дані можуть уміститися в єдиному пакеті), коли витрати встановлення TCP-з'єднання небажані або коли додатки або протоколи верхніх рівнів гарантують надійну доставку.

Транспортний рівень надає усю функціональність транспортного рівня в моделі OSI і частину функціональності її сеансового рівня.

4.1.3.4 Прикладний рівень

Прикладний рівень (application layer) забезпечує додаткам доступ до сервісів інших рівнів і визначає протоколи, по яких додатки можуть обмінюватися даними. На прикладному рівні передбачено досить багато протоколів, постійно розробляються нові.

Найпоширеніші протоколи прикладного рівня – ті, котрі застосовуються для обміну користувацькою інформацією.

• HTTP (Hypertext Transfer Protocol) – протокол для передавання файлів, що утворюють зміст Web-сторінок у World Wide Web.

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

• SMTP (Simple Mail Transfer Protocol) – протокол для передавання поштових повідомлень і вкладень.

• Telnet – протокол емуляції термінала; використовується для реєстрації на віддалених мережевих хостах.

• Наступні протоколи прикладного рівня спрощують використання і керування TCP/IP-мережами.

• DNS (Domain Name System) – призначений для дозволу хост-імен у IP-адресі.

• RIP (Routing Information Protocol) – застосовується маршрутизаторами для обміну відповідною інформацією.

• SNMP (Simple Network Management Protocol) – забезпечує взаємодію між консоллю керування мережею і мережевими пристроями (маршрутизаторами, мостами, "інтелектуальними" хабами), дозволяючи збирати інформацію, необхідну для керування мережею, і обмінюватися нею.

4.1.4 IP-адресація

Кожен TCP/IP-хост ідентифікується логічною IP-адресою. IP-адреса – це адреса мережевого рівня, незалежна від адреси канального рівня (наприклад, від MAC-адреси мережевого адаптера). Унікальна IP-адреса необхідна для кожного хоста і мережевої компоненти, що використовує комунікаційний зв'язок за TCP/IP. IP-адреса визначає місцезнаходження системи в мережі точно так само, як поштова адреса – будинок на вулиці. І подібно звичайній поштовій адресі вона повинна бути глобально унікальною і в єдиному форматі. Будь-яка IP-адреса включає ідентифікатор мережі й ідентифікатор хоста.

• Ідентифікатор мережі (network ID), також відомий як мережева адреса, визначає системи, що знаходяться в одній фізичній мережі, обмеженій IP-маршрутизаторами. Ідентифікатор мережі повинен бути однаковий у всіх систем в одній фізичній мережі й унікальний у міжмережевому просторі.

• Ідентифікатор хоста (host ID), також відомий як адреса хоста, визначає робочу станцію, сервер, маршрутизатор або інший TCP/IP-хост у мережі. Адреса кожного хоста повинна бути унікальна для даного ідентифікатора мережі.

IP-адреса складається з 32 бітів, що розбиваються на чотири октети – поля по 8 бітів. Кожен октет перетворюється в десяткове число в діапазоні 0–255 і відокремлюється крапкою. Такий формат називається точково-десятковою нотацією.

Запис у виді w_x_y_z застосовується при посиланні на узагальнену IP-адресу; вона показана на рис. 4.2.

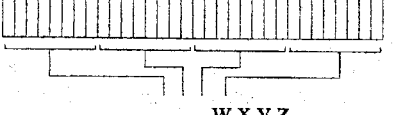

Рисунок 4.2 – IP-адреса

4.1.4.1 Класи адрес

Співтовариством Інтернету визначено п'ять класів адрес, що відповідають мережам різних розмірів. Microsoft TCP/IP підтримує адреси класів A, B і C.

Клас адреси задає, скільки біт в IP-адресі відводиться ідентифікаторам мережі і хоста. А виходить, клас адреси також визначає максимальну кількість мереж даного класу і хостів кожної з цих мереж.

Клас A. Адреси класу A призначаються мережам з дуже великою кількістю хостів. Старший біт в адресі класу A завжди дорівнює 0. Наступні 7 бітів (завершальні перший октет) утворять ідентифікатор мережі. Інші 24 біти (останні три октети) – це ідентифікатор хоста. У такий спосіб клас A допускає максимум 126 мереж, а в кожній на них до 16 777 214 хостів. Структуру адрес класу A ілюструє рис. 4.3.

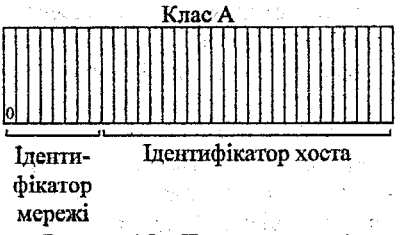

Рисунок 4.3 – IP-адреси класу A

Клас B. Адреси класу B призначаються мережам середнього і великого розміру. Два старших біти в адресі класу B завжди є комбінацією двійкових чисел 1 і 0. Наступні 14 бітів (завершальні перші два октети) утворять ідентифікатор хоста. Таким чином, клас B допускає максимум 16 384 мережі, а в кожній з них до 65 534 хостів. Структуру адрес класу B ілюструє рис. 4.4.

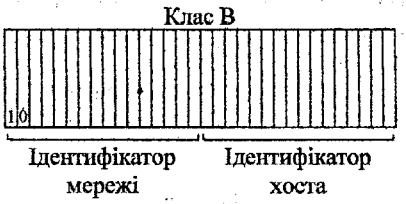

Рисунок 4.4 – IP-адреси класу B

Клас C. Адреси класу C призначаються малим мережам. Три старших біти в адресі класу C завжди є комбінацією двійкових чисел 1, 1 і 0. Далі 21 біт (завершальні перші три октети) утворить ідентифікатор мережі. Інші 8 бітів (останній октет) – це ідентифікатор хоста. Таким чином, клас C допускає максимум 2 097 152 мереж.

Клас D. Адреси класу D резервуються для адрес групового IP-розсилання. Чотири старших біти в адресі класу D завжди є комбінацією двій-

кових чисел 1, 1, 1 і 0. Інші біти містять адреси, відомі зацікавленим хостам. Microsoft підтримує адреси цього класу для додатків, що поширюють дані на хости з підтримкою групового розсилання.

Рисунок 4.5 – IP-адреси класу С

Клас Е. Цей клас передбачає єдину експериментальну адресу, зарезервовану на майбутнє. Чотири старших біти в адресі класу Е завжди є комбінацією двійкових чисел 1, 1, 1 і 1.

У зведеній таблиці 4.3 показано характеристики адрес класів А, В і С, які можна використовувати як IP-адреси хостів.

Таблиця 4.3 – Характеристики класів IP-адрес

Клас	Значення октету w	Октети для ID мережі	Октети для ID хоста	Максимальне число мереж	Число хостов у мережі
A	1-126	u	x y z	126	16777 214
B	128-191	u x	y z	16 384	65534
C	192-223	u x y	z	2097152	254

Адреса 127.x.y.z класу А зарезервований для тестування міжпроцесорного зв'язку на локальному комп'ютері.

4.1.4.2 Підмережі і маски підмереж

Адреси класів Інтернету дозволяють працювати з мережами трьох розмірів, розподіляючи 32 біти IP-адреси між ідентифікаторами мережі і хост залежно від кількості мереж і числа хостів у кожній мережі. Але задумайтеся: мережа класу А допускає наявність більше 16×10^6 хостів, а всі хости у фізичній мережі, зв'язані IP-маршрутизаторами, поділяють той самий широкомовний трафік і знаходяться в одному домені широкомовлення (broadcast domain). Створювати вузький домен з 16×10^6 вузлів украй непрактично. І навіть мережа класу В з 65000 хостів була б незручною в роботі.

У зв'язку з цим IP-мережу можна розбити на кілька менших мереж (підмереж), розмежувавши їх IP- маршрутизаторами і присвоївши кожній з них свій ідентифікатор мережі, що містить ідентифікатор підмережі (subnetted network ID). Останній формується з частини бітів, що відводяться для ідентифікатора хоста в даному класі IP-адрес.

Розглянемо приклад на рис. 4.6. У мережі 139.12.0.0 класу В може бути максимум 65534 хости. Така кількість хостів занадто велика, і ця мережа була б переповнена широкомовним трафіком. Отже, мережу 139.12.0.0 потрібно розбити на підмережі, причому так, щоб не вплинути на іншу частину межмережевого IP-середовища й обійтися без його переконфігурації.

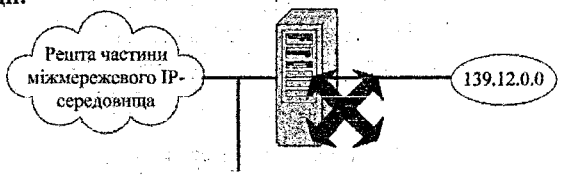

Рисунок 4.6 – Мережа 139.12.0.0 перед розбивкою на підмережі

Мережа 139.12.0.0 розбивається на три підмережі (рис. 4.7) за рахунок формування ідентифікаторів підмереж з перших восьми бітів ідентифікатора хоста (тобто з третього октету IP-адреси класу В): 139.12.1.0. 139.12.2.0, 139.12.3 0. Маршрутизатор розпізнає ці ідентифікатори і спрямовує IP-пакети у відповідну підмережу.

Помітьте, що для іншої частини міжмережевого IP-середовища всі хости в цих трьох підмережах як і раніше знаходяться в мережі 139.12.0.0. Інші IP-маршрутизатори в міжмережевому середовищі нічого не знають про розбивку мережі 139.12.0.0 на підмережі і тому не вимагають переналаштування.

З появою підмереж покладатися на визначення класів IP-адрес для вибірки ідентифікатора мережі з IP-адреси більше не можна. Потрібна якась нова величина, що дозволяла б зрозуміти, яка частина IP-адреси відноситься до ідентифікатора мережі, а яка – до ідентифікатора хоста, а також чи не містить ідентифікатор мережі ідентифікатор підмережі.

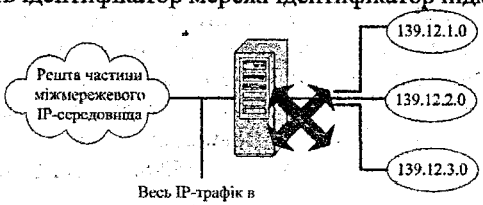

Рисунок 4.7 – Мережа 139.12.0.0 після розбивки на підмережі

Маска підмережі (також називана маскою адреси) визначена в RFC 950 як 32-бітове значення, використовуване для того, щоб відрізнити ідентифікатор мережі від ідентифікатора хоста в довільній IP-адресі. Біти маски підмережі задаються так:

- усі біти, що відповідають ідентифікатору мережі, встановлюються в 1;
- усі біти, що відповідають ідентифікатору хоста, встановлюються в 0.

Будь-який хост у TCP/IP-мережі вимагає наявності маски підмережі, навіть якщо ця мережа складається з єдиного сегмента. Тому в кожному TCP/IP-вузлі застосовується або стандартна маска підмережі (для ідентифікаторів мереж на основі класів), або нестандартна (для ідентифікаторів мереж, що містять ідентифікатори підмереж або надмереж).

Маски підмереж часто записуються в точково-десятковій нотації. Установивши всі біти для ідентифікаторів мережі і хоста, отримане 32-бітове значення перетворюють у точково-десяткову форму. Але навіть у такій нотації маска підмережі не є IP-адресою.

Стандартна маска підмережі заснована на класі IP-адреси і використовується в TCP/IP-мережах, не розбитих на підмережі. Стандартні маски підмереж у точково-десятковій нотації перераховані в таблиці 4.4.

Нестандартні маски використовуються при створенні підмереж або надмереж. Наприклад, мережева адреса 138.96.58.0 містить восьмибітовий ідентифікатор підмережі, створеної в мережі класу B. Ці 8 бітів запозичаються з біт, що відводяться під ідентифікатор хоста. Для визначення ідентифікатора мережі, що включає ідентифікатор підмережі, застосовується маска підмережі 255.255255.0. Вона вказує на те, що в даній IP-адресі утримується не тільки ідентифікатор мережі, але й ідентифікатор подсети.

Таблиця 4.4 – Стандартні маски підмереж (у точково-десятковій нотації)

Клас адреси	Біти маски підмережі	Маска підмережі
A	1111111 00000000 00000000 00000000	255.0.0.0
B	1111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Хоча з концептуальної точки зору розбивка на підмережі за рахунок використання частини бітів IP-адреси, що відводяться під ідентифікатор хоста, достатньо зрозуміла, реальний механізм цього процесу трохи складніший. Для розбивки на підмережі потрібно виконати процедуру, що складається з трьох етапів.

Визначення кількості бітів для ідентифікатора підмережі.

1. Перерахунок нових ідентифікаторів мереж (разом з ідентифікаторами підмереж).

2. Перерахунок IP-адрес для кожного з нових ідентифікаторів мереж (разом з ідентифікаторами підмережі).

Етап 1: визначення кількості бітів для ідентифікатора підмережі.

Число бітів, які виділяються під ідентифікатор підмережі, визначає можливу кількість підмереж і хостів у кожній з них. Перш ніж зробити свій вибір, ви повинні передбачити, скільки підмереж і хостів з'явиться у Вас у майбутньому. Виділивши трохи більше бітів, ніж це потрібно в даний момент, можна уникнути перепризначення IP-адрес.

Чим більше бітів відбирається в ідентифікатора хоста, тим більше можливе число підмереж і тим менша максимальна кількість хостів у цих підмережах. Виділивши занадто багато таких бітів, Ви зможете в міру необхідності збільшувати кількість підмереж, але обмежите число хостів. І навпаки, виділивши занадто мало бітів, Ви зможете нарощувати кількість хостів, але обмежите число підмереж.

Приклад на рис. 4.8 ілюструє, що відбувається при виділенні для ідентифікаторів підмереж від одного до восьми бітів у IP-адресі класу B. При виділенні одного біта Ви одержуєте дві підмережі з 16382 хостами в кожній, а при виділенні восьми бітів – 256 підмереж з 254 хостами в кожній.

Рисунок 4.8 – Формування ідентифікаторів підмереж у IP-адресі класу B

Етап 2: перерахунок нових ідентифікаторів мереж

Виходячи з обраної кількості бітів, Ви повинні скласти список нових ідентифікаторів мереж, що включають ідентифікатори підмереж. Такий список можна підготувати, використовуючи або двійковий, або десятковий спосіб з наступним перетворенням отриманих значень у точково-десятковий формат. У будь-якому випадку результат один: повний список нових ідентифікаторів мереж.

4.1.5 Базові протоколи TCP/IP

Компонент підтримки протоколів TCP/IP, встановлюваний у Вашій мережевій операційній системі, – це набір протоколів для підключення до мережі, називаних базовими протоколами TCP/IP. Всі інші додатки і протоколи з набору протоколів TCP/IP опираються на базові сервіси, надані протоколами IP, ARP. ICMP, IGMP. TCP і UDP.

4.1.5.1 Протокол IP

Це не потребуючий з'єднань ненадійний протокол, відповідальний головним чином за адресацію і маршрутизацію пакетів між хостами. Оскільки цей протокол не вимагає з'єднань, перед обміном даними сеанс не встановлюється. А ненадійність полягає в тому, що доставка пакетів не гарантується. Протокол IP не завжди докладає максимум зусиль для доставки пакета. IP-пакети можуть бути загублені, доставлені не в тому порядку,

продубльовані або затримані. Такого роду помилки IP не виправляє. За підтвердження прийому пакета і відновлення втрачених пакетів відповідає протокол вищого рівня, наприклад, TCP. Протокол IP визначений у RFC 791.

IP-пакет складається з заголовка і власне даних. Ключові поля в заголовку IP-пакета описуються в таблиці 4.5.

Таблиця 4.5 – Ключові поля в IP-заголовку

Поле	Опис
IP-адреса відправника	IP-адреса первісного відправителя IP-дейтаграми
IP-адреса одержувача	IP-адреса кінцевого одержувача IP- дейтаграми
Ідентифікації	Використовується для ідентифікації конкретної IP-дейтаграми і усіх її фрагменттів (якщо відбулася фрагментація)
Протокол	Повідомляє IP на хості-одержувачі, якому протоколові варто передати пакет – TCP. UDP. ICMP або іншому
Контрольна сума	Використовується для перевірки цілісності IP-заголовка
Час життя (Time-to-Live, TTL)	Установлюється хостом-відправником і визначає кількість мереж, по яких може пройти дейтаграма до того, як її відкине один з маршрутизаторів. TTL запобігає нескінченній циркуляції пакетів між мережами. При пересиланні IP-пакета маршрутизатор зобов'язаний зменшити значення TTL мінімум на одиницю

4.1.5.2 Протокол ICMP

Цей протокол підтримує засоби діагностики і повідомляє про помилки, якщо доставити пакети не вдається. Наприклад, якщо IP не може доставити пакет хосту-одержувачу, ICMP посилає хосту-відправнику повідомлення Destination Unreachable (Адресат недоступний). Список найчастіше використовуваних ICMP-повідомлень наведений у таблиці 4.6.

Таблиця 4.6 – Часто використовувані ICMP-повідомлення

ICMP-повідомлення	Опис
EchoRequest (Ехо-запит)	Діагностичне повідомлення, використовуване для перевірки можливості з'єднання по IP з потрібним хостом: такі повідомлення посилає утиліта ping
Echo Reply (Ехо-відповідь)	Відповідь і повідомлення Echo Request
Redirect (Перенаправлення)	Посилається маршрутизатором для повідомлення хоста-відправника про ефективніший маршрут до IP-адреси одержувача
Source Queach (Уповільнення джерела)	Посилається маршрутизатором для повідомлення хоста-відправника про те, що його IP-дейтаграми відкидаються через "пробки на маршрутизаторі"; у цьому випадку хост-відправник повинен зменшити свою швидкість передавання (повідомлення Source Quench відноситься до числа необов'язкових і звичайно не реалізується)
Destination Unrea chable (Адресат недоступний)	Посилається маршрутизатором для повідомлення хоста-відправника про те, що дейтаграму не можна доставити

Існує цілий набір ICMP-повідомлень Destination Unreachable. Найбільше часто використовувані з них описуються в таблиці 4.7.

ICMP не робить протокол IP надійнішим. Він просто повідомляє про помилки і забезпечує зворотний зв'язок у певних ситуаціях. ICMP-повідомлення передаються як IP-дейтаграми, не потребуючі підтвердження про прийом, а отже, вони теж ненадійні. Протокол ICMP визначений у RFC 792.

Таблиця 4.7 – Часто використовувані ICMP-повідомлення Destination Unreachable

Повідомлення Destination Unreachable	Опис
Network Unreachable (Мережа недоступна)	Посилається IP-маршрутизатором, коли він не може знайти маршрут до кінцевої мережі, це повідомлення застаріле
Unreachable (Вузол недоступний)	Посилається IP-маршрутизатором, коли він не може знайти IP-адресу одержувача
Protocol Unreachable (Протокол недоступний)	Посилається IP-вузлом одержувача, якщо значення поля протоколу в IP-заголовок не відповідає поточному клієнтському IP-протоколові
Port Unreachable (Порт недоступний)	Посилається IP-вузлом одержувача, якщо порт одержувача у UDP-заголовку не можна зіставити з процесом, що використовує цей порт
Fragmentation Needed and DF Set (Потрібна фрагментація, але встановлюний прапорець DF)	Посилається IP-мартрутизатором, коли необхідна фрагментація, але її проведення заборонене через те, що вузол відправника установив в IP-заголовку прапорець DF (Don't Fragment)
Source Route Failed (Помилка маршрутизації джерела)	Посилається IP-маршрутизатором, коли не вдається доставити IP-пакет з використанням інформації про маршрутизації джерела

4.1.5.3 Протокол IGMP

Даний протокол керує членством хоста в групах IP-розсилання (IP multicast groups), також називаних групами хостів (host groups). Хости, що входять у таку групу, "слухають" IP-трафік, що направляється на певну адресу. Цей трафік надходить на єдину MAC-адресу, але обробляється декількома IP-хостами. Конкретний хост слухає за конкретною адресою групової IP-розсилки і приймає всі пакети, що надсилаються на цю адресу. Нижче перераховані деякі інші аспекти групової (багатоадресної) IP-розсилки (IP multicast).

Хости можуть у будь-який момент приєднуватися до будь-якої групи і залишати її.

- Група хостів може бути будь-якого розміру.
- Члени групи хостів можуть бути розкидані по декількох мережах. Для цього IP-маршрутизатори повинні підтримувати групове IP-розсилання, а в хостів повинна бути можливість реєстрації їхнього членства в

групі за допомогою локальних маршрутизаторів. Така реєстрація здійснюється за протоколом IGMP.

• Хост може спрямовувати трафік на адресу групової IP-розсилки, не входячи у відповідну групу хостів.

Щоб хост приймав групові розсилання, додаток повинен повідомити IP про те, що він буде приймати їх за певною адресою. Тоді, якщо дана мережева технологія передбачає підтримку групового IP-розсилання, мережевий інтерфейс одержить вказівку передавати пакети на цю адресу. У Ethernet мережевий адаптер програмується так, щоб відповідати на Mac-адресу, що відповідає заданій адресі групового IP-розсилання. Хост підтримує групове IP-розсилання на одному з таких рівнів:

0 – передавання або приймання графіка групового розсилання не підтримується;

1 – передавання графіка групового розсилання підтримується, а приймання – ні;

2 – підтримується і передавання, і приймання графіка групового розсилання.

Інформація, що відноситься до групи хостів, реєструється за протоколом IGMP, який необхідний на всіх хостах, що підтримують групове IP-розсилання рівня 2. IGMP-пакети відсилаються з використанням IP-заголовка. IGMP-повідомлення бувають двох видів.

• Коли хост приєднується до групи, він посилає повідомлення Host Membership Report (Звіт про членство вузла) або всім хостам за загальною адресою групового IP-розсилання (224.0.0.1), або конкретній групі хостів за заданою адресою групового IP-розсилання.

• Коли маршрутизатор опитує мережу, щоб з'ясувати, чи є в ній члени певної групи хостів, він посилає повідомлення Host Membership Query (Запит про членство вузла) усім хостам, але за загальною адресою групового IP-розсилання. Не одержавши відповідь після декількох опитувань, маршрутизатор вважає, що в цій мережі немає членів даної групи хостів, і припиняє посилати інформацію про неї (групу) іншим маршрутизаторам.

4.1.5.4 Протокол TCP

Це надійний транспортний протокол, що вимагає з'єднання. Дані передаються сегментами. Перед обміном даними за цим протоколом хости повинні установити з'єднання. Надійність досягається за рахунок присвоєння порядкового номера кожному переданому сегменту. Хост-одержувач передає підтвердження про прийом (ACK) кожного сегмента. Таке підтвердження повинно надходити протягом певного періоду. Якщо відправник не одержує ACK, він повторно передає відповідні дані. TCP визначений у RFC 793. TCP передає дані як потік байтів; уміст TCP-сегмента розглядається як послідовність байтів. Основні поля TCP-заголовка описуються в таблиці 4.8.

Таблиця 4.8 – Основні поля в TCP-заголовка

Поле	Опис
Порт відправника	TCP-порт хоста- відправника
Порт одержувача	TCP-порт хоста- одержувача
Порядковий номер	Порядковий номер першого байта даних у TCP-сегменті
Номер підтвердження	Порядковий номер наступного байта, очікуваного відправником від одержувача
Вікно	Поточний розмір TCP-буфера (для збереження сегментів, що надходять) на хості, що посилає даний TCP-сегмент
Контрольна сума	Використовується для перевірки цілісності TCP-заголовка даних

4.1.5.5 Протокол UDP

UDP надає не потребуючу з'єднань службу дейтаграм, що забезпечує ненадійну доставку даних, переданих у вигляді повідомлень. Це означає, що UDP не гарантує ні доставку дейтаграм, ні правильну послідовність пакетів, що доставляються. У UDP не підтримується відновлення загублених даних за рахунок їхнього повторного передавання. Даний протокол визначений у RFC 768.

UDP використовується додатками, що не вимагають підтвердження прийому даних і звичайно передають дані невеликими порціями. Служба імен NetBIOS, служба дейтаграм NetBIOS і SNMP – от лише деякі з додатків і служб, що працюють з UDP.

4.2 IP-маршрутизація

Після того як хост- або NetBIOS-ім'я перетворено на IP-адресу, хост-відправник посилає IP-пакет цій адресі. Маршрутизація (routing) – це процес пересилання пакета на IP-адресу одержувача. Вона виконується на TCP/IP-хості, що надсилає пакет, і на IP-маршрутизаторі. Маршрутизатор (router) – це пристрій, що пересилає пакети з однієї мережі в іншу. Такі пристрої часто називають шлюзами (gateways).

Хост-відправник і маршрутизатор повинні визначити, куди переслати пакет. Для цього IP переглядає таблицю маршрутизації (routing table), що зберігається в пам'яті. Стандартні записи (маршрути за замовчуванням) у цій таблиці створюються при ініціалізації TCP/IP, а додаткові – вносяться або вручну (системним адміністратором), або автоматично (опитуванням маршрутизаторів).

4.2.1 Протоколи маршрутизації

4.2.1.1 Класифікація протоколів маршрутизації

Автоматично створювані таблиці маршрутизації забезпечують раціональність маршрутів проходження пакетів через мережу, при цьому критерії вибору маршрутів можуть бути різними. У IP-мережах сьогодні засто-

совуються протоколи маршрутизації, в яких маршрут вибирається або за критерієм найкоротшої відстані, де під відстанню, яку пройшов пакет, розуміється кількість проміжних маршрутизаторів (хопів), або за комплексним показником, що враховує також номінальну пропускну спроможність каналів між маршрутизаторами, надійність каналів або затримки, що вносяться ними.

Протокол маршрутизації повинен створювати в маршрутизаторах узгоджені один з одним таблиці маршрутизації, тобто такі, які забезпечать доставку пакета від початкової мережі в мережу призначення за кінцеве число кроків. Можна подати і неузгоджену пару таблиць, коли таблиця маршрутизатора 1 показує, що пакет для мережі А потрібно передати маршрутизатору 2, а таблиця маршрутизатора 2 відправляє цей самий пакет маршрутизатору 1. Сучасні протоколи маршрутизації забезпечують узгодженість таблиць, проте ця властивість не абсолютна – при змінах в мережі, наприклад, при відмові каналів передачі даних або самих маршрутизаторів, виникають періоди нестабільної роботи мережі, викликані тимчасовою неузгодженістю таблиць різних маршрутизаторів. Протоколу маршрутизації звичайно потрібний деякий час, що називається часом конвергенції, щоб після декількох ітерацій обміну службовою інформацією всі маршрутизатори мережі внесли зміни в свої таблиці і в результаті таблиці знову стали узгодженими. Різні протоколи маршрутизації мають різний час конвергенції.

Відповідно до принципу масштабованості, маршрутизація в Інтернеті функціонує в межах автономних систем (Autonomous Systems, AS).

В IP-мережах як внутрішні шлюзові протоколи, тобто протоколи, які використовуються усередині автономних систем, сьогодні активно використовуються три протоколи – RIP, OSPF і IS-IS. Зовнішнім шлюзовим протоколом, тобто протоколом вибору маршруту між автономними системами, сьогодні є протокол BGP.

4.2.1.2 Адаптивна маршрутизація

У тих випадках, коли маршрутизація здійснюється на підставі таблиць, розрізняють статичну і адаптивну (динамічну) маршрутизацію.

При статичній маршрутизації таблиці складаються і вводяться в пам'ять кожного маршрутизатора вручну адміністратором мережі. Всі записи в таблиці мають статус статичних, що має на увазі нескінченний термін їх життя. При істотній зміні стану мережі адміністратору необхідно терміново внести зміни у відповідні таблиці маршрутизації, інакше мережа працюватиме некоректно.

При адаптивній маршрутизації всі зміни конфігурації мережі автоматично відображаються в таблицях маршрутизації протоколами маршрутизації. Ці протоколи засновані на зборі інформації про топологію зв'язків в мережі, що дозволяє їм оперативно відпрацьовувати всі поточні зміни. У

таблицях маршрутизації при адаптивній маршрутизації звичайно є інформація про інтервал часу, протягом якого даний маршрут залишатиметься дійсним. Цей час називають часом життя (TTL) маршруту. Якщо після закінчення часу життя існування маршруту не підтверджується протоколом маршрутизації, то він вважається неробочим, пакети по ньому більше не посилаються.

Протоколи маршрутизації можуть бути розподіленими і централізованими.

При розподіленому підході в мережі відсутні будь-які виділені маршрутизатори, які збирали б і узагальнювали топологічну інформацію: робота розподіляється між всіма маршрутизаторами мережі. Кожен маршрутизатор будує власну таблицю маршрутизації, грунтуючись на даних, що одержуються за протоколом маршрутизації від решти маршрутизаторів мережі.

Адаптивні алгоритми маршрутизації повинні відповідати декільком важливим вимогам.

По-перше, вони повинні забезпечувати раціональність маршруту. При централізованому підході в мережі існує один маршрутизатор, який збирає всю інформацію про топологію і стан мережі від інших маршрутизаторів. Потім цей виділений маршрутизатор (який іноді називають сервером маршрутів) може побудувати таблиці маршрутизації для всієї решти маршрутизаторів мережі, а потім поширити їх у мережі, щоб кожен маршрутизатор одержав власну таблицю і надалі самостійно ухвалював рішення про просування кожного пакета.

По-друге, алгоритми повинні бути достатньо простими, вони не повинні вимагати дуже великого об'єму обчислень або породжувати інтенсивний службовий трафік.

Алгоритми маршрутизації повинні мати властивість збіжності, тобто завжди приводити до узгодженої побудови таблиць маршрутизації на всіх маршрутизаторах мережі за прийнятний час.

Адаптивні протоколи обміну маршрутною інформацією, в даний час в обчислювальних мережах, діляться на дві групи:

- дистанційно-векторні алгоритми (Distance Vector Algorithms, DVA);
- алгоритми стану зв'язків (Link State Algorithms, LSA).

4.2.1.3 Дистанційно-векторні алгоритми

В дистанційно-векторних алгоритмах (DVA) кожен маршрутизатор періодично і широкомовно розсилає по мережі вектор, компонентами якого є відстані від даного маршрутизатора до всіх відомих йому мереж. Пакети протоколів маршрутизації звичайно називають оголошеннями, оскільки з їх допомогою маршрутизатор оголошує решті маршрутизаторів відомості про конфігурацію мережі. Відстань в DVA звичайно вимірюють за числом хопів. Можлива і інша метрика, яка враховує не тільки число

проміжних маршрутизаторів, але і пропускну спроможність між сусідніми маршрутизаторами.

Одержавши від деякого сусіда 1 вектор відстаней до відомих мереж, маршрутизатор 2 нарощує компоненти вектора на величину відстані від себе до сусіда 1. Крім того, він доповнює вектор інформацією про відомі йому самому нові мережі, про які 1 дізнався безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів. Потім 1 знову розсилає нове значення вектора по мережі. Врешті-решт кожен маршрутизатор дізнається через сусідні маршрутизатори інформацію про всі наявні мережі і про відстані до них.

Потім 1 обирає з декількох альтернативних маршрутів до кожної мережі той маршрут, який має найменшу метрику. Найближчий маршрутизатор, який передав інформацію про цей маршрут, оголошується в таблиці маршрутизації як наступний (next hop).

Найпоширенішим протоколом, який заснований на дистанційно-векторному алгоритмі, є протокол RIP, який є в двох версіях – версія RIP IP працює з протоколом IP, а версія RIP IPX працює з протоколом IPX.

4.2.2 Протокол RIP

Протокол RIP (Routing Information Protocol – протокол маршрутної інформації) є внутрішнім протоколом маршрутизації дистанційно-векторного типу, він є одним з найбільш ранніх протоколів обміну маршрутною інформацією і дотепер надзвичайно поширений в обчислювальних мережах зважаючи на простоту реалізації.

4.2.2.1 Побудова таблиці маршрутизації

Для IP є дві версії RIP – RIPv1 і RIPv2. Протокол RIPv1 не підтримує масок. Протокол RIPv2 передає інформацію про маски мереж, тому він більшою мірою відповідає вимогам сьогоднішнього дня. Оскільки побудова таблиць маршрутизації в обох версіях принципово не відрізняється, надалі для спрощення записів описуватиметься робота версії 1.

Для вимірювання відстані до мережі стандарти протоколу RIP допускають різні види метрик: хопи, значення пропускної спроможності, затримки, що вносяться, надійність мереж (тобто відповідні ознакам D, T і R в полі якості сервісу IP-пакета), а також будь-які комбінації цих метрик. Метрика повинна мати властивість адитивності – метрика складеного шляху повинна дорівнювати сумі метрик складових цього шляху. У більшості реалізацій RIP використовується проста метрика – кількість хопів, тобто кількість проміжних маршрутизаторів, які потрібно подолати пакету до мережі призначення.

Розглянемо процес побудови таблиці маршрутизації за допомогою протоколу RIP на прикладі складеної мережі, зображеної на рис. 4.9.

Етап 1 – створення мінімальної таблиці.

У цій мережі є вісім IP-мереж, зв'язаних чотирма маршрутизаторами з ідентифікаторами: RI R2, R3 і R4. Маршрутизатори, що працюють за протоколом RIP, можуть мати ідентифікатори, проте для протоколу вони не є необхідними. У RIP-повідомленнях ці ідентифікатори не передаються.

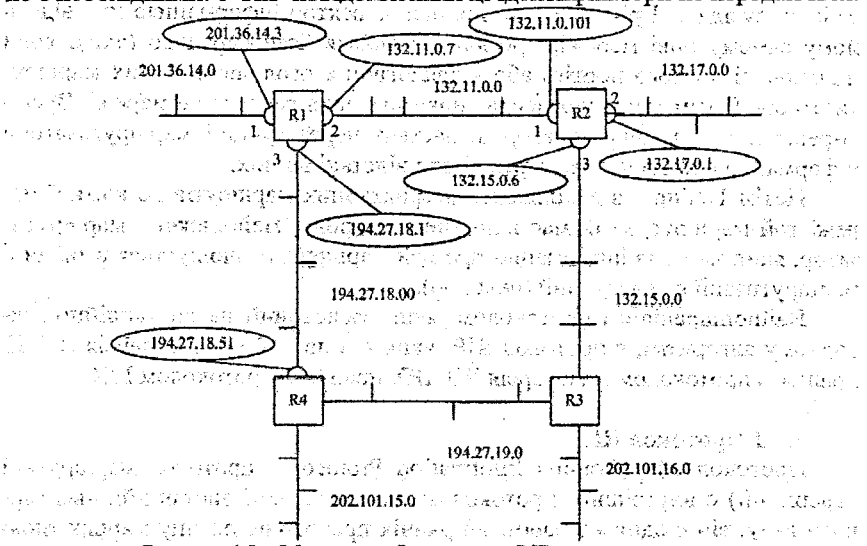

Рисунок 4.9 – Мережа, побудована на RIP-маршрутизаторах

У початковому стані в кожному маршрутизаторі програмним забезпеченням стека TCP/IP автоматично створюється мінімальна таблиця маршрутизації, в якій враховуються тільки безпосередньо приєднані мережі. На малюнку адреси портів маршрутизаторів на відміну від адрес мереж поміщені в овали.

Таблиця 4.9 дозволяє оцінити зразковий вид мінімальної таблиці маршрутизації маршрутизатора R1.

Таблиця 4.9 – Мінімальної таблиці маршрутизації маршрутизатора R1

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Мінімальні таблиці маршрутизації в інших маршрутизаторах виглядатимуть відповідно, наприклад, таблиця маршрутизатора R2 складатиметься з трьох записів (табл. 4.10).

Етап 2 – розсилка мінімальної таблиці сусідам.

Після ініціалізації кожного маршрутизатора він починає посилати своїм сусідам повідомлення протоколу RIP, в яких міститься його мінімальна таблиця.

Таблиця 4.10 – Мінімальна таблиця маршрутизації маршрутизатора R2

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
132.11.0.0	132.11.0.101	1	1
132.17.0.0	132.17.0.1	2	1
132.15.0.0	132.15.0.6	3	1

RIP-повідомлення передаються в дейтаграмах протоколу UDP і включають два параметри для кожної мережі: її IP-адресу і відстань до неї від маршрутизатора.

Сусідами є маршрутизатори, яким даний маршрутизатор може передати IP-пакет по якій-небудь своїй мережі, не користуючись послугами проміжних маршрутизаторів. Наприклад, для маршрутизатора R1 сусідами є маршрутизатори R2 і R3, а для маршрутизатора R4 – маршрутизатори R2 і R3.

Таким чином, маршрутизатор R1 передає маршрутизаторам R2 і R3 такі повідомлення:

- мережа 201.36.14.0, відстань 1;
- мережа 132.11.0.0, відстань 1;
- мережа 194.27.18.0, відстань 1.

Етап 3 – отримання RIP-повідомлень від сусідів і оброблення одержаної інформації.

Після отримання аналогічних повідомлень від маршрутизаторів R2 і R3 маршрутизатор R1 нарощує кожне одержане поле метрики на одиницю і запам'ятовує, через який порт і від якого маршрутизатора одержана нова інформація (адреса цього маршрутизатора стане адресою наступного маршрутизатора, якщо цей запис буде внесений в таблицю маршрутизації). Потім маршрутизатор починає порівнювати нову інформацію з тією, яка зберігається в його таблиці маршрутизації (табл. 4.11.).

Таблиця 4.11 – Таблиця маршрутизації маршрутизатора R1

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2

Записи з четвертого по дев'ятий одержані від сусідніх маршрути заторів, і вони претендують на розміщення в таблиці. Проте тільки записи з четвертого по сьомий потрапляють в таблицю, а записи вісім і дев'ять – ні. Це відбувається тому, що вони містять дані про вже наявні в таблиці маршрутизатора R1 мережі, а відстань до них більша, ніж в існуючих записах.

Протокол RIP заміщає запис про яку-небудь мережу тільки в тому випадку, якщо нова інформація має кращу метрику (відстань в хопах менша) від наявної. В результаті в таблиці маршрутизації про кожну мережу залишається тільки один запис; якщо ж є декілька записів, рівнозначних відносно відстані шляхів до однієї і тієї ж мережі, то все одно в таблиці залишається один запис, який прийшов в маршрутизатор першим за часом. Для цього правила існує виключення – якщо гірша інформація про яку-небудь мережу прийшла від того ж маршрутизатора, на підставі повідомлення якого був створений даний запис, то гірша інформація заміщує кращу.

Аналогічні операції з новою інформацією виконують і решту маршрутизаторів мережі.

Етап 4 – розсилання нової таблиці сусідам.

Кожен маршрутизатор посилає нове RIP-повідомлення всім своїм сусідам. У цьому повідомленні він поміщає дані про всі відомі йому мережі – як безпосередньо підключених, так і віддалених, про які маршрутизатор дізнався з RIP-повідомлень.

Етап 5 – отримання RIP-повідомлень від сусідів і оброблення одержаної інформації. Цей етап повторює етап 3 – маршрутизатори приймають RIP-повідомлення, обробляють інформацію, що міститься в них, і на її підставі коректують свої таблиці маршрутизації.

Подивимося, як це робить маршрутизатор R1 (табл. 4.12).

Таблиця 4.12 – Таблиця маршрутизації маршрутизатора R1

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.16.0	132.11.0.101	2	3

На цьому етапі маршрутизатор R1 одержує від маршрутизатора R3 інформацію про мережу 132.15.0.0, яку той в свою чергу на попередньому циклі роботи отримав від маршрутизатора R4. Маршрутизатор вже знає

про мережу 132.15.0.0, причому стара інформація має кращу метрику, ніж нова, тому нова інформація про цю мережу відкидається.

Про мережу 202.101.16.0 маршрутизатор R1 дізнається на цьому етапі вперше, причому дані про неї приходять від двох сусідів – від R3 і R4. Оскільки метрики в цих повідомленнях вказані однакові, то в таблицю потрапляють дані, що прийшли першими. У нашому прикладі вважається, що маршрутизатор R2 випередив маршрутизатор R3 і першим переслав своє RIP-повідомлення маршрутизатору R1.

Якщо маршрутизатори періодично повторюють етапи розсилання і оброблення RIP-повідомлень, то за кінцевий час в мережі встановиться коректний режим маршрутизації. Під коректним режимом маршрутизації тут розуміється такий стан таблиць маршрутизації, коли всі мережі досяжні з будь-якої мережі за допомогою деякого раціонального маршруту. Пакети доходитимуть до адресатів і не попадатимуть у петлі, подібні тій, яка утворюється (рис. 4.9) маршрутизаторами R1, R2, R3 і R4.

Очевидно, якщо в мережі всі маршрутизатори, їх інтерфейси і з'єднувальні їх лінії зв'язку залишаються роботоздатними, то оголошення за протоколом RIP можна робити досить рідко, наприклад один раз в день. Проте в мережах постійно відбуваються зміни – змінюється роботоздатність маршрутизаторів і ліній зв'язку, крім того, маршрутизатори і лінії зв'язку можуть додаватися в існуючу мережу чи ж виводитися з її складу.

4.2.2.2 Адаптація RIP-маршрутизаторів до змін стану мережі

Для адаптації до змін в мережі протокол RIP використовує ряд механізмів.

До нових маршрутів RIP-маршрутизатори пристосовуються просто – вони передають нову інформацію в черговому повідомленні своїм сусідам і поступово ця інформація стає відома всім маршрутизаторам мережі. А ось до змін, пов'язаних з втратою якого-небудь маршруту, RIP-маршрутизатори адаптуються складніше. Це пов'язано з тим, що у форматі повідомлень протоколу RIP немає поля, яке б указувало на те, що шлях до даної мережі більше не існує.

Для повідомлення про те, що деякий маршрут недійсний, використовуються два механізми:

- закінчення часу життя маршруту;
- вказання спеціальної (нескінченної) відстані до мережі, що стала недоступною.

Механізм закінчення часу життя маршруту заснований на тому, що кожен запис таблиці маршрутизації (як і записи таблиці просування моста/комутатора), одержаний за протоколом RIP, має час життя (TTL). Під час надходження чергового RIP-повідомлення, яке підтверджує справедливість даного запису, таймер TTL встановлюється в початковий стан, а потім з нього кожну секунду віднімається одиниця. Якщо за час тайм-ауту не

прийде нове повідомлення про цей маршрут, він позначається як недійсний.

Час тайм-ауту пов'язаний з періодом розсилання векторів по мережі. У протоколі RIP IP період розсилання вибраний рівним 30 секундам, а як тайм-аут вибрано шестикратне значення періоду розсилання, тобто 180 секунд. Шестикратний запас часу потрібен для упевненості в тому, що мережа дійсно стала недоступною, а не просто відбулися втрати RIP-повідомлень (а це можливо, оскільки протокол RIP використовує транспортний протокол UDP, який не забезпечує надійного доставлення повідомлень). Якщо який-небудь маршрутизатор відмовляє, перестає відсилати своїм сусідам повідомлення про мережі, які можна досягти через нього, то через 180 секунд всі записи, породжені цим маршрутизатором, стануть недійсними у його найближчих сусідів. Після цього процес повториться вже для сусідів найближчих сусідів – вони викреслять подібні записи вже через 360 секунд.

Як видно, відомості про недоступні через маршрутизатор, що відмовив, мережі поширюються по мережі не дуже швидко. У цьому полягає одна з причин вибору як період розсилання невеликої величини в 30 секунд. Механізм таймауту працює в тих випадках, коли маршрутизатор не може послати сусідам повідомлення про маршрут, що відмовив, оскільки або він сам нерoботоздатний, або нерoботоздатна лінія зв'язку, по якій можна було б передати повідомлення.

Коли ж повідомлення послати можна, RIP-маршрутизатори використовують прийом, подається вказівка про нескінченну відстань до мережі, що стала недоступною. У протоколі RIP нескінченною умовно вважається відстань, рівна 16 хопам. Одержавши повідомлення, в якому відстань до деякої мережі рівна 16 (або 15, що приводить до того ж результату, оскільки маршрутизатор нарощує набуте значення на 1), маршрутизатор повинен перевірити, чи виходить ця "погана" інформація про мережу від того ж маршрутизатора, повідомлення якого стало свого часу підставою для запису про дану мережу в таблиці маршрутизації. Якщо це той самий маршрутизатор, то інформація вважається достовірною і маршрут позначається як недоступний.

Те, що за "нескінченну" відстань прийнято таке невелике число, викликане тим, що в деяких випадках відмови зв'язків в мережі викликають тривалі періоди некоректної роботи RIP-маршрутизаторів, що виражається в зацикленні пакетів в петлях мережі. І чим менша відстань, використовувана як "нескінченна", тим такі періоди коротші.

4.2.2.3 Методи боротьби з помилковими маршрутами в протоколі RIP

Хоча протокол RIP не в змозі повністю виключити в мережі перехідні стани, коли деякі маршрутизатори користуються застарілою інформацією

про неіснуючі маршрути, є декілька методів, які у багатьох випадках вирішують подібні проблеми.

Практично всі сьогоднішні маршрутизатори, що працюють за протоколом RIP, використовують техніку розщеплювання горизонту. Якби маршрутизатор R2, у розглянутому вище прикладі підтримував техніку розщеплювання горизонту, то він би не передав маршрутизатору R1 застарілу інформацію про мережу 201.36.14.0, оскільки одержав її саме від маршрутизатора R1.

Проте розщеплювання горизонту не допомагає в тих випадках, коли петлі утворюються не двома, а декількома маршрутизаторами. Розглянемо детальніше ситуацію, яка виникне в мережі, наведеній на рис.4.9, у разі втрати зв'язку маршрутизатора R1 з мережею 201.36.14.0. Хай всі маршрутизатори цієї мережі підтримують техніку розщеплювання горизонту. Маршрутизатори R2 і R3 не повертатимуть маршрутизатору в цій ситуації дані про мережу 201.36.14.0 з метрикою 2, оскільки вони одержали цю інформацію від маршрутизатора R1. Проте вони передаватимуть маршрутизатору інформацію про досяжність мережі 201.36.14.0 з метрикою 4 через себе, оскільки одержали цю інформацію по складному маршруту, а не безпосередньо від маршрутизатора R1. Наприклад, маршрутизатор R2 одержав цю інформацію по ланцюжку R4–R3–R1, тому маршрутизатор R1 знову може бути "обдурений", поки кожний з маршрутизаторів в ланцюжку R3-R4-R2 не викреслить запис про досяжність мережі 201.36.14.0.

Для запобігання зациклення пакетів по складених петлях при відмовах зв'язків застосовуються два інші прийоми, звані тригерними оновленнями і заморожуванням змін.

Прийом тригерних оновлень полягає в тому, що маршрутизатор, одержавши дані про зміну метрики до якої-небудь мережі, не чекає закінчення періоду передавання таблиці маршрутизації, а передає дані про маршрут, що змінився, негайно. Цей прийом може у багатьох випадках запобігти передаванню застарілих відомостей про маршрут, що відмовив, але він перенавантажує мережу службовими повідомленнями, тому тригерні оголошення також робляться з деякою затримкою. З цієї причини можлива ситуація, коли регулярне оновлення в якому-небудь маршрутизаторі трохи випереджає за часом прихід тригерного оновлення від попереднього в ланцюжку маршрутизатора, і даний маршрутизатор встигає передати по мережі застарілу інформацію про неіснуючий маршрут.

Другий прийом – заморожування змін – дозволяє виключити подібні ситуації. Він пов'язаний з введенням тайм-ауту на ухвалення нових даних про мережу, яка тільки що стала недоступною. Цей тайм-аут запобігає ухваленню застарілих відомостей про деякий маршрут від тих маршрутизаторів, які знаходяться на деякій відстані від зв'язку, що відмовив, і передають застарілі відомості про його роботоздатність. Передбачається, що протягом тайм-ауту "заморожування змін" ці маршрутизатори викреслять

даний маршрут з своїх таблиць, оскільки не одержать про нього нових записів і не поширюватимуть застарілі відомості по мережі.

4.2.2.4 Застосування декількох протоколів маршрутизації

У одній і тій самій мережі можуть одночасно працювати декілька різних протоколів маршрутизації. Це означає, що на деяких (не обов'язково всіх) маршрутизаторах мережі встановлено і функціонує декілька протоколів маршрутизації, але при цьому, природно, через мережу взаємодіють тільки однакові протоколи. Тобто, якщо маршрутизатор 1 підтримує, наприклад, протоколи RIP і OSPF, маршрутизатор 2 – тільки RIP, а маршрутизатор 3 – тільки OSPF, то маршрутизатор 1 взаємодіятиме з маршрутизатором 2 за протоколом RIP, з маршрутизатором 3 – за OSPF, а маршрутизатори 2 і 3 взагалі безпосередньо один з одним взаємодіяти не можуть.

У маршрутизаторі, який підтримує одночасно декілька протоколів, кожен запис в таблиці є результатом роботи одного з цих протоколів. Якщо про деяку мережу з'являється інформація від декількох протоколів, то для однозначності вибору маршруту (а дані від різних протоколів можуть привести до різних раціональних маршрутів) встановлюються пріоритети протоколів маршрутизації. Звичайно перевага надається протоколам LSA, як таким що мають в своєму розпорядженні повнішу інформацію про мережу порівнянно з протоколами DVA. У деяких ОС у формах висновку на екран і друк в кожному записі таблиці маршрутизації є відмітка про те, за допомогою якого протоколу маршрутизації цей запис одержаний. Але навіть якщо ця відмітка на екран і не виводиться, вона обов'язково є у внутрішньому поданні таблиці маршрутизації. За замовчуванням кожен протокол маршрутизації працює на певному маршрутизаторі, поширює тільки ту інформацію, яка була одержана цим маршрутизатором за даним протоколом. Таким чином, якщо про маршрут до деякої мережі маршрутизатор дізнався від протоколу RIP, то і поширювати по мережі оголошення про цей маршрут він буде за допомогою протоколу RIP.

4.2.3 Пряма і непряма доставка

Вид доставки IP-пакетів залежить від того, як саме вони пересилаються одержувачеві – прямо або через IP-маршрутизатор.

Пряма доставка (direct delivery) відбувається, коли IP-вузол (хост-відправник або IP- маршрутизатор) пересилає пакет на кінцеву адресу по прямо підключеній мережі. IP-вузол інкапсулює IP-дейтаграму в кадр формату, використовуваного рівнем мережевого інтерфейсу (наприклад, Ethernet або Token Ring), і посилає його на фізичну адресу одержувача.

Непряма доставка (indirect delivery) відбувається, коли IP-вузол (хост-відправник або IP-маршрутизатор) пересилає пакет на проміжний вузол (IP-маршрутизатор) через те, що одержувач знаходиться в іншій мережі, не підключеній напряму. IP-вузол інкапсулює IP-дейтаграму в кадр формату,

використовуваного рівнем мережевого інтерфейсу (наприклад, Ethernet чи Token Ring), і посилає його на фізичну адресу IP-маршрутизатора.

IP-маршрутизація – це комбінація прямої і непрямої доставки. Як показано на рис. 4.10, вузол А при посиланні пакетів вузлу В здійснює пряму доставку, а при посиланні пакетів вузлу С – непряму доставку маршрутизатору 1, що виконує непряму доставку пакетів маршрутизатору 2, а звідти вони прямо доставляються вузлові С.

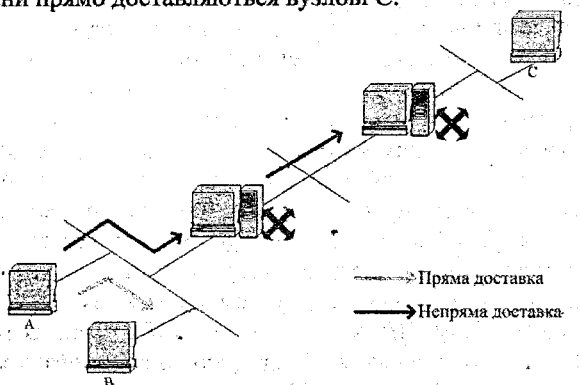

Рисунок 4.10 – Пряма і непряма доставка

4.2.4 Таблиця маршрутизації

У таблиці маршрутизації зберігається інформація про IP-мережі і про маршрути до них (прямі або непрямі). Оскільки всі IP-вузли в тій або іншій формі здійснюють IP-маршрутизацію, такі таблиці не є винятковою приналежністю IP-маршрутизаторів. Таблиця маршрутизації є на кожному вузлі, на якому завантажується TCP/IP, і містить набір записів, стандартних для даної конфігурації вузла. Додаткові записи можна вносити вручну за допомогою утиліт TCP/IP або динамічно (автоматичним опитуванням маршрутизаторів). Перед пересиланням IP-пакета таблиця маршрутизації дозволяє визначити:

- пересильну IP-адресу (forwarding IP address) або IP-адресу наступного переходу (next-hop IP address). При прямій доставці пересильна IP-адреса є IP-адресою одержувача пакета, а при непрямій – IP-адресою маршрутизатора:
- інтерфейс (фізичний або логічний), який потрібно використовувати при пересиланні пакета відправникові або наступному маршрутизаторові

Кожен запис у таблиці маршрутизації містить такі дані.

Мережева адреса. Як цей параметр може бути зазначений ідентифікатор мережі (на основі класу, а також з ідентифікатором підмережі або надмережі) або IP-адреса хоста-одержувача.

Маска мережі. Використовується для порівняння IP-адреси призначення з ідентифікатором мережі. Наступний перехід (або шлюз). Наступна проміжна IP-адреса.

Інтерфейс. IP-адреса, що відповідає мережевому інтерфейсу (мережевому адаптеру), по якому потрібно переслати IP-пакет.

Метрика. Значення, що показує "ціну" маршруту; звичайно виражається числом переходів (тобто кількістю перехресних маршрутизаторів) до кінцевої мережі. Якщо до адресата веде кілька маршрутів, вибирається той, у якого мінімальна метрика – записи можуть зберігати маршрути наступних типів.

Ідентифікатор прямо підключеної мережі. Маршрут до мережі, підключеної прямо. Для таких мереж поле наступного переходу може бути пустим або містити IP-адресу локального мережевого адаптера.

Ідентифікатор віддаленої мережі. Маршрут до мережі, не підключеної напряму, але доступної через інші маршрутизатори. Для таких мереж поле наступного переходу може містити IP-адресу локального маршрутизатора, що знаходиться між пересилаючим вузлом і вилученою мережею.

Маршрут до хосту. Шлях до конкретної IP-адреси. В маршрутах до хостів ідентифікатор мережі є IP-адресою зазначеного хосту, а маска мережі дорівнює 255.255.255.255. Маршрут за замовчуванням. Використовується в тих випадках, коли знайти конкретний ідентифікатор мережі або маршрут до хосту не удасться. У маршрутах за замовчуванням ідентифікатор мережі є значенням 0.0.0.0 а маска – 0.0.0.0.

4.2.5 Визначення маршруту

Вибираючи необхідний для пересилання пакета запис з таблиці маршрутизації, IP використовує такий процес.

- Для кожного запису між IP-адресою одержувача і маскою мережі проводиться побітова логічна операція AND. Результат порівнюється з ідентифікатором мережі в поточному записі.
- Вибирається запис, у якому з IP-адресою одержувача збігається найбільше число бітів. При наявності декількох таких записів (декількох маршрутів до однієї мережі) маршрутизатор вибирає запис з найменшою метрикою, тобто найкоротший маршрут. Якщо метрики в цих записах однакові, маршрутизатор може використовувати будь-як запис.

У кінцевому рахунку з таблиці маршрутизації відбирається єдиний запис. За ним маршрутизатор пізнає пересильну IP-адресу (IP-адреса наступного переходу) і конкретний інтерфейс. Якщо ж знайти маршрут не вдається, IP повідомляє про помилку маршрутизації. Приклад таблиці маршрутизації в Windows 2000 показаний у таблиці 4.13. Він відноситься до хосту (не маршрутизатора) під керуванням Windows 2000 з одним мережевим адаптером і такою конфігурацією. IP-адреса – 157.55.27.90, маска підмереж – 255.255.240.0 (/20), основний шлюз- 15755.16.1.

Маршрут за замовчуванням. Запис, що відповідає конфігурації з основним шлюзом, містить мережеву адресу 0.0.0.0 і маску 0.0.0.0. Будь-яка IP-адреса одержувача, об'єднана з 0.0.0.0 за логічною операцією AND, дає в результаті 0.0.0.0. Отже, маршрут за замовчуванням підходить для будь-якої IP-адреси. Якщо цей маршрут вибирається через відсутність інших маршрутів – IP-пакет пересилається на IP-адресу, зазначену в стовпчику "Адреса шлюзу", по інтерфейсу, що відповідає IP-адресі в колонці "Інтерфейс".

Зворотна мережева адреса. Використовується IP-вузлом для надсилання пакетів самому собі. Ця спеціальна зворотна адреса типу "зворотна петля" (loopback address) завжди дорівнює 127.0.0.1.

Таблиця 4.13 – Таблиця маршрутизації в Windows 2000

Мережева адреса	Маска мережі	Адреса шлюзу	Інтерфейс	Опис
0.0.0.0	0.0.0.0	157..55.16.1	157.55.27.90	Маршрут за замовчуванням
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	Повернення на мережеву адресу
157 .55.16.0	255 255.240.0	157.55.27.90	157.55.27.90	До напряму підключена мережа
157.55.27.90	255.255.255.255	127.0.0.1	127.0.0.1	Локальний хост
157.55.255.255	255.255.255.255	157.55.27.90	157.55.27.90	Адреса широкомовного розсилання
224.0.0.0	224 .0.0.0	157.55.27.90	157.55.27.90	Адреса групового розсилання
255.255.255.255	255.255.255.255	157.55.27.90	157.55.27.90	Адреса обмеженого широкомовного розсилання

4.2.6 Керування таблицею маршрутизації

Керування таблицею маршрутизації на маршрутизаторах у великій розподіленій мережі є складним завданням. Таблиці маршрутизації для відображення поточної мережевої топології повинні бути динамічними. Маршрутизатор обмінюється з іншими маршрутизаторами інформацією про маршрути. До протоколів маршрутизації, що обмінюються інформацією про маршрути в мережах IP, відносяться: Routing Information Protocol (RIP), Open Shortest Path First Protocol (OSPF), Integrated Intermediate System to Intermediate System (IS-IS), Exterior Gateway Protocol (EGP) і Border Gateway Protocol (BGP).

Залежно від структури розподіленої мережі деякі маршрутизатори можуть одночасно підтримувати кілька протоколів маршрутизації. У табл. 4.14 наведено приклад простої таблиці маршрутизації. У цій таблиці містяться записи, типові для таких протоколів маршрутизації, як RIP IP, які використовують як метрика маршруту кількість переходів (hop count). У деяких технічних джерелах зустрічається термін "транзитний вузол".

Кожний запис у таблиці маршрутизації містить таку інформацію:

• наступний маршрутизатор на шляху – IP-адреса вилученого маршрутизатора, якому необхідно надіслати дейтаграми для доставки їх за призначенням;

• кількість переходів – число переходів між поточним маршрутизатором і одержувачем пакета. Кількість переходів – це число маршрути заторів, які повинен перетнути пакет на шляху до одержувача;

• протокол маршрутизації – це набір правил, згідно яких робляться записи у таблицю маршрутизації;

• таймер – час, що пройшов з моменту останнього відновлення запису. Таймер скидається при кожному відновленні.

Таблиця 4.14 – Запис у таблиці маршрутизації

Номер мережі одержувача 128.3.0.0			
Наступний маршрутизатор у шляху	**Кількість переходів**	**Протокол маршрутизації**	**Таймер**
128.5.3.2	3	RIP	145
128.5.4.7	3	RIP	170
128.5.3.9	6	RIP	25

Як правило, у таблицях маршрутизації міститься тільки один маршрут для кожної мережі. Але деякі реалізації протоколів маршрутизації, наприклад OSPF, підтримують кілька маршрутів.

На рис. 4.11 показана невелика розподілена мережа, що складається із чотирьох локальних мереж, зв'язаних трьома маршрутизаторами. У табл. 4.15 показано вміст таблиць маршрутизації сполучних маршрутизаторів. Таблиці маршрутизації містять один запис для кожного маршруту.

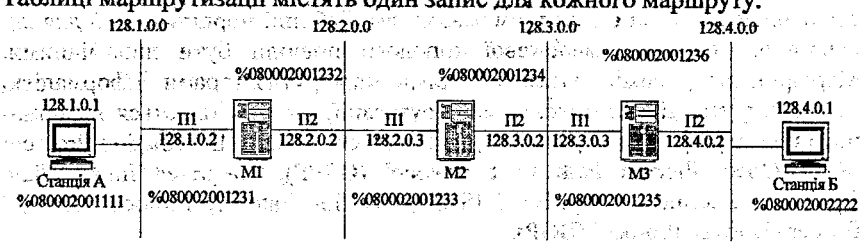

Рисунок 4.11 – Приклад розподіленої мережі

Грунтуючись на рис. 4.11, розглянемо процес передавання інформації від станції А до станції Б через три проміжних маршрутизатори й чотири мережі.

Розподілену мережу можна розглядати як одну велику віртуальну мережу. Шлях, по якому буде передаватися дейтаграма, не визначається її відправником. Кожний маршрутизатор відповідає за доставку дейтаграми тільки на один крок, тобто покладається на наступний маршрутизатор. Ці

проміжні маршрутизатори пересилають її в наступну мережу. Тільки коли дейтаграма досягне одержувача, локальний драйвер IP витягне передане повідомлення з дейтаграми й передасть його протоколам верхнього рівня.

Таблиця 4.15 – Таблиці маршрутизації

Маршрутизатор М1		
Номер мережі	**Наступний маршрутизатор у шляху**	**Кількість переходів**
128.1.0.0	Підключений прямо. Порт 1	0
128.2.0.0	Підключений прямо. Порт 2	0
128.3.0.0	128.2.0.3	1
128.4.0.0	128.2.0.3	2
Маршрутизатор М2		
Номер мережі	**Наступний маршрутизатор у шляху**	**Кількість переходів**
128.1.0.0	128.2.0.2	1
128.2.0.0	Підключений прямо. Порт 1	0
128.3.0.0	Підключений прямо. Порт 2	0
128.4.0.0	128.3.0.3	1
Маршрутизатор М3		
Номер мережі	**Наступний маршрутизатор у шляху**	**Кількість переходів**
128.1.0.0	128.3.0.2	2
128.2.0.0	128.3.0.3	1
128.3.0.0	Підключений прямо. Порт 1	0
128.4.0.0	Підключений прямо. Порт 2	0

Припустимо, що станції А в мережі з адресою 128.1.0.0 необхідно передати інформацію станції Б у мережі з адресою 128.4.0.0. При передачі дейтаграм від маршрутизатора до маршрутизатора потрібно звернути увагу, що IP-заголовок дейтаграми, сформований станцією А, залишається незмінним, а змінюються тільки фізичні адреси кадру канального рівня.

Оскільки станції А і Б розташовуються в різних мережах, то станції А доводиться виконувати непряму маршрутизацію. Для цього вона повинна послати інформацію на найближчий відомий їй маршрутизатор або на маршрутизатор за замовчуванням. Після ініціалізації станція А знає тільки адресу маршрутизатора за замовчуванням – 128.1.0.2. Тому станція А буде використовувати маршрутизатор М1 для передавання інформації будь-якому пристрою, розташованому у вилученій мережі. Якщо в ARP-таблиці станції А немає запису про маршрутизатор за замовчуванням, то вона сформує ARP-запит і буде чекати, коли маршрутизатор М1 відповість на нього. Після того як буде з'ясована фізична адреса маршрутизатора (%080002001231, порт 1 маршрутизатора М1), станція А передасть йому кадр канального рівня.

Після одержання кадру маршрутизатор М1 видалить його заголовок канального рівня й прочитає номер мережі в IP-дейтаграмі – 128.4.0.0. Потім він відшукає відповідний запис у своїй таблиці маршрутизації. Маршрути-

затор М1 знає, що потрібна мережа перебуває на відстані двох переходів від нього, і що він повинен передати цю дейтаграму на порт 1 маршрутизатора М2 з IP-адресою 128.2.0.3. Якщо маршрутизатор М1 не має у своєї ARP-таблиці фізичної адреси порту 1 маршрутизатора М2, він сформує ARP-запит і буде чекати, коли маршрутизатор М2 відповість на нього. Після цього маршрутизатор М1 передасть кадр із фізичною адресою %080002001233 (порт 1 маршрутизатора М2).

Після одержання кадру маршрутизатор М2 видалить його заголовок канального рівня й прочитає номер мережі в IP-дейтаграмі – 128.4.0.0. Потім він відшукає відповідний запис у своїй таблиці маршрутизації. Маршрутизатор М2 знає, що потрібна мережа перебуває на відстані одного переходу від нього, і він повинен передати цю дейтаграму на порт 1 маршрутизатора М3 із IP-адресою 128.3.0.3. Якщо маршрутизатор М2 не має у своїй ARP-таблиці фізичної адреси порту 1 маршрутизатора М3, він сформує ARP-запит і буде чекати, коли маршрутизатор М3 відповість на нього. Після цього маршрутизатор М2 передасть кадр із фізичною адресою %080002001235 (порт 1 маршрутизатора М3).

Після одержання кадру маршрутизатор М3 видалить заголовок канального рівня й прочитає номер мережі в IP-дейтаграмі – 128.4.0.0. Потім він відшукає відповідний запис у своїй таблиці маршрутизації. У такий спосіб він довідається, що потрібна мережа підключена прямо до його порту 2, так що він не повинен передавати цю дейтаграму іншому маршрутизатору. Він може прямо доставити її одержувачеві. Якщо маршрутизатор М3 не має у своєї ARP-таблиці фізичної адреси станції Б, він сформує ARP-запит і буде чекати, коли станція відповість на нього. Після цього маршрутизатор М3 передасть кадр за фізичною адресою %080002002222 станції Б.

Як видно, маршрутизатори повинні перевіряти свої таблиці маршрутизації для визначення того, куди доставити кожну дейтаграму. Якщо маршрут не знайдено, то маршрутизатор повинен видалити дейтаграму. Однак існує спеціальна IP-адреса 0.0.0.0, що власне і є маршрутом за замовчуванням. Якщо шлях у необхідну мережу не знайдений, а в таблиці маршрутизації є запис для маршруту за замовчуванням, маршрутизатор не буде видаляти дейтаграму, а передасть її по цьому маршруту. Введення маршруту за замовчуванням дозволяє зменшити розмір таблиць маршрутизації. У результаті процес маршрутизації спрощується, тому що таблиця маршрутизації містить кілька записів для локальних мереж і маршрут за замовчуванням для всіх інших. Маршрут за замовчуванням незамінний у таких великих мережах, як Internet. Крім зменшення розміру таблиць маршрутизації, використання маршруту за замовчуванням дозволяє значно зменшити розміри повідомлень, якими обмінюються маршрутизатори. Недоліком маршруту за замовчуванням є можливість утворення петель маршрутизації.

4.2.7 Статична і динамічна IP-маршрутизація

Для ефективнішої маршрутизації між маршрутизаторами в міжмережевому IP-середовищі або вони повинні знати ідентифікатори віддалених мереж, або на них повинні бути коректно налаштовані маршрути за замовчуванням. Модифікувати записи в таблицях маршрутизації для IP-маршрутизації можна двома способами.

Вручну. На статичних IP-маршрутизаторах таблиці залишаються незмінними доти, доки їх не модифікує мережевий адміністратор.

Статична маршрутизація заснована на адмініструванні таблиць маршрутизації вручну. У цьому випадку маршрутизаторам не відомі ідентифікатори віддалених мереж і їх потрібно конфігурувати вручну. Статичні маршрутизатори не забезпечують стійкість до збоїв. Якщо такий маршрутизатор аварійно зупиняється, сусідні маршрутизатори не розпізнають цей збій і не повідомляють про нього іншим маршрутизаторам.

Автоматично. На динамічних IP-маршрутизаторах таблиці змінюються автоматично за рахунок обміну інформацією з іншими маршрути заторами. При динамічній маршрутизації для автоматичного відновлення таблиць маршрутизації використовуються маршрутизувальні протоколи, наприклад RIP і OSPF, що дозволяють обмінюватися відповідними даними між маршрутизаторами. Динамічні маршрутизатори одержують інформацію про ідентифікатори віддалених мереж, і вона автоматично вводиться в їхні таблиці маршрутизації. Динамічні маршрутизатори забезпечують стійкість до збоїв. Якщо один з них аварійно зупиняється, сусідні маршрутизатори розпізнають цей збій і передають змінену інформацію про маршрутизацію іншим маршрутизаторам у міжмережевому середовищі.

Контрольні питання до розділу 4

1. Стандарти за TCP/IP.
2. Архітектура стека протоколів TCP/IP.
3. Відповідність протоколів еталонній моделі OSI.
4. Призначення IP-адрес. Пояснити їх необхідність.
5. Охарактеризувати основні класи адрес.
6. Доцільність розбиття мережі на підмережі.
7. Охарактеризувати основні складові стека протоколів TCP/IP.
8. Пояснити необхідність маршрутизації.
9. Основні види маршрутизації. Їх переваги та недоліки для конкретних випадків.
10. Описати основні етапи побудови таблиці маршрутизації.
11. Яким чином можна змінити таблицю маршрутизації залежно від зміни структури мережі?
12. Описати види доставки пакетів в мережі та принципи визначення маршруту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сети TCP/IP. Ресурсы Microsoft Windows 2000 Server / Пер. с англ. – М.: Издательско-торговый дом «Русская Редакция», 2001. – 784 с.
2. Айвенс К. Компьютерные сети. Хитрости. – СПб.: Питер, 2006. – 298 с.
3. Куроуз Дж., Росс К. Компьютерные сети. 2-е изд. – СПб.: Питер, 2004. – 765 с.
4. Компьютерные сети. Практика построения. Для профессионалов. 2-е изд. / М.В.Кульгин. - СПб.: Питер, 2003. - 462 с.
5. Иванова Т. И. Корпоративные сети связи. – М.: ЭКО-ТРЕНДЗ, 2001. – 282 с.
6. Новиков Ю. В., Кондратенко С. В. – Локальные сети: архитектура, алгоритмы, проектирование. – М.: Издательство ЭКОНОМ, 2000. – 312 с.
7. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.
8. Джерри Ли Форд. Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2002. – 272 с.
9. Принципы маршрутизации в Internet, 2-е издание. Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 448 с.
10. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003. – 992 с.
11. Буров Є. Комп'ютерні мережі. – Львів: БаК, 1999. – 468 с.
12. Нейбауэр Алан. Коммуникабельный дом. Локальные сети и Интернет для бизнеса и дома / Практ. Пособ. / Пер. с англ. – М.: Издательство ЭКОМ, 2002. – 560 с.
13. Компьютерная сеть своими руками. Самоучитель / В. Холмогоров. – СПб.: Питер, 2003. - 171 с.
14. Гольдштейн Б. С., Ехриель И. М., Рерле Р. Д. Интеллектуальные сети. – М.: Радио и связь, 2000. – 500 с.
15. Рошан Педжман, Лиэри Джонатан. Основы построения беспроводных локальных сетей стандарта 802.11. / Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 304 с.
16. Сергеев А. П. Офисные локальные сети. Самоучитель. – М.: Издательский дом "Вильямс", 2003. – 320 с.
17. Старовойтов А. А. Сеть на Linux: проектирование, прокладка, эксплуатация. – СПб.: БХВ-Петербург, 2006. – 288 с.
18. Гольдштейн В. С., Пинчук А. В., Суховицкий А. Л. IP-Телефония. – М.: Радио и связь, 2001. – 336 с.
19. Вязовик Н. А. Программирование на Java. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2003. – 592 с.

Навчальне видання

Олена Іванівна Суприган

ОСНОВИ ПРОЕКТУВАННЯ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Навчальний посібник

Оригінал-макет підготовлено Суприган О. І.

Редактор Старічек Т. О.

Науково – методичний відділ ВНТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку 30.12.2008 р.
Формат 29,7×42 1/4
Друк різографічний
Тираж 85 прим.
Зам. № 2009-006

Гарнітура Times New Roman
Папір офсетний
Ум. друк. арк 8.6

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету
Свідоцтво Держкомінформу України
Серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ