МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

КУЗНІЧЕНКО С. Д.

КОМП'ЮТЕРНІ МЕРЕЖІ

Конспект лекцій

Одеса
Одеський державний екологічний університет
2018

УДК 004.7
К89

Рекомендовано методичною радою Одеського державного екологічного університету Міністерства освіти і науки України як конспект лекцій (протокол №9 від 27.06. 2018 р.)

Кузніченко С. Д.
Комп'ютерні мережі: конспект лекцій. Одеса, Одеський державний екологічний університет, 2018. 173 с.

Конспект лекцій містить основи теорії і будови комп'ютерних мереж. Розглянуто структуру каналів зв'язку, передавання сигналів, властивості ліній зв'язку різної фізичної природи, принципи будови мереж на моделі відкритих систем, властивості протоколів, пакетів, технології обміну інформацією. Наведено базові технології найбільш популярних локальних мереж. Розглядаються також основні питання мережного програмного забезпечення.

Рекомендовано для студентів галузі знань 12 "Інформаційні технології" першого (бакалаврського) рівня.

ISBN 978-966-186-098-7

ЗМІСТ

ВСТУП

Дисципліна «Комп’ютерні мережі» є однією з основних дисциплін формуючих фахівців зі спеціальності 122 «Комп’ютерні науки», яка розглядає моделі та методи побудови сучасних локальних і глобальних мереж. Головна увага приділяється аналізу використовуваних протоколів передачі даних як основи побудови механізмів функціювання сучасних комп'ютерних мереж.

Дисципліна викладається у напрямі бакалаврської підготовки і відноситься до циклу професійної та практичної підготовки.

В курсі “Комп’ютерні мережі” викладаються основні принципи організації мереж, топологія фізичних зв'язків і адресація вузлів мережі. Обговорюються питання стандартизації і викладається загальна характеристика моделі ISO/OSI. Описуються різні типи ліній зв'язку і сучасні методи передачі дискретної інформації в мережах.

Аналізуються основні технології локальних мереж, устаткування мереж, що працює на фізичному і канальному рівнях, – структуровані кабельні системи, мережеві адаптери, повторювачі і концентратори різних технологій, а також мости і комутатори. Послідовно розглядаються принципи і механізми об'єднання мереж на основі протоколів мережевого рівня. Оскільки у даний час стек TCP/IP є самим популярним засобом організації міжмережевої взаємодії, то виклад матеріалу проводиться на прикладі IP-мереж.

Дисципліна «Комп’ютерні мережі» знайомить студентів з основними принципами, методами та можливостями технологій комп'ютерних мереж, які включають: топології мереж, багаторівневу системою передачі даних, методи фізичної та логічної структуризації за допомогою мережевого комунікаційного обладнання, особливості адресації вузлів у мережі, протоколи мереж передачі даних, технології локальних та глобальних комп'ютерних мереж.

Внаслідок вивчення дисципліни студент повинен **знати:** архітектури комп’ютерних мереж; принципи структурування мереж; методи передачі дискретних даних на фізичному і канальному рівнях; характеристики ліній зв'язку; принципи стандартизації в комп'ютерних мережах; технології Ethernet, Token Ring, FDDI локальних мереж; етапи діагностики мережі; структуру та основні протоколи стека TCP/IP; типи адресації в IP-мережах.

Студент повинен **вміти:** організовувати обмін інформації між декількома ПЕОМ; використовувати тестові програми і утиліти діагностики мережі; аналізувати конфігурацію мережі; налаштовувати

апаратні мережеві засоби, проводити розрахунки пропускної здатності і конфігурації мережі; організовувати захист комп’ютерних мереж.

1 ОСНОВИ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ

1.1 Загальні принципи будови комп’ютерних мереж

Комп'ютерна мережа (КМ) представляє собою сукупність взаємопов'язаних технічних засобів та програмного забезпечення, призначених для розподіленого оброблення даних, а також для обміну та передачі даних між будь-якими користувачами (абонентами) мережі. До складу технічних засобів входять персональні комп'ютери і сервери, а також вузли комутації та розподілу інформації, об'єднані між собою каналами передачі даних. Інформаційний потік даних, який передається між комп'ютерами мережі, називається *мережевим трафіком* або просто *трафіком*.

Розглянемо основні поняття комп’ютерних мереж, які використовуються в конспекті лекцій у наступних розділах.

– *Абонент* - це пристрій, який підключається до мережі та активно бере участь в обміні інформацією. Частіше всього це комп'ютер, мережевий принтер, модем.

– *Сервер* - це абонент, який обслуговує мережу, віддає в мережу свої ресурси, надає доступ до свого диску. Виділений сервер – сервер, який займається лише обслуговуванням мережі.

– *Клієнт* – це абонент, який не обслуговує мережу, а використовує ресурси мережі. Любий комп'ютер може бути одночасно і сервером, і клієнтом.

– *Проміжний мережевий пристрій* – це пристрій, підключений між комп'ютерами, який бере участь у роботі мережі на низькому рівні. Як правило, проміжний мережевий пристрій поліпшує мережевий обмін, збільшує відстань, зменшує навантаження на частини мережі (сегменти).

– *Середовище передачі даних* – фізична субстанція, по якій відбувається передача інформації від передавача до приймача. Інформація переноситься за допомогою сигналів. Сигнали можуть мати різну природу: електричну, механічну, електромеханічну, електромагнітну, оптичну. Середовище передачі даних є складовою частиною *каналу зв'язку*. Штучні середовища передачі даних здебільшого представлені проводами і кабелями: коаксіальний кабель, кручена пара, оптичний кабель.

– *Мережевий адаптер* – пристрій, що забезпечує інтерфейс між комп'ютером і кабелем. Тобто пристрій сполучення комп'ютерного сигналу

і сигналу, який передається каналами зв’язку. Він часто входить до материнської плати.

– *Швидкість обміну в мережі* – швидкість передачі бітів в одному сеансі передачі. Тобто з якою швидкістю комп'ютер видає біти в середовище передачі даних та навпаки. Цю швидкість найчастіше вказують виробники мереж, але реальна швидкість інтегральна, менша і залежить від багатьох факторів, наприклад, від методу доступу до мережі.

– *Час доступу до мережі* – це часовий інтервал, який проходить між моментом виникнення у комп'ютера бажання передавати інформацію та безпосередньо початком передачі. Цей час очікування впливає на інтегральну швидкість обміну в мережі.

– *Метод доступу до мережі* – це алгоритм дій, який дозволяє комп'ютеру отримати право на передачу.

– *Навантаження на мережу* – це відсоток часу протягом якого в мережі відбувається передача інформації.

– *Мережева технологія* – це погоджений набір програмних і апаратних засобів (наприклад, драйверів, мережевих адаптерів, кабелів і рознімань), а також механізмів передачі даних лініями зв'язку, достатній для побудови обчислювальної мережі.

1.1.1 Класифікація комп'ютерних мереж

Компютерні мережі класифікуються за призначенням, складом обладнання, програмним забезпеченням і функціональними можливостями, за просторовим розміщенням і способом встановлення з’єднання та ін.

За функціональним призначенням розрізняють обчислювальні, інформаційні, інформаційно-обчислювальні і інформаційно-керуючі мережі. *Обчислювальні мережі* призначені для вирішення задач користувачів з розподілом ресурсів між комп’ютерами мережі. *Інформаційні мережі* орієнтовані на інформаційне обслуговування за запитами користувачів. *Інформаційно-обчислювальні мережі* об’єднують функції обчислювальних і інформаційних мереж. *Інформаційно-керуючі мережі* здійснюють збір та обробку оперативної інформації, приймають рішення щодо керування об’єктами або процесами, які розподілені у просторі. Більшість мереж є інформаційно-обчислювальними [1].

За призначанням розрізняють комп’ютерні мережі загального використання (*універсальні*), що обслуговують широке коло різних користувачів, і *спеціалізовані* мережі, що обслуговують спеціалізовані установи чи виробництво.

За типом комп’ютерів, що використовуються розрізняють однорідні *(гомогенні)* мережі, які містять програмно-сумісні комп’ютери, і різнорідні *(гетерогенні)*.

За типом передавального середовища, що використовується, мережі можуть розрізняться на: аналогові, цифрові, радіомережі (у тому числі стільникові мережі і супутникові мережі), кабельні і оптоволоконні мережі.

За розташуванням у просторі (чи за територіальною ознакою) розрізняють *локальні* і *глобальні* мережі.

Локальні мережі (Local Area Networks) – це об'єднання комп'ютерів, зосереджених на невеликій території, зазвичай в радіусі не більше 1-2 км, хоча в окремих випадках локальна мережа може мати і великі розміри, наприклад кілька десятків кілометрів. У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації [2]. Характерною особливістю локальних мереж є використання в якості середовища передачі сигналів високоякісних електричних, оптичних чи інших ліній зв'язку, з передачею зі швидкістю від 10 Мбіт/с до десятків тисяч Мбіт/с. В даний час найбільш широко використовуються наступні локальні мережі: *Fast-* і *Gigabit Ethernet, Token Ring* і *FDDI*.

Глобальні мережі (Wide Area Network, WAN) – мережі, які об'єднують територіально розосереджені комп'ютери, можливо такі, що знаходяться в різних містах і країнах (прикладом може служити мережа Інтернет). У цей час як передавальне середовище в глобальних мережах використовуються аналогові або цифрові провідні канали, а також супутникові канали зв'язку (звичайно для зв'язку між континентами). Глобальна комп'ютерна мережа, як правило, є частиною глобальної телекомунікаційної мережі оператора зв'язку. Глобальні мережі надають послуги двох типів: інформаційні та транспортні. Основними типами транспортних послуг глобальних комп'ютерних мереж є послуги виділених ліній, доступу в Інтернет і віртуальних приватних мереж (VPN). Більшість сучасних глобальних мереж є складовими IP-мережами. Прикладами мережевих технологій глобальних мережах, є мережі PDH, SDH, Frame Relay, ATM, X.25, DWDM, AON.

В окремий клас можна також виділити *регіональні мережі (Metropolitan Area Networks)*, як правило, охоплюють територію в масштабі міста, району, області. Залежно від конкретної реалізації ці мережі можуть ґрунтуватися на технології локальних або глобальних мереж. Регіональні мережі, як правило, різнорідні. *Корпоративні мережі* – це мережі масштаба предпріємства, які об’єднують підмережі окремих підрозділів, що розташовані територіально в різних частинах міста, страни чи континента. Для передачі інформації використовуються лінії і канали зв’язку, які застосовуються як в локальних так і в глобальних мережах. У загальному випадку корпоративна мережа має гетерогенний характер.

Сьогодні розрив між локальними і глобальними мережами постійно скорочується багато в чому через появу високошвидкісних територіальних каналів зв'язку, які не поступаються за якістю кабельним системам локальних мереж. У глобальних мережах з'являються служби доступу до ресурсів, такі ж зручні і прозорі, як і служби локальних мереж. Локальні мережі стали об'єднувати в одну, при цьому як пов'язуюче середовище використовуються глобальні мережі.

За способом встановлення з'єднань між взаємодіючими кінцевими пристроями розрізняють мережі з постійним включенням каналів зв'язку (некомутовані мережі), мережі з комутацією каналів і мережі з комутацією повідомлень і пакетів. У *мережах з комутацією каналів* користувачі з'єднуються наскрізними фізичними або логічними каналами тільки на час обміну інформацією. У *мережах з комутацією повідомлень* передача інформації здійснюється без попереднього з'єднання взаємодіючих вузлів. У цих мережах повідомлення від відправника надходить на вузол комутації повідомлень, де запам'ятовується (ставиться в чергу) і передається за зазначеною адресою відповідно до категорії терміновості. Якщо, необхідні ділянки мережі зайняті, то повідомлення зберігаються на вузлах до звільнення каналу зв’язку або чергового вузла. Під *повідомленням* розуміється логічно завершена послідовність даних – запит на передачу файлу, відповідь на цей запит і т.п. Повідомлення можуть мати довільну довжину – від декількох байт до багатьох мегабайт. Мережа з комутацією пакетів є різновидом мережі з комутацією повідомлень. Довжина *пакета* становить від десятків до декількох тисяч байтів і являє собою послідовність байтів, що складається із заголовка з керуючою інформацією і безпосередньо даних, передану мережею як мінімальна незалежна одиниця повідомлень.

За типом розділення ресурсів (доступу до ресурсів) існуючі комп'ютерні мережі можна поділити на *одноранговi мережі* та *мережі на базі файлового серверу*.

Мережа є одноранговою, якщо кажний ПК може бути одночасно і файловим сервером, і робочою станцією (рис.1.1). Комп'ютери, за допомогою яких користувачі отримують доступ до комп'ютерної мережі, називають *робочими станціями*. В одноранговій ЛОМ дисковий простір і файли на комп'ютерах стають спільними. Одноранговi мережі економічні та вигідні для невиликих колективів. Однією з переваг одноранговых комп'ютерних мереж є те, що користувачеві не потрібно копіювати файл на сервер для того, щоб ним могли користуватися інші. Залежно від того, як встановлений захист даних, інші користувачі зможуть користуватися цими даними одразу ж після їхнього створення.

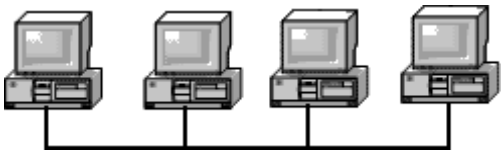


Рисунок 1.1 – Одноранговa ЛОМ

В протилежність одноранговим ЛОМ мережі на базі файл-серверів мають ліпші характеристики і підвищену надійність (рис.1.2). Організація такої мережі можлива за рахунок спеціальних програмних модулів двох типів: *клієнтів (client)*, які формують запити на доступ до віддалених комп'ютерів, та *серверів (server)*, що приймають ці запити з мережі і надають потрібні ресурси.

Рисунок 1.2 – ЛОМ на базі файлового сервера

Мережеві адаптери і канали зв'язку передають повідомлення із запитами і відповідями від одного комп'ютера до іншого, а основну роботу

організації спільного використання ресурсів виконують клієнтські і серверний частини операційних систем. Декілька клієнтів можуть звертатися до одного сервера.

Терміни «клієнт» і «сервер» використовуються не тільки для позначення програмних модулів, але і комп'ютерів, підключених до мережі. У мережах з *архітектурою клієнт/сервер* основна частина спільно використовуваних ресурсів зосереджена на окремих комп'ютерах, які називаються серверами. *Сервер* – це будь-який комп'ютер, підключений до локальної мережі, на якому перебувають ресурси, які використовуються іншими пристроями локальної мережі. *Клієнт* – це будь-який комп'ютер, що через локальну мережу звертається до ресурсів, які зберігаються на сервері. Іноді один і той же комп'ютер може одночасно грати ролі і сервера, і клієнта. Пара модулів «клієнт-сервер» забезпечує спільний доступ користувачів, до певного типу ресурсів, наприклад до файлів. У цьому випадку кажуть, що користувач має справу з *файловою службою (service).* Мережеві служби завжди являють собою розподілені програми. *Розподілена програма* – це програма, яка складається з декількох взаємодіючих частин (в приведеному на рис. 1.3 прикладі з двох), причому кожна частина, як правило, виконується на окремому комп'ютері мережі.

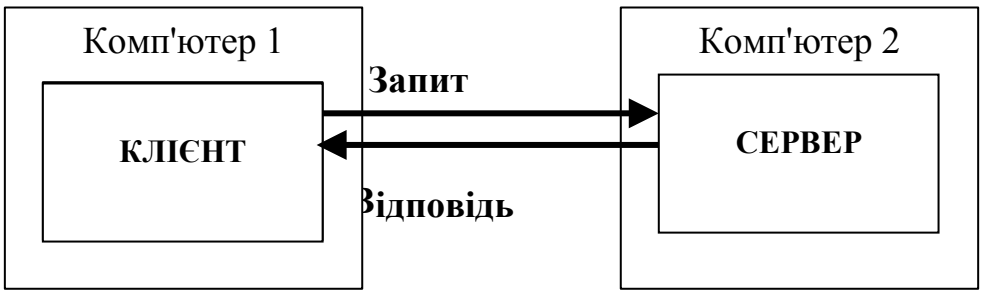


Рисунок 1.3 – Взаємодія частин розподіленого додатку

1.1.2 Топологія комп’ютерних мереж

Кожна мережа має свою топологію. Топологія мережі може мати різні визначення, тобто під поняттям «топологія» можуть розуміти наступне:

- схему розташування комп’ютерів, підключених до мережі;
- структуру кабелів або інших каналів зв’язку, що об’єднують комп’ютери мережі;
- структуру шляхів розповсюдження сигналів мережею;

– спосіб організації інформаційного обміну (розподіл функцій комп’ютерів, напрям основних інформаційних потоків).

В цьому розділі будемо розглядати топологію окремо як структуру кабелів і структуру шляхів розповсюдження сигналів, тому дамо ій наступне визначення.

Мережева топологія – це геометрична форма (або фізична зв’язність) мережі. Конфігурація *фізичних зв'язків* визначається електричними з'єднаннями комп'ютерів між собою і може відрізнятися від конфігурації *логічних зв'язків* між вузлами мережі. Логічні зв'язки являють собою маршрути передачі даних між вузлами мережі і утворюються шляхом відповідного налагодження комунікаційного обладнання.

Деякі базові фізичні топології комп’ютерних мереж наведені на рис.1.4. Для їх порівняння будемо використовувати наступні критерії:

– Стійкість до несправностей комп’ютерів, підключених до мережі – властивість комп'ютерної мережі після виникнення несправності в будь-якому комп’ютері мережі (в його програмному забезпеченні) продовжувати роботу без втручання людини.

– Стійкість до несправностей мережевого обладнання (адаптери, рознімання та ін.) – властивість комп'ютерної мережі після виникнення будь-якої несправності в її апаратному забезпеченні продовжувати роботу без втручання людини, забезпечувати безперервність функціонування і цілісність даних.

– Стійкість до пошкоджень кабелю. Для електричних кабелів – коротке замикання в кабелі.

– Обмеження довжини кабелю через загасання сигналу, який поширюється в ньому.

В залежності від способу з’єднання ланок мережі між собою, розрізняють *двохточкові* та *багатоточкові* з’єднання. У двохточкових з’єднаннях (*Point to Point)* інформація від відправника поступає на один приймач, а в багатоточкових до лінії передачі підключений ряд приймальних пристроїв. Тобто, інформація в багатоточкових підключеннях може передаватися одночасно всім приймачам – *широкомовна передача (broadcasting)*, частині приймачів – *групова передача (multicasting)*, або будь-якому приймачу за вибором – *адресна передача (unicasting)*.

Найбільш оптимальною з погляду надійності (можливості функціонування мережі при виході з ладу окремих вузлів або каналів

зв'язку) є *повнозв'язна мережа*, тобто мережа, в якій кожен вузол мережі пов'язаний зі всіма іншими вузлами. Проте при великої кількості вузлів така мережа вимагає великої кількості каналів зв'язку і її технічно складно реалізувати. Тому практично всі мережі є *неповнозв'язними*.

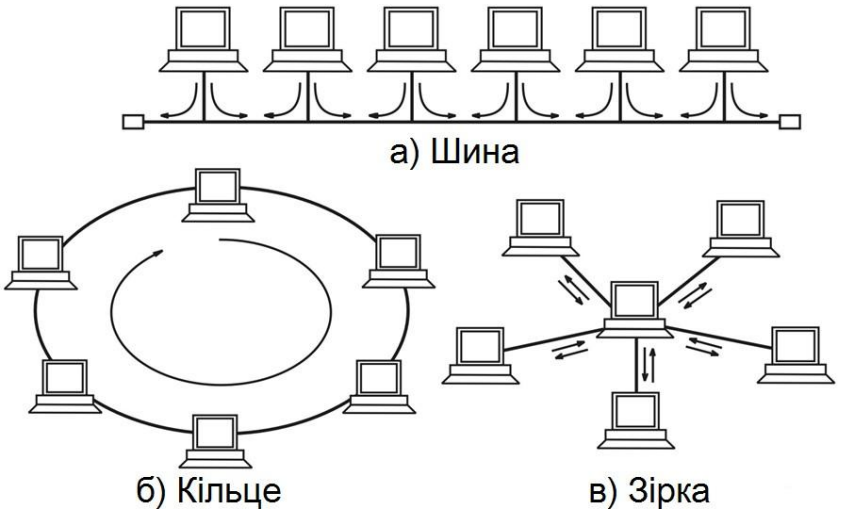


Рисунок 1.4 – Базові топології фізичних зв'язків

Розрізняють наступні базові топології.

Загальна шина (рис.1.4, а) – базова топологія, комп'ютери підключаються до одного коаксіального кабелю за схемою «монтажного АБО». Передана інформація може поширюватися в обидва боки і доступна одночасно всім комп'ютерам. Таким чином, за допомогою шини можна організувати багатоточкову передачу даних. Основними перевагами такої схеми є дешевизна і простота розводки кабелю в приміщеннях. Недоліки загальної шини полягають в її низькій надійності (будь-який дефект кабелю або якого-небудь з численних рознімань повністю паралізує всю мережу) та невисокій продуктивності, оскільки пропускна здатність каналу зв'язку ділиться між всіма вузлами мережі. На кінцях шини знаходяться *термінатори* – кінцеві узгоджувачі. Без включення термінаторів в шину сигнал відбивається від кінців кабелю і спотворюється так, що зв'язок в мережі стає неможливим. Таким чином при розриві або пошкодженні кабелю порушується узгодження лінії зв'язку, і припиняється обмін навіть між тими комп'ютерами, які залишилися фізично з'єднаними між собою. Коротке замикання в будь-якій точці кабелю шини виводить з ладу всю мережу. Хоча в цілому надійність шини все ж порівняно висока, так як вихід з ладу окремих комп'ютерів не порушить працездатність мережі в

цілому, але пошук несправності в шині ускладненний. Будь-яку відмову мережевого обладнання в шині дуже важко локалізувати, тому що всі мережеві адаптери включені паралельно, і складно зрозуміти, який з них вийшов з ладу.

Кільце (рис.1.4, б) – базова топологія, що забезпечує підключення типу point-to-point. У мережах, побудованих відповідно до топології кільце, передача даних здійснюється від одного комп'ютера до іншого по кільцю через мережеві адаптери, поки інформація не дійде до адресата, записується в його внутрішній буфер, потім далі рухається по кільцю до відправника і відправник її видаляє. Кільце являє собою дуже зручну конфігурацію для організації зворотного зв'язку. Дані, зробивши повний обіг, повертаються до вузла-джерела, тому цей вузол може контролювати процес доставки даних адресату. Часто ця властивість кільця використовується для тестування зв'язаності мережі і пошуку вузла, працюючого некоректно. Крім того, кожний комп’ютер посилює сигнала, що проходить через нього, тому ця топологія використовується для побудови великих мереж. Топологія кільце не стійка до несправностей комп'ютерів та обриву кабелю. Щоб усунути цей недолік використовують два кільця для підключення вузлів. Одне основне, інше – резервне на випадок обриву. Тому кільцеві топології вимагають багато кабелю, особливо при використанні подвійного підключення.

Зірка (рис.1.4, в) – базова топологія в якій кожний комп'ютер приєднується окремим кабелем до загального пристрою, що перебуває в центрі мережі. Якщо цей пристрій є комп’ютером, то топологія носить назву *активна зірка*, якщо в центрі розташовується проміжний пристрій концентратор (hub) – *пасивною зіркою* (рис.1.5). У функції концентратора входить направлення переданої комп'ютером інформації одному або всім іншим комп'ютерам мережі. Головна перевага цієї топології перед загальною шиною – істотно більша надійність. Будь-які несправності кабелю стосуються лише того комп'ютера, до якого цей кабель приєднаний, і тільки несправність концентратора може вивести з ладу всю мережу. До недоліків топології типу зірка відноситься більш висока вартість мережевого обладнання через необхідність придбання концентратора. Крім того, можливості по нарощуванню вузлів в мережі обмежуються кількістю портів концентратора.

Дерево (рис.1.6) – топологія, яка будується з використанням декількох концентраторів, ієрархічно з'єднаних між собою зв'язками типу зірка. У

цей час ієрархічна зірка або дерево є найпоширенішим типом топології зв'язків як у локальних, так і глобальних мережах.

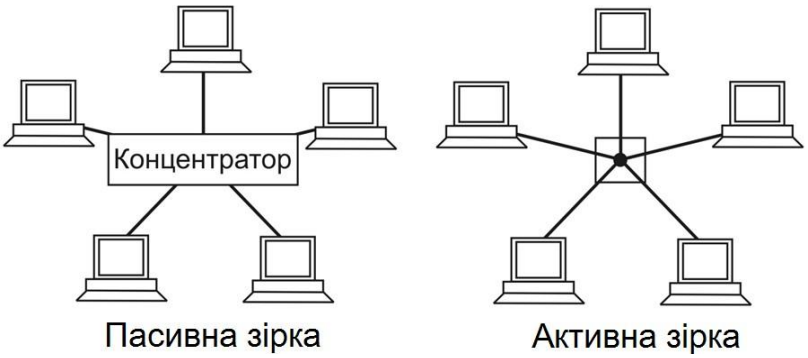


Рисунок 1.5 – Топології активна і пасивна зірка

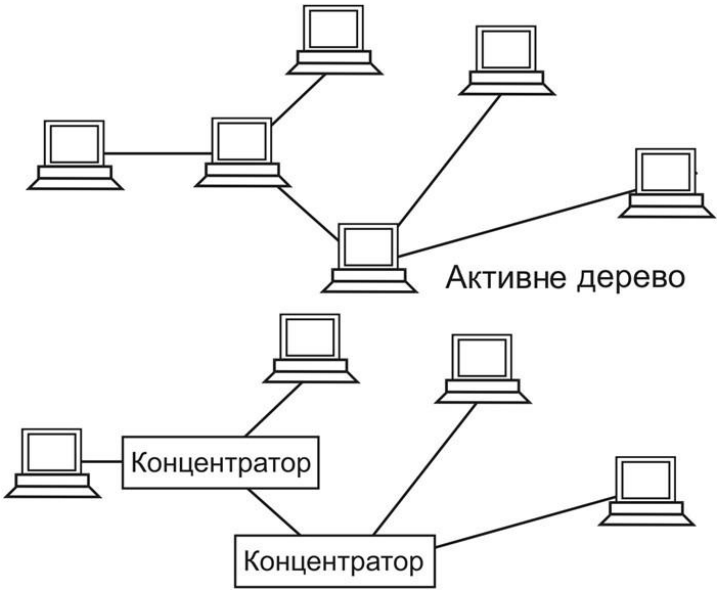


Рисунок 1.6 – Топологія дерево

Мережі можуть бути також змішаної топології, коли окремі частини мережі мають різну типову топологію. Прикладом може служити локальна мережа FDDI, в якій основні (магістральні) вузли підключаються до кільцевого каналу, а до них за ієрархічною топологією підключаються інші вузли (рис.1.7).

1.1.3 Типи адрес комп’ютерів. Адресація в IP-мережах

Адреса комп’ютера повинна унікально ідентифікувати комп'ютер в мережі будь-якого масштабу. У цей час найбільше поширення отримали три схеми адресації вузлів. Розглянемо їх на прикладі адресації в IP – мережах, побудованих на базі стека протоколів TCP/IP.

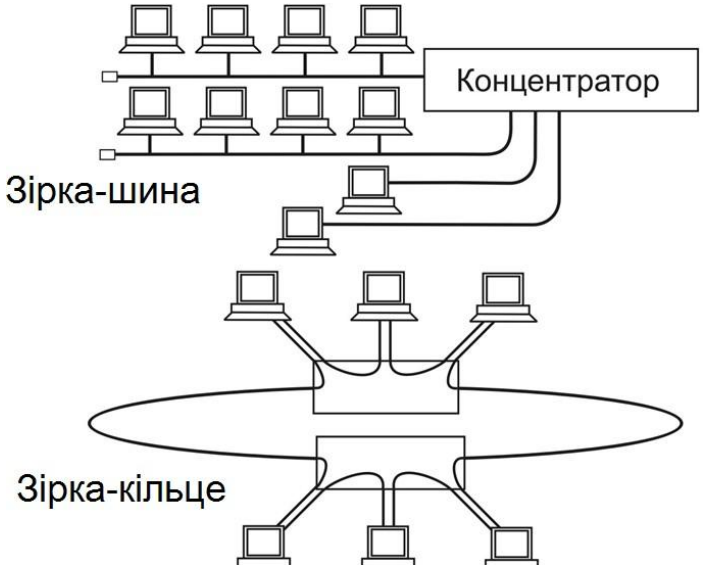


Рисунок 1.7 – Змішані топології

Локальна або *апаратна (hardware)* адреса вузла використовується для доставки даних в межах тільки однієї мережі. Для вузлів, що входять у локальні мережі – це *MAC-адреса* (від *Media Access Control*) мережевого адаптера або порту маршрутизатора. Записують її у вигляді двійкового або шістнадцядкового значення, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками устаткування і є унікальними адресами, тому що управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байтів: старші 3 байти - ідентифікатор фірми виробника, а молодші 3 байти призначаються унікальним чином самим виробником (рис.1.8).

1 біт	1 біт	22 біта	24 біта
I/G	U/L		

Рисунок 1.8 - Структура MAC-адреси

Крайній лівий біт числа називається ознакою індивідуальної або групової адреси (I/G). Якщо біт дорівнює 0, то інші біти визначають індивідуальну адресу; значення 1 вказує на те, що інші біти визначають групову адресу. Якщо другий біт (U/L) дорівнює 0, то адреса підмережі є універсальною, тобто призначеною комітетом IEEE, у противному випадку адреса є локальною.

Символьні адреси. Доменне, або символьне ім'я, наприклад, www.cisco.com – адреса, що призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домена. Така адреса, що також називається DNS-ім'ям, використовується на прикладному рівні, наприклад, у протоколах FTP або telnet. Ці адреси призначені для запам'ятовування людьми і тому звичайно несуть смислове навантаження. Символьне ім'я може мати складну ієрархічну структуру. Ієрархія доменних імен аналогічна ієрархії імен файлів, однак запис доменного імені починається із наймолодшої складової, а закінчується найстаршою. Наприклад, в імені partnering.microsoft.com складова partnering є ім'ям одного з комп'ютерів у домені microsoft.com. Сукупність імен, у яких кілька старших складових частин збігаються, утворять домен (domain) імен. Наприклад, імена www.chip.kiev.ua, www.itc.kiev.ua і www.infocity.kiev.ua входять у домен kiev.ua. Структура DNS схожа на структуру дерева каталогів комп'ютера. На вершині ієрархії перебуває кореневий каталог, що не має імені. Кожний домен, так само, як і каталог комп'ютера, має власне ім'я. Так само як каталог може мати підкаталоги, кожний домен в DNS може поділятися на декілька піддоменів. Відразу після кореневого домена розташовані групи доменів верхнього рівня, які можуть позначати організацію, до якої належить власник даної мережі (табл.1.1) або географічне місце розташування, у відповідності зі списком, розробленим національним інститутом стандартів (ISO 3166), наприклад, ua (Україна), ru (Росія), uk (Великобританія).

Мережеві (числові) адреси. Символьні імена зручні для людей, але через змінний формат і велику довжину їх передача в мережі не економічна. Тому для роботи у великих мережах використовують числові адреси фіксованого і компактного форматів. Типовим представниками адрес цього типу є IP і IPX-адреси.

IP-адреса використовується на мережевому рівні і призначається адміністратором мережі під час конфігурування комп'ютерів і маршрутизаторів. Адресація (IPv4) припускає використання 32-бітного

коду. IP-адресу прийнято записувати у вигляді чотирьох октетів, у десятковій системі числення, наприклад:

Таблиця 1.1 – Трибуквені домени верхнього рівня

Домен	Опис
com	Комерційні організації
edu	Освітні установи, наприклад, коледжі і університети
gov	Урядові заклади США
int	Міжнародні організації
mil	Військові організації США
net	Мережа, що не попадає в жодну з перерахованих вище категорій
org	Організація, що не попадає в жодну з перерахованих вище категорій

IP-адреса 192.168.7.129 – це код 11000000 10101000 00000111 10000001.

IP-адреса складається із двох частин: адреси мережі (net) і адреси вузла (host). Адресу мережі часто звуть *префіксом* мережевої адреси, а адресу хоста – *суфіксом*. Адреса вузла в протоколі IP призначається незалежно від його локальної адреси. Поділ IP-адрес на поле адреси мережі і адреси вузла – гнучкий, а межа між цими полями може встановлюватися довільно. Вузол може входити до декількох IP-мереж. В цьому випадку вузол повинний мати декілька IP-адрес за кількістю мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

Існує 5 класів IP-адрес (рис.1.9).

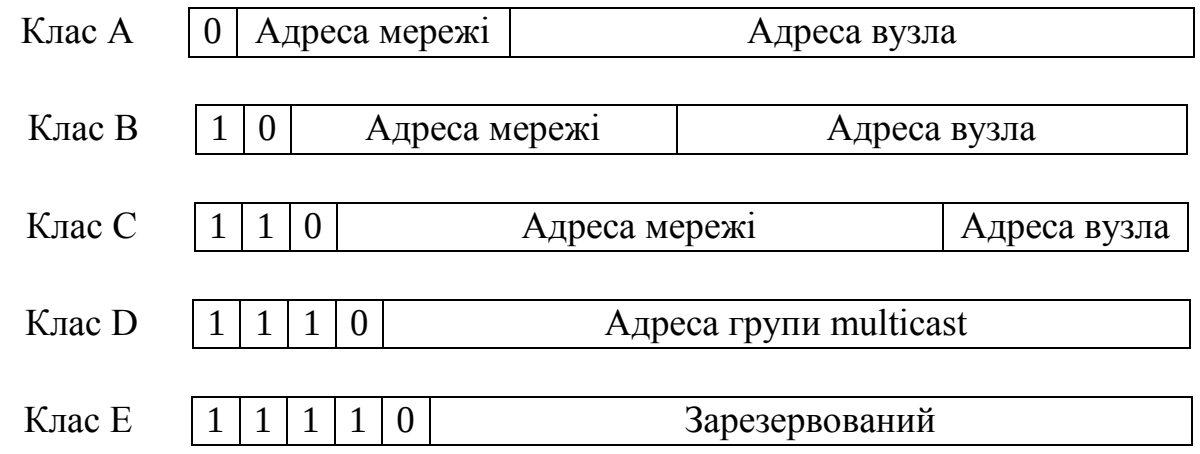


Рисунок 1.9 – Структура IP-адрес

Для виділення адрес мережі та хоста (вузла) використовується маска підмережі (*net mask*) – бітовий шаблон, в якому бітам, що використовуються для адреси мережі, присвоюються значення 1, а бітам адреси вузла – значення 0. Так, маска мережі 255.255. 255.0 (11111111 11111111 11111111 00000000) визначає, що поле адреси мережі містить 24 біта, а поле адреси вузла – 8 біт. Наприклад, для адреси 192.168.7.129 це означає: 192.168.7 – мережева частина (адресу мережі прийнято записувати 192.168.7.0), а 129 – адреса вузла в цій мережі. Відповідно до класової моделі IP-адресації існує певний пул адрес кожного класу, який дозволяє адресувати лише певну кількість мережевих вузлів. Так у класі В можливо адресувати 2^6 = 16 384 мереж і 2^{16}-2 = 65 534 вузлів в мережі.

У кожному із класів IP-мереж визначено «приватний простір IP-мереж» (табл.1.2), адреси якого призначені для використання лише в локальних комп'ютерних мережах і не маршрутизуються в глобальних мережах (відкидаються на магістралях Інтернет).

Таблиця 1.2 – Приватні IP-адреси

Клас мережі	Початкова адреса	Кінцева адреса	Кількість мереж	Кількість вузлів у мережі
A	10.0.0.0	10.255.255.255	1	16 777 214
B	172.16.0.0	172.31.255.255	16	65 534
C	192.168.0.0	192.168.255.255	256	254

Крім того, визначені особливі IP-адреси, що мають спеціальне призначення, і не можуть використовуватися в якості унікальної мережевої адреси вузла (табл.1.3).

IP-адреса призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів, при цьому номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet *(Network Information Center, NIC)*, якщо мережа повинна працювати як складова частина Internet. У великих мережах підтримується автоматичний розподіл адрес на основі протоколу *Dynamic Host Configuration Protocol (DHCP)***.** Протокол DHCP працює відповідно до моделі клієнт-сервер. Під час старту системи комп'ютер, що є DHCP-клієнтом, посилає всім комп'ютерам мережі повідомлення-запит (таке повідомлення називається *широкомовним*) на одержання IP-адреси. DHCP-сервер відгукується й посилає повідомлення-відповідь, що містить

IP-адресу, із заздалегідь визначеного адміністратором діапазону вільних для розподілу адрес, і деякі інші конфігураційні параметри. Передбачається, що DHCP-сервер і DHCP-клієнт находяться в одній IP-мережі.

Таблиця 1.2 – Спеціальні «особливі» IP-адреси

Адреса мережі	Адреса вузла	Опис
Усі «0»	Усі «0»	Адреса вузла, що згенерував пакет[1].
Усі «0»	Адреса вузла	Вузол призначення належить до тієї ж IP-мережи, що і вузол відправлення
Адреса мережі	Усі «0»	Адреса IP-мережі
Адреса мережі	Усі «1»	Обмежена широкомовна адреса (в межах даної IP-мережі)
Усі «1»	Усі «1»	«Глобальна» широкомовна адреса
127.0.0.1		Адреса зворотного зв’язку (loopback), призначена для тестування обладнання без реального відсилання пакету

У сучасних мережах для адресації вузлів застосовуються, як правило, одночасно всі три приведені вище схеми. Користувачі адресують комп'ютери символьними іменами, які автоматично замінюються в повідомленнях, що передаються по мережі, на IP-адреси. За допомогою цих мережевих адрес повідомлення передаються з однієї мережі в іншу, а після доставки повідомлення в мережу призначення замість IP-адреси використовується локальна MAC-адреса комп'ютера.

Проблемою встановлення відповідності між адресами різних типів займається *служба дозволу імен.*

Протокол ARP. Для реалізації механізму перетворення IP-адрес у локальні MAC-адреси був розроблений протокол перетворення адрес *ARP (Address Resolution Protocol)*. ARP веде таблицю відповідності між IP-адресами і локальними адресами, яка називається *таблицею APR*. Крім того, ARP підтримує кеш записів - *кеш ARP*.

Алгоритм роботи протоколу ARP:

1. Звичайно пошук починається з кеша ARP, і тільки у випадку невдачі дані шукаються в таблиці ARP. Записи кеша ARP, які були динамічно

[1] Може використовуватися у випадку коли вузол був щойно підключений до мережі, ще не має унікальної адреси і виконує запит на одержання IP-адреси до DHCP-серверу.

згенеровані, стають недійсними при закінченні інтервалу тайм-ауту, тоді як на статичні записи тайм-аут не поширюється. Знищення статичних записів у результаті тайм-ауту є ознакою псування даних у кеші ARP.

2. Якщо в записах таблиці необхідна IP-адреса не знайдена, то вихідний IP-пакет запам'ятовується в буфері, а протокол ARP формує запит (*ARP запит*) і розсилає його широкомовно.

3. Всі інтерфейси підмережі одержують ARP-запити і порівнюють зазначену там адресу з власною. При збігу вузол чи маршрутизатор формує *ARP - відповідь*, вказуючи в ньому свої IP і MAC адреси та відправляє його за IP-адресою вузла відправника ARP-запиту.

Структура ARP-запита наведена на рис.1.10.

<table>
<tr><td colspan="2">Тип мережі (16 біт)</td></tr>
<tr><td colspan="2">Тип протоколу (16 біт)</td></tr>
<tr><td>Довжина локальної адреси</td><td>Довжина мережевої адреси</td></tr>
<tr><td colspan="2">Код операції (16 біт)</td></tr>
<tr><td colspan="2">Локальна адреса відправника</td></tr>
<tr><td colspan="2">IP-адреса відправника</td></tr>
<tr><td colspan="2">Локальна адреса одержувача</td></tr>
<tr><td colspan="2">IP-адреса одержувача</td></tr>
</table>

Рисунок 1.10 – Структура запитів і відповідей ARP

Поле «Тип протоколу» дозволяє використовувати протокол ARP не тільки для протоколу IP, але й для інших мережевих протоколів. У полі коду операції для ARP-запитів вказується значення 1, якщо це запит, і 2, якщо це відповідь.

4. Якщо в мережі немає машини із шуканою IP-адресою, то ARP-відповіді не буде. Протокол IP знищує IP-пакети, спрямовані за цією адресою.

5. Якщо відповідність знайдена, то вона записується в ARP-таблицю відповідного інтерфейсу. Новий запис в ARP-таблиці з'являється автоматично, через декілька мілісекунд після того, як модуль ARP проаналізував ARP-відповідь. Крім динамічних записів, побудованих на підставі даних широкомовних розсилань, ARP-таблиці можуть містити

статичні записи, які створюються вручну за допомогою утиліти arp і не мають строку старіння по тайм-ауту.

Недоліком такого підходу є необхідність широкомовних повідомлень такі повідомлення перевантажують мережу, оскільки вони вимагають обов'язкової обробки всіма вузлами, а не тільки вузлом призначення.

Для перетворення MAC-адреси в IP-адресу використовується реверсивний протокол *ARP (Reverse Address Resolution Protocol, RARP)*.

Служба DNS. У великих мережах поширення широкомовних повідомлень по всіх її сегментах стає практично нереальним, тому для них характерний централізований підхід. У разі централізованого підходу в мережі виділяється один комп'ютер (*сервер імен*), в якому зберігається таблиця відповідності один одному імен різних типів, наприклад символьних імен і мережевих адрес. Всі інші комп'ютери звертаються до сервера імен, щоб за символьним ім'ям знайти мережеву адресу комп'ютера, з яким необхідно обмінятися даними.

Найбільш відомою службою централізованого дозволу імен є служба *Domain Name System (DNS)* мережі Internet. Служба DNS використовує протокол типу «клієнт-сервер». У ньому визначені DNS-сервери і DNS-клієнти, які звертаються до серверів із запитами про перетворення доменних імен в IP-адресу. Для кожного домена імен створюється свій DNS-сервер. Кожний DNS-сервер крім таблиці відображень імен містить посилання на DNS-сервери своїх піддоменів. Ці посилання зв'язують окремі DNS-сервери в єдину службу DNS. Спілкуючись один з одним, сервер із сервером, будь-який сервер DNS може перетворити будь-яку мережеву адресу в Internet. На рис. 1.11 показана схема роботи серверів DNS в Internet.

Кореневий сервер (root) знає, який із серверів може перетворити адреси кожного з доменів верхнього рівня. Сервери наступного рівня знають про сервери своїх підлеглих рівнів і т.д.

Кожний сервер обслуговує одну або кілька зон у дереві DNS. Адміністратор DNS спеціально налаштує сервер на роботу зі своєю зоною відповідальності. За правилами Internet, кожній зоні відповідає один первинний (primary) і один або декілька вторинних (secondary) серверів. Вторинні сервери вступають у роботу, коли первинний виявляється перевантаженим або виходить із ладу. Первинні і вторинні сервери DNS незалежні. Ціль наявності декількох серверів DNS в одній і тій же зоні -

забезпечити надійність функціонування. Збій у роботі одного із серверів DNS не спричинить повної зупинки роботи цієї служби.

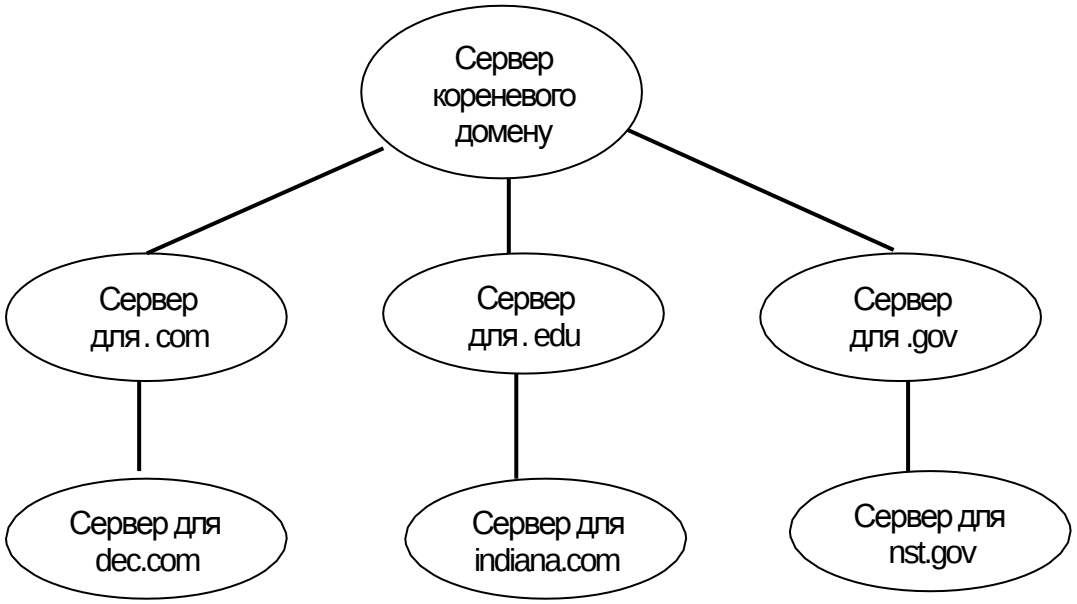


Рисунок 1.11 – Схема роботи серверів DNS в Internet

1.1.4 Безкласова модель IP-адресації, маска змінної довжини

Недоліком класової системи адресації є нерівномірне і не ефективне використання адресного простору всередині класу. Наприклад, якщо користувачу потрібно побудувати мережу з 1000 хостами, то йому може бути виділений один адрес класу В. Тобто з 2^{16} можливих адрес комп'ютерів буде використовуватися лише невелика частина, інші адреси (більше 64 тис.) ніким іншим не можуть бути використані.

Технологія безкласової міждоменної маршрутизації (Classess Inter Domain Routing, CIDR) дозволяє замінити традиційне використання класів адрес протоколів IP на узагальнений *мережевий префікс*. Довжина мережевого префікса допомагає визначити кількість старших біт, що відповідають адресі мережі. Таким чином, блок адрес може бути розбитий довільним чином на префікс мережі і суфікс хосту. Була запропонована спеціальна скорочена форма запису, яку назвали *формою запису CIDR (CIDRnotation)*,і відповідно якої спочатку вказують початкову адресу блока, а потім через косу риску – довжину маски в бітах, яка виражена

цілим десятковим числом. Наприклад, 128.211.168.0/21, тут маска дорівнює 255.255.255.248.0.

Одним зі способів вирішити проблему дефіциту IP-адрес і зростання розмірів таблиць маршрутизації складається у використанні механізму підмереж *(subnetting).* Суть цього механізму складається в розбитті вузлової частини IP-адреси на два поля: поле адреси підмережі і поле адреси вузла (хоста). При цьому внутрішня структура мережі (розбиття її на підмережі) «не видна ззовні», що означає незалежність зовнішньої маршрутизації (доставки пакетів *до* або *від* даної мережі) від її внутрішньої структури. Для виділення підмереж у мережі адміністратору необхідно визначити кількість підмереж і кількість вузлів у кожній підмережі з урахуванням потреб мережі. Наприклад, якщо необхідно розбити мережу 192.168.7.0 (блок містить 256 адрес) на 8 підмереж з максимальною кількістю вузлів 30 у кожній підмережі, те по-перше, потрібно визначити кількість біт у полі адреси підмережі (3 біти тому що 2^3=8) і в полі адреси вузла (5 біт тому що 2^5=32). Максимальна кількість вузлів у підмережі дорівнює 30-ти, а не 32, тому що коди, що містять всі одиниці і всі нулі, не можуть бути адресою вузла. Визначивши поля адреси підмережі і вузла, запишемо маску підмережі:

11111111 11111111 11111111 11100000 – *255.255. 255. 224.*

Адреси підмереж, отримані в результаті застосування маски підмережі:

192. 168.7. 0 підмережа №0
192. 168.7.32 підмережа №1
192. 168.7.64 підмережа №2
192. 168.7.96 підмережа №3
192. 168.7. 128 підмережа №4
192. 168.7. 160 підмережа №5
192. 168.7. 192 підмережа №6
192. 168.7. 224 підмережа №7

В наш час 32-бітова адресація *IPv4* вже не задовольняє потреби мережі Інтернет. Нова версія *IPv6* має 128-бітовий формат IP-адреси і підтримує автоматичне призначення адрес. У новій версії не підтримуються класи адрес (A, B, C, D, E), але широко використовується технологія CIDR.

Розробники стандарту запропонували використовувати замість десяткової шістнадцяткову форму записи IP-адреси. Кожні чотири шістнадцяткові цифри відокремлюються одна від одної двокрапкою,

наприклад, FEDC: 0A98: 0: 0: 0: 0: 7654: 3210. Для мереж, що підтримують обидві версії протоколу (IPv4 та IPv6), дозволяється задіяти для молодших чотирьох байт традиційну для IPv4 десяткову запис: 0: 0: 0: 0: 0: FFFF: 129.144.52.38.

У новій версії IPv6 передбачено три основні типи адрес:

– *Індивідуальна адреса (unicast)* є унікальним ідентифікатором окремого інтерфейсу кінцевого вузла або маршрутизатора. Призначення цього типу адреси збігається з призначенням унікальних адрес в версії IPv4.

– *Групова адреса (multicast)* аналогічна за призначенням груповій адресі IPv4 – ідентифікує групу інтерфейсів, що відносяться, як правило, до різних вузлів. Пакет з такою адресою доставляється всім інтерфейсам, що має таку адресу. У версії IPv6 групова адресу має ознаку *scope*, яка відсутня в груповій адресі версії IPv4. Ця ознака дозволяє гнучко задавати область дії групової адреси, яка може являти собою, наприклад, тільки одну підмережу, тільки все підмережі даного підприємства або весь Інтернет. Це спрощує роботу маршрутизаторів, яким необхідно виявляти всі вузли, які відносяться до будь-якої групі.

– *Адреса довільної розсилки (anycast)* – це новий тип IP-адреси, що визначає групу інтерфейсів. Але на відміну від групової адреси пакет, в поле адреси призначення якого знаходиться адреса довільної розсилки, доставляється одному з інтерфейсів групи, як правило, «найближчому», відповідно за метрикою, що використовується протоколами маршрутизації.

1.1.5 Багаторівнева модель OSI. Протокол, інтерфейс, стек протоколів

Комп’ютерна мережа представляє собою складну систему, елементами якої є різні апаратні і програмні засоби, для узгодженої роботи яких необхідні правила і стандарти взаємодії цих засобів на різних рівнях.

На підставі досвіду розробки і експлуатації комп’ютерних мереж міжнародною організацією по стандартизації ISO (International Standard Organization) була розроблена *еталонна модель взаємодії відкритих систем OSI (Open Systems Interconnection)*, яка прийнята в якості міжнародного стандарту. Модель OSI розділяє процеси, які беруть участь у сеансі зв'язку, на сім функціональних рівнів (рис.1.12): *фізичний, канальний, мережевий, транспортний, сеансовий, представницький* і

прикладний. Структура рівнів відповідає природній послідовності подій, що відбуваються під час сеансу зв'язку.

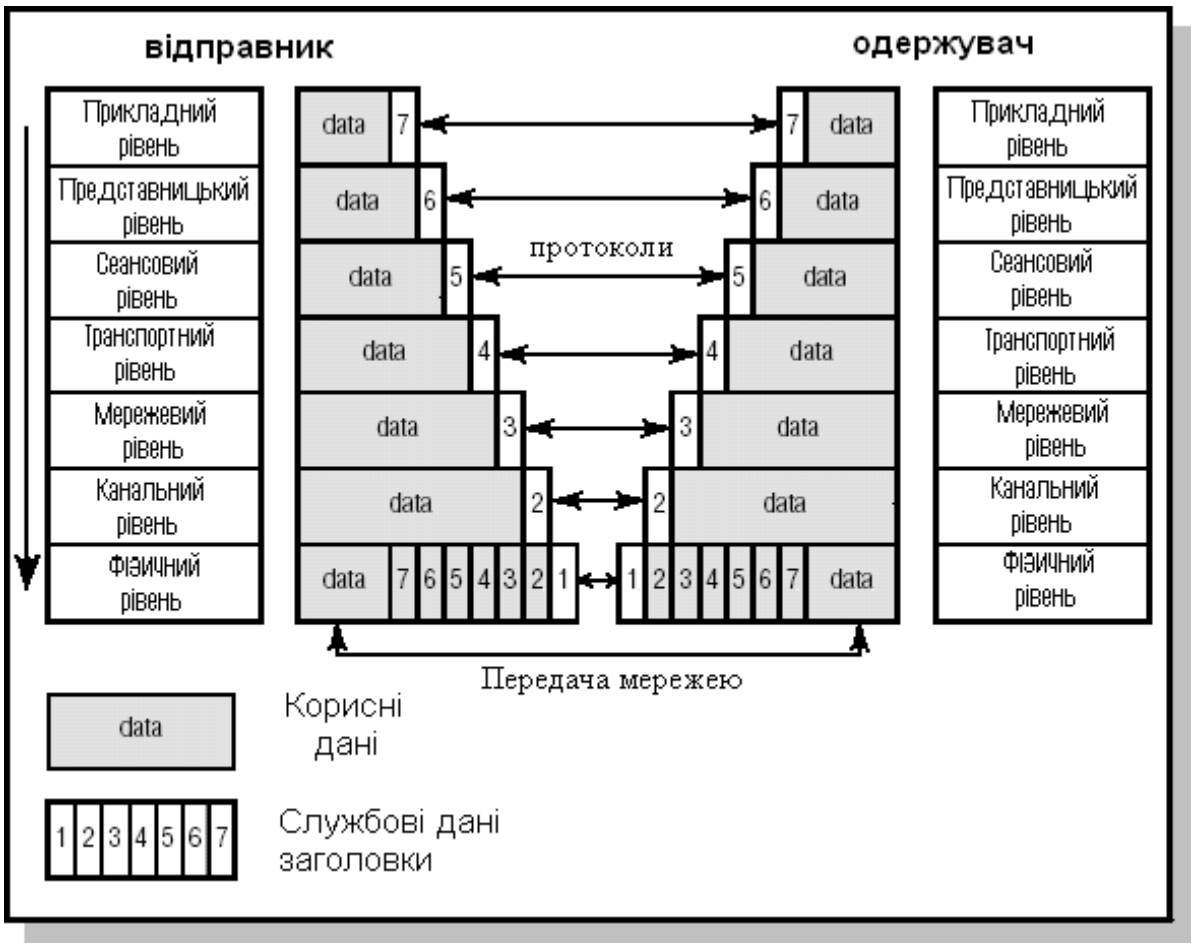


Рисунок 1.12 - Модель взаємодії відкритих систем ISO/OSI

Обмін даними між рівнями здійснюється інформаційними пакетами певного формату. Пакет представляє собою коротке повідомлення (порцію інформації) довжиною до декількох тисяч байтів. Він є самостійною частиною повідомлення, що адресується, і пересувається мережею незалежно від інших пакетів. В кожному пакеті окрім даних міститься керуюча інформація, що розміщується в заголовках. Структура пакету може розрізнятися в різних мережах, але найчастіше пакет містить в собі такі основні поля або частини (рис. 1.13):

– Стартова комбінація, або преамбула, яка забезпечує настройку апаратури адаптера або іншого мережевого пристрою для отримання і обробки пакета. Це поле може бути відсутнім або зводитися до одного-єдиного стартовому біту.

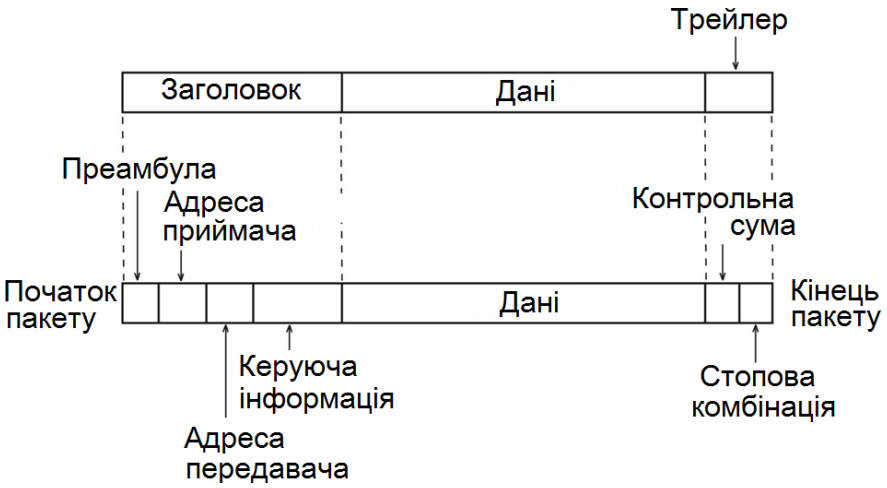


Рисунок 1.13 – Типовий формат пакета

– Мережевий адреса приймача, тобто індивідуальний або груповий номер, який має кожний приймаючий абоненту в мережі.

– Мережевий адреса передавача, тобто індивідуальний або груповий номер, який має кожний абоненту, що передає дані. Включення в пакет адреси передавача необхідно в тому випадку, коли до одного приймача можуть поперемінно приходити пакети від різних передавачів.

– Службова керуюча інформація, яка вказує на тип пакета, його номер, розмір, формат, маршрут його доставки, на те, що з ним треба робити приймача і т.п.

– Дані – та інформація, заради передачі якої використовується даний пакет. Можуть існувати спеціальні керуючі пакети, які не мають поля даних. Їх можна розглядати як мережеві команди. Пакети, що включають поле даних, називаються інформаційними пакетами. Керуючі пакети можуть виконувати функцію початку сеансу зв'язку, кінця сеансу зв'язку, підтвердження прийому інформаційного пакета, запиту інформаційного пакета і т.п.

– Контрольна сума пакета – це числовий код, що формується передавачем за певними правилами і містить в згорнутому вигляді інформацію про пакет. Приймач, повторюючи обчислення, зроблені передавачем, з прийнятим пакетом, порівнює їх результат з контрольною сумою і робить висновок про правильність або помилковість передачі пакета. Якщо пакет помилковий, то приймач запитує його повторну передачу.

– Стопова комбінація служить для інформування апаратури приймача про закінчення пакету, забезпечує вихід апаратури приймача зі стану прийому. Це поле може бути відсутнім.

При просуванні пакету зверху вниз по рівням моделі (передача в мережу) кожен рівень додає до пакету свій заголовок. При просуванні пакету від низу до верху (прийом з мережі) кожен рівень обробляє пакет згідно керуючої інформації в заголовку, доданої до пакету відповідним рівнем сторони, яка передає. Таким чином, однакові рівні на різних системах спілкуються між собою за певними правилам. Сукупність процедур і правил взаємодії об'єктів однойменних рівнів називається *протоколом*. Вкладений набір рівнів утворює набір протоколів, який достатній для організації взаємодії вузлів в мережі, і отримав назву *стек протоколів*. Правила взаємодії суміжних рівнів однієї і тієї ж системи визначають *міжрівневий інтерфейс*. Інтерфейс визначає набір сервісів, що надається даним рівнем сусідньому рівню.

У моделі OSI розрізнюються два основних типи протоколів. У протоколах *з встановленням з'єднання* (connection-oriented) перед обміном даними відправник і одержувач повинні спочатку встановити з'єднання і, можливо, вибрати деякі параметри протоколу, які вони будуть використовувати при обміні даними. Після завершення діалогу вони повинні розірвати це з'єднання.

Друга група протоколів – протоколи *без попереднього встановлення з'єднання* (connectionless). Такі протоколи називаються також *дейтаграмними* протоколами. Відправник просто передає повідомлення, коли воно готове. При взаємодії комп'ютерів використовуються протоколи обох типів.

Розглянемо більш детально рівні моделі OSI.

Фізичний рівень забезпечує механічні, електричні, функціональні та процедурні засоби організації фізичних з’єднань при передачі даних фізичним об’єктам, тобто виконує передачу бітів по фізичним каналам зв'язку (коаксіальному кабелю, крученій парі або волоконно-оптичному кабелю), визначає характеристики електричних сигналів, які передають дискретну інформацію (рівні напруги або струм сигналу, тип кодування, швидкість передачі сигналів) та стандартизує типи гнізд і призначення кожного контакту.

Канальний рівень керує передачею даних каналами зв'язку. Основними функціями цього рівня є розбивка даних на порції, які

називаються кадрами, виділення даних з потоку біт, переданих на фізичний рівень, для обробки на мережевому рівні, перевірка доступності середи передачі даних, виявлення помилок передачі та відновлення неправильно переданих даних.

Мережевий рівень служить для утворення єдиної транспортної системи, що об'єднує декілька мереж, і вирішує проблему маршрутизації даних (які називаються на цьому рівні пакетами) у складеної мережі.

Транспортний рівень забезпечує додаткам передачу даних з тим ступенем надійності, котрий їм потрібний, у відповідності з обумовленими даним рівнем класами сервісу. Для цього використаються механізми для установки, підтримки і розриву віртуальних каналів, визначення і виправлення помилок при передачі, керування потоком даних (з метою запобігання переповнення або втрат даних).

Сеансовий рівень забезпечує управління взаємодією: фіксує, яка із сторін є активною в даний момент, надає засоби синхронізації (забезпечує поновлення аварійно перерваного сеансу).

Представницький рівень надає засоби, що дозволяють перебороти синтаксичні розходження у представленні даних або ж розходження у кодах символів і може виконувати шифрування і дешифрування даних.

Прикладний рівень забезпечує виконання прикладних процесів користувачів та визначає семантику, тобто зміст інформації, якою обмінюються системи в процесі їх взаємодії (передача файлів, віртуальний термінал, електронна пошта).

Три нижніх рівні фізичний, канальний і мережевий є *мережезалежними*, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі і комунікаційним обладнанням, що використовується. Вони забезпечують передачу даних.

Три верхніх рівні прикладний, представницький і сеансовий є *мереженезалежними*, вони орієнтовані на додатки і мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають які б то не було зміни в топології мережі, заміна обладнання або перехід на іншу мережеву технологію.

Транспортний рівень є *проміжним*, він приховує всі деталі функціонування нижніх рівнів від верхніх. Це дозволяє розробляти додатки, що не залежать від технічних засобів безпосереднього транспортування повідомлень.

На рис. 1.14 показана відповідність функцій різних комунікаційних пристроїв рівням моделі OSI. В залежності від типу комунікаційний пристрій може працювати або тільки на фізичному рівні (повторювач), або на фізичному і канальному (міст і комутатор), або на фізичному, канальному і мережевому (маршрутизатор).

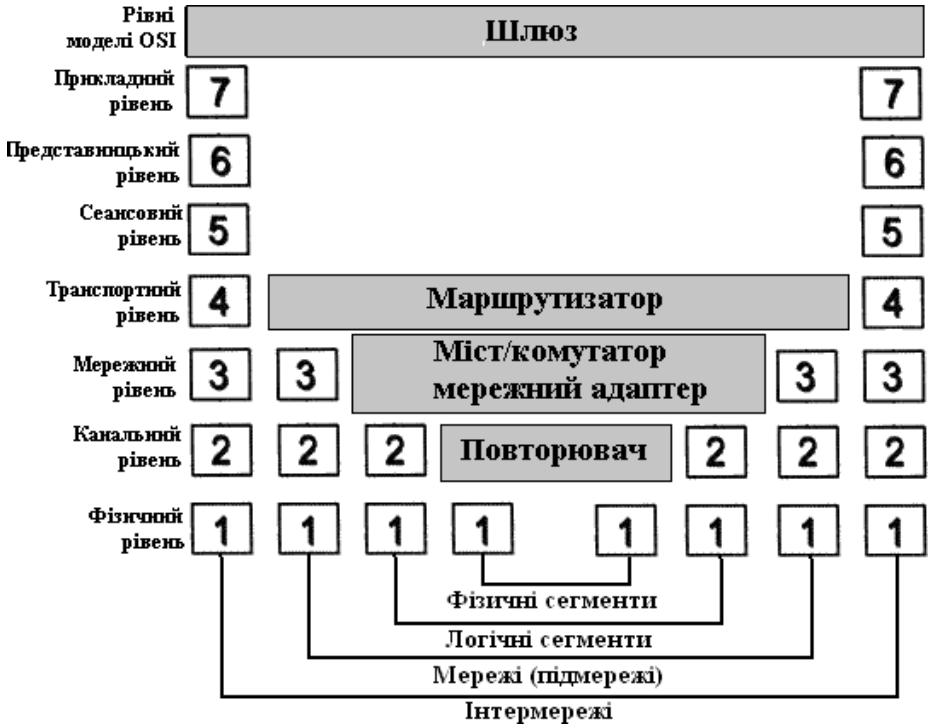


Рисунок 1.14 - Відповідність функцій різних пристроїв мережі рівням моделі OSI

1.1.6 Стандартні стекі протоколів

За час розроблення комп'ютерних мереж було створено багато стеків комунікаційних протоколів. Найбільш популярними є стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA і OSI, більша частина яких зараз вже не використовуються. Розглянемо деякі з них більш докладно.

Стек OSI. Стек OSI – це набір специфікацій протоколів, які повністю відповідають моделі OSI. Він включає специфікації протоколів для всіх семи рівнів, визначених в цій моделі. На нижніх рівнях стек OSI підтримує Ethernet, Token Ring, FDDI, протоколи глобальних мереж, X.25 і ISDN, тобто використовує розроблені поза стеком протоколи нижніх рівнів, як і всі інші стеки. Найбільш популярними протоколами стека OSI є прикладні протоколи. До них відносяться: протокол передачі файлів

FTAM, протокол емуляції термінала VTP, протоколи довідкової служби X.500, електронної пошти X.400 і ряд інших. Протоколи стека OSI відрізняє велика складність і неоднозначність специфікацій, тому протоколи OSI вимагають великих витрат обчислювальної потужності центрального процесора, що робить їх найбільш відповідними для могутніх машин, а не для мереж персональних комп'ютерів.

Стек IPX/SPX. Стек протоколів фірми Novell одержав свою назву від скорочень двох основних протоколів мережевого і сеансового рівнів: Internetwork Packet Exchange (IPX) і Sequenced Packet Exchange (SPX). Стек був розробленим ще на початку 80-х років для мережевої операційної системи NetWare. Багато які особливості стека IPX/SPX зумовлені орієнтацією ранніх версій ОС NetWare (до версії 4.0) на роботу в локальних мережах невеликих розмірів, що складаються з персональних комп'ютерів зі скромними ресурсами, тому протоколи стека IPX/SPX добре працювали в локальних мережах і не дуже у великих корпоративних мережах, оскільки вони дуже перевантажували повільні глобальні зв'язки широкомовними пакетами, які інтенсивно використовуються декількома протоколами цього стека (наприклад, для встановлення зв'язку між клієнтами і серверами). Ця обставина, а також той факт, що стек IPX/SPX є власністю фірми Novell і на його реалізацію треба отримувати ліцензію, довгий час обмежували поширеність його тільки мережами NetWare. Однак з моменту випуску версії NetWare 4.0 Novell внесла в свої протоколи серйозні зміни, направлені на їх адаптацію для роботи в корпоративних мережах. Стек IPX/ SPX був реалізований не тільки в NetWare, але і в декількох інших популярних мережевих ОС, наприклад SCO UNIX, Sun Solaris, Microsoft Windows NT.

Стек NetBIOS/SMB. Цей стек широко використовувався в продуктах компаній IBM і Microsoft. На фізичному і канальному рівнях цього стека працюють найбільш поширені протоколи Ethernet, Token Ring, FDDI та інші. На верхніх рівнях – протоколи NetBEUI і SMB. NetBEUI розроблявся як ефективний протокол, що споживає небагато ресурсів і призначений для мереж, що нараховують не більше за 200 робочих станцій. Цей протокол містить багато корисних мережевих функцій, які можна віднести до мережевого, транспортного і сеансового рівнів моделі OSI, однак з його допомогою неможлива маршрутизація пакетів. Це обмежує застосування протоколу NetBEUI локальними мережами, не розділеними на підмережі, і робить неможливим його використання в складових мережах. Деякі

обмеження NetBEUI знімала реалізація цього протоколу NBF (NetBEUI Frame), яка була включена в операційну систему Microsoft Windows NT. Протокол SMB (Server Message Block) виконує функції сеансового, представницького і прикладного рівнів. На основі SMB була реалізовується файлова служба, а також служби друку і передачі.

Стеки протоколів SNA фірми IBM, DECnet корпорації Digital Equipment і AppleTalk/AFP фірми Apple застосовувалися в основному в операційних системах і мережевому обладнанні цих фірм.

Стек TCP/IP. Стек TCP/IP був розроблений з ініціативи Міністерства оборони США. Великий внесок в розвиток стека TCP/IP вніс університет Берклі, який реалізував протоколи стека в своїй версії ОС UNIX. Популярність цієї операційної системи привела до широкого поширення протоколів TCP, IP і інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Internet, а також у величезному числі корпоративних мереж.

Стек TCP/IP на нижньому рівні підтримує всі популярні стандарти фізичного і канального рівнів: для локальних мереж це Ethernet, Token Ring, FDDI та відомі глобальні протоколи. Основними протоколами стека, що дали йому назву, є протоколи IP і TCP. Ці протоколи в термінології моделі OSI відносяться до мережевого і транспортного рівнів відповідно. IP забезпечує просування пакету між підмережами, а TCP гарантує надійність його доставки.

Стек TCP/IP увібрав в себе велику кількість протоколів прикладного рівня. До них відносяться такі популярні протоколи, як протокол пересилки файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, що використовується в електронній пошті мережі Internet, гіпертекстові сервіси служби WWW і багато інших. Стрімке зростання популярності Internet обумовило те, що сьогодні стек TCP/IP є одним з самих поширених стеків транспортних протоколів обчислювальних мереж. Він широко використовується як в глобальних, так і локальних мережах. Стек є незамінним при організації роботи в складених мережах.

Оскільки стек TCP/IP спочатку створювався для глобальної мережі Internet, він має багато особливостей, що дають йому перевагу перед іншими протоколами: здатність фрагментувати пакети, гнучка система адресації, економне використання можливості широкомовних розсилок. Як недолік стека слід зазначити високі вимоги до ресурсів і складність адміністрування IP-мереж.

Відповідність деяких, найбільш популярних протоколів рівням моделі OSI показана на рис.1.15.

<table>
<tr><th>Модель OSI</th><th>IBM /Microsoft</th><th>TCP/IP</th><th>Novell</th><th>Стек OSI</th></tr>
<tr><td>Прикладний</td><td rowspan="2">SMB</td><td rowspan="2">Telnet,
FTP,
SNMP,
WWW</td><td rowspan="3">NCP,
SAP</td><td>X.400,
X.500,
FTMA</td></tr>
<tr><td>Представницький</td><td>Представницький протокол OSI</td></tr>
<tr><td>Сеансовий</td><td rowspan="2">NetBios</td><td rowspan="2">TCP</td><td>Сеансовий протокол OSI</td></tr>
<tr><td>Транспортний</td><td>SPX</td><td>Транспортний протокол OSI</td></tr>
<tr><td>Мережевий</td><td></td><td>IP,
RIP,
OSPF</td><td>IP,
RIP,
NLSP</td><td>ES-TS,
IS-IS</td></tr>
<tr><td>Канальний</td><td colspan="4">802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP</td></tr>
<tr><td>Фізичний</td><td colspan="4">Коаксіальний, екранована і неекранована вита пара, оптичневолокно, радіохвилі</td></tr>
</table>

Рисунок 1.15 – Відповідність популярних стеків протоколів моделі OSI

1.1.7 Багаторівнева структура стека TCP/IP

Стек протоколів TCP/IP поділяється на 4 рівня: прикладний (application), транспортний (transport), мережевий (internet) і рівень мережевого доступу (network access). На відміну від еталонной моделі OSI, модель TCP/IP більшою мірою орієнтується на забезпечення мережевих взаємодій, ніж на чіткий поділ функціональних рівнів.

Терміни, що застосовуються для позначення блоку переданих даних, різні при використанні різних протоколів транспортного рівня – TCP і UDP, тому на рис. 1.16 зображено два стека.

Як і в моделі OSI, дані верхніх рівнів інкапсулюються в пакети нижніх рівнів (рис.1.17).

Співвідношення рівнів стеків OSI і TCP/IP показано на рис. 1.18.

Протоколи прикладного рівня стека TCP/IP працюють на комп'ютерах, що виконують додатки користувачів. Навіть повна зміна мережевого встаткування в загальному випадку не повинна впливати на роботу додатків, якщо вони одержують доступ до мережевих можливостей через протоколи прикладного рівня.

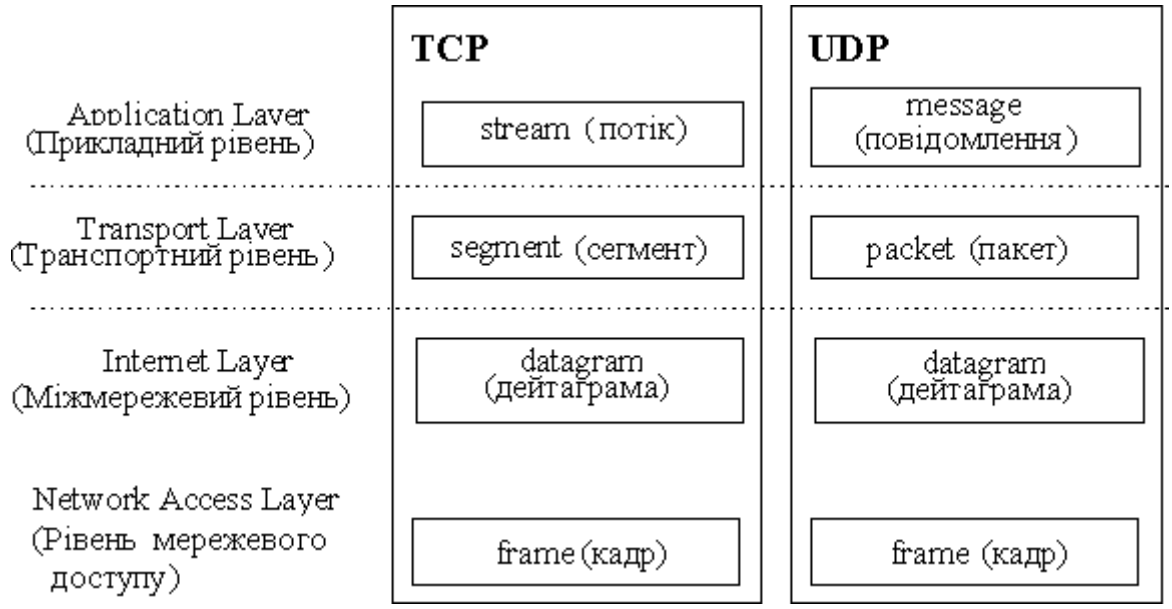


Рисунок 1.16 – Стек протоколів TCP/IP

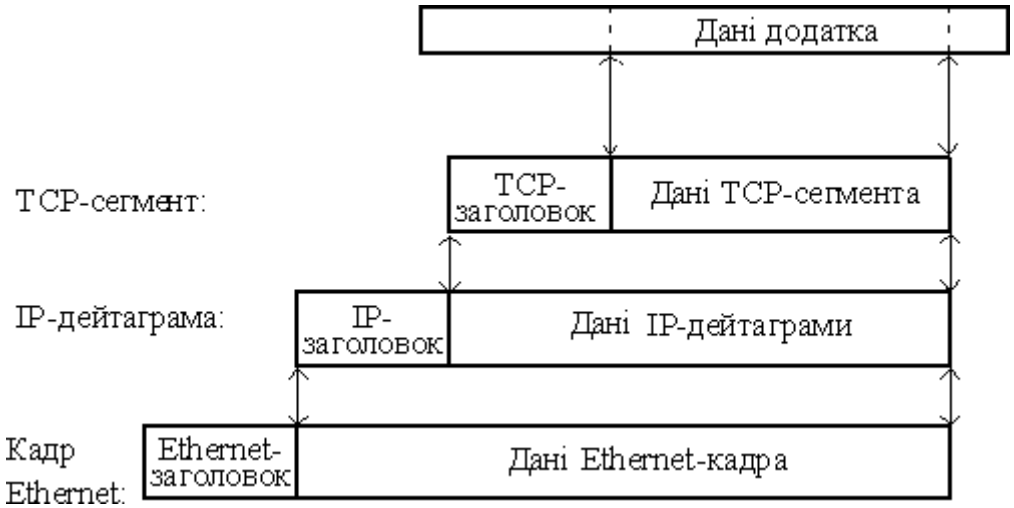


Рисунок 1.17 – Приклад інкапсуляції пакетів у стеці TCP/IP

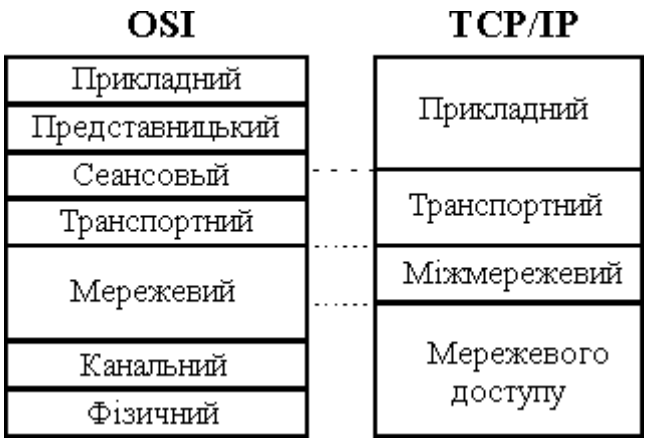


Рисунок 1.18 – Співвідношення рівнів стеків OSI і TCP/IP

Розглянемо більш докладно функції кожного рівня і приклади протоколів.

Прикладний рівень (application layer) поєднує всі служби, що надаються системою користувальницьким додаткам: традиційні мережеві служби типу telnet (протокол емуляції терміналу), FTP (протокол передачі файлів), DNS (система доменних імен), SNMP (протокол пересилання поштових повідомлень), HTTP (протокол передачі гіпертексту), гіпертекстові сервіси служби WWW. Прикладний рівень реалізується програмними системами, побудованими в архітектурі клієнт-сервер, що базуються на протоколах нижніх рівнів. На відміну від протоколів інших трьох рівнів, протоколи прикладного рівня займаються деталями конкретного застосунка і "не цікавляться" способами передачі даних в мережі.

Транспортний рівень (transport layer) вирішує завдання забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами. Він контролює, щоб всі пакети були доставлені в місце призначення цілими та непошкодженими і у тому же порядку, у якому вони були відправлені.

На транспортному рівні працюють два основних протоколи: UDP і TCP. *TCP (Transmission Control Protocol – протокол контролю передачі)* – надійний протокол із встановленням з'єднання: він управляє логічним сеансом зв'язку (встановлює, підтримує і закриває з'єднання) між процесами та забезпечує надійну (безпомилкову і гарантовану) доставку прикладних даних від процесу до процесу. TCP ділить потік байтів на частини – сегменти, і передає їх нижньому мережевому рівню. Після того

як ці сегменти будуть доставлені засобами мережевого рівня в пункт призначення, протокол TCP знову збирає їх у безперервний потік байтів.

Протокол *UDP (User Datagram Protocol – протокол користувальницьких дейтаграм)* забезпечує передачу прикладних пакетів дейтаграмним способом, як і головний протокол мережевого рівня IP, і виконує тільки функції сполучної ланки (мультиплексора) між мережевим протоколом і службами прикладного рівня або користувальницькими процесами.

На *мережевому рівні (network layer) о*сновним протоколом є протокол *IP (Internet Protocol),* який доставляє блоки даних, що називаються дейтаграмами, від одного IP-адреса до іншого. Дані передаються протоколу IP транспортним рівнем. Протокол IP додає до цих даних заголовок, що містить IP-адреси відправника і одержувача та іншу службову інформацію, і сформована в такий спосіб дейтаграмма передається на рівень мережевого доступу (наприклад, одному з фізичних інтерфейсів) для відправлення каналом передачі даних. Протокол IP є дейтаграмним протоколом, тому він не гарантує доставку пакетів до вузла призначення, але намагається це зробити. Не всі комп'ютери можуть безпосередньо зв'язатися один з одним; часто для того, щоб передати дейтаграму за призначенням, потрібно направити її через один або кілька проміжних абонентів за тим або іншим маршрутом. Завдання визначення маршруту для кожної дейтаграми вирішується протоколом IP.

До рівня мережевого доступу відносяться і всі протоколи маршрутизації, такі як: протоколи збору маршрутної інформації *RIP (Routing Internet Protocol)* і *OSPF (Open Shortest Path First)*, а також протокол мережевих керуючих повідомлень *ICMP (Internet Control Message Protocol).* Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі та вузлом-джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляє про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета із фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи й т.п.

Рівень мережевого доступу (link layer) забезпечує інтеграцію в складену мережу інших підмереж, тому мережа TCP/IP повинна мати засоби включення в себе будь-якої іншої підмережі, яку б внутрішню технологію передачі даних ця підмережа не використовувала. Звідси

зрозуміло, що цей рівень не можна визначити раз і назавжди. Для кожної технології, що включається, повинні бути розроблені власні інтерфейсні засоби. До таких інтерфейсних засобів відносяться протоколи інкапсуляції IP-пакетів в кадри локальних технологій.

Рівень мережевого доступу у протоколах TCP/IP не регламентується, але він підтримує всі популярні стандарти фізичного і канального рівнів: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet. Функції цього рівня:

– відображення IP-адрес у фізичні адреси мережі (MAC-адреси, наприклад, Ethernet-адреса у випадку мережі Ethernet). Цю функцію виконує протокол ARP (див. п.1.1.3).

– інкапсуляція IP-дейтаграм у кадри та вилучення дейтаграм із кадрів. При цьому не потрібно якого-небудь контролю безпомилковості передачі (хоча він може й бути присутнім), оскільки в стеці TCP/IP такий контроль покладений на транспортний рівень.

– визначення методу доступу до середовища передачі – тобто способу, за допомогою якого комп'ютер встановлює своє право на передачу даних.

– пересилання та прийом кадрів.

1.2 Мережеві архітектурні рішення

1.2.1 Фізична та логічна структуризації мереж за допомогою різних типів комунікаційного обладнання

Розрізняють топологію фізичних зв'язків (*фізичну структуру мережі*) і топологію логічних зв'язків *(логічну структуру мережі)*. Фізична структура мережі визначається електричними з'єднаннями комп'ютерів, тут ребра графа відповідають відрізкам кабелю, що зв'язує пари вузлів. Логічні зв'язки являють собою маршрути передачі даних між вузлами мережі й утворюються шляхом відповідного налаштування комунікаційного устаткування.

Для структуризації мережі використовують спеціальне комунікаційне устаткування – *повторювачі, концентратори, мости, комутатори, маршрутизатори.*

Повторювач (repeater) – використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою збільшення загальної

довжини мережі і дозволяє перебороти обмеження на довжину ліній зв'язку за рахунок поліпшення якості переданого сигналу. Наприклад, технологія Ethernet на тонкому коаксіальному кабелі дозволяє використати кабель довжиною не більше за 185 метрів, але якщо у мережі використовуються повторювачі, її довжина може бути збільшена (рис.1.19).

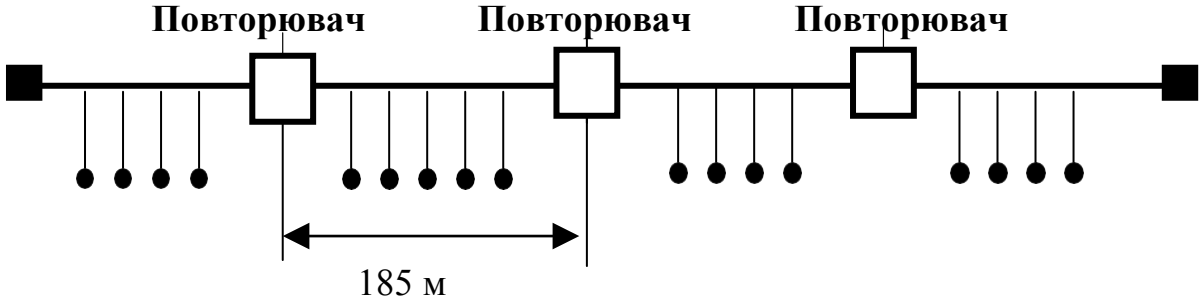


Рисунок 1.19 – Приклад використання повторювачів для збільшення довжини мережі Ethernet

Повторювач, що має кілька портів і з'єднує кілька фізичних сегментів, часто називають *концентратором (concentrator)*, або *хабом (hub)* – він повторює сигнали, що прийшли з одного порту, на інших своїх портах. Так, концентратор Ethernet повторює вхідні сигнали на всіх своїх портах, крім того, з якого сигнали поступають (рис.1.20). А концентратор Token Ring повторює вхідні сигнали, що поступають з деякого порту, тільки на одному порту на тому, до якого підключений наступний в кільці комп'ютер. Таким чином, концентратор змінює фізичну топологію мережі, але при цьому залишає без зміни її логічну топологію (загальна шина для технології Ehternet і кільце - для Token Ring).

Відрізки кабелю, що з'єднують два комп'ютери або два інших мережевих пристрою називаються *фізичними сегментам*. Таким чином, концентратори і повторювачі, які використаються для додавання нових фізичних сегментів, є засобом фізичної структуризації мережі.

Концентратори утворюють із окремих фізичних відрізків кабелю загальне середовище передачі даних – *логічний сегмент*.

Колективне використання багатьма комп'ютерами загальної кабельної системи в режимі поділу часу приводить до істотного зниження продуктивності мережі при інтенсивному трафіку. Загальне середовище перестає справлятися з потоком переданих кадрів і в мережі виникають

черга комп'ютерів, що очікують доступу. Це явище характерно для всіх технологій, що використовують загальне середовища передачі даних. Тому мережі, побудовані на основі концентраторів, не можуть розширюватися в необхідних межах – при певній кількості комп'ютерів у мережі завжди відбувається насичення передавального середовища, і затримки в її роботі стають неприпустимими.

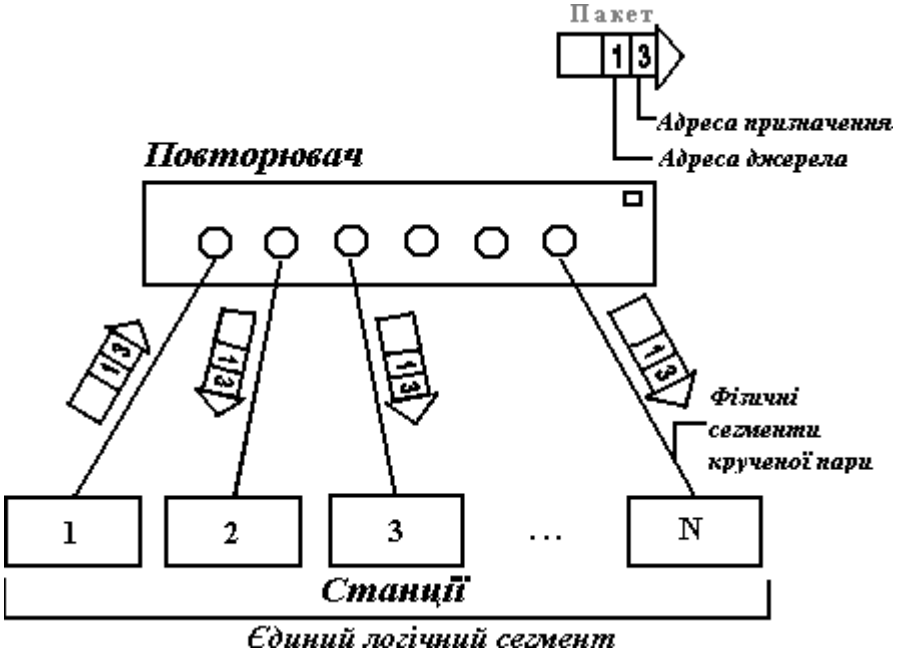


Рисунок 1.20 – Повторювач Ethernet синхронно повторює біти кадру на всіх своїх портах

Ця проблема може бути вирішена шляхом логічної структуризації мережі, тобто завдяки *локалізації трафіку*, коли трафік призначений для комп'ютерів деякого сегмента мережі, поширюються тільки в межах цього сегмента. Таким чином, *логічна структуризація мережі* – це процес розбиття мережі на сегменти з локалізованим трафіком. Для логічної структуризації мережі використаються такі комунікаційні пристрої, як мости, комутатори, маршрутизатори і шлюзи.

Міст (bridge) ділить поділюване середовище передачі мережі на логічні сегменти. Логічний сегмент може утворюватися шляхом об'єднання декількох фізичних сегментів (відрізків кабелю) за допомогою одного або декількох концентраторів. Кожний логічний сегмент підключається до окремого порту моста (рис. 1.21). При надходженні кадру на який-небудь із портів міст повторює цей кадр, але не на всіх

портах, а тільки на тому порту, до якого підключений сегмент, де знаходиться вузол-адресат. Тим самим міст ізолює трафік однієї підмережі від трафіка іншої. Локалізація трафіка не тільки економить пропускну здатність, але і зменшує можливість несанкціонованого доступу до даних.

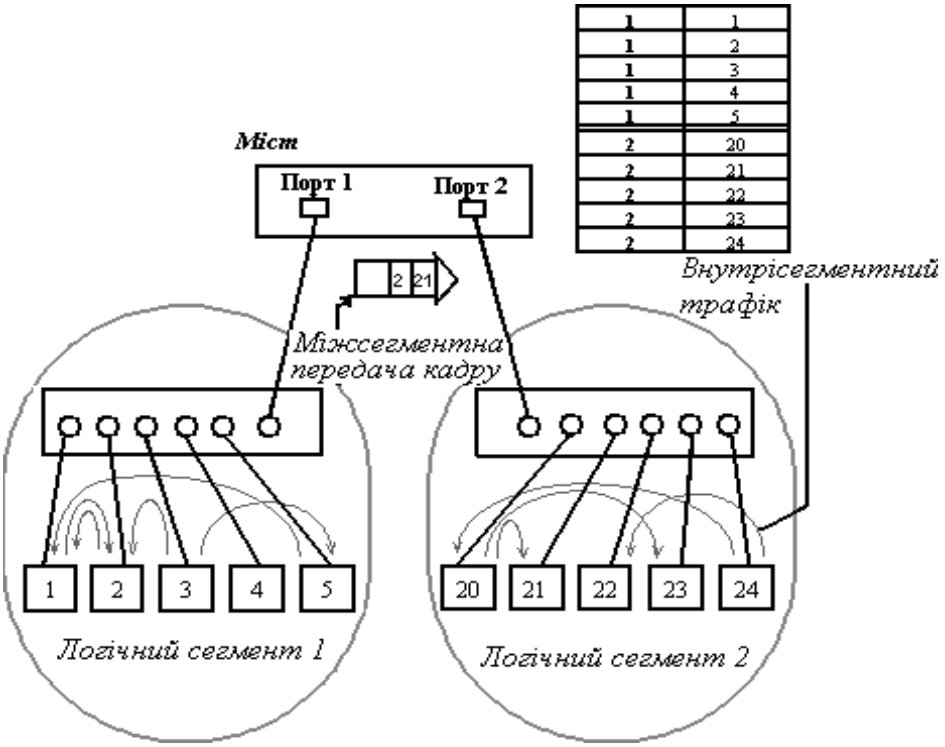


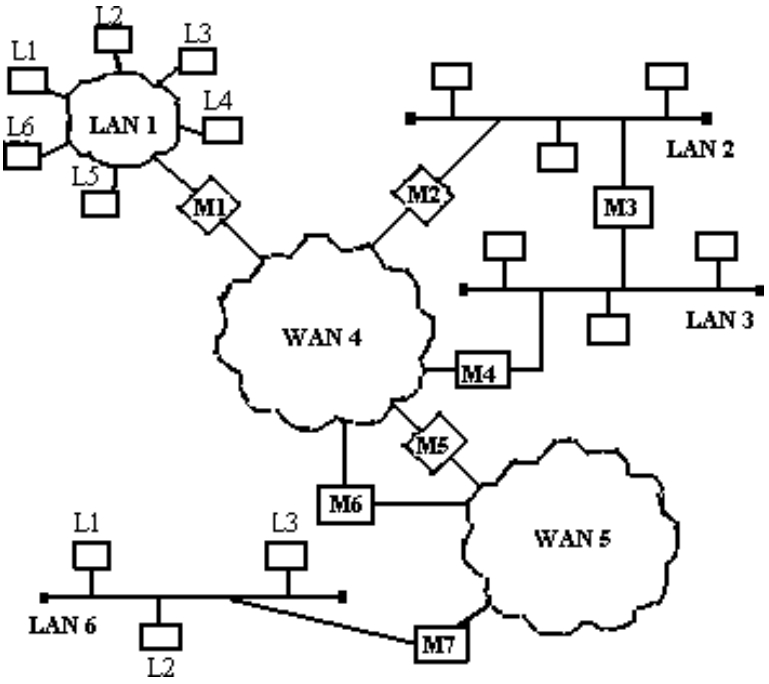
Рисунок 1.21 – Поділ мережі на логічні сегменти

Для локалізації трафіка мости використовують апаратні адреси комп'ютерів. Це утрудняє розпізнавання приналежності того або іншого комп'ютера до певного логічного сегмента - сама адреса не містить ніякої інформації із цього приводу. Тому міст досить спрощено представляє розподіл мережі на сегменти – він запам'ятовує, через який порт на нього надійшов кадр даних від кожного комп'ютера мережі, і надалі передає кадри, призначені для цього комп'ютера, на цей порт.

Комутатор (switch) за принципом обробки кадрів нічим не відрізняється від мосту. Основна його відмінність від мосту полягає в тому, що він є свого роду комунікаційним мультипроцесором, тому що кожний його порт оснащений спеціалізованим процесором, що обробляє кадри за алгоритмом моста незалежно від процесорів інших портів у паралельному режимі. За рахунок цього загальна продуктивність

комутатора звичайно набагато вище продуктивності традиційного моста, що має один процесорний блок.

Маршрутизатор (router) – ізолює трафік окремих частин мережі один від одного, утворюючи логічні сегменти за допомогою явної адресації, оскільки використовує не плоскі апаратні, а складові числові адреси. Всі комп'ютери, у яких значення поля *адреси мережі* однакові, належать до одного сегмента, який називається в цьому випадку *підмережою (subnet)*. Сукупність декількох підмереж, з'єднаних між собою маршрутизаторами, утворює *складену мережу або інтермережу (internetwork, або internet)*. Приклад інтермережі наведений на рис.1.22. Компонентами інтермережі можуть бути як локальні, так і глобальні мережі. Всі вузли в межах однієї інтермережі взаємодіють, використовуючи єдину для них технологію.



M1, M2, ... , M7 – маршрутизатори;
LAN1, LAN2, LAN3, WAN4, WAN5, LAN6 - унікальні номери мереж у єдиному форматі;
L1, L2, ... - локальні номери вузлів (дублюються, різний формат)

Рисунок 1.22 – Структура інтермережі, побудованої на основі маршрутизаторів

Маршрутизатори здійснюють вибір найбільш раціонального маршруту з декількох можливих. В даному випадку під маршрутом розуміють послідовність проходження пакетом маршрутизаторів. Наприклад, на рис. 1.22 для зв'язку станцій L2 мережі LAN1 і L1 мережі LAN6 є два маршрути: M1-M5-M7 і M1-M6-M7.

Маршрутизатор може вибрати оптимальний маршрут при наявності декількох альтернативних маршрутів. Рішення про вибір того або іншого маршруту приймається кожним маршрутизатором, через який проходить повідомлення. Для того, щоб скласти топологію зв'язків у мережі, маршрутизатори обмінюються спеціальними службовими повідомленнями, у яких знаходиться інформація про ті зв'язки між підмережами, про які вони знають (ці підмережі підключені до них безпосередньо або ж вони дізналися про цю інформацію від інших маршрутизаторів).

Побудова графа зв'язків між підмережами та вибір оптимального за яким-небудь критерієм маршруту на цьому графі являють собою складне завдання. При цьому можуть використовуватися різні критерії вибору маршруту – найменша кількість проміжних вузлів, час, вартість або надійність передачі даних. Важлива функція маршрутизаторів – здатність зв'язувати в єдину мережу (інтермережу) підмережі, що побудовані з використанням різних мережевих технологій. Тому маршрутизатори можуть поєднувати не тільки локальні мережі з різною технологією, але й локальні мережі із глобальними. Маршрутизатори не тільки поєднують мережі, але й надійно захищають їх, краще ніж комутатори. Наприклад, при надходженні кадру з неправильною адресою комутатор зобов'язаний повторити його на всіх своїх портах, що робить мережу незахищеною від некоректно працюючого вузла. Маршрутизатор же в такому випадку просто відмовляється передавати "неправильний" пакет далі, ізолюючи дефектний вузол від іншої мережі. Тому маршрутизатор – це складний інтелектуальний пристрій, побудований на базі одного, а іноді і декількох потужних процесорів. Такий спеціалізований мультипроцесор працює, як правило, під керуванням спеціалізованої операційної системи.

Крім перерахованих пристроїв окремі частини мережі може з'єднувати *шлюз (gateway)*. Звичайно основною причиною, за якою у мережі використають шлюз, є необхідність об'єднати мережі з різними типами системного та прикладного програмного забезпечення, а не бажання локалізувати трафік. Проте шлюз забезпечує і локалізацію трафіка як деякий побічний ефект.

1.2.2 Типи мережевих сполучень та методи комутації

Комутація – це спосіб передачі даних між кінцевими вузлами. У комп'ютерних мережах для передачі даних між вузлами мережі використовуються наступні методи: *комутація каналів*, *комутація повідомлень* і *комутація пакетів*.

Комутація каналів дозволяє за допомогою комутаторів установити пряме з'єднання між абонентами мережі. При цьому скрізний канал складається вузлами комутації каналів з окремих ділянок мережі і, як правило, встановлюється лише на час сеансу зв’язку. Після завершення обміну даними канал розбирається і його складові частини можуть бути надані іншим користувачам. Типовим прикладом мережі з комутацією каналів є міська телефонна мережа загально призначення.

При *комутації повідомлень* передача даних здійснюється без встановлення скрізного з’єднання між взаємодіючими абонентами. Дані від абонента спочатку передаються до найближчого вузла комутації, до якого він приєднаний, і заноситься до запам’ятовуючого пристрою вузла. Із звільненням каналів у напрямку передачі і наявності вільної пам’яті в сусідньому вузлі комутації, повідомлення передається до наступного вузла, займаючи канал тільки на період часу передачі даних між суміжними вузлами. Так процедура повторюється на кожному вузлі, через який проходить повідомлення, доти поки повідомлення не дійде до адресату. Тому, навіть при відсутності вільних ресурсів, мережі з комутацією повідомлень працюють без відмов. Це є однією з основних переваг мереж з комутацією повідомлень. До переваг таких мереж також відноситься більш висока ефективність використання каналів за рахунок виключення повторних викликів при відмовах і більш висока надійність доставки повідомлень за рахунок передачі даних обхідними напрямками мережі при виході з ладу або перевантаженнях основного шляху. Головний недолік мереж з комутацією повідомлень – наявність затримок при доставці інформації, причому затримка є випадковою. Крім того, при передачі великих повідомлень підвищується вірогідність появи в них помилок, що призводить до необхідності повторної передачі всього повідомлення і, відповідно, до зниження ефективної швидкості доставки інформації.

Для побудови комп’ютерних мереж використовують принцип комутації каналів, який є різновидом комутації повідомлень. В

комп’ютерних мережах дані часто містяться у вигляді файлів, які мають відносно великі розміри. Якщо передавати весь інформаційний блок, то він заповніть канал і буде перешкоджати взаємодії інших абонентів.

При *пакетній комутації* дані користувача розбиваються на дрібніші порції – пакети, причому кожний пакет містить службові поля і поле даних. Існують два основних способи передачі даних при пакетній комутації: *віртуальний канал*, коли між вузлами встановлюється та підтримується з'єднання ніби то за виділеним каналом (хоча насправді фізичний канал передачі даних розділений між декількома користувачами) і *дейтаграмний режим*, коли кожний пакет з набору пакетів, що містить дані користувача, передається між вузлами незалежно один від іншого. Перший спосіб з'єднання називають також контактним режимом (connection mode), другий – безконтактним (connectionless mode).

Контрольні питання й завдання

1. Дайте визначення поняттю «топологія мережі».
2. Приведіть порівняльну характеристику фізичних топологій локальних мереж.
3. Логічна структуризація мережі. Чи завжди логічна структура збігається з фізичною топологією локальної мережі? Поясніть наступні твердження: логічна зірка на основі загальної шини і логічне кільце на основі фізичної зірки.
4. Визначите функціональне призначення основних типів комунікаційного встаткування: повторювачів, концентраторів, мостів, комутаторів, маршрутизаторів. У чому складаються особливості логічної структуризації мережі за допомогою мостів і комутаторів?
5. Що таке мережева служба? Опишіть сутність і принципи взаємодії розподіленої програми.
6. Дайте повну характеристику рівням моделі OSI.
7. Приведіть структуру стека протоколів TCP/IP і її відповідність моделі OSI. Дайте коротку характеристику кожному рівню стека TCP/IP.
8. Які функції виконує протокол IP стека протоколів TCP/IP. У чому проявляється ненадійність протоколу IP?
9. Дайте характеристику протоколам транспортного рівня стека TCP/IP.

10. Що таке IP- адреса? Які класи адрес існують? Дайте визначення масці підмережі.

2 ПЕРЕДАЧА ДАНИХ НА НИЖНІХ РІВНЯХ МЕРЕЖ

2.1 Протоколи нижнього рівня комп’ютерних мереж

2.1.1 Загальні характеристики та параметри середовищ передавання

2.1.1.1 Типи ліній зв'язку

Лінія зв'язку (рис. 2.1) складається в загальному випадку з фізичного середовища, за яким передаються електричні інформаційні сигнали, апаратури передачі даних та проміжної апаратури. Синонімом терміна *лінія зв'язку (line)* є термін *канал зв'язку(channel)*.

Інформаційно-комп'ютерні системи містять наступні основні компоненти:

DTE - кінцеве встаткування даних (Data Terminal Equipment);

DCE – апаратура передачі даних (Data Circuit - terminating Equipment);

DSE – проміжне встаткування (Data Switching Equipment);

Фізичне середовище передачі даних.

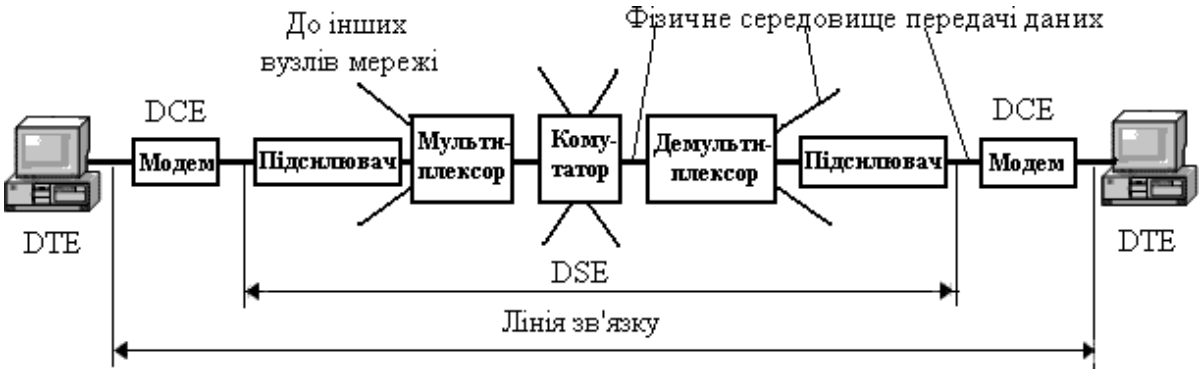


Рисунок 2.1 – Склад лінії зв’язку

DTE - це узагальнене поняття, що використовується для опису системи кінцевого користувача мережі, у якості якого може виступати комп'ютер або термінальний пристрій (будь-який пристрій вводу-виводу або відображення інформації). Комп'ютери у вузлах мережі іноді називають хост-машинами або просто *хостами*.

Основна функція *DCE* полягає в тому, щоб забезпечити доступ кінцевому встаткуванню даних - DTE до передавального середовища. Спочатку DCE являли собою пристрої, що реалізують винятково комунікаційні функції, однак останнім часом у них включається також частина функцій користувача (наприклад, стиск даних). Прикладом DCE

може служити модем, що виконує перетворення сигналів із цифрової в аналогову форму (модуляцію сигналів) і зворотне перетворення (демодуляцію) для передачі даних телефонними каналами зв'язку. Іншим прикладом DCE є плата для підключення комп'ютера до локальної мережі - мережевий адаптер.

Основною функцією *DSE* є передача даних, поліпшення якості сигналу, і, при необхідності, комутація і маршрутизація трафіка (даних користувача) у мережі від джерела до адресата.

Прикладами DSE є концентратор, на вхід якого надходять дані з декількох джерел (від кожного своїм каналом), а на виході – канал, у який передається сумарний потік даних від вхідних джерел, і комутатор, що перенаправляє потоки даних різними каналами, залежно від адресата даних або за яким-небудь іншим критерієм.

Існує безліч типів і видів DTE, DCE і DSE, однак слід зазначити, що для них не існує стандартизованих найменувань і пристрої, які називаються по-різному різними фірмами-виготовлювачами або розроблювачами мережевих протоколів, можуть виконувати однакові функції, і навпаки, призначення пристроїв з однаковими назвами може не збігатися в різних виробників і розроблювачів. Адміністративно мережа може включати тільки передавальне середовище, DSE і, можливо, DCE. У цьому випадку мережа називається *мережею передачі даних*, до якої на певних умовах підключаються DTE кінцевих користувачів, які називаються *абонентами* мережі. Часто такі мережі називають *первинними* або *опорними (backbone)* мережами. У випадку, якщо мережа включає всі компоненти, то її називають просто комп'ютерною мережею. Якщо в складі DTE мережі переважають термінали, то таку мережу називають *термінальною* мережею.

Залежно від типу проміжної апаратури всі лінії зв'язку діляться на аналогові і цифрові. В *аналогових лініях* проміжна апаратура призначена для посилення аналогових сигналів, тобто сигналів, які мають безперервний діапазон значень.

Аналогові канали зв'язку першими почали застосовуватися для передачі даних у комп'ютерних мережах і дозволили використати вже існуючі тоді розвинені телефонні мережі загального користування. Передача даних аналоговими каналами може виконуватися двома способами. При першому способі телефонні канали (одна або дві пари проводів) через телефонні станції фізично з'єднують два DCE з

підключеними до них DTE. Такі з'єднання називають *виділеними лініями* або безпосередніми з'єднаннями. Другий спосіб – це встановлення з'єднання за допомогою набору телефонного номера (з використанням *комутованих ліній*).

З ростом трафіка в мережах сильніше стали проявлятися недоліки аналогових каналів: низька швидкість, нераціональне використання смуги пропущення та низька вірогідність передачі (особливо неприпустима при передачі аудіо і відеоданих).

Паралельно з використанням аналогових телефонних мереж для міжкомп'ютерної взаємодії почали розвиватися й методи передачі даних у дискретній (цифровий) формі ненавантаженими телефонними каналами (тобто телефонними каналами, до яких не підведене електрична напруга, яка використовується в телефонній мережі) – *цифровими каналами*.

У *цифрових каналах* зв'язку передані сигнали мають кінцеве число станів. Звичайно, сигнал, переданий за один такт роботи передавальної апаратури, має 2,3 або 4 стану, які передаються лініями зв'язку імпульсами або потенціалами прямокутної форми. Разом з дискретними даними цифровими каналами можна передавати й аналогову інформацію (голосову, відео та інш.), перетворену в цифрову форму.

2.1.1.2 Фізичне середовище передачі даних (medium)

Фізичне середовище передачі даних може являти собою кабель, тобто набір проводів, ізоляційних і захисних оболонок і з'єднувальних рознімань, а також земну атмосферу або космічний простір, через які поширюються інформаційні сигнали. У сучасних телекомунікаційних системах інформація передається за допомогою електричного струму або напруги, радіосигналів або світлових сигналів - всі ці фізичні процеси являють собою коливання електромагнітного поля різної частоти і природи.

Основними типами передавальних середовищ, що використовуються у комп'ютерних мережах, є:

- аналогові телефонні канали загального користування;
- цифрові канали;
- вузькосмугові та широкосмугові кабельні канали;
- радіоканали і супутникові канали зв'язку;
- оптоволоконні канали зв'язку.

Розглянемо більш докладно склад і характеристики кабельних ліній зв'язку.

До основних типів кабелів можна віднести:

- електричні кабелі з кручених пар проводів (twister pair, TP): екранованих (shielded TP, STP) і неекранованих (unshielded TP, UTP);
- електричні коаксіальні кабелі (coaxial cable, CC);
- оптоволоконні кабелі (fiber optic, FO).

Коаксіальний кабель (coaxial) складається із двох концентричних провідників. Його назва пов'язана з тим, що обидва провідника розташовані на одній загальній осі. У найпоширенішому варіанті цей кабель складається з однієї провідної мідної жили, оточеної діелектричним матеріалом. Цей діелектричний матеріал екранується ще одним циліндричним провідником. Після цього йде ще один шар ізоляції, і вся ця конструкція розташовується в захисну зовнішню оболонку з полівінілхлориду або тефлону (рис.2.2).

Рисунок 2.2 – Коаксіальний кабель

Коаксіальні кабелі діляться на різні класи за опором. Для цього застосовується шкала Radio Grade (RG). В локальних комп’ютерних мережах використовуються коаксіальні кабелі з різним хвильовим опором від 50 Ом до 120 Ом, хоч перевага надається кабелю з опором 50 Ом. RG-8 і RG-11 - «товстий» коаксіальний кабель. Має хвильовий опір 50 Ом і зовнішній діаметр 0,5 дюйма. Цей кабель має досить товстий внутрішній провідник діаметром 2,17 мм, що забезпечує гарні механічні та електричні характеристики. Однак кабель складно монтувати тому, що він погано гнеться. RG-58/U і RG-58 A/U – різновиди «тонкого» коаксіального кабелю. Кабель RG-58/U має суцільний внутрішній провідник, а кабель RG-58 A/U – багатожильний. Хвильовий опір 50 Ом. Мають гірші механічні та електричні характеристики в порівнянні з "товстим"

коаксіальним кабелем. Тонкий внутрішній провідник 0,89 мм не такий міцний, але більш гнучкий, що зручно при монтажі.

Слід зазначити, що в локальних мережах коаксіальні канали вже практично не застосовуються і витісняються каналами на витих парах і оптоволоконними каналами зв'язку.

Витою парою (twisted pair) називається скручена пара проводів**.** Кабелі на основі витої пари називаються симетричними кабелями через те, що вони складаються із двох однакових у конструктивному відношенні провідників. Скручування проводів знижує вплив зовнішніх перешкод на корисні сигнали, які передаються по кабелю. У локальних мережах звичайно використовується кабель із чотирьох витих пар у загальній оболонці, що складається з полівінілхлориду або тефлону (рис.2.3).

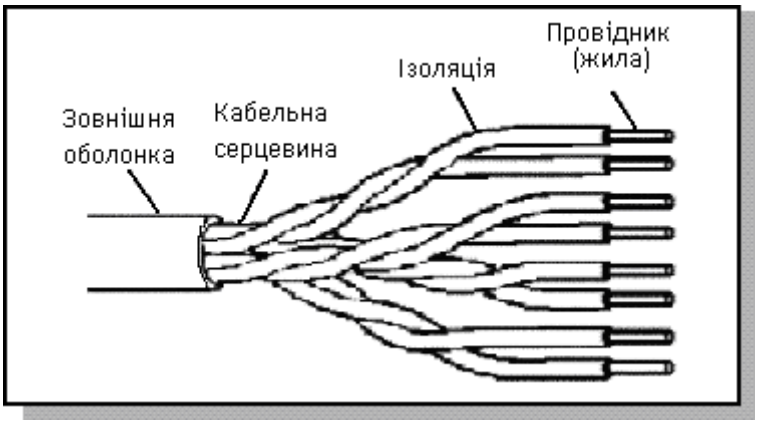


Рисунок 2.3 – Кабель «вита пара»

Кабель UTP виробляється в 4-парному виконанні. Звичайно дві пари призначені для передачі даних, а дві – для передачі голосу. Для з'єднання кабелів з устаткуванням використовуються 8-контактні рознімання RJ-45 (рис.2.4).

Крім того, для захисту от електромагнітної взаємодії, виті пари можуть бути ізольовані одна від одної за допомогою тонкої металевої трубки - екрана, який особливо ефективний на високих частотах (кілька МГц). Такі виті пари звичайно називають у специфікаціях STP – екранованою витою парою (Shielded Twisted Pair) у відмінність от UTP – неекранованої витої пари (Unshielded Twisted Pair).

Кабель UTP залежно від електричних і механічних характеристик розділяється на категорії:

Категорія 1 – Використовується для телефонних комунікацій і не підходить для передачі даних у комп'ютерних мережах

Рисунок 2.4 – Вита пара і рознімання RJ-45

Категорія 2 – Використовується для передачі даних зі швидкістю до 4 Мбіт/с включно. Цей тип проводки характерний для мереж застарілої кільцевої топології, що використають протокол з передачею маркера. Кабель тактується частотою 1МГц.

Категорія 3 – Використовується для передачі даних зі швидкістю до 10 Мбіт/с включно. Застосовується в мережах. Тактується частотою 16 МГц.

Категорія 4 – Використовується для передачі даних зі швидкістю до 16 Мбіт/с включно. Застосовується в мережах Token Ring. Тактується частотою 20 МГц.

Категорія 5 – Використовується для передачі даних зі швидкістю 100 Мбіт/с, а в технології Gigabit Ethernet - 1000 Мбіт/с. Застосовується в сучасних мережах. Тактується частотою 100 МГц. Існує поліпшена версія категорії 5e (5 enhanced), яка була розроблена спеціально для більш якісної підтримки протоколу Gigabit Ethernet, в основному за рахунок більш жорстких обмежень на перехресні наведення.

Категорія 6 – Використовується для підтримки високошвидкісних протоколів технології 10G Ethernet. Може бути як екранованим, так і неекранованим. Тактується частотою 250 МГц, категорії 6а – до 500 МГц.

Категорія 7 – Використовується для підтримки високошвидкісних протоколів. Обов'язково екрануються, причому як кожна пара, так і весь кабель у цілому. Тактується частотою 600 Мгц. Максимальна довжина сегмента 10G Ethernet на кабелі категорії 6 дорівнює 55 м, а на кабелях категорій 6а і 7 – 100 м.

Екранована вита пара призначена для прокладки кабелю в середовищі, чутливому до впливу електромагнітних перешкод. Покриття провідника металевим екраном захищає сигнали від зовнішніх випромінювань. Основним стандартом, що визначає параметри екранованої витої пари, є фірмовий стандарт IBM. Кабель Type 1 стандарту IBM складається із двох пар скручених проводів, екранованих провідниковим обплетенням, що заземлюється. Для приєднання екранованих кабелів до устаткування використовується рознімання конструкції IBM.

Одним з недоліків витої пари є можливість перехоплення інформації, що передається. Це робиться або за допомогою уткнутих в кабель двох голок, або шляхом зчитування випромінюваного кабелем електромагнітного поля. Екранування забезпечує захист від електромагнітних наведень і несанкціонованого підслуховування. З іншого боку, екранований кабель значно дорожче, тому використовується рідше.

Отже, перевага витої пари полягає в простоті монтажу і ремонту, а також у низькій вартості кабелю. З іншого боку, неекрановані кабелі на основі витих пар мають ряд недоліків: вони схильні до впливу електромагнітних перешкод і не гарантують захист інформації, що передається. Максимальна довжина кабелю складає 100 м.

Волоконно-оптичний кабель (optical fiber) складається з тонких (5-60 мікрон) гнучких скляних волокон, за якими поширюються світлові сигнали (рис.2.5). Це найбільш якісний тип кабелю – він забезпечує передачу даних з дуже високою швидкістю (10 Гбіт/с і вище) і до того ж краще інших типів передавального середовища забезпечує захист даних від зовнішніх перешкод. Кожний світлодіод складається із центрального провідника світла (серцевини) – скляного волокна, і скляної оболонки, що має менший показник заломлення, чим серцевина. Поширюючись

серцевиною, промені світла не виходять за її межі, відбиваючись від покриваючого шару оболонки.

Рисунок 2.5 – Волоконно–оптичний кабель

В якості джерела світла в волоконно-оптичному кабелі використовуються світловипромінюючі діоди (LED – Light Emitting Diode) або лазерні діоди (Laser Diode), а як приймачі – фотоелементи. Розрізняють два види волоконно-оптичних кабелів: *багатомодові (Multi Mode Fiber, MMF)* та *одномодові (Single Mode Fiber, SMF)*. Останні мають центральний провідник дуже малого діаметра (5-10 мкм) і всі промені світла поширюються уздовж оптичної осі світловода, не відбиваючись від зовнішнього провідника (рис.2.6).

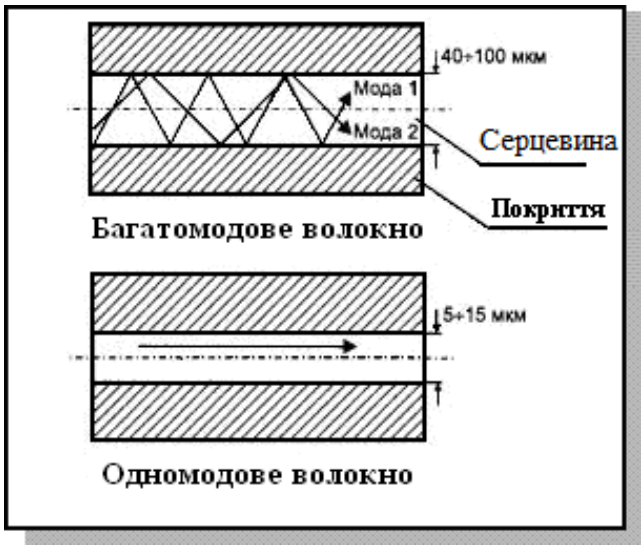


Рисунок 2.6 – Типи оптичного кабелю

Цей кабель складніший при виготовленні (і, відповідно, дорожчий), чим багатомодові. Крім того, для генерації світла в одномодових кабелях можуть використовуватися тільки лазерні діоди. SMF забезпечує

максимальну довжину кабелю (без підсилювача) більше 100 км і швидкість передачі даних у кілька десятків гигабіт у секунду.У багатомодових кабелях використовуються більш широкі внутрішні серцевини (62,5/125 мкм і 50/125 мкм, де 62,5 мкм або 50 мкм – діаметр центрального провідника, а 125 мкм - діаметр зовнішнього провідника), які легше виготовити технологічно. В якості джерела випромінювання світла застосовуються більш дешеві світлодіодні випромінювачі. У багатомодовому кабелі у внутрішньому провіднику одночасно існує кілька світлових променів, що відбиваються від зовнішнього провідника під різними кутам (рис.2.6). Кут відбиття проміня називається *модою*. MMF використовується в основному для передачі даних на невеликі відстані (до 300 - 2000 м) на швидкостях не більше 1 Гбіт/с.

Волоконно-оптичні кабелі мають відмінні електромагнітні та механічні характеристики, але недоліком даного виду кабелю є складність з'єднання волокон з розніманнями і між собою при необхідності нарощування довжини кабелю.

Середовища передавання бездротових мереж. На сьогоднішній день великий розвиток в області передачі даних отримали бездротові мережі – мережі радіозв'язку. Це пояснюється зручністю їх використання, дешевизною і прийнятною пропускною спроможністю. Виходячи з поточної динаміки розвитку, можна зробити висновок про те, що за кількістю і поширеності бездротові мережі скоро перевершать провідні мережі.

Радіомережі (бездротові мережі) забезпечують обмін даними між локальними комп'ютерними мережами, коли використання традиційних кабельних технологій утруднено або недоцільно (дорого). Прикладом ефективного використання бездротової технології радіодоступу є забезпечення зв'язку між сегментами локальних мереж при нестачі коштів або відсутності дозволу на проведення кабельних робіт.

В даний час в бездротових комп'ютерних мережах для передачі даних застосовуються види випромінювань: інфрачервоне (теплове); оптичне (видиме); радіохвильове.

Інфрачервоне випромінювання представляє собою різновид оптичного випромінювання з довжиною хвилі більшою, ніж у видимих променів. За довжиною хвилі коливань інфрачервоне випромінювання підрозділяється на короткохвильове (від 800 до 1400 нм), середньохвильове (від 1400 до 3000 нм), довгохвильове (від 3000 до 10000

нм). Інфрачервоне (теплове) випромінювання випускається всіма тілами, що мають температуру вище абсолютного нуля. Джерелом інфрачервоного випромінювання в бездротових системах можуть виступати лазер або фотодіод. В інфрачервоних бездротових мережах необхідно генерувати досить сильний сигнал, тому що на нього впливають перешкоди інших джерел тепла. Цей спосіб дозволяє передавати сигнали з великою швидкістю, оскільки інфрачервоні коливання мають широкий діапазон частот, проте можуть виникати труднощі при передачі сигналу на відстань більше 30 м.

Технологія, що використовує *видимі оптичні промені*, схожа на інфрачервону тим, що вимагає прямої видимості між передавачем і приймачем. Якщо з якихось причин оптичний промінь буде перерваний, то це призведе до припинення обміну даними.

Відмінною особливістю *радіоліній* є поширення електромагнітних сигналів у вільному простірі. Кожен вузол бездротової мережі оснащується антеною, яка одночасно є передавачем і приймачем електромагнітних хвиль. Електромагнітні хвилі поширюються в атмосфере або вакуумі у всіх напрямках або ж в межах певного сектора. Радіовипромінювання здійснюється на частотах від сотень кГц до сотень ГГц.

Так як при поширенні ненаправлених електромагнітних хвиль вони заповнюють весь простір (в межах певного радіуса, що визначається загасанням потужності сигналу), то цей простір може служити середовищем, що розділяється. Якщо дротове середовище визначає напрямок поширення сигналу в просторі, то бездротове середовище є ненаправленим. Для передачі дискретної інформації за допомогою бездротової лінії зв'язку необхідно модулювати електромагнітні коливання передавача відповідно до потока бітів, що передаються. Цю функцію здійснює пристрій DCE, який розташовується між антеною і пристроєм DTE.

За максимальним радіусом дії протоколи бездротових мереж можно класифікувати:

WWAN (Wireless Wide area network) –мережі стільникового зв'язку, їх радіус дії становить десятки кілометрів. До цих мереж відносяться такі протоколи: GSM, CDMAone, iDEN, PDC, GPRS і UMTS.

WMAN (Wireless Metropolitan Area Networks) – це бездротові мережі масштабу міста. Радіус дії таких мереж кілька кілометрів. Прикладом протоколу цієї мережі служить WiMAX.

Wireless LAN (Wireless Local Area Network; WLAN) – це бездротова локальна обчислювальна мережа. Радіус дії цього класу мереж – кілька сотень метрів. До них належать такі протоколи: UWB, ZigBee, Wi-Fi.

WPAN застосовуються для зв'язку різних пристроїв, включаючи комп'ютери, побутові прилади та оргтехніку, засоби зв'язку і т. д. Радіус дії WPAN становить від декількох метрів до декількох десятків метрів. WPAN використовується як для об'єднання окремих пристроїв між собою, так і для зв'язку їх з мережами більш високого рівня. Прикладом таких мереж можуть служити протоколи RuBee, X10, Insteon, Bluetooth, Z-Wave,ANT, RFID.

2.1.1.3 Характеристики ліній зв'язку

З теорії гармонійного аналізу відомо, що будь-який періодичний процес можна представити у вигляді суми синусоїдальних коливань різних частот і різних амплітуд. Кожна складова синусоїда називається також гармонікою, а набір всіх гармонік називають *спектральним розкладанням вихідного сигналу*.

Викривлення передавальним каналом синусоїди якої-небудь частоти приводить до викривлення амплітуди і форми переданого сигналу будь-якого виду. Викривлення форми проявляються в тому випадку, коли синусоїди різних частот спотворюються неоднаково. Внаслідок цього на прийомному кінці лінії сигнали можуть погано розпізнаватися.

До основних причин, внаслідок яких відбувається викривлення сигналу лінією зв'язку, варто віднести:

– Неідеальність параметрів лінії зв'язку. Наприклад, мідні провода мають *хвильовий опір* – це повний опір, що зустрічає електромагнітна хвиля певної частоти при поширенні по лінії зв'язку, що пояснюється наявністю активного опору, погонних індуктивності і ємності. Оптоволокно теж має відхилення від ідеального середовища передачі світла – вакууму.

– Викривлення, які вносяться проміжними апаратурами.

– Зовнішні та внутрішні перешкоди лінії зв'язку (електричні двигуни, атмосферні явища, наведення однієї пари провідників на іншу).

– Спектральна характеристика передавача, тобто спектральне розкладання генеруючого ним сигналу. Для генерації якісних прямокутних імпульсів необхідно, щоб спектральна характеристика передавача являла собою як можна більш вузьку смугу. Наприклад, лазерні діоди мають

значно меншу ширину спектра випромінювання (1-2 нм) у порівнянні зі світлодіодами (30-50 нм) при генерації імпульсів, тому частота модуляції лазерних діодів може бути набагато вище, ніж світлодіодів.

Ступінь викривлення синусоидальніх сигналів лініями зв'язку оцінюється за такими характеристиками, як загасання та смуга пропускання.

Загасання показує, на скільки зменшується потужність еталонного синусоїдального сигналу на виході лінії зв'язку стосовно потужності сигналу на вході цієї лінії. Загасання звичайно вимірюється в децибелах, дБ (d) і обчислюється $\mathbf{A = 10log_{10} P_{вих} / P_{вх}}$, де $P_{вих}$ – потужність сигналу на виході лінії, $P_{вх}$ - потужність сигналу на вході лінії.

Загасання кабелю завжди є від'ємною величиною, тому що потужність вихідного сигналу кабелю без проміжних підсилювачів завжди менше, чим потужність вхідного сигналу. Часто оперують абсолютним значеним затухання, опускаючи його знак. Чим менше загасання, тим вище якість лінії зв'язку.

Ступінь затухання потужності синусоїдального сигналу при проходженні ним по лінії зв'язку звічайно залежить від частоти синусоїди, тому повною характеристикою буде залежність затухання від частоти на усьому діапазоні, який представляє інтерес для практики (рис.2.7). Звичайно досить знати загасання на основній частоті (гармоніка якої має найбільшу амплітуду та потужність), щоб приблизно оцінити викривлення переданих сигналів.

Рисунок 2.7 – Залежність затухання від частоти

В якості характеристики потужності передавача часто використовують *абсолютний рівень потужності сигналу***,** який обчислюється по наступній формулі: p = 10 $\log_{10}$ P/1мВт [дБм], де p – потужність сигналу в міліватах. При цьому як базове значення потужності сигналу, до якого вимірюється поточна потужність, приймається значення в 1 мВт.

NVP (Nominal Velocity of Propagation) – швидкість поширення сигналу в лінії, яка виражається як відношення швидкості поширення сигналу до швидкості світла.

NEXT (Near End CrossTalk) – перехідне загасання, або перехресні наведення на ближньому кінці. Воно характеризує вплив сусідніх кручених пар один на одну і розглядається тільки при двосторонній передачі інформації. Даний ефект проілюстрований на рис. 2.8. Сигнал, який передається по верхній крученій парі, наводить перешкоду на нижню. При односторонньому обміні в розрахунок приймається параметр *FEXT (Far End CrossTalk)*, що характеризує взаємодію пар на дальньому кінці. Для ослаблення наведень застосовується фольгування.

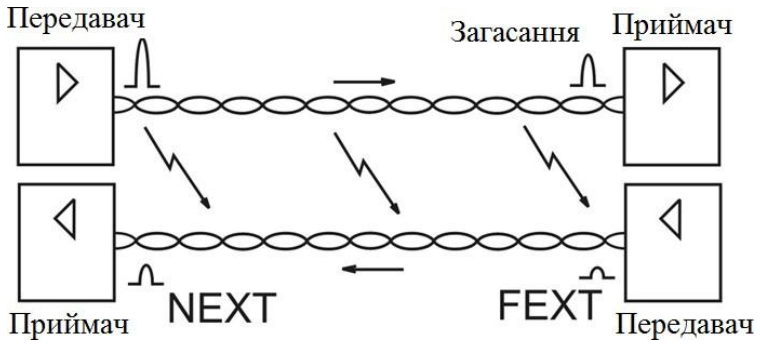


Рисунок 2.8 – Перехресні перешкоди в кабелі на основі витої пари

Часова затримка поширення сигналу між двома парами в кабелі (Pair-to-Pair Skew). Вона з'являється через те, що пари не ідеально однакові, одна з них обов'язково довша за іншу, тому сигнал проходить по ній більший шлях. Типове значення затримки становить близько 25 нс/100 м, але може доходити і до 45 нс/100 м. Цей параметр враховується при швидкостях передачі 100 Мбіт/с і вище.

Часова затримка поширення сигналу всередині однієї пари (Intra-Pair Skew). Вона виникає в разі, якщо довжини провідників в парі не збігаються.

Також однією важливою характеристикою лінії зв'язку є смуга пропускання, яка прямо впливає на максимально можливу швидкість передачі інформації.

Смуга пропускання (bandwidth) визначає діапазон частот синусоїдального сигналу, при якому цей сигнал передається по лінії зв'язку без значних викривлень. Ширина смуги пропускання впливає на максимально можливу швидкість передачі інформації. Граничними частотами вважаються частоти, на яких потужність вихідного сигналу зменшується в 2 рази стосовно вхідного, що відповідає загасанню -3дб. Смуга пропускання залежить від типу лінії та її довжини. Ширина смуги пропускання дорівнює W = f2 - f1 (у герцах), де f2 і f1 – відповідно верхня і нижня границі смуги пропускання.

Важливою характеристикою, що прямо впливає на продуктивність і надійність створюваної мережі, є пропускна здатність. *Пропускна здатність (throughput)* лінії характеризує максимально можливу швидкість передачі даних по лінії зв'язку. Пропускна здатність виміряється в бітах за секунду і залежить, з одного боку, від характеристик фізичного середовища (затухання та смуги пропускання), а з іншого боку - визначається характеристиками способу передачі даних, тобто способом кодування.

Зв'язок між смугою пропускання лінії і її максимально можливою пропускною здатністю незалежно від прийнятого способу фізичного кодування, установив Клод Шеннон:

$$C = F \log_2 (1 + Pc/Pш),$$

де C – максимальна пропускна здатність лінії в бітах за секунду, F – ширина смуги пропускання лінії в герцах, Pc – потужність сигналу, Pш – потужність шуму.

Пропускна здатність залежить також від спектра переданих сигналів. Якщо значимі гармоніки сигналу (тобто ті гармоніки, амплітуди яких вносять основний вклад у результуючий сигнал) попадають у смугу пропускання лінії, то такий сигнал буде добре передаватися даною лінією зв'язку. Від обраного способу кодування залежить спектр сигналів і, відповідно, пропускна здатність лінії.

Формула Найквіста визначає максимально можливу пропускну здатність лінії зв'язку, але без урахування шуму на лінії:

$$C = 2F \log_2 M,$$

де M - кількість станів інформаційного параметра.

Якщо сигнал має 2 стани, то пропускна здатність дорівнює подвоєному значенню ширини смуги пропускання лінії зв'язку. Якщо ж передавач використає більш ніж 2 стійких стани сигналу для кодування даних, то пропускна здатність лінії підвищується, тому що за один такт роботи передавач передає декілька біт вихідних даних (рис.2.8).

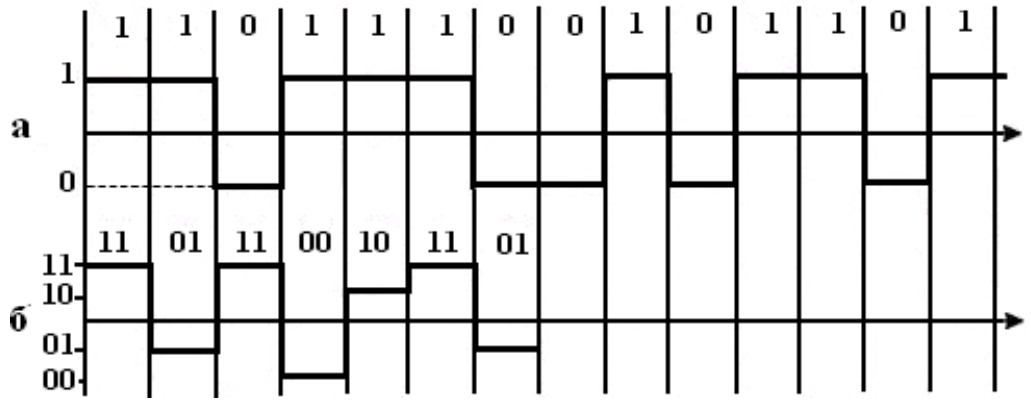


Рисунок 2.8 – Підвищення швидкості передачі даних за рахунок додаткових станів сигналу

2.1.2 Сигнали та коди. Протоколи фізичного рівня

При передачі даних каналами зв'язку використовується два види фізичного кодування:

- аналогова модуляція;
- цифрове кодування.

При аналоговій модуляції інформація кодується зміною амплітуди, частоти або фази синусоїдального сигналу несучої частоти.

При цифровому кодуванні дискретної інформації застосовують потенційні та імпульсні коди.

У потенційних кодах для представлення логічних одиниць і нулів використовується тільки значення потенціалу сигналу, а його перепади, що формують закінчені імпульси, в увагу не приймаються. Імпульсні коди дозволяють представити двійкові дані або імпульсами визначеної полярності, або частиною імпульсу – перепадом потенціалу.

Основними вимогами, які пред’являються до методів цифрового кодування є:

– забезпечення при одній і тій же бітовій швидкості найменшої ширини спектра результуючого сигналу;

– забезпечення синхронізації між передавачем та приймачем;

– здатність розпізнавати помилки;

– меньша кількість рівнів сигналу кода;

– низька вартість реалізації.

Якщо більш вузький спектр сигналів дозволяє на одній і тій же лінії (з однієї й тією же смугою пропускання) домагатися більш високої швидкості передачі даних, то синхронізація передавача та приймача потрібна для того, щоб приймач точно знав, у який момент часу необхідно зчитувати нову інформацію з лінії зв'язку. Існує кілька способів, що дозволяють домогтися синхронізації передавача та приймача. Перший спосіб – виділення окремої тактуючої лінії зв'язку. Однак він має ряд недоліків – на великих відстанях з'являється нерівномірність швидкості поширення сигналу через неоднорідність характеристик провідників у кабелях і збільшення витрат кабелю, який дорого коштує.

Перспективнішим способом є застосування кодів, що самосинхронізуються, сигнали яких несуть для передавача вказівки про те, у який момент часу потрібно здійснювати розпізнавання чергового біта. Будь-який різкий перепад сигналу – так званий фронт – може служити гарною вказівкою для синхронізації приймача з передавачем.

Розглянемо більш докладно найбільш популярні методи цифрового кодування, представлені на діаграмі рис.2.9.

Потенційний код без повернення до нуля (Non Return to Zero, NRZ). Сигнал кодується двома значеннями потенціалів, що не змінюються протягом такту. При передачі послідовності одиниць не вертається до нуля протягом такту (рис.29). До достоїнств методу слід віднести простоту в реалізації та гарне розпізнавання помилок. Код NRZ має досить низьку частоту основної гармоніки f_0, що дорівнює N/2 Гц, де N – бітова швидкість передачі даних у біт/с.

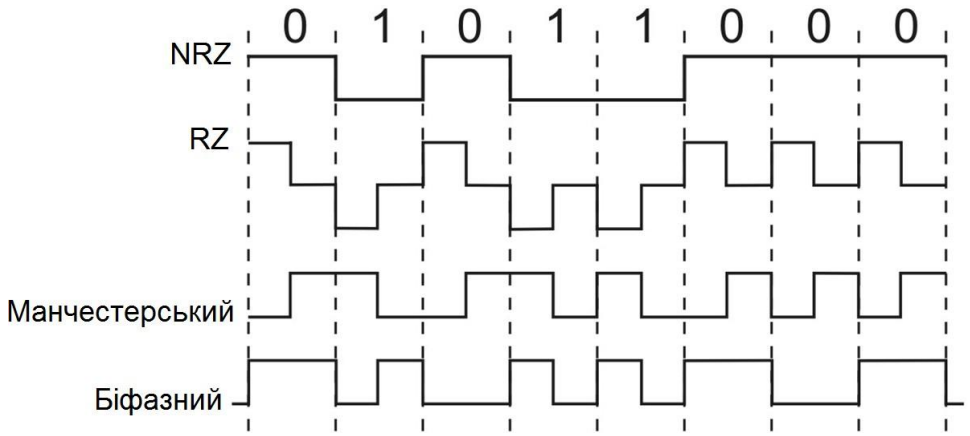


Рисунок 2.9 – Стандартні коди локальних мереж

Недоліком методу є те, що він не має властивість самосинхронізації. При довгій послідовності 0 або 1 виникають низькочастотні складові спектра, які наближаються до постійної складової (виникає постійний потенціал). У зв'язку із цим у чистому виді код NRZ у мережах не використовується. Однак, як буде видно далі, використовуються його різні модифікації, у яких усуваються дані проблеми.

Код RZ. Це імпульсний код, у якому одиниця представлена імпульсом однієї полярності, а нуль – іншої (рис. 2.9). Кожний імпульс триває половину такту. Код має відмінні самосинхронізуючі властивості, але постійна складова, може бути присутня, наприклад, при передачі довгої послідовності одиниць або нулів. Крім того, спектр у нього ширше, ніж у потенційних кодів. Так, при передачі всіх нулів або одиниць частота основної гармоніки коду буде дорівнювнювати N Гц, що вище основної гармоніки коду NRZ. Через занадто широкий спектр біполярний імпульсний код використовується рідко.

Манчестерський код. Найпоширеніший метод кодування в локальних мережах. Він застосовується в технологіях Ethernet і Token Ring. При манчестерському кодуванні кожний такт ділиться на дві частини. Інформація кодується перепадами потенціалу, що відбувається в середині кожного такту. Одиниця кодується перепадом від низького рівня сигналу до високого, а нуль – зворотним перепадом (рис.2.9). На початку кожного такту може відбуватися службовий перепад сигналу, якщо потрібно представити кілька одиниць або нулів підряд. Манчестерский код має гарні самосинхронізуючі властивості. Смуга пропускання манчестерського коду вужче, ніж у біполярного імпульсного. У нього також немає постійної складової, а основна гармоніка має частоту N Гц

(при передачі послідовності одиниць або нулів), або N/2 Гц (при передачі одиниць, що чергуються, і нулів). У середньому основна гармоніка коливається поблизу значення 3N/4. На відміну від біполярного імпульсного коду у манчестерському коді для передачі даних використовується два рівні сигналу.

Потенційний код з інверсією при одиниці (Non Return to Zero with ones Inverted, NRZI). Код NRZI при передачі нуля передає потенціал, що був установлений у попередньому такті (тобто не міняє його), а при передачі одиниці потенціал інвертується на протилежний (рис.2.10). Цей код зручний у тих випадках, коли використання третього рівня сигналу небажано, наприклад при передачі по оптоволоконному кабелю. Використовується в технологіях FDDI і Fast Ethernet 100 Base-FX.

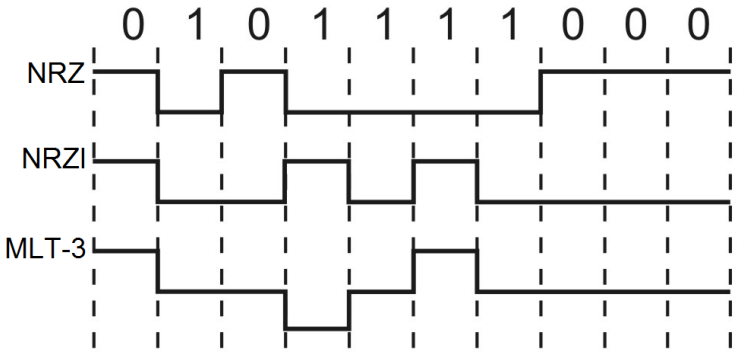


Рисунок 2.10 – Додаткові коди NRZI і MLT-3

Код MLT-3 (Multilevel transmission) – код з трьома рівнями сигналів (рис. 2.10). Зміна сигналу відбувається на початку передавання біта. Якщо передається нуль, то зміни нема, а якщо одиниця, то відбувається зміна рівня сигналу на наступний (0, 1, 0, -1, 0,…). Недоліком коду MLT-3, як і коду NRZ, є відсутність синхронізації. Ця проблема вирішується за допомогою перетворення даних, яке виключає довгі послідовності нулів і, отже, можливість рассинхронизации. Однак сигнал коду MLT-3 генерує менже завад за рахунок меншої інтенсивності змін кодового сигналу. Використовується в технологіях FDDI і Fast Ethernet 100 Base-TX.

Кодом PAM-5 кодують комбінації з двох бітів. Чотирьом можливим комбінаціям (00, 01, 10, 11) відповідає певний рівень сигналу (рис.2.11). П’яте значення зумовлює надлишковість, яку використовують для виявлення помилок. Код PAM-5 застосовують для передавання в 1000 Base-TX паралельно по чотирьох парах. Якщо врахувати, що кабель 5-ї

категорії розрахований на частоту 125 МГц, тобто інформаційна швидкість по одній парі складе 250 Мбіт/с. Якщо задіяти всі чотири пари, то можна підвищити швидкість передачі до 1000 Мбіт/с, тобто досягти бажаної швидкості.

Рисунок 2.11 – Код PAM-5

Для поліпшення потенційних кодів типу NRZI використовується логічне кодування. Логічне кодування повинно замінювати довгі послідовності біт, що приводять до постійного потенціалу, вкрапленнями одиниць. Для логічного кодування характерні два методи – надлишкові коди і скремблірування.

Надлишковий код 4B/5B, який використовується у технологіях FDDI і Fast Ethernet, замінює вихідні символи довжиною в 4 біти на символи довжиною в 5 бітів. У коді 4B/5B результуючі символи можуть містити 32 бітові комбінації, у той час як вихідні символи - тільки 16 (рис.2.12). Тому в результуючому коді можна відібрати 16 таких комбінацій, які не містять великої кількості нулів, а інші прийнято вважати *забороненими кодами*. Символи коду 4B/5B довжиною 5 бітів гарантують, що при будь-якому їхньому сполученні на лінії не може зустрітися більше трьох нулів підряд. Тому поліпшені потенційні коди усувають постійну складову та здобувають властивість самосинхронізації. Крім того, якщо приймач приймає заборонений код, то це свідчить про те, що на лінії відбулося викривлення сигналу.

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

Рисунок 2.12 – Символи коду 4B/5B

Скремблірування – це спосіб логічного кодування інформації, що ґрунтується на перемішуванні даних за відповідним алгоритмом скремблером перед передачею їх у лінію за допомогою потенційного коду, так щоб кількість 0 і 1 у результуючому коді було приблизно однаковим. Методи скремблірування полягають у побітному обчисленні результуючого коду на підставі біт вихідного коду і отриманих у попередніх тактах бітах результуючого коду. Наприклад, скремблер може реалізувати наступне співвідношення: $B_i = A_i \oplus B_{i-3} \oplus B_{i-5}$, де B_i - двійкова цифра результуючого коду, що отримана на і-му такті роботи скремблера, A_i - двійкова цифра вихідного коду, що надходить на і-му такті на вхід скремблера, B_{i-3} і B_{i-5} - двійкові цифри результуючого коду, отримані на попередніх тактах роботи скремблера, відповідно на 3 і на 5 такті раніше поточного такту, $\oplus$ - операція додавання по модулю 2.

Після одержання результуючої послідовності приймач передає її дескремблеру, який відновлює вихідну послідовність на підставі зворотного співвідношення, у нашому випадку

$$C_i = B_i \oplus B_{i-3} \oplus B_{i-5} = (A_i \oplus B_{i-3} \oplus B_{i-5}) \oplus B_{i-3} \oplus B_{i-5} = A_i .$$

Поліпшені потенційні коди мають більш вузький спектр, чим імпульсні коди і знаходять застосування у високошвидкісних технологіях (FDDI, Fast Ethernet, Gigabit Ethernet).

2.1.3 Методи виявлення і корекції помилок

Канальний рівень повинен виявляти помилки передачі даних, пов'язані з викривленням бітів у прийнятому кадрі даних або із втратою кадру, і по можливості їх коректувати. Розглянемо більш докладно декілька найбільш популярних методів виявлення помилок і відновлення викривлених і втрачених кадрів.

2.1.3.1 Методи виявлення помилок

Методи виявлення помилок засновані на передачі у складі кадру даних службової надлишкової інформації – *контрольної суми (Frame Check Sequence, FCS)*, по якій можна судити про достовірність прийнятих даних. Контрольна сума обчислюється як функція від основної інформації. Приймаюча сторона повторно обчислює контрольну суму кадру по відомому алгоритму і у випадку її збігу з контрольною сумою, обчисленою передавальною стороною, робить висновок про коректність прийнятих даних. Існує кілька розповсюджених методів обчислення контрольної суми.

Контроль за паритетом. Метод заснований на підсумовуванні по модулю 2 всіх бітів інформації, що контролюється. Наприклад, для даних 100101011 результатом контрольного підсумовування буде значення 1. Результат підсумовування, один біт даних пересилається разом з інформацією. При викривленні при пересиланні будь-якого одного біта вихідних даних результат підсумовування буде відрізнятися від прийнятого контрольного розряду, що говорить про помилку. Однак подвійна помилка, наприклад 110101010, буде невірно прийнята за коректні дані. Тому контроль за паритетом застосовується до невеликих порцій даних, як правило, до кожного байта. Метод рідко застосовується в обчислювальних мережах через його велику надмірність і невисокі діагностичні здатності.

Циклічний надлишковий контроль (Cyclic Redundancy Check, CRC) у цей час є найбільш популярним методом контролю в обчислювальних мережах. Метод заснований на розгляді вихідних даних у вигляді одного багаторозрядного двійкового числа. Наприклад, кадр стандарту Ethernet, що складається з 1024 байтів, буде розглядатися як одне число, що складається з 8192 бітів. У якості контрольної інформації розглядається залишок від розподілу цього числа на відомий дільник R з розрядністю

(n+1). Звичайно як дільник вибирається сімнадцяти- або тридцяти трьохрозрядне число, щоб остача від ділення мала довжину n – 16 розрядів (2 байти) або 32 розряда (4 байти). При одержанні кадру даних знову обчислюється остача від ділення на той же дільник R, але при цьому до даних кадру додається й контрольна сума, що втримується в ньому. Якщо остача від ділення на R дорівнює нулю, то робиться висновок про відсутність помилок в отриманому кадрі, у противному випадку кадр вважається викривленим.

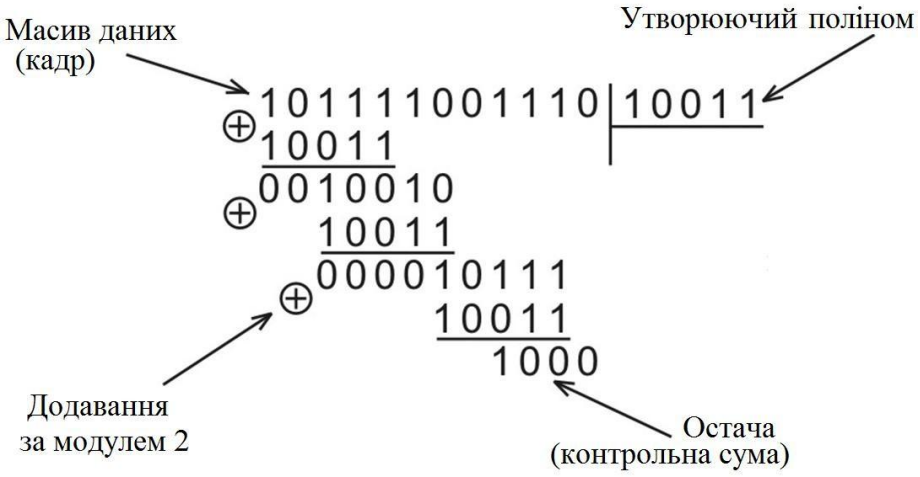


Рисунок 2.13 – Ділення за модулем 2 в методі CRC

Цей метод має високу обчислювальну складність і невисокий ступінь надмірності, а його діагностичні можливості набагато вище, ніж у методу контролю за паритетом. Імовірність виявлення одиночної помилки дорівнює 100%, імовірність виявлення помилок кратністю 2 і більше приблизно дорівнює: $(1 - 2^{-n})$, де n – розрядність контрольної суми (за умови N >> n, де N - кількість біт кадру);

Вибір утворюючого полінома відбувається за наступними правилами:

– кількість розрядів полінома дорівнює (n+1), де n – необхідна розрядність циклічної контрольної суми;

– старший біт полінома дорівнює 1;

– поліном ділиться (за модулем 2) без остачі тільки на одиницю і на самого себе (просте число);

– кількість одиниць в коді полінома має бути мінімально, щоб спростити апаратуру обчислювача контрольної суми (рис.2.14).

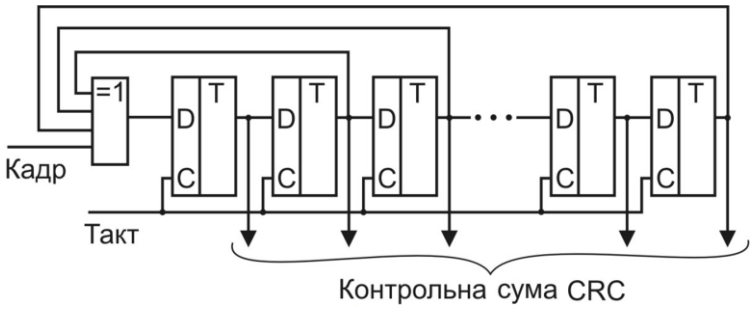


Рисунок 2.14 – Реалізація обчислювача контрольної суми

2.1.3.2 Методи відновлення викривлених і втрачених кадрів

Методи відновлення викривлених і втрачених кадрів ґрунтуються на тому, що якщо кадр не доходить до одержувача, то він повторно передається адресатові. Для цього відправник нумерує кадри даних, і для кожного кадру даних очікує від приймача *позитивної квитанції* – службового кадру, що сповіщає про те, що вихідний кадр був отриманий і дані в ньому виявилися коректними. Час очікування обмежений – при відправленні кожного кадру передавач запускає таймер, і, якщо за його витіканням позитивна квитанція не отримана, кадр вважається втраченим. Приймач у випадку одержання кадру з викривленими даними може відправити *негативну квитанцію* – вказівку на те, що даний кадр потрібно передати повторно.

На даному принципі роботи ґрунтується метод із простоями та метод «ковзного вікна».

У *методі із простоями* вузол, що послав кадр, очікує одержання квитанції (позитивної або негативної) від приймача і тільки після цього посилає наступний кадр (або повторює викривлений). Якщо ж квитанція не приходить протягом тайм-ауту, то кадр (або квитанція) вважається втраченим і його передача повторюється (рис.2.15, а).

У *методі «ковзного вікна»* джерело передає деяку кількість кадрів у безперервному режимі, без одержання на ці кадри позитивних квитанцій. Кількість кадрів, що дозволяється передавати таким чином, називається *розміром вікна*. На рис.2.15 даний метод представлений для вікна розміром W.

У початковий момент, коли ще не послано жодного кадру, вікно визначає діапазон кадрів з номерами від 1 до W включно. Джерело починає передавати кадри й одержувати у відповідь квитанції. Для

простоти припустимо, що квитанції надходять у тій же послідовності, що й кадри, яким вони відповідають. У момент t_1 при одержанні першої квитанції K_1 вікно зсувається на одну позицію, визначаючи новий діапазон від 2 до (W+1) (рис.2.15, б).

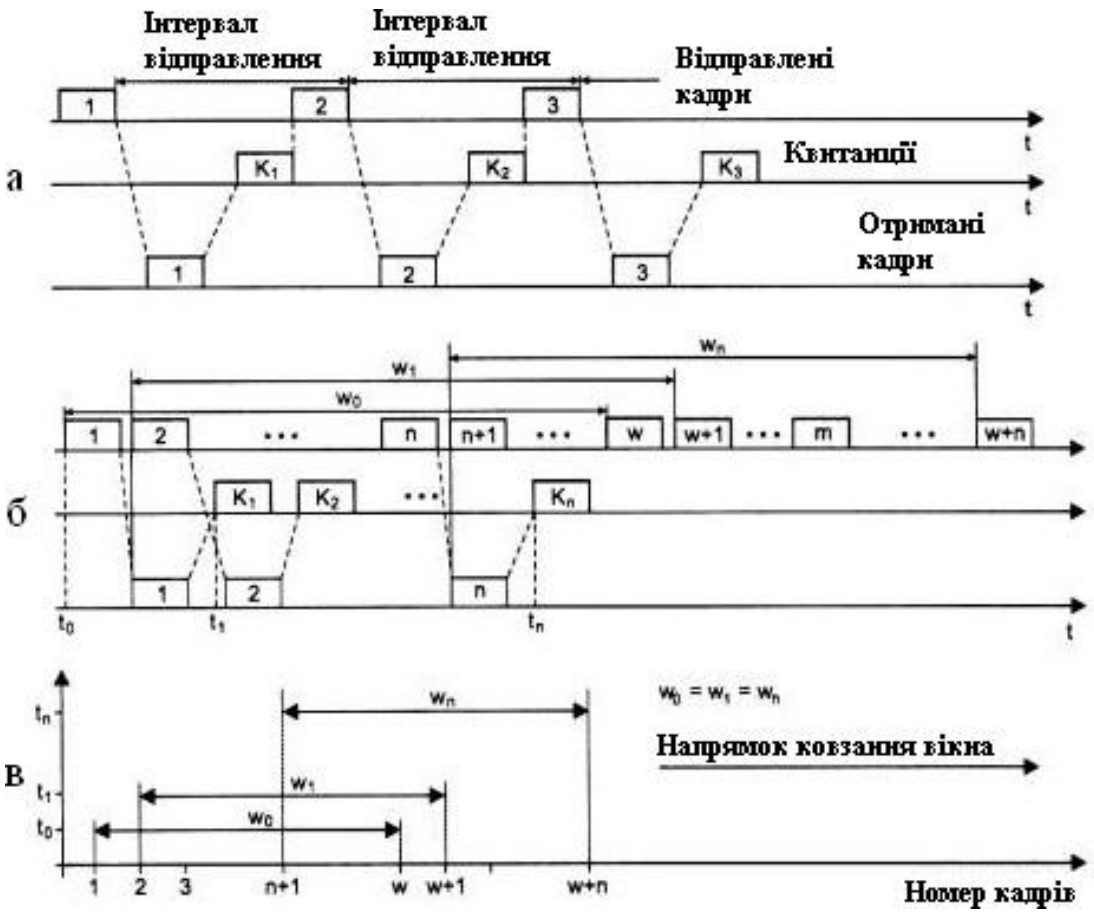


Рисунок 2.15 – Діаграми методів відновлення перекручених і загублених кадрів

Переміщення вікна уздовж послідовності номерів кадрів показане на рис. 2.15, в. Тут t_0 - вихідний момент, t_1 і t_n - моменти приходу квитанцій на перший і n-й кадр відповідно. Щораз, коли приходить квитанція, вікно зсувається вліво, але його розмір при цьому не міняється і залишається рівним W. Помітимо, що хоча в даному прикладі розмір вікна в процесі передачі залишається постійним, у реальних протоколах (наприклад, TCP) можна зустріти варіанти даного алгоритму з розміром вікна, що змінюється.

Отже, при відправленні кадру з номером n джерелу дозволяється передати ще W-1 кадрів до одержання квитанції на кадр n, так що в мережу

останнім піде кадр із номером (W+n-1). Якщо ж за цей час квитанція на кадр n так і не прийшла, то процес передачі припиняється, і після закінчення деякого тайм-ауту кадр n (або квитанція на нього) вважається втраченими, і він передається знову.

Метод ковзного вікна складніший у реалізації, чим метод із простоями, тому що передавач повинен зберігати в буфері всі кадри, на які поки не отримані позитивні квитанції. Крім того, потрібно відслідковувати кілька параметрів алгоритму: розмір вікна W, номер кадру, на який отримана квитанція, номер кадру, що ще можна передати до одержання нової квитанції.

У деяких реалізаціях методу приймач може не посилати квитанції на кожний прийнятий коректний кадр. Якщо кілька кадрів прийшли майже одночасно, то приймач може послати квитанцію тільки на останній кадр. При цьому мається на увазі, що всі попередні кадри також дійшли благополучно.

Інші методи використовують негативні квитанції. Негативні квитанції бувають двох типів – групові та виборчі. Групова квитанція містить номер кадру, починаючи з якого потрібно повторити передачу всіх кадрів, відправлених передавачем у мережу. Виборча негативна квитанція вимагає повторної передачі тільки одного кадру.

Метод ковзного вікна має два параметри, які можуть помітно впливати на ефективність передачі даних між передавачем і приймачем, - розмір вікна та величина тайм-ауту очікування квитанції. У надійних мережах, коли кадри спотворюються і втрачаються рідко, для підвищення швидкості обміну даними розмір вікна потрібно збільшувати, тому що при цьому передавач буде посилати кадри з меншими паузами. У ненадійних мережах розмір вікна варто зменшувати, тому що при частих втратах і викривленнях кадрів різко зростає обсяг удруге переданих через мережу кадрів, а виходить, пропускна здатність мережі буде витрачатися вхолосту - корисна пропускна здатність мережі буде падати. Вибір тайм-ауту залежить не від надійності мережі, а від затримок передачі кадрів мережею.

Метод ковзного вікна реалізований у багатьох протоколах: LLC2, LAP-B, X.25, TCP, Novell NCP Burst Mode.

Метод із простоями є окремим випадком методу ковзного вікна, коли розмір вікна дорівнює одиниці.

Реалізація ковзного вікна в протоколі TCP. У протоколі TCP реалізований різновид алгоритму квитування з використанням вікна. Квитанція посилається тільки у випадку правильного прийому даних, негативні квитанції не посилаються. Таким чином, відсутність квитанції означає або прийом викривленого сегмента, або втрату сегмента, або втрату квитанції.

У якості квитанції одержувач сегмента відсилає відповідне повідомлення (сегмент), у яке поміщається число, на одиницю більше максимального номеру байта в отриманому сегменті. Якщо розмір вікна дорівнює W, а остання квитанція містила значення N, то відправник може посилати нові сегменти доти, поки в черговий сегмент не потрапить байт із номером N+W. Цей сегмент виходить за рамки вікна, і передачу в такому випадку необхідно призупинити до приходу наступної квитанції.

Вибір часу очікування (тайм-ауту) чергової квитанції є важливим завданням, результат рішення якої впливає на продуктивність. У протоколі TCP тайм-аут визначається за допомогою досить складного адаптивного алгоритму, ідея якого полягає в наступному. При кожній передачі засікається час від моменту відправлення сегмента до приходу квитанції (час обороту). Одержувані значення часів обороту усереднюються з ваговими коефіцієнтами, що зростають від попереднього виміру до наступного. Це робиться для того, щоб підсилити вплив останніх вимірів. В якості тайм-ауту вибирається середній час обороту, помножений на деякий коефіцієнт. Практика показує, що значення цього коефіцієнта повинно перевищувати 2. У мережах з більшим розкидом часу обороту при виборі тайм-ауту враховується і дисперсія цієї величини.

Варіюючи величину вікна, можна вплинути на завантаження мережі. Так при переповненні прийомного буфера кінцевого вузла "перевантажений" протокол TCP, відправляючи квитанцію, поміщає в неї новий, зменшений розмір вікна. Якщо він зовсім відмовляється від прийому, то у квитанції вказується вікно нульового розміру. Однак навіть після цього додаток може послати повідомлення на порт, що відмовився від прийому. Для цього, повідомлення повинно супроводжуватися позначкою "терміново" (біт URG у запиті встановлений в 1). У такій ситуації порт зобов'язаний прийняти сегмент, навіть якщо для цього прийде витиснути з буфера дані, що вже перебувають там.

Після прийому квитанції з нульовим значенням вікна протокол-відправник час від часу робить контрольні спроби продовжити обмін

даними. Якщо протокол-приймач уже готовий приймати інформацію, то у відповідь на контрольний запит він посилає квитанцію із вказівкою ненульового розміру вікна.

Іншим проявом перевантаження мережі є переповнення буферів у маршрутизаторах. У таких випадках вони можуть централізовано змінити розмір вікна, посилаючи керуючі повідомлення деяким кінцевим вузлам, що дозволяє їм диференційоване управляти інтенсивністю потоку даних у різних частинах мережі.

2.2 Локальні мережі

2.2.1 Базові технології локальних мереж

2.2.1.1 Структура стандартів IEEE 802.x

Переважна більшість функціонуючих у цей час локальних мереж відповідають стандартам, розробленим Інститутом інженерів по електротехніці та радіоелектроніці (Institute of Electrical and Electronic Engineers – IEEE) і Американським національним інститутом стандартів (American National Standard Institute – ANSI). Узагальнено групи називаються *IEEE 802 LAN Standards Committees* (комітетами IEEE 802 по стандартам в області локальних мереж). Результатом їхньої роботи стало прийняття сімейства стандартів IEEE 802.x, які містять рекомендації з проектування нижніх рівнів локальних мереж. ANSI були розроблені стандарти на локальну мережу FDDI (на волоконно-оптичному кабелі).

Стандарти сімейства IEEE 802.x охоплюють тільки два нижніх рівні моделі OSI – фізичний і канальний. Причому канальний рівень був розділений на два підрівня:

- керування логічним каналом (Logical Link Control, LLC);
- керування доступом до середовища (Media Access Control, MAC).

Рівень MAC забезпечує коректне спільне використання загального середовища. Він надає його в розпорядження того або іншого вузла мережі відповідно до певного алгоритму. Після того як доступ до середовища отриманий, ним може користуватися більш високий рівень – рівень LLC, що відповідає за передачу кадрів даних між вузлами з різним ступенем надійності, а також реалізує функції інтерфейсу із прилягаючим до нього мережевим рівнем. На рівні LLC існує кілька режимів роботи, що відрізняються наявністю або відсутністю на цьому рівні процедур

відновлення кадрів у випадку їхньої втрати або викривлення, тобто транспортних послуг, що відрізняються якістю, цього рівня. Структура стандартів IEEE 802 наведена на рис. 2.16.

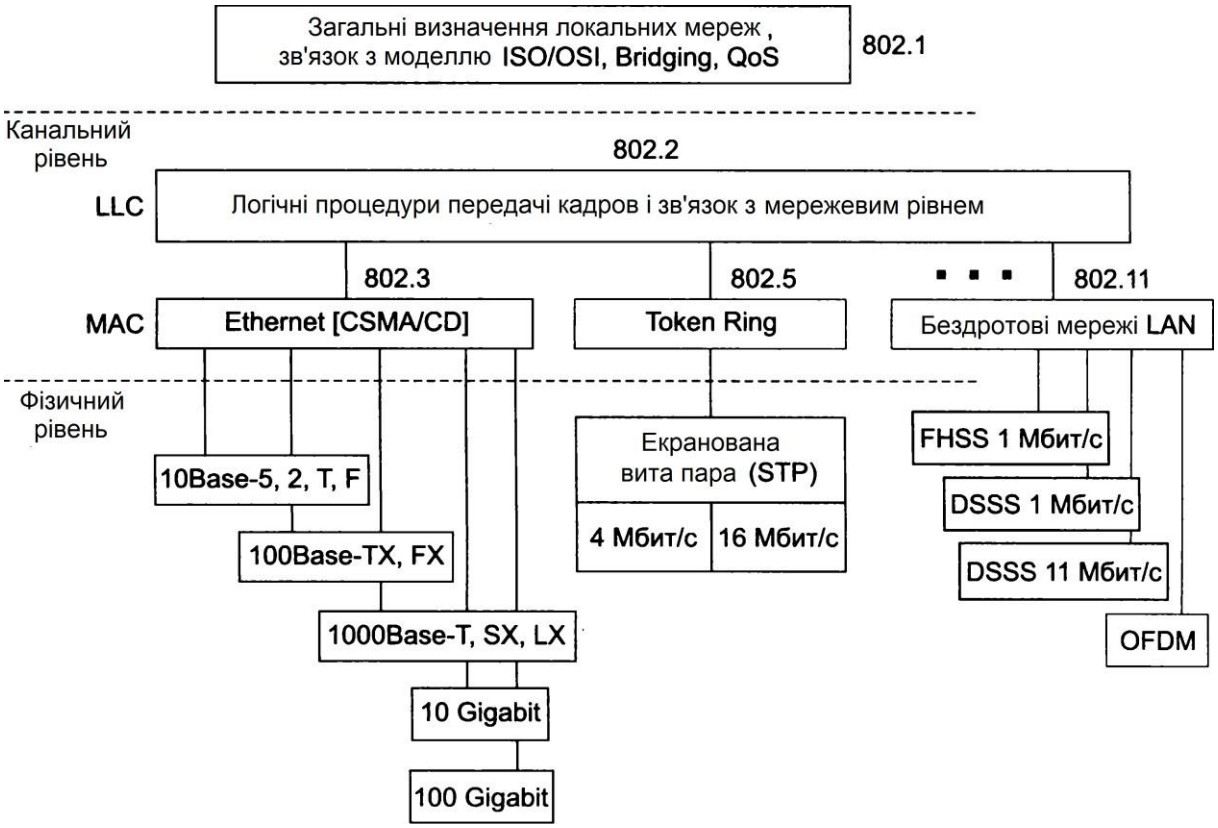


Рисунок 2.16 – Структура стандартів IEEE 802.x

Стандарти підкомітету 802.1 носять загальний для всіх технологій характер і постійно поповнюються. Поряд з визначенням локальних мереж і їхніх властивостей, стандартами міжмережевої взаємодії, описом логіки роботи моста/комутатора до результатів роботи комітету ставиться й стандартизація порівняно нової технології віртуальних локальних мереж VLAN.

Підкомітет 802.2 розробив і підтримує стандарт LLC. Стандарти 802.3, 802.4, 802.5 і 802.12 описують технології локальних мереж, які з'явилися в результаті поліпшень фірмових технологій, що лягли в їхню основу, відповідно Ethernet, ArcNet, Token Ring. Опис кожної технології розділено на дві частини: опис рівня MAC і опис фізичного рівня, причому єдиному протоколу MAC може відповідати кілька варіантів протоколів фізичного рівня.

Комітет 802.11 займається розробкою локальних радіомереж з методами доступу до середовища, близькими до тих, які використовуються в мережах Ethernet (радіо-Ethernet).

2.2.1.2 Технологія Ethernet

Ethernet – це найпоширеніша на сьогоднішній день специфікація локальних мереж, яку в 1980 році спільно опублікували корпорації Xerox, Intel і Digital Equipment Corporation (DEC). Пізніше вона була представлена в комітети IEEE 802 і з деякими змінами включена в стандарт IEEE 802.3.

Залежно від типу фізичного середовища стандарт IEEE 802.3 має різні модифікації - l0Base-5, l0Base-2, l0Base-T, l0Base-FL, l0Base-FB, що забезпечують пропускну здатність 10Мбіт/с, використовується манчестерский код.

В 1995 році був прийнятий стандарт Fast Ethernet зі швідкістю 100 Мбіт/с, а в 1998 році стандарт Gigabit Ethernet з бітовою швидкістю 1000 Мбіт/с. Всі види стандартів Ethernet (у тому числі Fast Ethernet і Gigabit Ethernet) використовують однаковий метод поділу середовища передачі даних – метод CSMA/CD.

Структура кадра Ethernet. Кадр, що передається кожним вузлом, містить дані маршрутизації, керування і корекції помилок. Для мереж Ethernet параметри кадрів визначені стандартом 802.3 IEEE.Базова довжина кадру може змінюватися від 72 до 1526 байтів при типовій структурі, наведеній на рис.2.17.

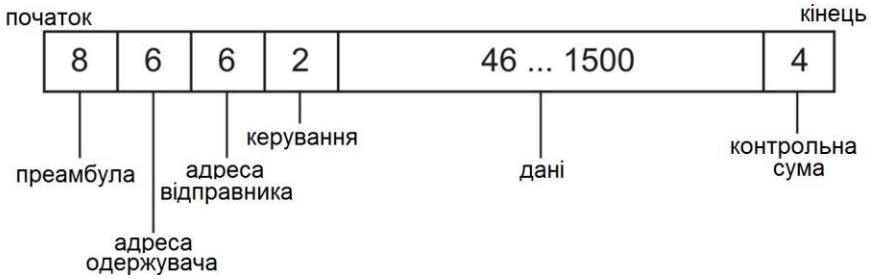


Рисунок 2.17 – Базова структура кадра Ethernet

Призначення полів кадру Ethernet:

Преамбула – призначена для синхронізації прийому: перші сім байтів – код 10101010, восьмий байт – код 10101011 (признак початку кадра).

Адреса одержувача і адреса відправника – 6-байтні стандартні MAC-адреси;

Поле керування (2 байта, L/T – Length/Type) – кількість байт в полі даних (до 1500) або тип кадру (більше 1500);

Поле даних – от 46 до 1500 байт даних. Якщо передається менше 46 байт – поле заповнення;

Поле контрольної суми (FCS – Frame Check Sequence) – 32-розрядна циклічна контрольна сума (CRC);

Довжина кадра – от 512 біт (64 байта) до 12144 біт (1518 байт).

Метод доступу CSMA/CD (Carrier Sense Multiple Access/Collision Detection CSMA/CD) – метод колективного доступу з контролем несучої та виявленням колізій.

Розглянемо докладніше алгоритм доступу CSMA/CD:

- Щоб одержати можливість передавати кадр, станція повинна переконатися, що поділюване середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, що також називається несучою частотою (carrier-sense, CS). Ознакою незайнятості середовища є відсутність на ній несучої частоти.
- Якщо середовище вільне, то вузол має право почати передачу кадру. Всі станції, підключені до кабелю, можуть розпізнати факт передачі кадру, і та станція, що впізнає власну адресу в заголовках кадру, записує його у свій внутрішній буфер, обробляє отримані дані, а потім посилає в середовище кадр-відповідь.
- Після закінчення передачі кадру всі вузли мережі зобов'язані витримати технологічну паузу в 9,6 мкс. Ця пауза називається також *міжпакетним інтервалом (Inter Packet Gap)*. Вона потрібна для приведення мережевих адаптерів у вихідний стан, а також для запобігання монопольного захоплення середовища однією станцією. Після закінчення технологічної паузи вузли мають право почати передачу свого кадру, тому що середовище вільне.

Виникнення колізії. Механізм прослуховування середовища та пауза між кадрами не гарантують від виникнення такої ситуації, коли дві або більше станції одночасно вирішать, що середовище вільне, і почнуть передавати свої кадри. Говорять, що при цьому відбувається *колізія (collision)*, тому що вміст обох кадрів зіштовхується на загальному кабелі і відбувається викривлення інформації.

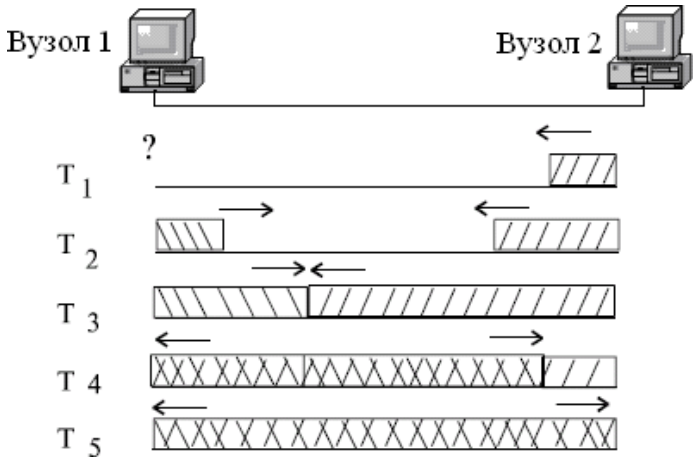


Рисунок 2.18 – Схема виникнення і поширення колізії

Найчастіше колізія виникає через те, що один вузол починає передачу раніше іншого, але до другого вузла сигнали першого просто не встигають дійти на той час, коли другий вузол вирішує почати передачу свого кадру. Тобто колізії – це наслідок розподіленого характеру мережі (рис.2.18).

Щоб коректно обробити колізію, всі станції одночасно спостерігають за виникаючими на кабелі сигналами. Якщо передані і спостережувані сигнали відрізняються, то фіксується *виявлення колізії (collision detection, CD)*. Для збільшення ймовірності швидкого виявлення колізії станція, що виявила колізію, перериває передачу свого кадру і підсилює ситуацію колізії посилкою в мережу спеціальної послідовності з 32 біт, яка називається *jam-послідовністю*.

Після цього передавальна станція, що виявила колізію, зобов'язана припинити передачу і зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища і передачі кадру. Випадкова пауза вибирається за наступним алгоритмом:

Пауза = L *(інтервал відстрочки), де інтервал відстрочки дорівнює 512 бітовим інтервалам (у технології Ethernet прийнято всі інтервали вимірювати в бітових інтервалах; бітовий інтервал позначається як bt і відповідає часу між появою двох послідовних біт даних на кабелі; для швидкості 10 Мбіт/с величина бітового інтервалу дорівнює 0,1 мкс або 100 нс);

L являє собою ціле число, обране з рівною ймовірністю з діапазону $[0, 2^N]$, де N – номер повторної спроби передачі даного кадру: 1,2,..., 10.

Після 10-ї спроби інтервал, з якого вибирається пауза, не збільшується. Таким чином, випадкова пауза може приймати значення від 0 до 52,4 мс.

Якщо 16 послідовних спроб передачі кадру викликають колізію, то передавач повинен припинити спроби і відкинути цей кадр.

Час подвійного обороту. Для надійного розпізнавання колізій повинно виконуватися наступне співвідношення:

$$T_{min} >= PDV, \qquad (2.1)$$

де T_{min} – час передачі кадру мінімальної довжини, а PDV – час, за який сигнал колізії встигає поширитися до самого далекого вузла мережі. Тому що в найгіршому випадку сигнал повинен пройти двічі між найбільш вилученими один від одного станціями мережі. Цей час називається *часом подвійного обороту (Path Delay Value, PDV)*.

При виконанні цієї умови передавальна станція повинна встигнути виявити колізію, яку викликав переданий нею кадр, ще до того, як вона закінчить передачу цього кадру.

Виконання цієї умови залежить, з одного боку, від довжини мінімального кадру і пропускної здатності мережі, а з іншого боку, від довжини кабельної системи мережі і швидкості поширення сигналу в кабелі (для різних типів кабелю ця швидкість трохи відрізняється).

Всі параметри протоколу Ethernet підібрані таким чином, щоб при нормальній роботі вузлів мережі колізії завжди чітко розпізнавалися. У стандарті Ethernet прийнято, що мінімальна довжина поля даних кадру становить 46 байтів (що разом зі службовими полями дає мінімальну довжину кадру 64 байта або 512 бітів, а разом із преамбулою – 72 байта або 576 бітів). Звідси можуть бути визначені обмеження на відстань між станціями.

У результаті врахування всіх факторів було ретельно підібране співвідношення між мінімальною довжиною кадру та максимально можливою відстанню між станціями мережі, що забезпечує надійне розпізнавання колізій. Цю відстань називають також *максимальним діаметром мережі*.

В табл. 2.1 наведені значення основних параметрів процедури передачі кадру стандарту 802.3, які не залежать від реалізації фізичного середовища. Важливо відзначити, що кожний варіант фізичного

середовища технології Ethernet додає до цих обмежень свої, часто більш суворі обмеження, які будуть розглянуті пізніше.

Таблиця 2.1

Параметри рівня MAC Ethernet

Параметри	Значення
Бітова швидкість	10 Мбіт/з
Інтервал відстрочки	512 бітових інтервала
Міжкадровий інтервал (IPG)	9,6 мкс
Максимальне число спроб передачі	16
Максимальне число зростання діапазону паузи	10
Довжина jam - послідовності	32 біта
Максимальна довжина кадру (без преамбули)	1518 байт
Мінімальна довжина кадру (без преамбули)	64 байт (512 біт)
Довжина преамбули	64 біт
Мінімальна довжина випадкової паузи після колізії	0 бітових інтервалів
Максимальна довжина випадкової паузи після колізії	524 000 бітових інтервалів
Максимальна відстань між станціями мережі	2500 м
Максимальне число станцій у мережі	1024

Максимальна продуктивність мережі Ethernet. На характеристики продуктивності мережі велике значення робить коефіцієнт використання мережі, що відбиває її завантаженість. При значеннях цього коефіцієнта понад 50% корисна пропускна здатність мережі різко падає: через ріст інтенсивності колізій, а також збільшення часу очікування доступу до середовища (рис.2.19).

Максимально можлива пропускна здатність сегмента Ethernet у кадрах за секунду досягається при передачі кадрів мінімальної довжини й становить 14 880 кадр/с.

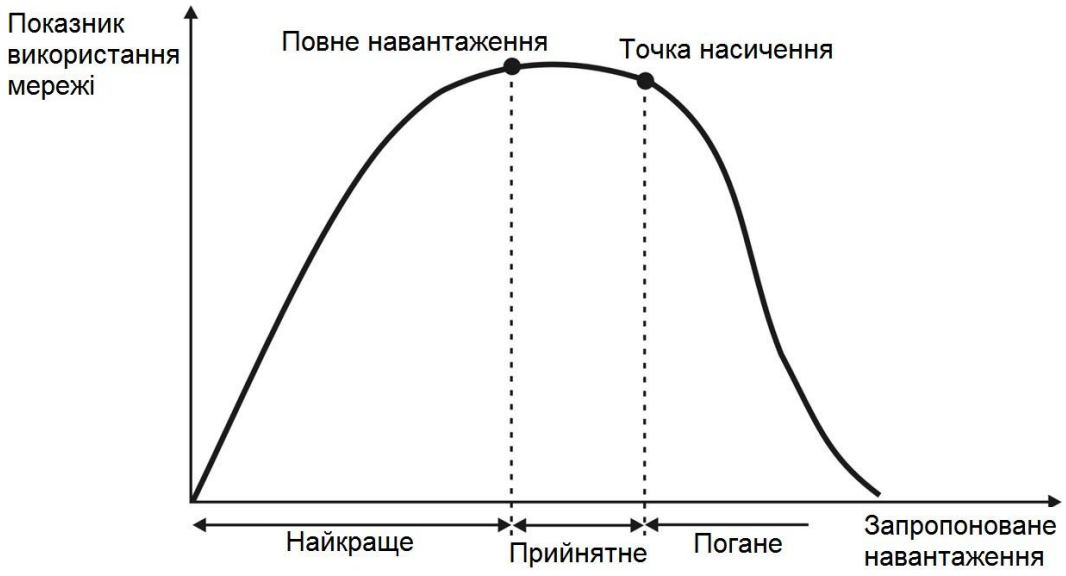


Рисунок 2.19 – Продуктивність мережі Ethernet

Під корисною пропускною здатністю протоколу розуміється швидкість передачі користувальницьких даних, які переносяться полем даних кадру. Ця пропускна здатність завжди менше номінальної бітової швидкості протоколу Ethernet за рахунок декількох факторів: службової інформації кадру; міжпакетних інтервалів (IPG); очікування доступу до середовища. При цьому корисна пропускна здатність мережі для кадрів мінімальної довжини становить усього 5,48 Мбіт/с, а максимально можлива корисна пропускна здатність мережі Ethernet становить 9,75 Мбіт/с, що відповідає використанню кадрів максимальною довжиною 1518 байтів, які передаються мережею зі швидкістю 513 кадр/с.

Наведемо приклад розрахунків максимальної швидкості передачі для технології FastEthernrt. Найменша надмірність – пакет максимальної довжини (1500 байт корисної інформації + 26 байт службової інформації + 96 біт IPG = 12304 біта);

Якщо немає колізій, то швидкість передачі пакетів (при швидкості мережі 100 Мбіт/с) складе: 108/12304 = 8127,44 пакета в секунду;

Пропускна здатність мережі (швидкість передачі корисної інформації) буде дорівнює: 8127,44 · 1500 байт = 12,2 Мбайт/с;

Ефективність використання швидкості мережі:

8127,44 · 12000 біт /108 = 98%.

2.2.1.3 Фізичний рівень технологій Ethernet

Фізичні специфікації технологій Ethernet на сьогоднішній день включають наступні стандартні сегменти.

Мережа Ethernet (10 Мбіт/с, IEEE 802.3, шина і пасивна зірка):

– 10BASE5 (товстий коаксіальний кабель) – до 500 м;
– 10BASE2 (тонкий коаксіальний кабель) – до 185 м;
– 10BASE-T (дві виті пари) – до 100 м;
– 10BASE-FL (оптоволоконний кабель) – до 2 км.

Стандарт 10Base-5. На рис.2.20 наведений приклад мережі 10Base-5. Мережа складається із трьох сегментів, з'єднаних повторювачами, що виконані на товстому коаксіальному кабелі (RG-8 і RG-11).

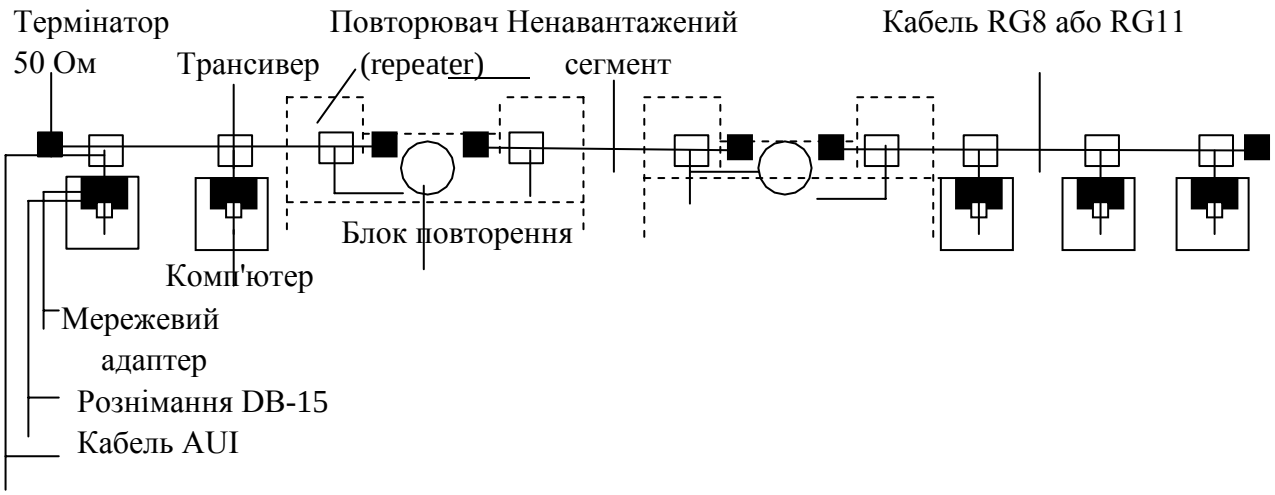


Рисунок 2.20 – Приклад мережі 10Base-5

При проектуванні мережі відповідно до стандарту 10Base-5 варто мати на увазі наступні особливості:

– сегмент кабелю максимальної довжини без повторювачів – 500 м, повинен мати на кінцях термінатори – "заглушки" опором 50 Ом, які запобігають відбиванню хвиль від кінців лінії та сприяють поглинанню сигналу на кінцях кабелю;

– станція підключається до кабелю за допомогою трансивера (приймач+передавач transmitter + receiver=transceiver), що встановлюється на кабелі та живиться від мережевого адаптера;

– трансивер з'єднується з адаптером інтерфейсним кабелем AUI довжиною до 50 м, що складається з 4 витих пар. Для приєднання до інтерфейсу AUI використовується рознімання DB-15.

Стандарт дозволяє використовувати в мережі не більше 4 повторювачів і 5 сегментів кабелю. При максимальній довжині сегмента кабелю в 500 м це дає максимальну довжину мережі 10Base-5 в 2500 м. Тільки 3 сегменти з 5 можуть бути навантаженими, тобто такими, до яких підключаються кінцеві вузли. Між навантаженими сегментами повинні бути ненавантажені сегменти. Правило застосування повторювачів у мережі Ethernet 10Base-5 зветься *"правило 5-4-3"*. Обмежене число повторювачів пояснюється додатковими затримками поширення сигналу, які вони вносять. Застосування повторювачів збільшує час подвійного поширення сигналу PDV. Кожний повторювач підключається до сегмента одним своїм трансивером, тому до навантажених сегментів можна підключити не більше 99 вузлів. Максимальне число кінцевих вузлів у мережі 10Base-5 таким чином, становить 99*3 = 297 вузлів.

До переваг стандарту 10Base-5 відносять: гарну захищеність кабелю від зовнішніх впливів; порівняно велику відстань між вузлами; можливість простого переміщення робочої станції в межах довжини кабелю AUI.

Недоліками 10Base-5 є: складність прокладення кабелю через значну твердість; потреба в спеціальному інструменті для закладення кабелю; вихід з ладу всієї мережі при ушкодженні кабелю або поганому з'єднанні; необхідність заздалегідь передбачити підводку кабелю до всіх можливих місць установки комп'ютерів.

Стандарт 10Base-2. При проектуванні мереж у відповідності зі стандартом 10Base-2 використовується кабель RG-58/U, RG-58 A/U. Максимальна довжина сегмента без повторювача – 185 м. Станції підключаються до кабелю за допомогою високочастотного (BNC) Т-коннектора, що являє собою трійник, один відвід якого з'єднується з мережевим адаптером, а два інших - із двома кінцями розриву кабелю (рис.2.21).

Максимальна кількість станцій підключених до одного сегмента - 30. Діє правило "5-4-3". Максимальна довжина мережі 5*185=925 м. Приклад мережі 10Base-2 представлений на рис 2.22.

Кабель RG-58/U має гіршу перешкодозахищеність та дешевше за товстий коаксіальний кабель. Має багато контактів і з'єднань, які нерідко порушуються, що приводить до непрацездатності мережі. Достоїнством кабелю є його гнучкість, зручність у монтажі, легкість нарощування.

Рисунок 2.21 – Вигляд BNC коннектора

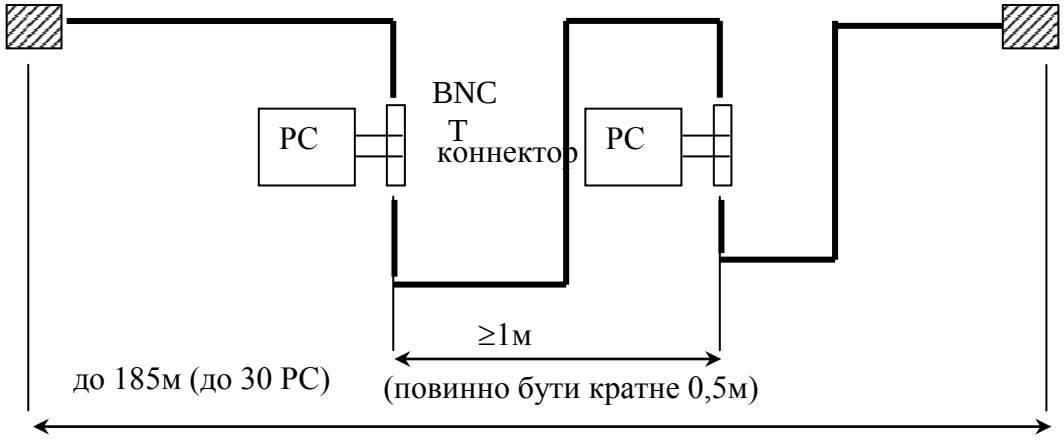


Рисунок 2.22 – Приклад мережі 10Base2

Загальним недоліком стандартів 10Base-5 і 10Base-2 є відсутність оперативної інформації про стан моноканала. Ушкодження кабелю виявляються відразу ж (мережа перестає працювати), але для пошуку відрізка кабелю, що відмовив, необхідний спеціальний прилад – кабельний тестер.

Стандарт 10Base-T. Стандарт був прийнятий в 1991 році. Мережі 10Base-T використовують в якості передавального середовища дві неекрановані виті пари UTP категорії 3. Кінцеві вузли з'єднуються за допомогою двох витих пар за топологією "точка-точка" зі спеціальним пристроєм – багатопортовим повторювачем (hub). Повторювач приймає сигнали від одного з кінцевих вузлів і синхронно передає їх на всі інші порти, крім того, з якого надійшли сигнали, тобто реалізує логічну загальну шину (рис.2.23).

Якщо одночасно надходять сигнали на декілька Rx входів, то повторювач розпізнає колізію та посилає jam-послідовність на всі свої Tx виходи. Максимальна відстань відрізка витої пари між двома зв'язаними вузлами і концентраторами повинно бути не більше 100 м.

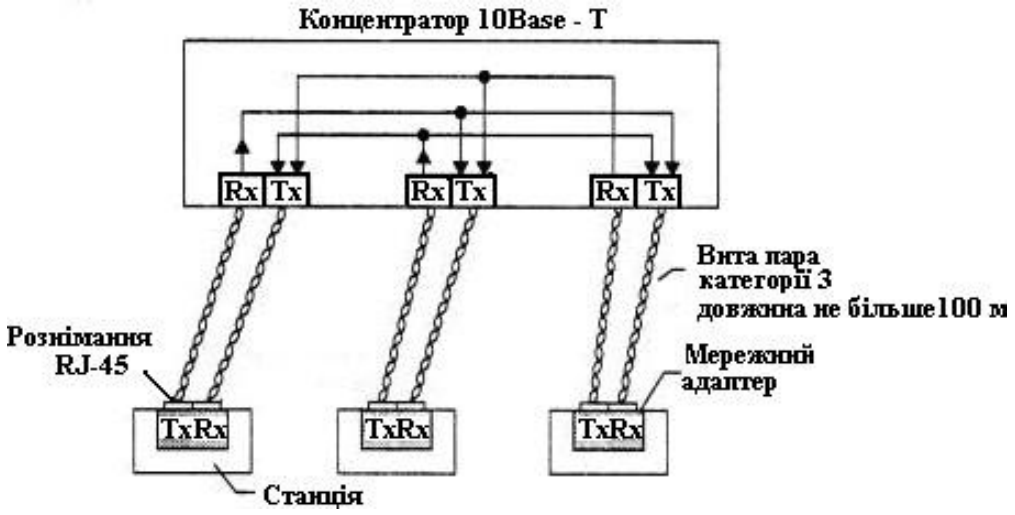


Рисунок 2.23 – Мережа стандарта 10Base-T: T_x - передавач; R_x - приймач

Для забезпечення синхронізації станцій при реалізації процедур доступу CSMA/CD і надійного розпізнавання станціями колізій у стандарті багатосегментне з'єднання здійснюється *за правилом 4-х hub(ів)*, що означає, що між будь-якими 2-ма станціями не повинно бути більше 4-х hub(ів) (рис.2.24).

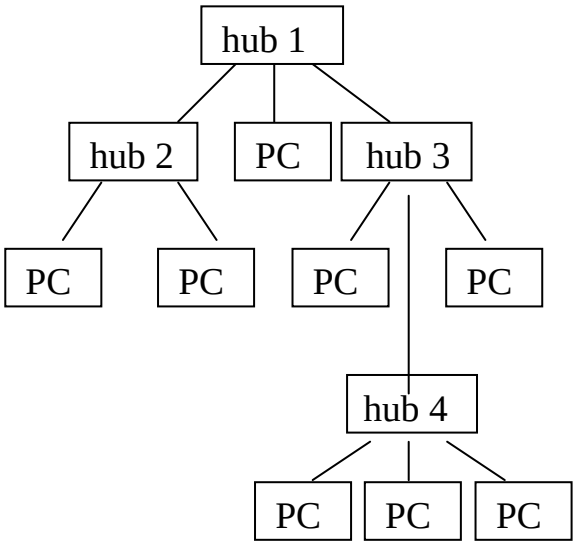


Рисунок 2.24 – Мережа стандарта 10Base-T. Деревоподібне з'єднання

Загальна кількість станцій не повинна перевищувати 1024. Для даного типу фізичного рівня ця кількість дійсно може бути досягнена. Для цього досить створити дворівневу ієрархію концентраторів, розташувавши

на нижньому рівні достатню кількість концентраторів із загальною кількістю портів 1024 (рис. 2.25). Кінцеві вузли потрібно підключити до портів концентраторів нижнього рівня. Правило 4-х хабів при цьому виконується – між будь-якими кінцевими вузлами буде рівно 3 концентратори. Відповідно до правила 4-х hub(ів) максимальний діаметр мережі дорівнює 5*100=500 м.

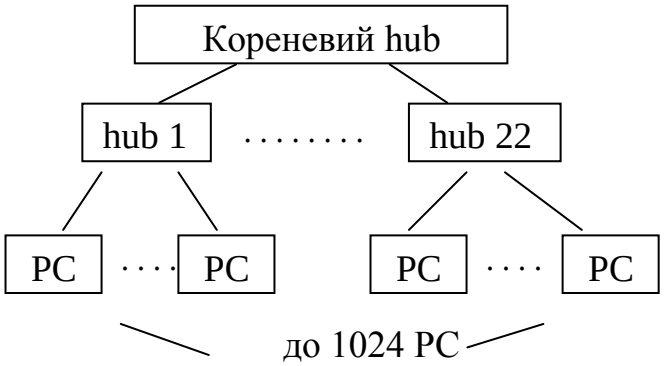


Рисунок 2.25 – Схема з максимальною кількістю станцій

Головною перевагою технології 10Base-T, у порівнянні зі складними в експлуатації коаксіальними мережами, є поява між кінцевими вузлами активного пристрою, що може контролювати роботу мережі та ізолювати некоректно працюючі робочі станції.

Специфікація 10 Base – F,FL,FB. В якості середовища передачі даних специфікація використовує оптичне волокно. Для одномодового оптичного волокна потрібно застосовувати спеціальний тип трансивера. Як і у випадку витої пари, для з'єднання адаптера з повторювачем використовують два оптоволокна – одне з'єднує вихід Tx адаптера із входом Rx повторювача, а інше – вхід Rx адаптера з виходом Tx повторювача (рис.2.26).

Стандарт *FOIRL (Fiber Optic Inter-Repeater Link)* гарантує довжину волоконно-оптичного зв'язку між повторювачами до 1 км при загальній довжині мережі не більше 2500 м.

В стандарті *10Base-FL* збільшена потужність передавачів, тому максимальна відстань між вузлом і концентратором доягає 2000 м. Максимальне число повторювачів між вузлами залишилося рівним 4, а максимальна довжина мережі – 2500 м.

Стандарт *10Base-FB* призначений тільки для з'єднання повторювачів. Кінцеві вузли не можуть використовувати цей стандарт для приєднання до портів концентратора. Між вузлами мережі можна встановити до 5 повторювачів 10Base-FB при максимальній довжині одного сегмента 2000м і максимальній довжині мережі 2740 м.

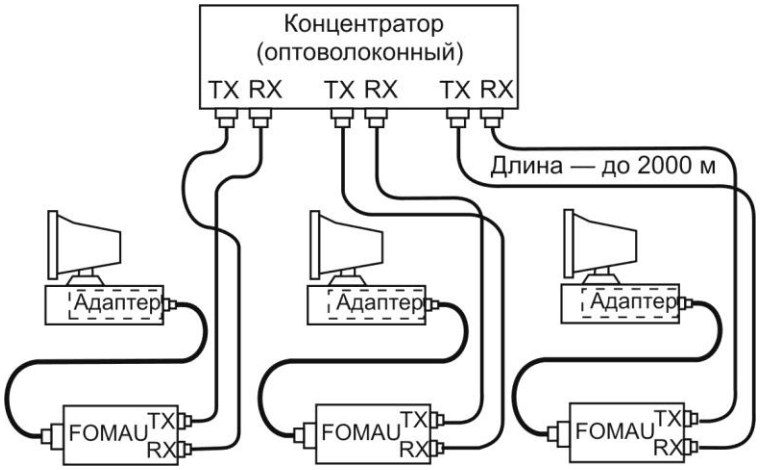


Рисунок 2.26 – Підключення сегментів 10Base-FL

Повторювачі, з'єднані за 10Base-FB, при відсутності кадрів для передачі постійно обмінюються спеціальними послідовностями сигналів, що відрізняються від сигналів кадрів даних, для підтримки синхронізації. Тому вони вносять менші затримки при передачі даних з одного сегмента в інший, і це є головною причиною, по якій кількість повторювачів удалося збільшити до 5. Як і в стандарті 10Base-T, волоконно-оптичні стандарти Ethernet дозволяють з'єднувати концентратори тільки в деревоподібні ієрархічні структури.

Таблиця 2.2

Загальні обмеження для всіх стандартів Ethernet

Номінальна пропускна здатність	10 Мбіт/с
Максимальне число станцій у мережі	1024
Максимальна відстань між вузлами мережі	2500 м (в 10Base-FB 2750м)
Максимальне число коаксіальних сегментів у мережі	5

Таблиця 2.3

Параметри специфікацій фізичного рівня для стандарту Ethernet

	10Base-5	10Base-2	10Base-T	10Base-F
Кабель	Товстий коаксіал RG-8, RG-11	Тонкий коаксіал RG-58	Неекранована вита пара категорій 3,4,5	Багато-модовий оптичний кабель
Максимальна довжина сегмента,м	500	185	100	2000
Максимальна відстань між вузлами мережі (при використанні повторювачів), м	2500	925	500	2500 (2740 для 10Base-FB)
Максимальне число станцій у сегменті	100	30	1024	1024
Максимальне число повторювачів між будь-якими PC	4	4	4	4 (5 для 10Base-FB)

Розрахунок конфігурації мережі Ethernet. Щоб мережа Ethernet, яка складається із сегментів різної фізичної природи, працювала коректно, необхідно виконання чотирьох основних умов:

- кількість станцій у мережі не більше 1024;
- максимальна довжина кожного фізичного сегмента не більше величини, що визначена відповідним стандартом фізичного рівня;
- час подвійного обороту сигналу (Path Delay Value, PDV) між двома самими далекими станціями мережі не більше 512 бітових інтервалів (bt). Загальну затримку складають: затримки в мережевих адаптерах, затримки в концентраторах, затримки в кабелях;
- скорочення міжпакетного інтервалу IPG (Path Variability Value, PVV) при проходженні послідовності кадрів через всі концентратори повинне бути не більше, ніж 49 бітових інтервалів (bt).

Дотримання цих вимог забезпечує коректність роботи мережі навіть у випадках, коли порушуються прості правила конфігурування, що визначають максимальну кількість повторювачів і загальну довжину мережі в 2500 м.

Обмеження на значення PDV і PVV повинні виконуватися для всіх доменів колізій мережі. *Домен колізій (Collision Domain)* – це частина мережі Ethernet, всі вузли якої конкурують за загальну середу передачі і, отже, кожен вузол якої може створити колізію з будь-яким іншим вузлом цієї частини мережі. Для поділу домену колізій застосовуються комутатори (рис.2.27).

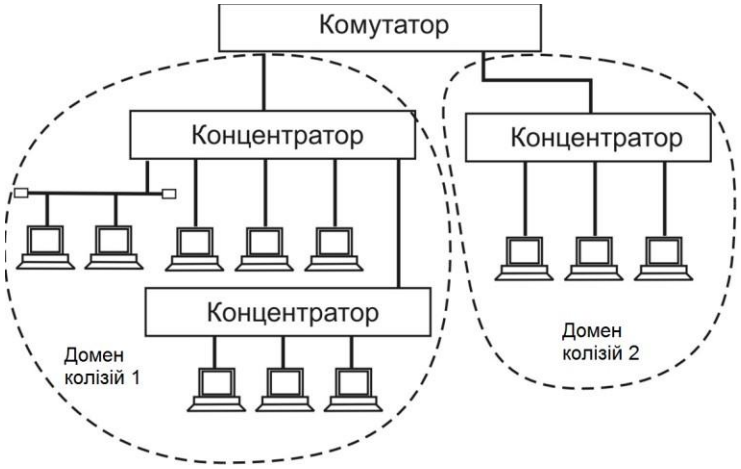


Рисунок 2.27 – Домени колізій

Розрахунок PDV виконують для максимального шляху проходження сигналу (рис.2.28). Внесок кожного джерела затримки обирають відповідно до даних, наведених на рис 2.29.

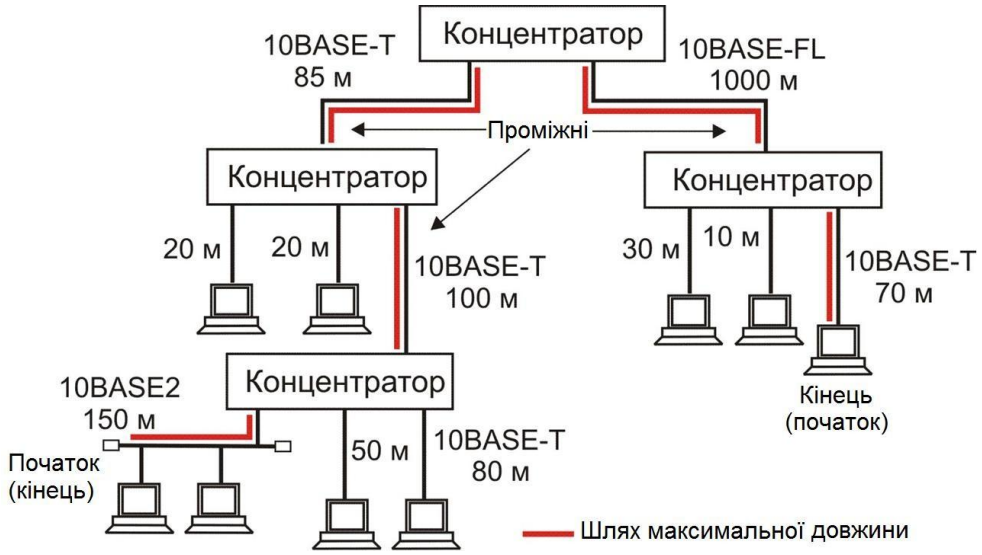


Рисунок 2.28 – Шлях максимальної довжини в мережі Ethernet

Тип сегменту	t_o поч. сегм.	t_o пром. сегм.	t_o кін. сегм.	t_l на метр
10BASE5	11,8	46,5	169,5	0,087
10BASE2	11,8	46,5	169,5	0,103
10BASE-T	15,3	42,0	165,0	0,113
10BASE-FL	12,3	33,5	156,5	0,100

$PDV = \Sigma\, PDV_S \le 512$ BT

$PDV_S = t_o + L \cdot t_l$, где L — довжина кабелю сегмента в метрах

Рисунок 2.29 – Розрахунок PDV

Початковим сегментом названий сегмент, з якого починається шлях сигналу від виходу передавача кінцевого вузла, кінчевим називається найбільш далекий сегмент мережі, у якому і виникає колізія, інші сегменти є проміжними. З кожним сегментом зв'язана затримка поширення сигналу уздовж кабелю сегмента, що залежить від довжини сегмента і обчислюється шляхом множення часу поширення сигналу за один метр кабелю (у бітових інтервалах) на довжину кабелю в метрах.

Початковий і кінцевий сегменти мають різні величини базової затримки, тому у випадку різних типів сегментів на самих далеких краях мережі необхідно виконати розрахунки двічі: один раз прийняти у якості початкового сегменту один тип, а в другий — сегмент іншого типу. Результатом можна вважати максимальне значення PDV.

При розрахунку зменшення міжкадрового інтервалу концентраторами аналізують тільки початковий і проміжні сегменти. Значення IPG не повинне перевищувати 49 bt (рис.2.30).

Сегмент	Початковий	Проміжний
10BASE2	16	11
10BASE5	16	11
10BASE-T	16	11
10BASE-FL	11	8

Скорочення IPG:

$\Delta IPG = \Sigma\, \Delta IPG_S \le 49$ BT

Рисунок 2.30 – Розрахунок IPG

2.2.1.4 Фізичний рівень технології Fast Ethernet

Стандарт Fast Ethernet IEEE 802.3u з'явився значно пізніше стандарту Ethernet – в 1995 році. Його розробка була пов'язана з вимогами підвищення швидкості передачі інформації.

Якщо порівнювати набір стандартних сегментів Ethernet і Fast Ethernet, то головна відмінність – відсутність в Fast Ethernet шинних сегментів і коаксіального кабелю. Залишилися лише сегменти на витій парі і оптичному кабелі. Технологія Fast Ethernet при роботі на витої парі дозволяє за рахунок процедури автопереговорів двом портам вибирати найбільш ефективний режим роботи – швидкість 10 Мбіт/с або 100 Мбіт/с, а також напівдуплексний або повнодуплексний режим.

Фізичні специфікації технології Fast Ethernet включають середовища передачі даних наведені у табл. 2.4.

Таблиця 2.4

Характеристики фізичних специфікацій технології Fast Ethernet

Параметр	100BASE-TX	100BASE-T4	100BASE-FX
Кабель	UTP кат.5	UTP кат. 3 або 5	Оптичний
Кіл-ть ВП	2	4	–
Довжина	100 м (90 м)	100 м (90 м)	412 м
Код	4B/5B + MLT-3	8B/6T	4B/5B + NRZI
Топологія	Пасивна зірка	Пасивна зірка	Пасивна зірка

Стандарт 100 Base-TX – мережа з топологією пасивна зірка з концентратором в центрі. Використовується вита пара (UTP) категорії 5 або вище, що пов'язане з необхідною пропускною здатністю кабелю. Для приєднання кабелю використовуються 8-контактні рознімання типу RJ-45. Довжина кабелю не може перевищувати 100 метрів (стандарт рекомендує 90 метрів для 10-відсоткового запасу). Стандарт передбачає також можливість використання екранованого кабелю з двома витими парами проводів (хвильовий опір – 150 Ом). В цьому випадку використовується 9-контактне екрановане рознімання DB-9. На сьогоднішній день 100 Base-TX самий популярний тип мережі Fast Ethernet.

Стандарт 100 Base-T4 – передача здійснюється не двома, а чотирма неекранованими витими парами (UTP). При цьому кабель може бути менш якісним (категорії 3, 4 або 5). Прийнята в 100BASE-T4 система кодування сигналів забезпечує ту ж саму швидкість 100 Мбіт/с на любому з цих кабелів, але стандарт рекомендує все ж використовувати кабель категорії 5. Обмін даними іде по одній передавальній витой парі, по одній приймальній витой парі і по двом двонаправленим витим парам з використанням трьохрівневих диференціальних сигналів.

Стандарт 100 Base-FX – використовується топологія пасивна зірка з підключенням комп'ютерів до концентратору за допомогою двох різнонаправлених оптичних кабелів. Кабелі підключаються до адаптера (трансивера) і до концентратора за допомогою рознімань типу SC, ST бо FDDI. Максимальна довжина кабелю між комп'ютером і концентратором - 412 метрів (це обмеження визначається не якістю кабелю, а встановленими часовими співвідношеннями). Згідно стандарту, застосовується мультимодовий або одномодовий кабель з довжиною хвилі світла 1,35 мкм. В останньому випадку втрати потужності сигналу в сегменті (в кабелі и розніманнях) не повинні перевищувати 11 дБ.

Розрахунок конфігурації мережі Fast Ethernet. Для визначення працездатності мережі Fast Ethernet стандарт IEEE 802.3 пропонує дві моделі, які називаються *Transmission System Model 1* і *Transmission System Model 2*. Перша модель заснована на кількох нескладних правилах. Вона виходить з того, що всі компоненти мережі (зокрема, кабелі) мають найгірші з можливих часових характеристик, тому завжди дає результат зі значним запасом. Друга модель використовує систему точних розрахунків з реальними часовими характеристиками кабелів. У зв'язку з цим її застосування дозволяє іноді подолати жорсткі обмеження моделі 1.

Розрахунок за моделлю 1. Правила моделі 1:

– сегменти, які виконані на електричних кабелях (витих парах) не повинні бути довше 100 метрів. Це відноситься до кабелів усіх категорій – 3, 4 і 5, до сегментів 100BASE-T4 і 100BASE-TX;

– сегменти, які виконані на оптичних кабелях, не повинні бути довше 412 метрів;

– якщо використовуються адаптери з зовнішніми (виносними) трансиверами, то трансиверні кабелі (MII) не повинні бути довше 50 сантиметрів.

Модель 1 виділяє три можливі конфігурації мережі Fast Ethernet:

1) З'єднання двох абонентів (вузлів) мережі безпосередньо, без репітера або концентратора. Абонентами при цьому можуть виступати не

тільки комп'ютери, але і мережевий принтер, порт комутатора, моста чи маршрутизатора. Таке поєднання називається з'єднанням DTE-DTE або двоточковим.

Правила моделі 1 для даного випадку прості: електричний кабель не повинен бути довше 100 метрів, напівдуплексний оптоволоконний – не більше 412 метрів, повнодуплексний оптоволоконний – 2000 метрів (при цьому затримка сигналу в кабелі не має значення, так як метод CSMA/CD не працює).

2) З'єднання двох абонентів мережі за допомогою одного репітерного концентратора класу I чи класу II (рис.2.31).

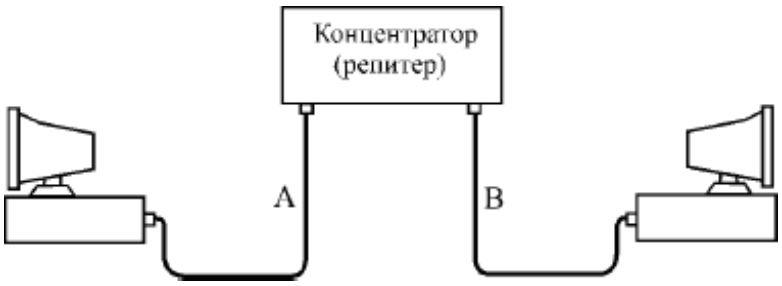


Рисунок 2.31 – З'єднання двох абонентів мережі за допомогою одного концентратора

В даному випадку треба обмежувати довжину кабелів А і В мережі відповідно до табл. 2.5.

Таблиця 2.5

Максимальна довжина кабелів у конфігурації з одним концентратором

Вид кабелю А	Вид кабелю В	Клас концентра-тора	Макс. довжина кабелю А, м	Макс. довжина кабелю В, м	Макс. розмір мережі, м
TX, T4	TX, T4	I или II	100	100	200
TX	FX	I	100	160,8	260,8
T4	FX	I	100	131	231
FX	FX	I	136	136	272
TX	FX	II	100	208,8	308,8
T4	FX	II	100	204	304
FX	FX	II	160	160	320

3) З'єднання двох абонентів мережі за допомогою двох репітерних концентраторів класу II (рис.2.32). При цьому передбачається, що для зв'язку концентраторів завжди використовується електричний кабель довжиною не більше 5 метрів.

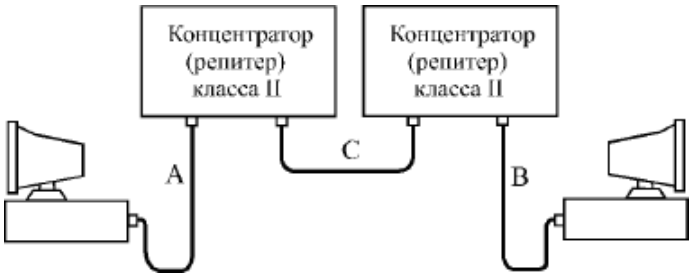


Рисунок 2.32 – З'єднання двох абонентів мережі за допомогою двох концентраторів

Концентратори класу II мають меншу затримку, тому їх може бути два. Використання трьох концентраторів відповідно до моделі 1 не допускається. В даному випадку треба обмежувати довжину кабелів A і B відповідно до таблиці. При цьому за умовчанням передбачається, що кабель C має довжину 5 метрів.

Таблиця 2.6

Максимальна довжина кабелів у конфігурації з двома концентраторами[2]

Вид кабелю A	Вид кабелю B	Макс. довжина кабелю A, м	Макс. довжина кабелю B, м	Макс. розмір мережі, м
TX, T4	TX, T4	100	100	205
TX	FX	100	116,2	221,2
T4	FX	136,3	136,3	241,3
FX	FX	114	114	233

В обох конфігураціях з концентраторами при використанні одночасно електричного і оптоволоконного кабелів можна за рахунок зменшення довжини електричного кабелю збільшити довжину оптоволоконного. Причому зменшення довжини електричного кабелю на 1 метр відповідає

[2] У всіх перерахованих випадках під розміром мережі розуміється розмір зони конфлікту (області колізії, collision domain).

збільшення довжини оптоволоконного кабелю на 1,19 метра. Наприклад, зменшивши кабель TX на 10 метрів, можна збільшити кабель FX на 11,9 метра, і його гранична довжина складе при двох концентраторах 128,1 метра.

У разі використання двох оптоволоконних кабелів можна зменшувати один з кабелів за рахунок збільшення іншого. При зменшенні одного кабелю на 10 метрів можна збільшити другий теж на 10 метрів. Якщо ж використовується два електричні кабелі, то збільшувати один з них за рахунок зменшення іншого не можна, так як їх довжина в принципі не може перевищувати 100 метрів через загасання сигналу в кабелі.

Розрахунок за моделлю 2. Друга модель для мережі Fast Ethernet, як і у випадку Ethernet, заснована на обчисленні сумарного подвійного часу проходження сигналу по мережі. Проводити розрахунки величини скорочення межпакетного інтервалу (IPG) не треба. Це пов'язано з тим, що навіть максимальна кількість репітерів і концентраторів, допустимих у Fast Ethernet (два), не може викликати неприпустимого скорочення межпакетного інтервалу.

Для розрахунків відповідно до другої моделі спочатку треба виділити шлях максимальної довжини. Якщо таких шляхів кілька, то розрахунок повинен проводитися для кожного з них. Розрахунок ведеться на підставі табл.. 2.7.

Таблиця 2.7

Подвійні затримки компонентів мережі Fast Ethernet (величини затримок надані в бітових інтервалах)

Тип сегменту	Затримка на метр	Макс. затримка
Два абонента TX/FX	-	100
Два абонента T4	-	138
Один абонент T4 і один TX/FX	-	127
Сегмент на кабелі категорії 3	1,14	114 (100 м)
Сегмент на кабелі категорії 4	1,14	114 (100 м)
Сегмент на кабелі категорії 5	1,112	111,2 (100 м)
Екранована вита пара	1,112	111,2 (100 м)
Оптичний кабель	1,0	412 (412 м)
Репітер (концентратор) класу I	-	140
Репітер (концентратор) класу II з портами TX/FX	-	92
Репітер (концентратор) класу II з портами T4	-	67

Для обчислення повного подвійного (кругового) часу проходження для сегмента мережі необхідно помножити довжину сегмента на величину затримки на метр, взяту з другого стовпця таблиці. Якщо сегмент має максимальну довжину, то можна відразу взяти величину максимальної затримки для даного сегмента з третього стовпця таблиці.

Потім затримки сегментів, що входять в шлях максимальної довжини, треба підсумувати і додати до цієї суми величину затримки для прийомопередавальних вузлів двох абонентів (це три верхні рядки таблиці) і величини затримок для всіх репітерів (концентраторів), що входять в даний шлях (це три нижні рядки табл. 2.7).

Сумарна затримка повинна бути менше, ніж 512 бітових інтервалів. При цьому треба пам'ятати, що стандарт IEEE 802.3u рекомендує залишати запас в межах 1 - 4 бітових інтервалів для урахування кабелів всередині з'єднувальних шаф і похибок вимірювання. Краще порівнювати сумарну затримку з величиною 508 бітових інтервалів, а не 512 бітових інтервалів.

2.2.1.5 Технологія Token Ring

Наведемо характеристики стандарту IEEE 802.5 (мережа Token Ring).

- Топологія – кільце (зірка-кільце);
- Середовище передачі – вита пара UTP;
- Швидкість передачі – 4 (16) Мбіт/с;
- Довжина кабелю між концентраторами – до 45 м;
- Довжина кабелю від абонента до концентратора – до 45 м;
- Максимальна довжина кільця – 120 м;
- Максимальна кількість абонентів – 96 (12 MAU);
- Метод доступу – маркерний;
- Код – біфазної.

Мережі Token Ring будуються на основі кільцевої топології (рис.2.33) за допомогою концентраторів *MAU (Multistation Access Unit)* і використовують *маркерний метод доступу*, що гарантує кожної станції одержання доступу до поділюваного кільця протягом часу обороту кадра спеціального формату, який називається маркером або *токеном (token)*. Мережі Token Ring працюють на двох швидкостях: 4 і 16 Мбіт/с.

Маркерний метод доступу. Для забезпечення доступу станцій до фізичного середовища по кільцю циркулює кадр спеціального формату і призначення – *маркер*. Станція, яка одержала маркер, аналізує його і при відсутності у неї даних для передачі забезпечує його просування до наступної станції. Станція, що має дані для передачі, при одержанні

маркера вилучає його з кільця, що дає їй право доступу до фізичного середовища і передачі своїх даних.

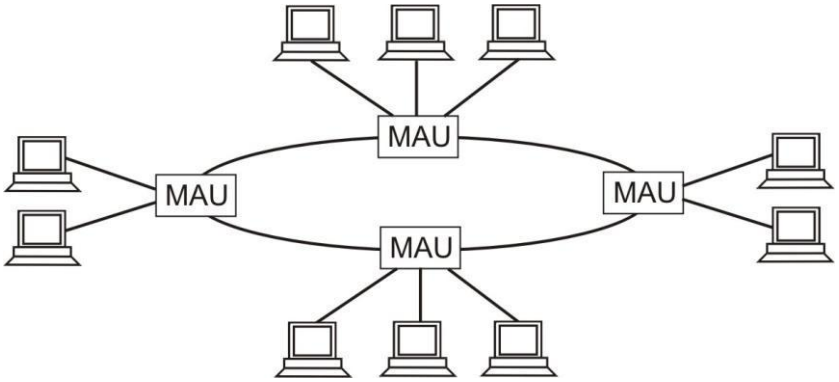


Рисунок 2.33 – Зірково-кільцева топологія мережі Token Ring

Всі станції кільця ретранслюють кадр побітно, як повторювачі. Якщо кадр проходить через станцію призначення, то, розпізнавши свою адресу, вона копіює кадр у свій внутрішній буфер і вставляє в кадр ознаку підтвердження прийому. Станція, що передала кадр даних у кільце, при зворотному його одержанні з підтвердженням прийому вилучає цей кадр із кільця і передає в мережу новий маркер для забезпечення можливості іншим станціям мережі передавати дані. Такий алгоритм доступу застосовується в мережах Token Ring зі швидкістю роботи 4 Мбіт/с.

Час володіння поділюваним середовищем у мережі Token Ring обмежується *часом утримання маркера*, після витікання якого станція зобов'язана припинити передачу власних даних (поточний кадр дозволяється завершити) і передати маркер далі по кільцю. Станція може встигнути передати за час утримання маркера один або декілька кадрів залежно від розміру кадрів і величини часу утримання маркера. Звичайний час утримання маркера за замовчуванням дорівнює 10 мс, а максимальний розмір кадру для мереж 4 Мбіт/с звичайно дорівнює 4 Кбайт, а для мереж 16 Мбіт/с – 16 Кбайт. Це пов'язане з тим, що за час утримання маркера станція повинна встигнути передати хоча б один кадр. При швидкості 4Мбіт/с за час 10 мс можна передати 5000 байт, а при швидкості 16 Мбіт/с – відповідно 20 000 байт. Максимальні розміри кадру обрані з деяким запасом.

Збільшення швидкості передачі даних до 16 Мбіт/с стало можливим за рахунок використання *алгоритму раннього вивільнення маркера*. Маркер передається відразу ж, як тільки станція закінчила передачу одного

або декількох кадрів за час утримання маркера, не чекаючи повернення по кільцю цього кадру з бітом підтвердження прийому. У цьому випадку пропускна здатність кільця використовується більш ефективно, тому що по кільцю одночасно просуваються кадри декількох станцій.

Для контролю за мережею одна зі станцій у кільці виконує роль *активного монітора*, що контролює наявність маркера, а також час обороту маркера і кадрів даних. Якщо активний монітор не одержує маркер протягом тривалого часу (наприклад, 2,6 с), то він породжує новий маркер.

Активний монітор вибирається під час ініціалізації кільця як станція з максимальним значенням MAC-адреси. Якщо активний монітор виходить із ладу, вибирається новий активний монітор. Щоб мережа могла виявити відмову активного монітора, останній у працездатному стані кожні 3 секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється в мережі більше 7 секунд, то інші станції мережі починають процедуру вибору нового активного монітора.

Формат кадрів Token Ring. В Token Ring існують різні формати кадрів: маркер і кадр даних (рис.2.34).

Рисунок 2.34 – Формати маркера і пакета Token Ring

Кадр маркера складається із трьох полів, кожне довжиною в один байт.

– *початковий обмежувач (Start Delimiter, SD)* з'являється на початку маркера, а також на початку будь-якого кадру, що проходить по мережі.

– *керування доступом (Access Control)* складається із чотирьох підполей: PPP, T, M и RRR, де PPP – біти пріоритету, T – біт маркера, M – біт монітора, RRR – резервні біти пріоритету. Біт T, установлений в 1, указує що даний кадр є маркером доступу. Біт монітора встановлюється в 1 активним монітором і в 0 будь-якою іншою станцією, що передає маркер або кадр. Якщо активний монітор бачить маркер або кадр, що містить біт монітора зі значенням 1, то активний монітор знає, що цей кадр або маркер уже один раз обійшов кільце і не був оброблений станціями. Якщо це кадр, то він вилучається з кільця. Якщо це маркер, то активний монітор передає його далі по кільцю.

– *кінцевий обмежувач (End Delimeter, ED)* – останнє поле маркера. Це поле містить дві однобітових ознаки: I та E. Ознака I (Intermediate) показує, чи є кадр останнім у серії кадрів (I=0) або проміжним (I=1). Ознака E (Error) – це ознака помилки. Вона установлюється в 0 станцією-відправником, і будь-яка станція кільця, через яку проходить кадр, повинна встановити цю ознаку в 1, якщо вона виявить помилку у контрольній сумі кадру.

Кадр даних може переносити або службові дані для керування кільцем (дані MAC-рівня), або користувальницькі дані (LLC-рівня). Тип кадру (MAC або LLC) визначає поле керування пакетом (Frame Control, FC). Стандарт Token Ring має 6 типів керуючих кадрів MAC-рівня, призначення яких описано нижче.

1) *Тест дублювання адреси (Duplicate Address Test, DAT)* посилає станція, коли вперше приєднується до кільця, щоб упевнитися, що її адреса унікальна.

2) *Існує активний монітор (Active Monitor Present, AMP)* періодично посилає в кільце активний монітор, щоб повідомити іншим станціям, що він працездатний.

3) *Існує резервний монітор* (Standby Monitor Present, SMP) відправляється будь-якою станцією, що не є активним монітором.

4) *Маркер заявки (Claim Token, CT)* відправляє резервний монітор, коли підозрює, що активний монітор відмовив.

5) *Сигнал (Beacon, BCN)* відправляє станція у випадку виникнення серйозних мережевих проблем, таких як обрив кабелю, виявлення станції, що передає кадри без очікування маркера, вихід станції з ладу. Визначаючи, яка станція відправляє кадр сигналу, можна локалізувати проблему.

6) *Очищення (Purge, PRG)* використовується новим активним монітором для того, щоб перевести всі станції у вихідний стан і очистити кільце від усіх раніше посланих кадрів.

Поле *стану пакета (Frame Status, FS)* містить 4 резервних біти і 2 поля: біт розпізнавання адреси A и біт копіювання кадру C. Поле статусу FS має вигляд ACXXACXX. Біти дублюються для надійності. Якщо біт розпізнавання адреси не встановлений під час одержання кадру, це означає, що станція призначення більше не присутня у мережі (можливо, внаслідок неполадок). Якщо обидва біти впізнавання адреси та копіювання кадру встановлені і біт виявлення помилки також встановлений, то вихідна станція знає, що помилка трапилася після того, як цей кадр був коректно отриманий.

Фізичний рівень технології Token Ring. У мережі Token Ring станції в кільце поєднуються за допомогою концентраторів MAU (Multistation Access Unit) або MSAU (Multi-Station Access Unit) (рис.2.35).

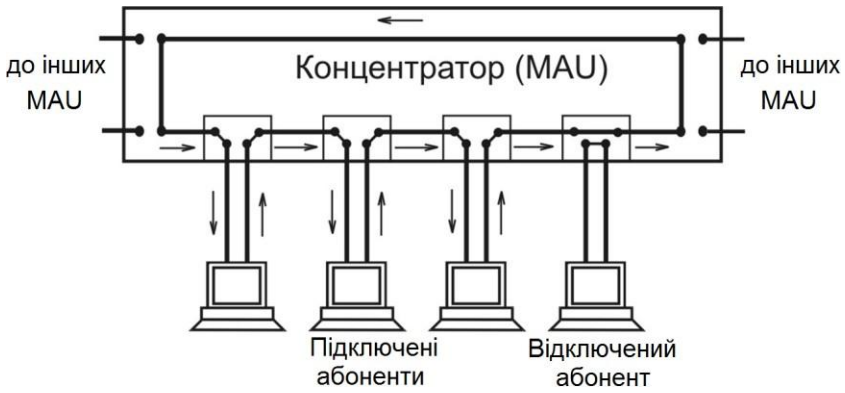


Рисунок 2.35 – Структура концентратора MAU

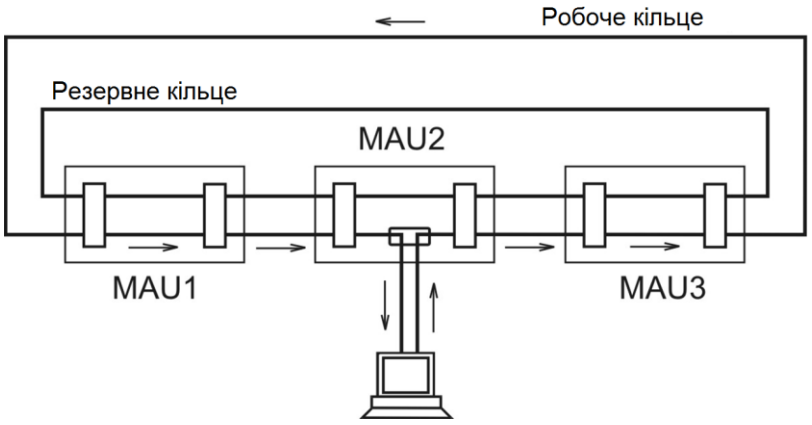


Рисунок 2.36 – Об’єднання концентраторов MAU

Концентратор Token Ring може бути активним або пасивним. Пасивний концентратор просто з'єднує порти внутрішніми зв'язками так, щоб станції утворили кільце, і забезпечує обхід якого-небудь порту, коли приєднаний до цього порту комп'ютер виключають. Звичайно обхід порту виконується за рахунок релейних схем, які живлються постійним струмом від мережевого адаптера, а при вимиканні мережевого адаптера нормально замкнуті контакти реле з'єднують вхід порту з його виходом (рис.2.37). Активний концентратор відрізняється від пасивного тим, що виконує ще й функції регенерації сигналів.

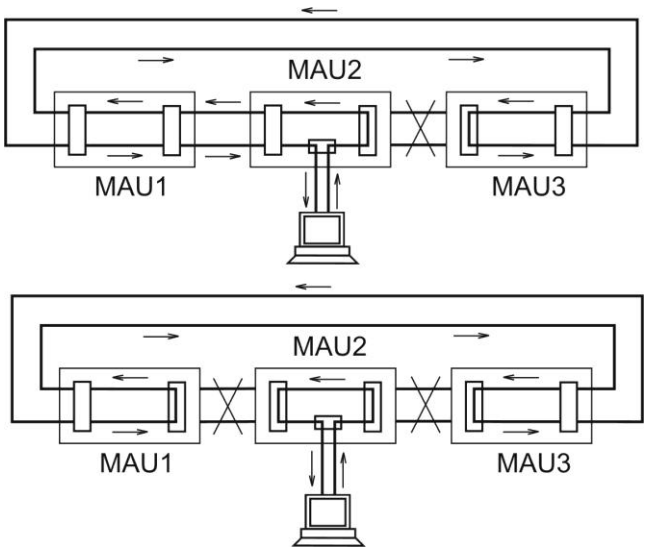


Рисунок 2.36 – Згортання і розпад кільця Token Ring

При використанні пасивного концентратора роль підсилювача сигналів бере на себе кожний мережевий адаптер, а роль ресинхронізуючого блоку виконує мережевий адаптер активного монітора. Кожний мережевий адаптер Token Ring має блок повторення, що вміє регенерувати та ресинхронізувати сигнали. Блок ресинхронізації складається з 30-бітного буфера, що приймає манчестерський код з трохи викривленими за час обороту по кільцю інтервалами проходження. Активний монітор "вставляє" свій буфер у кільце та синхронізує бітові сигнали, видаючи їх на вихід з необхідною частотою.

У загальному випадку мережа Token Ring має комбіновану зірково-кільцеву конфігурацію. Кінцеві вузли підключаються до MSAU по топології зірки, а самі MSAU поєднуються через спеціальні порти Ring In (RI) і Ring Out (RO) для утворення магістрального фізичного кільця.

Технологія Token Ring дозволяє використовувати для з'єднання кінцевих станцій і концентраторів різні типи кабелю: STP Type I, UTP Type 3, UTP Type 6, а також волоконно-оптичний кабель.

При використанні екранованої витої пари STP Type 1 у кільце допускається поєднувати до 260 станцій, а при використанні неекранованої витої пари максимальна кількість станцій скорочується до 72. Максимальна відстань від станції до MSAU та між пасивними MSAU – 100 м для STP і 45 м для UTP. Між активними MSAU максимальна відстань збільшується відповідно до 730 м або 365 м залежно від типу кабелю. Максимальна довжина кільця – 4 км.

Існує варіант технології Token Ring, названий High-Speed Token Ring, HSTR з бітовими швидкостями в 100 і 155 Мбіт/с, який підтримує основні особливості технології Token Ring 16 Мбіт/с.

2.2.1.6 Технологія FDDI

Характеристики мережі FDDI (стандарт ISO 9314):

– Топологія – кільце (зірка-кільце);

– Середовище передачі – оптоволоконний кабель, вита пара (TPDDI);

– Швидкість передачі – 100 Мбіт/с (200 Мбіт/с);

– Довжина кабелю між абонентами (станціями) – до 2 км;

– Максимальна довжина мережі – 20 км;

– Максимальна кількість абонентів – 1024;

– Метод доступу – маркерний (множинна передача маркера);

– Код – 4B/5B.

Для технології FDDI характерні кільцева топологія і маркерний метод доступу. Мережа будується на основі двох кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі (рис.2.37). У нормальному режимі роботи мережі дані проходять через всі вузли і всі ділянки кабелю тільки первинного (Primary) кільця, цей режим називається режимом Thru – "транзитним". Вторинне кільце (Secondary) у цьому режимі не використовується. У випадку якої-небудь відмови, коли частина первинного кільця не може передавати дані (наприклад, обрив кабелю або відмова вузла), первинне кільце поєднується із вторинним в єдине кільце. Цей режим роботи мережі називається Wrap, тобто "згортання" кілець. Операція згортання виробляється засобами концентраторів і/або

мережевих адаптерів FDDI. Для спрощення цієї процедури дані по первинному кільцю завжди передаються в одному напрямку, а по вторинному - у зворотному. Тому при утворенні загального кільця із двох кілець передавачі станцій як і раніше залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати й приймати інформацію сусідніми станціями.

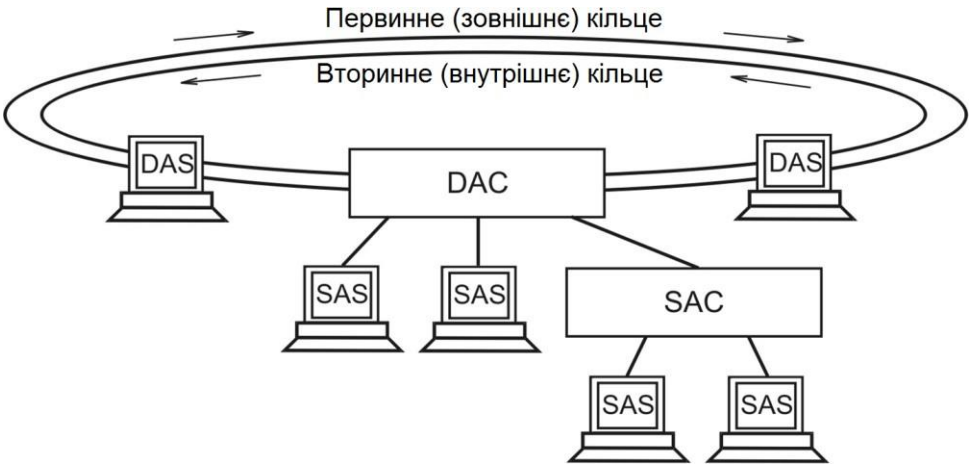


Рисунок 2.37 – Топологія FDDI

Мережа FDDI може повністю відновлювати свою працездатність у випадку одиничних відмов її елементів. При багаточисельних відмовах мережа розпадається на декілька не зв'язаних мереж.

Формат пакету технології FDDI схожий з форматом пакета Token Ring. Дані можуть займати від 0 до 4478 байт.

Особливості методу доступу FDDI. Метод доступу FDDI дуже близький до методу доступу мереж Token Ring. Відмінності полягають у тому, що час утримання маркера в мережі FDDI не є постійною величиною, як у мережі Token Ring. Цей час залежить від завантаження кільця – при невеликому завантаженні воно збільшується, а при більших перевантаженнях може зменшуватися до нуля. Ці зміни в методі доступу стосуються тільки асинхронного трафіка, який не критичний до невеликих затримок передачі кадрів.

Для передачі синхронних кадрів станція завжди має право захопити маркер при його надходженні. При цьому час утримання маркера має заздалегідь задану фіксовану величину.

Якщо ж станції кільця FDDI потрібно передати асинхронний кадр (тип кадру визначається протоколами верхніх рівнів), то для з'ясування

можливості захоплення маркера при його черговому надходженні станція повинна виміряти інтервал часу, що пройшов з моменту попереднього приходу маркера. Цей інтервал називається *часом обороту маркера (Token Rotation Time, TRT)*. Інтервал TRT порівнюється з іншою величиною – максимально припустимим часом обороту маркера по кільцю T_0p. У технології FDDI станції домовляються про величину T_0pr під час ініціалізації кільця. Кожна станція може запропонувати своє значення T_0pr, у результаті для кільця встановлюється мінімальне із запропонованих станціями часів. Це дозволяє враховувати потреби додатків, що працюють на станціях. Звичайно синхронним додаткам (додаткам реального часу) потрібно частіше передавати дані в мережу невеликими порціями, а асинхронним додаткам краще одержувати доступ до мережі рідше, але більшими порціями. Перевага віддається станціям, що передають синхронний трафік.

Таким чином, при черговому надходженні маркера для передачі асинхронного кадру порівнюється фактичний час обороту маркера TRT з максимально можливим T_0p. Якщо кільце не перевантажене, то маркер приходить раніше, ніж минає інтервал T_0pr, тобто TRT < T_0p. У цьому випадку станції дозволяється захопити маркер і передати свій кадр (або кадри) у кільце. Час утримання маркера THT дорівнює різниці T_0pr - TRT, і протягом цього часу станція передає в кільце стільки асинхронних кадрів, скільки встигне.

Якщо ж кільце перевантажене і маркер спізнився, то інтервал TRT буде більше T_0p. У цьому випадку станція не має права захопити маркер для асинхронного кадру. Якщо всі станції в мережі хочуть передавати тільки асинхронні кадри, а маркер зробив оборот по кільцю занадто повільно, то всі станції пропускають маркер у режимі повторення, маркер швидко робить черговий оборот і на наступному циклі роботи станції вже мають право захопити маркер і передати свої кадри.

Фізичний рівень технології FDDI. У стандарті FDDI допускаються два види приєднання станцій до мережі. Одночасне підключення до первинного та вторинного кілець називається подвійним підключенням – Dual Attachment, DA. Підключення тільки до первинного кільця називається одиночним підключенням – Single Attachment, SA.

Для станцій і концентраторів допустимо будь-який вид підключення до мережі – як одиночний, так і подвійний (рис.2.38). Пристрої мають відповідні назви: SAS (Single Attachment Station), DAS (Dual Attachment

Station), SAC (Single Attachment Concentrator) і DAC (Dual Attachment Concentrator).

Рознімання пристроїв маркуються. Рознімання типу A и B повинні бути у пристроїв з подвійним підключенням, рознімання M (Master) є в концентратора для одиночного підключення станції, у якої відповідне рознімання повиненне мати тип S (Slave).

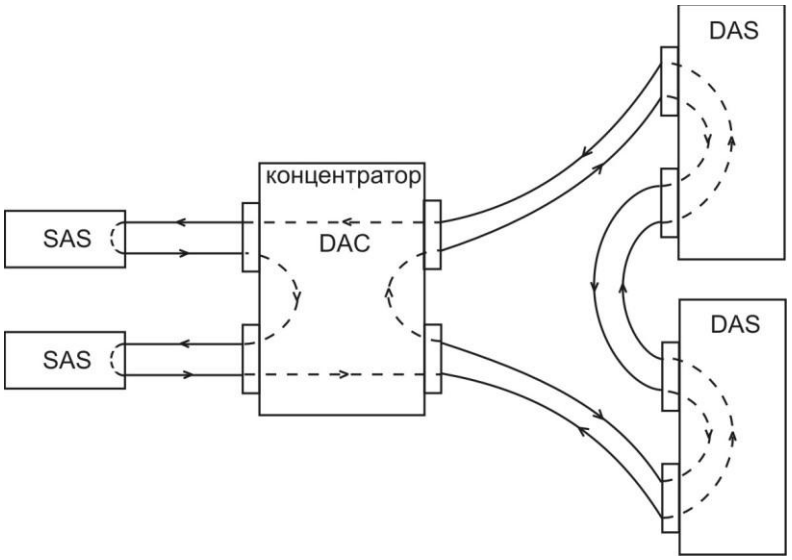


Рисунок 2.38 – Підключення вузлів до кілець FDDI

У випадку однократного обриву кабелю між пристроями з подвійним підключенням мережа FDDI зможе продовжити нормальну роботу за рахунок автоматичної реконфігурації внутрішніх шляхів передачі кадрів між портами концентратора (рис. 2.39). Дворазовий обрив кабелю приведе до утворення двох ізольованих мереж FDDI. При обриві кабелю, що йде до станції з одиночним підключенням, вона стає відрізаної від мережі, а кільце продовжує працювати за рахунок реконфігурації внутрішнього шляху в концентраторі – порт M, до якого була підключена дана станція, буде виключений із загального шляху.

Для збереження працездатності мережі при відключенні живлення в станціях з подвійним підключенням (DAS) останні повинні бути оснащені оптичними обхідними перемикачами (Optical Bypass Switch), які створюють обхідний шлях для світлових потоків при зникненні живлення, яке вони одержують від станції.

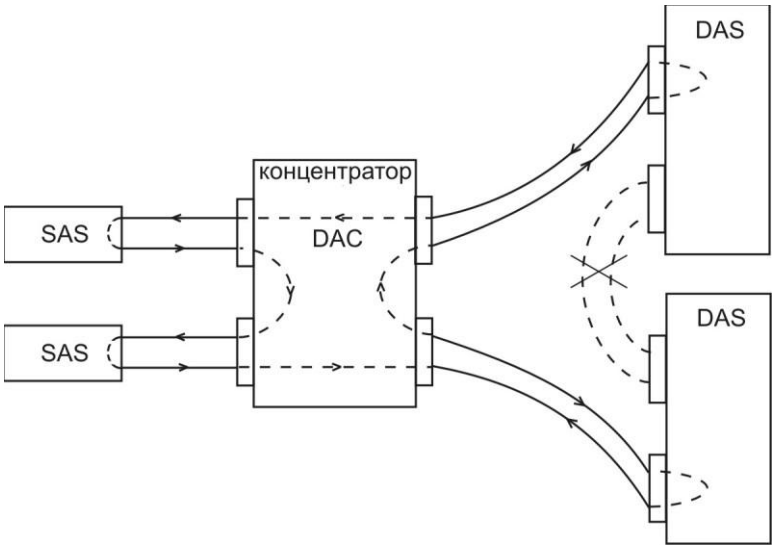


Рисунок 2.39 – Реконфігурація мережі FDDI при обриві кабелю

У мережі FDDI немає виділеного активного монітора – всі станції й концентратори рівноправні, і при виявленні відхилень від норми вони починають процес повторної ініціалізації мережі, а потім і її реконфігурації.

У технології FDDI для передачі світлових сигналів оптичними волокнами реалізоване логічне кодування 4B/5B разом з фізичним кодуванням NRZI. Ця схема приводить до передачі сигналів з тактовою частотою 125 МГц. З 32 комбінацій 5-бітних символів для кодування вихідних 4-бітних символів потрібно тільки 16 комбінацій, то з тих що залишилися обрано кілька кодів, які використовуються як службові. Найбільш важливим службовим символом є символ Idle, що постійно передається між портами протягом пауз між передачею кадрів даних. За рахунок цього станції і концентратори мережі FDDI мають постійну інформацію про стан фізичних з'єднань своїх портів. У випадку відсутності потоку символів Idle фіксується відмова фізичного зв'язку і проводиться реконфігурація внутрішнього шляху концентратора або станції, якщо це можливо.

У табл. 2.8 представлені результати порівняння технології FDDI з технологіями Ethernet і Token Ring.

Таблиця 2.8

Характеристики технологій FDDI, Ethernet, Token Ring

Характеристика	FDDI	Ethernet	Token Ring
Бітова швидкість	100 Мбіт/с	10 Мбіт/с	16 Мбіт/с
Топологія	Подвійне кільце дерев	Шина/зірка	Зірка/кільце
Метод доступу	Частка від часу обороту маркера	CSMA/CD	Пріоритетна система резервування
Середа передачі даних	Оптоволокно, неекранована вита пара категорії 5	Товстий коаксіал, тонкий коаксіал, вита пари категорії 3, оптоволокно	Екранована або неекранована вита пари, оптоволокно
Максимальна довжина мережі (без мостів)	200 км (100 км на кільце)	2500 м	4000 м
Максимальна відстань між вузлами	2 км (не більше 11 дБ втрат між вузлами)	2500 м	100 м
Максимальна кількість вузлів	500 (1000 з'єднань)	1024	260 для екранованої і 72 для неекранованої витої пари
Тактування та відновлення після відмов	Розподілена реалізація тактування і відновлення після відмов	Не визначений	Активний монітор

2.2.2 Бездротові мережі

Bluetooth. Протокол передачі інформації за допомогою бездротової технології Bluetooth був розроблений групою компаній Ericsson, IBM, Intel, Toshiba і Nokia на початку 1998 року. Забезпечує обмін інформацією між такими пристроями, як кишенькові і звичайні персональні комп'ютери, мобільні телефони, ноутбуки, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній,недорогий, повсюдно доступній радіочастоті для ближнього зв'язку. Зв'язок цих

пристроїв може здійснюватися в радіусі від 10 до 100 метрів один від одного навіть в різних приміщеннях.

Протокол UWB був розроблений альянсом компаній WiMedia, і в 2007 році затверджений в якості міжнародного стандарту IS/ IEC 26907. WiMedia UWB є стандартом широкосмугового бездротового зв'язку на коротких відстанях. Максимальна швидкість передачі даних між пристроями WiMedia UWB становить 480 Мбіт/с (як і у проводового USB), пристрої працюють в діапазоні частот від 3,1 до 10,6 ГГц. Протокол UWB конкурує з протоколом Bluetooth.

Протокол ZigBee – стандарт для недорогих, малопотужних бездротових мереж з комірковою топологією. Низька вартість дозволяє широко застосовувати дану технологію для бездротового контролю і спостереження, а завдяки малій потужності сенсори мережі здатні працювати довгий час, використовуючи автономні джерела живлення. Протокол був розроблений альянсом компаній ZigBee. Нижні рівні для даного стандарту розроблені IEEE і визначаються стандартами IEEE 802.15.4-2006.

Протокол INSTEON розроблений для управління бездротовими пристроями, призначеними для «розумного будинку». У протоколі передбачена зворотна сумісність зі старішим протоколом X10. Швидкість передачі сигналу управління за новим стандартом набагато вище, передбачаються вбудовані засоби виявлення помилок і повторної передачі сигналу, а для передачі використовується гібридний канал – радіозв'язок і мережу електроживлення. Однак на відміну від X10 специфікації INSTEON захищені патентами і використовуються тільки його розробниками - компанією Smarthome Technology.

Коміркова мережа Z-Wave з функціями самоорганізації і самовідновлення в поєднанні з гнучкими інсталяційними процедурами є простим у використанні мережевим рішенням. Протокол Z-Wave і чіп високого ступеня інтеграції забезпечує невисоку вартість. Реалізується сумісність додатків і пристроїв Z-Wave, випущених різними виробниками. Z-Wave підтримує повний спектр пристроїв, включаючи пристрої, що живляться від мережі змінного струму, від батарей, пристрої з фіксованим розташуванням і переміщувані пристрою, а також пристрої, що виконують роль мостів з іншими протоколами.В технології Z-Wave вузли діляться на три типи: контролери (Controllers), виконавчі механізми з маршрутизацією

(Routing Slaves) і виконавчі механізми (Slaves). У реальному мережі всі типи пристроїв можуть працювати в будь-якій комбінації.

Протокол передачі даних ANT був розроблений компанією Dynastream Innovations. Даний протокол насамперед розрахований на компактні пристрої з автономним живленням (трансивери, що використовують цей протокол, відрізняються виключно малим струмом споживання) для передачі відносно невеликих пакетів даних. протокол передбачає організацію відкритих і приватних бездротових мереж, в тому числі складного типу з динамічною конфігурацією. Він створений на основі технології PAN (Personal Area Network) і підтримує рівні 1-4 стека OSI (Open Systems Interconnection network model). Типове застосування такого протоколу – бездротові датчики. Несуча частота по протоколу ANT – 2,4 ГГц. Швидкість передачі даних по радіоканалу може становити до 1 Мбіт / с.

RuBee (IEEE P1902.1) – протокол бездротового зв'язку в місцевій регіональній мережі з використанням довгохвильового діапазону (LW) і пакетів даних не більше 128 байт. Протокол RUBee подібний протоколам серії IEEE 802, також відомим як Wi-Fi (IEEE 802.11), WPAN (IEEE 802.15.4) і Bluetooth (IEEE 802.15.1). RuBee networked працює за принципом точка-точка і є розвитком стандартів RFID. RuBee передбачає роботу на низькочастотної несучої (131 кГц), дозволяючи використовувати вузли мережі з малим споживанням енергії.

Wi-Fi створений в 1991 році NCR Corporation/AT&T в Нідерландах для бездротових мереж на базі стандарту IEEE 802.11. Зазвичай схема Wi-Fi мережі містить не менше однієї точки доступу (так званий режим infrastructure) і не менше одного клієнта. Також можливе підключення двох клієнтів в режимі точка-точка, коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережевих адаптерів «безпосередньо». Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів на швидкості 0.1 Мбіт / с кожні 100 мс. Тому 0.1 Мбіт/с – це найменша швидкість передачі даних для Wi-Fi. Знаючи SSID-мережі, клієнт може з'ясувати, чи можливе підключення до даної точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на підставі даних про рівень сигналу.

IDEN (Integrated Digital Enhanced Networks) – технологія для мереж транкінгового та стільникового зв'язку, розроблена компанією

MOTOROLA в 1994 році. В основі технології iDEN архітектура GSM, при передачі використовують частотні канали по 25 кГц, при цьому для передачі даних використовується частина каналу шириною 20 кГц, решта преназначено для захисту каналу. Протокол набув широкого поширення у всьому світі. Діапазон частот – 821-825 МГц.

Стандарт CDMAOne розроблений в 1995 році як технологічний стандарт групи ANSI. CDMAOne заснований на використанні CDMA (множинного доступу з кодовим поділом). Система CDMA IS-95 фірми Qualcomm розрахована на роботу в діапазоні частот 800 МГц, виділеному для стільникових систем стандартів AMPS, N-AMPS і D-AMPS. Подальший розвиток технології CDMA відбувається в рамках технології CDMA2000. При побудові системи мобільного зв'язку на основі технології CDMA2000 1X перша фаза забезпечує передачу даних зі швидкістю до 153 кбіт/с, що дозволяє надавати послуги голосового зв'язку, передачу коротких повідомлень, роботу з електронною поштою, Інтернетом, базами даних, передачу даних і нерухомих зображень.

WiMAX (Worldwide Interoperability for Microwave Access) – телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв'язку на великих відстанях для широкого спектру пристроїв (від робочих станцій і портативних комп'ютерів до мобільних телефонів). Заснована на стандарті IEEE 802.16, який також називають Wireless MAN. Назва «WiMAX» було запропоновано WiMAX Forum – організацією, заснованою в червні 2001 року для просування і розвитку WiMAX. Форум описує WiMAX як «засновану на стандарті технологію, яка надає високошвидкісний бездротовий доступ до мережі, альтернативний виділеним лініям і DSL »Максимальна швидкість - до 1 Гбіт/с.

GSM (від назви групи Groupe Special Mobile, пізніше перейменований в Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного стільникового зв'язку з розділенням частотного каналу за принципом TDMA та середньої ступенем безпеки. Розроблено під егідою Європейського інституту стандартизації електрозв'язку (ETSI) наприкінці 1980-х років. Комерційне використання стандарту почалося в середині 1991 року. GSM відноситься до мереж другого покоління (2 Generation), хоча на 2010 рік умовно знаходиться в фазі 2,75G завдяки численним розширень (1G - аналоговий стільниковий зв'язок, 2G - цифровий стільниковий зв'язок, 3G - широкосмуговий цифровий стільниковий зв'язок, коммутируемая багатоцільовими

комп'ютерними мережами, включаючи Інтернет). Стільникові телефони випускаються для 4 діапазонів частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

GPRS (General Packet Radio Service – пакетний радіозв'язок загального користування) – надбудова над технологією мобільного зв'язку GSM, що здійснює пакетну передачу даних. GPRS дозволяє користувачеві мережі стільникового зв'язку здійснювати обмін даними з іншими пристроями в мережі GSM і із зовнішніми мережами, включаючи Інтернет. Передача даних розділяється за напрямками «вниз» (downlink, DL) – від мережі до абонента і «вгору» (uplink, UL) – від абонента до мережі. Мобільні термінали поділяються на класи за кількістю одночасно використовуваних таймслотов для передачі і прийому даних.

UMTS (Universal Mobile Telecommunications System – Універсальна Мобільна Телекомунікаційна Система) – технологія стільникового зв'язку розроблена Європейським Інститутом Стандартів Телекомунікацій (ETSI) для впровадження 3G в Європі. В якості способу передачі даних через повітряний простір використовується технологія WCDMA, стандартизована відповідно до проекту 3GPP як відповідь європейських вчених і виробників на вимогу IMT-2000, опубліковане Міжнародним союзом електрозв'язку як набір мінімальних критеріїв для мережі стільникового зв'язку третього покоління. Згідно специфікаціям стандарту, UMTS використовує спектри частот: 1885-2025 МГц для передачі даних в режимі «від мобільного терміналу до базової станції» та 2110-2200 МГц для передачі даних в режимі «від станції до терміналу». У США через зайнятість спектра частот в діапазоні 1900 МГц мережами GSM виділені діапазони 1710-1755 МГц і 2110-2155 МГц відповідно. Крім того, оператори деяких країн (наприклад, американський AT & T Mobility) додатково експлуатують смуги частот 850 і 1900 МГц. Уряд Фінляндії на законодавчому рівні підтримує розвиток мережі стандарту UMTS900, що покриває важкодоступні райони країни і використовує діапазон 900 МГц (в даному проекті беруть участь такі компанії, як Nokia і Elisa).

Топології бездротових мереж. Всі перераховані бездротові мережі працюють в одному або декількох варіантах топології. На рис.2.40 наведені топології бездротових мереж різних конфігурацій. 5.1.

Найпростіший варіант організації мережі з двох пристроїв – итопологія точка-точка. Як правило, вузли цієї мережі є рівноправними,

тобто мережа однорангова. Ця топологія характерна для Bluetooth, ANT, RFID, RuBee, PDC, WI-FI, Insteon, UWB, ZigBee і інших.

Топологія «Зірка» є основою організації всіх сучасних мереж зв'язку та обчислювальних мереж. Дану топологію використовують протоколи WI-FI, Insteon, ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

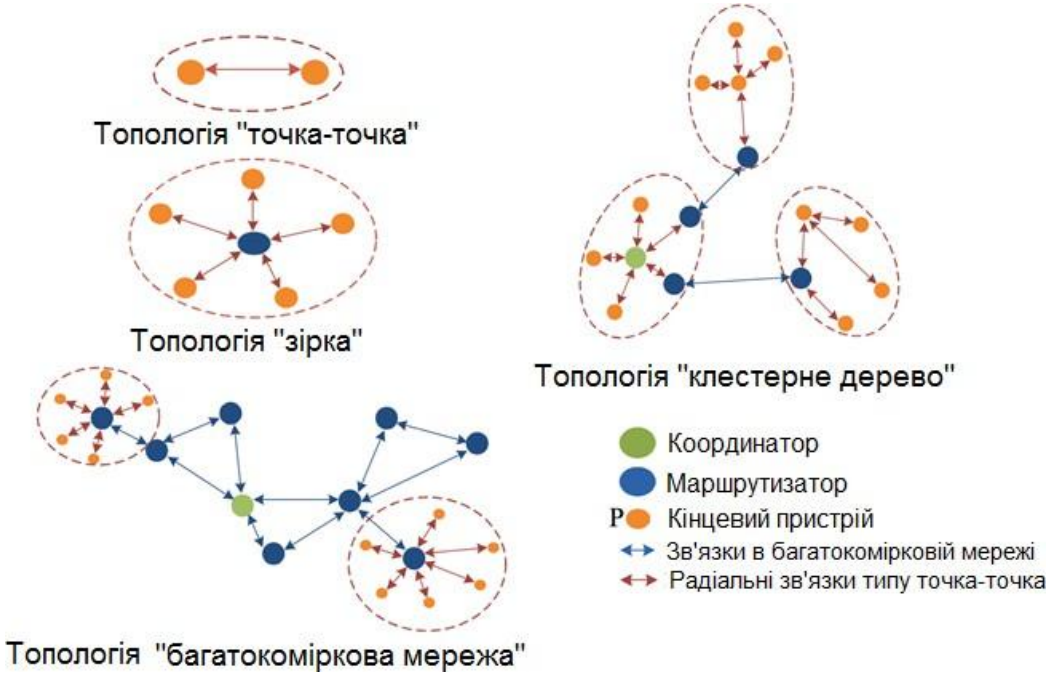


Рисунок 2.40 – Топології бездротових мереж

Багатокоміркова мережа – базова повнозвязна топологія комп'ютерних мереж і мереж зв'язку, в якій кожна робоча станція мережі з'єднується з усіма іншими робочими станціями цієї ж мережі. Характеризується високою стійкістю до відмов і складністю налаштування. Кожен вузол має кілька можливих шляхів сполучення з іншими вузлами, за рахунок цього така топологія дуже стійка. Ця топологія допускає з'єднання великої кількості вузлів і характерна, як правило, для великих мереж. Топологія може бути застосована для мереж з використанням протоколів UWB, WI-FI, Insteon,ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

Топологія «Кластерний дерево» утворюється в основному у вигляді комбінацій вищезгаданих топологій обчислювальних мереж. Основа дерева обчислювальної мережі розташовується в точці (корінь), в якій збираються комунікаційні лінії інформації (гілки дерева). Обчислювальні

мережі з деревоподібної структурою будуються там, де неможливо безпосереднє застосування базових мережних структур в чистому вигляді.

Технологія Wi-Fi. Розглянемо більш докладно стандарти технології Wi-Fi:

– 802.11 – первинний стандарт WLAN. Швидкість передачі – від 1 до 2 Мбіт/с. Зараз не використовується;

– 802.11a – високошвидкісна локальна мережа для радіочастоти 5 ГГц. Швидкість передачі – до 54 Мбіт/с. Відстані – до 100 м;

– 802.11b – локальна мережа для радіочастоти 2,4 ГГц. Швидкість передачі – до 11 Мбіт/с. Відстані – до 300 м (зазвичай – до 160 м);

– 802.11g – високошвидкісна мережа для радіочастоти 2,4 ГГц. Швидкість передачі – до 54 Мбіт/с. Відстані – до 300 м. Зворотно сумісна з 802.11b;

– 802.11n – високошвидкісна мережа для радіочастот 2,4-2,5 або 5,0 ГГц. Швидкість передачі по одній антені – до 150 Мбіт/с. Відстані – до 300 м. Сумісна з 802.11a/b/g;

– Топологія – шина (можливі логічна зірка і логічне кільце);

– Метод доступу – випадковий із запобіганням колізій (CSMA/CA).

Як видно, стандарт 802.11n підвищує швидкість передачі даних практично вчетверо в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 600 Мбіт/с застосовуючи передачу даних відразу по чотирьох антен. Крім того, пристрої 802.11n можуть працювати в трьох режимах:

– успадкованому (Legacy), в якому забезпечується підтримка пристроїв 802.11b/g і 802.11a;

– змішаному (Mixed), в якому підтримуються пристрої 802.11b/g, 802.11a і 802.11n;

– «чистому» режимі – 802.11n (саме в цьому режимі і можна скористатися перевагами підвищеної швидкості і збільшеною дальністю передачі даних, що забезпечуються стандартом 802.11n).

Топологія для технології умовна. Структура мережі Wi-Fi наведена на рис.2.41. Сигнал посилається всім. Метод доступу випадковий CSMA/CA, але він відрізняється від методу доступу Ethernet. Кожен абонент, який хоче передавати чекає коли середовище звільниться і передає спеціальний пакет – запит. І деякий час чекає відповіді на цей запит. Якщо він отримує відповідь на запит – готовність. Тоді він передає свій пакет. Колізії звичайно можливі, але стикаються маленькі керуючі

пакети. І ситуація вирішується на більш високому рівні управління обміном.

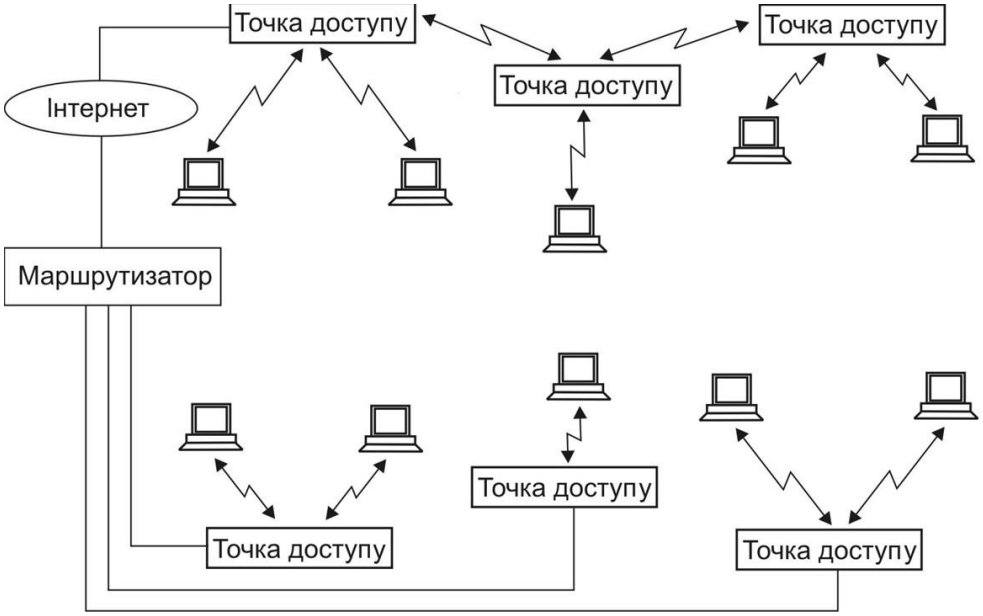


Рисунок 2.41 – Структура мережі Wi-Fi

Концентратори в мережі називаються *точками доступу*. Зона обслуговування визначається відстанню на який може пройти радіосигнал без спотворень. Точки доступу можуть розташовуватися близько одна від іншої створюючи зону обслуговування (*hot spot*), яка включає в себе покриття кожної з точок доступу. Таке покриття використовується для підключення абонентів до Інтернету.

Формат інформаційного пакету Wi-Fi наведений на рис.2.42. На відміну від формату пакета Ethernet додані окрім адреси відправника і одержувача, ще адреса передавальної станції і приймаючої станції (точок доступу), завдяки чому забезпечується роумінг для абонента між точками доступу.

Рисунок 2.42 – Формат інформаційного пакету Wi-Fi

Крім безперечних переваг технології Wi-Fi слід зазначити і численні недоліки, серед яких:

– невеликі відстані передачы даних;
– схильність до електромагнітних перешкод;
– низька секретність;
– вплив стін, металевих предметів, дзеркал;
– вплив листя, дощу, туману;
– сильна залежність швидкості передачі від кількості абонентів, від відстані, від рівня перешкод;
– взаємний вплив незалежних точок доступу;
– неповна сумісність обладнання різних виробників;
– високе енергоспоживання;
– електромагнітні випромінювання.

2.2.3 Розвиток технології Ethernet

Gigabit Ethernet підтримує швидкість передачі даних 1000 Мбіт/с і дозволяє ефективно будувати великі локальні мережі, у яких потужні сервери і магістралі нижніх рівнів мережі можуть працювати на швидкості 100 Мбіт/с, а магістраль Gigabit Ethernet поєднує їх, забезпечуючи досить великий запас пропускної здатності.

Gigabit Ethernet використовує ті ж формати кадрів, що й попередні версії Ethernet, працює в повнодуплексному і напівдуплексному режимах, підтримуючи на поділюваному середовищі той же метод доступу CSMA/CD з мінімальними змінами.

Для забезпечення прийнятного максимального діаметра мережі в 200 м у напівдуплексному режимі розроблювачі технології пішли на збільшення мінімального розміру кадру з 64 до 512 байт. Дозволяється також передавати кілька кадрів підряд, не звільняючи середовище, на інтервалі 8096 байт, тоді кадри не обов'язково доповнювати до 512 байт. Інші параметри методу доступу і максимального розміру кадру залишилися незмінними.

Влітку 1998 року був прийнятий стандарт 802.3z, котрий визначає використання в якості фізичного середовища трьох типів кабелю: багатомодового оптоволокна (відстань до 500 м), одномодового оптоволокна(відстань до 5000 м) і витої пари, якою дані передаються одночасно по двох мідних екранованих провідниках на відстань до 25 м.

Стандартні сегменти Gigabit Ethernet (IEEE 802.3z і IEEE 802.3ab):

– 1000BASE-T (IEEE 802.3ab) – вита пара категорій 5e або 6 довжиною до 100 м. Двонаправлена передача по всіх 4 парах (250 Мбіт/с по кожній парі), код PAM5;

– 1000BASE-TX – вита пара категорії 6 довжиною до 100 м. Дві пари на передачу, дві – на прийом (500 Мбіт/с по кожній парі). Код 8B/10B. Витісняється сегментом 1000BASE-T.

– 1000BASE-CX – екранована вита пара довжиною до 25 м. Не використовується.

– 1000BASE-SX – багатомодовий оптоволоконний кабель довжиною до 500 м;

– 1000BASE-LX – одномодовий оптоволоконний кабель довжиною до 2000 м.

До основних відмінностей мережі Gigabit Ethernet від попередніх стандартів слід віднести наступні:

– збільшення мінімального розміру пакета до 512 байт для збільшення розміру області колізії при напівдуплексному режимі;

– нові методи кодування (8B / 10B і PAM5);

– можливість блокового режиму передачі (абонент передає кілька пакетів поспіль сумарною довжиною до 8192 байт, до 512 байт розширюється тільки перший пакет)

– основний режим передачі – повнодуплексний, застосовуються комутатори і маршрутизатори;

– основне середовище передачі – оптоволоконний кабель;

– основне призначення – опорні мережі, зв'язок з швидкими серверами.

10 Gigabit Ethernet (10GE, 10GbE або 10 GigE) – це група комп'ютерних мережевих технологій для передачі кадрів Ethernet зі швидкістю 10 Гбіт/с. Вперше визначена стандартом IEEE 802.3ae-2002. На відміну від попередніх стандартів Ethernet, 10 Gigabit Ethernet визначає тільки дуплексні двоточкові з'єднання, які зазвичай підключаються мережевими комутаторами. Метод CSMA/CD не був перенесений з попередніх стандартів Ethernet, тому напівдуплексні операції і концентратори не існують в 10GbE.

Стандартні сегменти 10 Gigabit Ethernet (IEEE 802.3ae і IEEE 802.3an):

– 10GBASE-SR – багатомодовий оптоволоконний кабель з довжиною до 33-82-300 м;

– 10GBASE-LR – багатомодовий оптоволоконний кабель з довжиною до 220 м;

– 10GBASE-LX4 – багатомодовий оптоволоконний кабель з довжиною до 300 м, одномодовий – з довжиною до 10 км;

– 10GBASE-ER – одномодовий оптоволоконний кабель с довжиною до 40 км;

– 10GBASE-T (IEEE 802.3an, 2006) – вита пара категорії 6 з довжиною до 55 м або категорії 6a з довжиною до 100 м (двонаправлена передача по чотирьох витим парам, швидкість 2,5 Гбіт/с по кожній парі).

40 Gigabit Ethernet або 40GbE, а також *100 Gigabit Ethernet*, або *100GbE* – стандарти Ethernet, що розроблялися IEEE P802.3ba Ethernet Task Force з початку листопада 2007, та були остаточно прийняті в червні 2010. Ці стандарти підтримують передачу Ethernet пакетів на швидкості 40 та 100 Гбіт/с крізь декілька окремих 10 Гбіт/с або 25 Гбіт/с ліній. Робота над проектом була започаткована IEEE 802.3 Higher Speed Study Group з метою розширення протокола 802.3 до робочих швидкостей 40 Гбіт/с та 100 Гбіт/с для того щоб досягти значного збільшення пропускної здатності та максимально зберегти сумісність з існуючим обладнанням, що використовує стандарт 802.3, попередні інвестиції в дослідження та розробку, а також принципи роботи та керування мережами. Проект має за мету забезпечити зв'язок між обладнанням, враховуючи існуючі вимоги до дальності.

Як видно тенденція розвитку технології Ethernet спрямована на збільшення швидкості передачі даних. На інтегральну швидкість передачі інформації впливають час обміну інформацією з комп'ютером, затримка в кабелі, затримка в проміжних пристроях, швидкість комп'ютера і його пристроїв, тому збільшення швидкості мережі сприяє підвищенню пропускної здатності мережі, знижує навантаження на мережу і кількість колізій. Збільшення швидкості мережі знижує ймовірність передачі помилкових пакетів, так як зменшується тривалість кожного пакета.

Коротко сформулюємо основні тенденції розвитку технології Ethernet:

–підвищення швидкості 10 – 100 – 1000 – 10000 Мбіт/с;

–перехід на оптоволоконний кабель: коаксіальний кабель – вита пара – оптоволокно;

–зміна топології: шина – пасивна зірка (дерево) – активна зірка (дерево). Все більше ускладнюється центр, мережа наближається до

топології активна зірка. З використанням маршрутизаторів топологія дерево стала переходити в топологію хмара, що є кроком до конвергенції локальних і глобальних мереж;

–зміна проміжних пристроїв: репітер – концентратор – комутатор – маршрутизатор. Зараз основними пристоями в мережі є комутатор і маршрутизатор;

–зміна методу управління: CSMA/CD – полудуплексне комутування – повний дуплекс;

–зміна кодів передачі: манчестерський код – 4B/5B – 8B/10B і PAM 5.

Перехід на оптоволоконний кабель зумовлюється необхідністю збільшення розміру мережі (для повного дуплексу довжина кабелю може досягати до 2-10 км), а також збільшенням перешкодозахищеності і секретності (рівень перешкод оптоволокна весь час зростає). Крім того, волоконно-оптичний кабель не потребує гальванічної розв'язки, узгодження і заземлення. Вартість кабелю, а також оптоволоконних трансиверів, мережевих адаптерів і комутаторів постійно знижається, зараз оптоволокно дешевше за виту пару категорії 7. А для швидкості вище 10 000 Мбіт / с волоконно-оптичний кабель – це єдиний можливий варіант.

2.3 Загальні питання проектування мереж

2.3.1 Структуризація LAN на фізичному та канальному рівнях

Типи апаратури локальної мережі. До основної апаратури ЛОМ можно віднести наступну апаратуру:

- кабелі для передачі інформації;
- рознімання (конектори) для приєднання кабелів;
- термінатори (кінцеві погоджувачі);
- мережеві адаптери (мережеві інтерфейсні карти, NIC);
- репітери (повторювачі, ретранслятори);
- трансивери (приймачі), медіаконвертори;
- концентратори (хаби);
- комутатори (перемикачі, свитчи);
- мости;
- маршрутизатори (роутери);
- шлюзи.

Апаратура наведена у порядку збільшення її інтелектуальних властивостей, функціональних можливостей і вартості. Відповідно до росту складності апаратури росте і затримка, яку вносить ця апаратура в лінію зв’язку.

Мережеві адаптери (мережеві інтерфейсні карти, NIC) – додатковий пристрій, що дозволяє комп'ютеру взаємодіяти з іншими пристроями мережі. В даний час в персональних комп'ютерах і ноутбуках контролер і компоненти, що виконують функції мережевої плати, досить часто інтегровані в материнські плати для зручності, в тому числі уніфікації драйвера і здешевлення всього комп'ютера в цілому.Мережевий адаптер виконує функції фізичного і канального рівнів моделі OSI (рис.2.43). Більш точно, в мережевій операційній системі пара адаптер і драйвер виконує тільки функції фізичного і MAC-рівнів, в той час як LLC-рівень звичайно реалізується модулем операційної системи, єдиним для всіх драйверів і мережевих адаптерів.

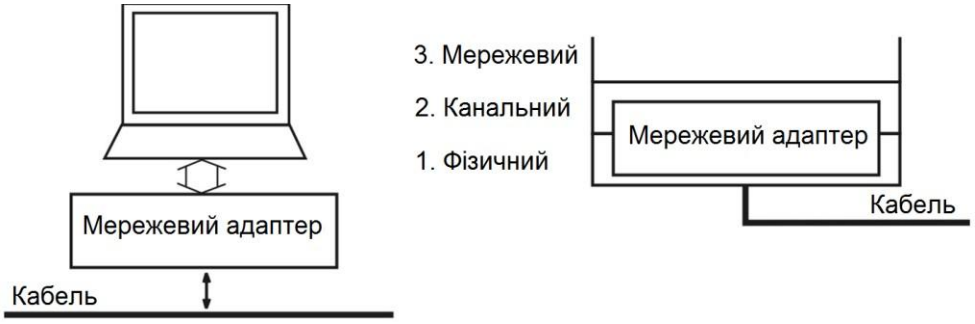


Рисунок 2.43 – Мережевий адаптер в моделі OSI

За конструктивною реалізацією мережеві адаптери поділяються на:

– внутрішні – окремі плати, що вставляються в ISA, PCI або PCI-E слот;

– зовнішні, що підключаються через LPT, USB або PCMCIA інтерфейс, переважно використовуються в ноутбуках;

– вбудовані в материнську плату.

На 10-мегабітних мережевих платах для підключення до локальної мережі використовуються 4 типи рознімань:

– 8P8C для витої пари;

– BNC-коннектор для тонкого коаксіального кабелю;

– 15-контактний роз'єм AUI трансивера для товстого коаксіального кабелю.

– оптичний роз'єм (10BASE-FL і інші стандарти 10 Мбіт Ethernet).

Ці рознімання можуть бути присутніми в різних комбінаціях, але в будь-який даний момент працює тільки один з них.

На 100-мегабітних платах встановлюють або рознімання для витої пари (8P8C), або оптичне рознімання (SC, ST, MIC).

До основних мережевих функцій адаптеров відносяться:

– гальванічна розв'язка комп'ютера і кабелю (зазвичай ─ трансформатори);

– перетворення логічних сигналів в мережеві (електричні або світлові);

– кодування і декодування мережевих сигналів (формування надлишкових кодів 4B/5B, скремблірування);

– розпізнавання прийнятих пакетів (вибір з пакетів тих, які адресовані даному абоненту або всім абонентам);

– перетворення паралельного коду в послідовний при передачі і зворотне перетворення при прийомі;

– буферизація переданої та прийнятої інформації в буферній пам'яті;

– організація доступу до мережі;

– підрахунок контрольної суми пакетів при передачі і прийомі.

Медіаконвертер (також перетворювач середовища) – це пристрій, що перетворює середу поширення сигналу з одного типу в інший (рис.2.44). Найчастіше середовищем поширення сигналу є мідні дроти і оптичні кабелі. Під середовищем поширення сигналу може розумітися будь-яке середовище передачі даних, проте в сучасній термінології медіаконвертер працює як сполучна ланка тільки між двома середовищами – оптичним і мідним кабелями.

Традиційно, стосовно до мережевих технологій, медіаконвертери здійснюють свою роботу на фізичному рівні моделі OSI. У цьому випадку неможливо перетворення швидкості передачі даних між двома середовищами, а також неможлива інша інтелектуальна обробка даних. В цьому випадку медіаконвертери також можуть називати *трансиверами*. З розвитком технологій медіаконвертери забезпечили додатковими інтелектуальними можливостями, щоб забезпечити стикування старих пристроїв з більш новими. Медіаконвертери стали працювати на канальному рівні моделі OSI і отримали можливість перетворювати не тільки середовище, а також і швидкість передачі даних, володіти іншими

сервісними функціями, як оповіщення про обрив лінії зв'язку на протилежному боці, контроль за потоком передачі даних, іншими технічними можливостями. Ethernet-медіаконвертери традиційно діляться на прості (1-й рівень моделі OSI), які підпорядковуються правилу 5-4-3 і на комутуючі (2-й рівень моделі OSI), на які не діють обмеження за кількістю медіаконвертерів на ділянці мережі, що з'єднує її сегменти. У таких медіаконвертерів в описі вказується 10/100TX для Fast Ethernet, або 10/100/1000T для Gigabit Ethernet, що означає їх можливість перетворювати не тільки середовище передачі, а також і швидкість, що характерно для комутуючих пристроїв.

Рисунок 2.44 – Медіаконвертер D-Link DMC-1910:
T (передавальний) і R (приймаючий)

Концентратори Ethernet – пристрої для об'єднання комп'ютерів в мережу Ethernet із застосуванням кабельної інфраструктури типу вита пара. В даний час витіснені мережевими комутаторами. Мережеві концентратори також могли мати рознімання для підключення до існуючих мереж на базі товстого або тонкого коаксіального кабелю.

Концентратор працює на першому (фізичному) рівні мережевий моделі OSI, ретранслюючи вхідний сигнал з одного з портів в сигнал на всі інші (підключені) порти, реалізуючи, таким чином, властиву Ethernet топологію загальна шина, з поділом пропускної здатності мережі між усіма пристроями і роботою в режимі напівдуплекса. Колізії (тобто спроба двох і більше пристроїв почати передачу одночасно) обробляються аналогічно мережі Ethernet на інших носіях – пристрої самостійно припиняють передачу і відновлюють спробу через випадковий проміжок часу, кажучи сучасною мовою, концентратор об'єднує пристрої в одному домені колізій.

Мережевий концентратор також забезпечує безперебійну роботу мережі при відключенні пристрою від одного з портів або пошкодженні кабелю, на відміну, наприклад, від мережі на коаксіальному кабелі, яка в такому випадку припиняє роботу цілком.

Характеристики мережевих концентраторів:

– кількість портів – рознімань для підключення мережевих ліній (від 4 до 48 портів);

– швидкість передачі даних – випускаються концентратори зі швидкістю 10, 100 і/або 1000 Мбіт/с. Швидкість може перемикатися як автоматично (на найменшу з використовуваних), так і за допомогою перемичок або перемикачів;

– наявність портів для підключення кабелів Ethernet інших типів – коаксіальних або оптичних;

– клас (клас I або клас II);

– можливість нарощування та об'єднання.

Функції мережевих концентраторів:

– пересилання пакетів з порту в порти. Затримка передачі (клас I – 140 bt, клас II – 46 bt (TX/FX) або 67 bt (T4);

– відключення портів в аварійних ситуаціях;

– виявлення та посилення колізій за методом CSMA/CD;

– виявлення та виправлення найпростіших помилок: помилкова несуча (частота) (FCE, False Carrier Event) – 5мкс немає початку кадру (для 100 Мбіт/с); множинні колізії (ECE, Excessive Collision Error) – понад 60 колізій поспіль; тривала передача (Jabber) – понад 400 мкс (для 100 Мбіт/с).

Керовані концентратори (клас 1) допускають управління з віддалених робочих станцій (NMS – Network Management Station) з прикладного протоколу SNMP (Simple Network Management Protocol), а також дозволяють контролювати:

– навантаження мережі на кожному порту і в цілому;

– стан портів;

– інтенсивність і характер помилок в мережі;

– відключати несправні сегменти.

Обмін інформацією проводиться дейтаграммами спеціального формату з використанням протоколів IP.

Мости і комутатори. Міст (bridge), а також його швидкодіючий аналог — комутатор (switching hub), ділять загальне середовище передачі

даних на логічні сегменти. Зараз мости використовуються рідко, їх практично витіснили комутатори. Фактично, міст – це не спеціалізований пристрій, а комп'ютер до якого підключено декілька мережевих адаптерів, як правило не більше 4-х (рис.2.45). Через мережеві адаптери до моста підключаються сегменти, і якщо мережеві адаптери різних технологій, то і сегменти, що підключаються до моста можуть бути різних мереж, тобто міст може об'єднувати сегменти Ethernet з іншими мережами, нприклад, з FDDI.

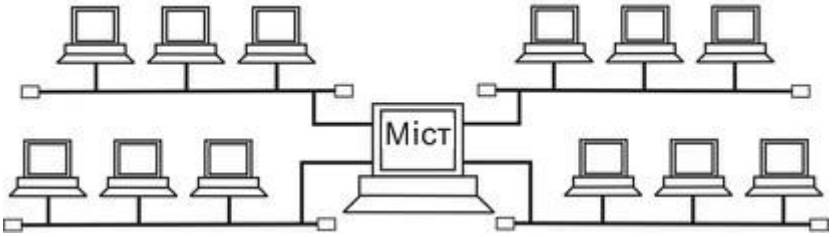


Рисунок 2.45 – Підключення сегментів до моста

До основних функцій моста Ethernet відносяться наступні функції:

– пересилка пакетів між сегментами;
– відфільтровування пакетів, призначених для комп'ютерів всередині сегменту;
– пересилка широкомовних пакетів;
– видалення пошкоджених пакетів;
– об'єднання сегментів Ethernet;
– зв'язок Ethernet з іншими типами мереж;
– видалення петель (замкнутих шляхів) з мережі.

При підключенні мости і комутатори підтримують лише деревовидні зв'язки, тобто такі яки не містять петель. Якщо в мережі помилково були утворені петлеві з'єднання, це може призвести до циркуляції широкомовних пакетів в замкнутих петлях і відповідно до перегруження мережі. Таке явище зветься «широкомовним штормом» (рис.2.46). Для автоматичного вирішення проблеми зациклення пакетів був запропонований так званий «алгоритм кістякового дерева». *Алгоритм кістякового дерева STA (Spanning Tree Algorithm)* забезпечує побудову деревовидної топології зв'язків мережі з єдиним шляхом мінімальної вартості від кожного комутатора і від кожного сегмента до деякого виділеного кореневого комутатора – кореня дерева. Реалізація алгоритму

здійснюється на основі протоколу *STP (Spanning Tree Protocol)* в результаті дії якого міст або комутатор самостійно виявляє зайві зв'язки та автоматично блокує з'єднання, що призвели до утворення петель. Протокол STP входить до складу протоколу мостів і комутаторів IEEE 802.1d.

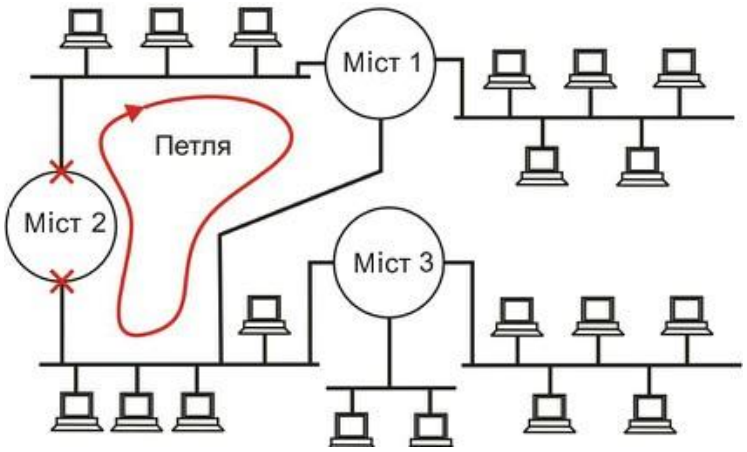


Рисунок 2.46 – Петля в мережі з мостами і її видалення за алгоритмом STA

Алгоритми роботи мостів і комутаторів схожі і засновані на *таблиці комутації (таблиці MAC-адрес)*, за записами якої пристрій здійснює передачу кадрів. Таблиця MAC-адрес містить записи відповідності MAC адреси комп'ютера і номера порта комутатора, до якого він підключений, формується автоматично на підставі аналізу виконаних комутатором передач. Оновлюється протягом тайм-ауту. Наведемо, загальний алгоритм роботи мостів і комутаторів:

– одержання пакету (кадра);

– перевірка наявності в таблиці MAC-адрес адреси відправника з номером порта. Якщо немає – занести. Якщо приписаний іншому порту – видалити;

– якщо пакет широкомовний, то пересилання його на всі порти, крім порта відправника;

– якщо пакет однопунктний (один одержувач), то пересілання його на порт, якому в таблиці MAC-адрес відповідає адреса одержувача;

– якщо пакет внутрисегментний, то він ігнорується;

– якщо адреси одержувача ще нема в таблиці, то пересилання пакета на всі порти, крім порту відправника;

– оновлення записей таблиці з урахуванням часу старіння (5 хвилин).

Різниця між мостом і комутатором полягає в тому, що міст в кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між усіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно. Крім того, комутатор – є спеціалізованим пристроїм, який працює швидше за міст. Має більшу кількість портів (4-8-16-24 і т.д.), тоді як міст – не більше 4-х. В залежності від типу прості комутатори можуть не підтримувати об’єднання різнорідних мереж і алгоритм кістякового дерева, тоді як складні комутатори можуть працювати на 3 рівні моделі OSI і заміняти маршрутизатор.

Логічна структура і типи комутаторів. Логічна структура комутатора досить проста. Вона включає в себе так звану *перехресну (комутаційну) матрицю (Crossbar Matrix)*, у всіх точках перетину якої можуть встановлюватися зв'язку на час передачі пакета (рис.2.47). В результаті пакет, що надходить з будь-якого сегмента, може бути переданий в будь-який інший сегмент. У разі широкомовного пакету, адресованого всім абонентам, він передається в усі сегменти одночасно, крім того сегмента, з якого він прийшов (рис. 2.48).

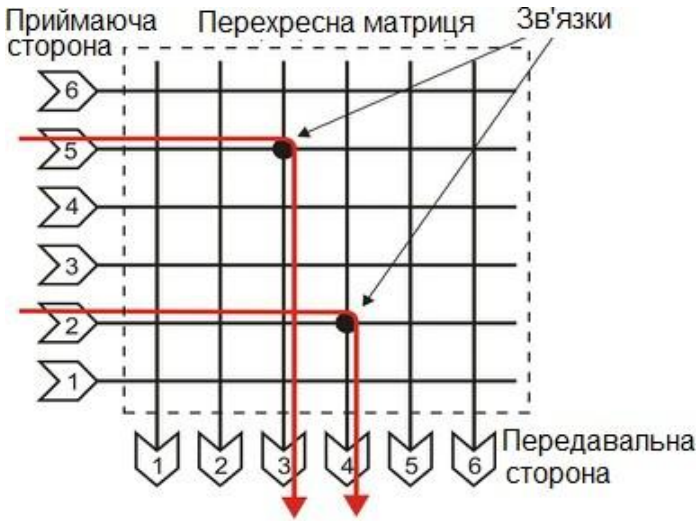


Рисунок 2.47 – Логічна структура комутатора

Крім перехресної матриці комутатор включає в себе пам'ять, в якій він формує таблицю MAC-адрес всіх комп'ютерів, підключених до кожного з його портів.

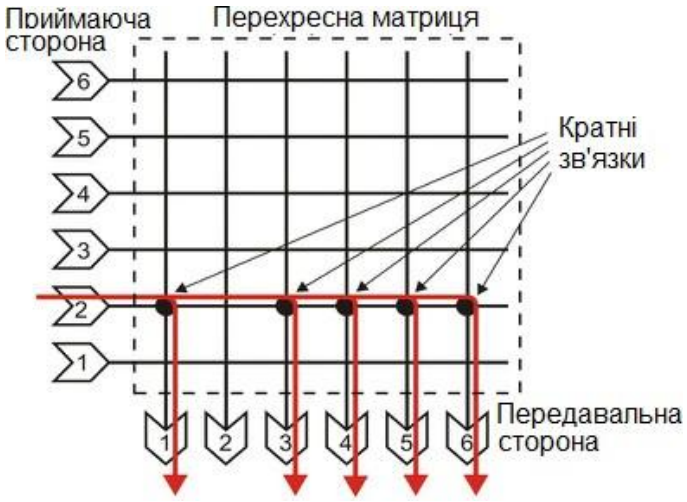


Рисунок 2.48 – Комутація широкомовного пакету

Комутатори можуть бути трьох типів:

– Наскрізні комутатори (Cut-Through) – прості, дешеві, швидкі (затримка до 150 bt), мають буфер тільки на заголовок пакету, не вирішують критичні ситуації;

– Комутатори з накопичуванням (Store-and-Forward, SAF) – складні, дорожче, більш повільні (затримка до 12 000 bt), мають буфер на весь пакет, вирішують критичні ситуації, допускають підтримку різних швидкостей і повнодуплексного режиму;

– Гібрідні (адаптивні) комутатори – при малому навантаженні працюють як наскрізні комутатори, при великому – як комутатори з накопичуванням.

Буферна пам'ять (з організацією FIFO) може розміщуватися на приймаючій стороні всіх портів (накопичення перед комутацією), на передавальній стороні портів (накопичення перед ретрансляцією), а також може бути загальною для всіх портів, причому ці методи часто комбінуються для досягнення найбільшої гнучкості і збільшення продуктивності. Чим більше обсяг пам'яті, тим краще комутатор справляється з перевантаженням. Але з ростом обсягу пам'яті підвищується і вартість обладнання.

До критичних ситуацій наскрізних комутаторів відносяться: втрата пакетів при одночасному надходженні на комутатор двох (чи більше) пакетів: одного з якогось порту, а іншого – на цей самий порт або адресованих в один і той же порт та надходження на комутатор

зіпсованого пакету (карликового менше 512 bt чи з невірною контрольною сумою), який потрібно видаліти.

Приклад алгоритму роботи комутатора. Як било сказано вищче, щоб передавати кадри комутатор використовує три базових механізми:

1) *Flooding* – кадр, отриманий на один з портів передається на інші порти комутатора. Комутатор виконує цю операцію в двох випадках:

– при отриманні широкомовного або multicast кадру;

– при отриманні unknown unicast кадру..

2) *Forwarding* – передача фрейму, отриманого на одному порту через інший порт відповідно до запису в таблиці комутації.

3) *Filtering* – якщо комутатор отримує кадр через певний порт, і MAC-адреса одержувача доступну через цей же порт, то комутатор відкидає фрейм.

Розглянемо приклад мережі, що демонструє використання передачі фреймів. На рис. 2.49 зображений комутатор sw1 і повторювач (hub) до якого підключені два хости.

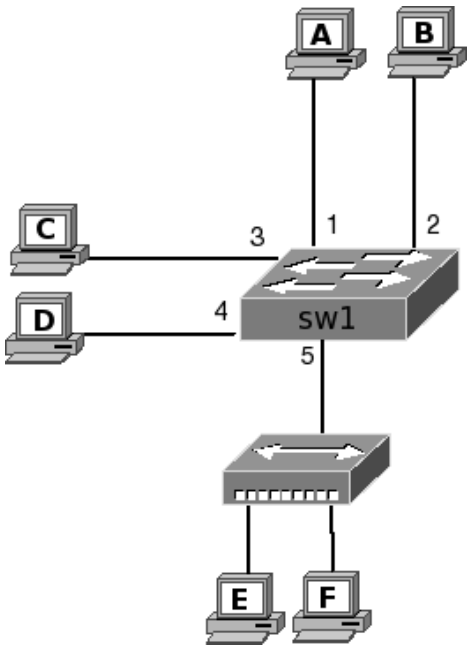


Рисунок 2.49 – Приклад мережі, що демонструє використання передачі фреймів

Спочатку до комутатора були підключені три хости A, B і C. Відповідно у комутатора була таблиця комутації, представлена в табл.2.9.

Таблиця 2.9

Вихідна таблиця комутації для схеми мережі, що представлена на рис. 2.49

Порт комутатора	MAC – адреса хоста
1	A
2	B
3	C

Коли хост A відправляє кадр хосту B, комутатор використовує механізм forwarding, тому що йому відомо, де знаходяться обидва хости і хости знаходяться на різних портах комутатора.

Далі до комутатора підключили хост D. Якщо хост A відправляє кадр хосту D, то для комутатора це unknown unicast фрейм, тому що в таблиці комутації немає запису про MAC-адресу D. У відповідності зі своїми правилами комутатор виконує flooding і передає фрейм на всі порти, крім 1 (з якого фрейм був отриманий).

Після того як комутатор отримає фрейм від хоста D, він запам'ятає його адресу і створить відповідний запис у таблиці комутації. До комутатора підключили повторювач з двома хостами і комутатор вивчив їх адреси. Відповідна таблиця комутації, наведена в табл.2.10.

Таблиця 2.10

Таблиця комутації комутатора після підключення всіх пристроїв за схемою, представленої на рис. 2.49

Порт комутатора	MAC – адреса хоста
1	A
2	B
3	C
4	D
5	E
5	F

Якщо після цього хост E буде передавати фрейм хосту F, то комутатор отримає його, але не передаватиме далі. У цій ситуації комутатор використовує механізм filtering, тому що MAC-адреса одержувача доступна через той же порт, що і відправника.

Головне правило, якого треба дотримуватися при розбитті мережі на частини (сегменти) за допомогою комутатора, називається *"правило 80/20"*. Тільки при його виконанні комутатор працює ефективно. Згідно з цим правилом, необхідно, щоб не менше 80 відсотків усіх передач відбувалося в межах однієї частини (одного сегмента) мережі. І тільки 20 відсотків всіх передач повинно відбуватися між різними частинами (сегментами) мережі, що проходить через комутатор. На практиці це зазвичай зводиться до того, щоб сервер і активно працюють з ним робочі станції (клієнти) розташовувалися на одному сегменті. Це ж правило 80/20 може бути застосовано і до мостів.

Маршрутизатори. Маршрутизатори, як і мости або комутатори ретранслюють пакети з однієї частини мережі в іншу (з одного сегмента в інший), але існують і принципові відмінності:

– маршрутизатор повноправний абонент в мережі, кожний його інтерфейс має свою IP-адресу, це непрозорий зв'язок, тому пакети адресуються маршрутизатору;

– працюють з логічними IP адресами, зберігають список MAC і IP адрес всіх підключених абонентів, список сусідних маршрутизаторів, адреси всіх підключених мереж;

– не пропускають широкомовні пакети – розділяють широкомовну область мережі;

– розрішають існування в мережі петель, обирають оптимальний маршрут доставки пакету;

– розмір маршрутизованої мережі не обмежений;

– працюють на 3-му рівні, можуть об’єднувати різні підмережі, різні мережі з глобальними мережами, тоді як комутатори звичайно працюють з мережами Ethernet;

– маршрутизатори складніше, повільніше і дорожче комутаторів.

Маршрутизатор беруть на себе роль моста і шлюзу. Моста тому, що можуть пов'язувати різні локальні мережі. А шлюзу, тому що можуть пов'язувати з глобальною мережею Інтернет. Комутатор і концентратор все таки виконує свої функції всередині локальної мережі (Ethernet).

Маршрутизатор об'єднують між собою. Множина пов'язаних один з одним маршрутизаторів можуть утворювати так звану *хмару (Cloud)*. Таке з'єднання забезпечує виключно гнучку і надійну зв'язок між усіма підключеними до нього локальними мережами (рис.2.49).

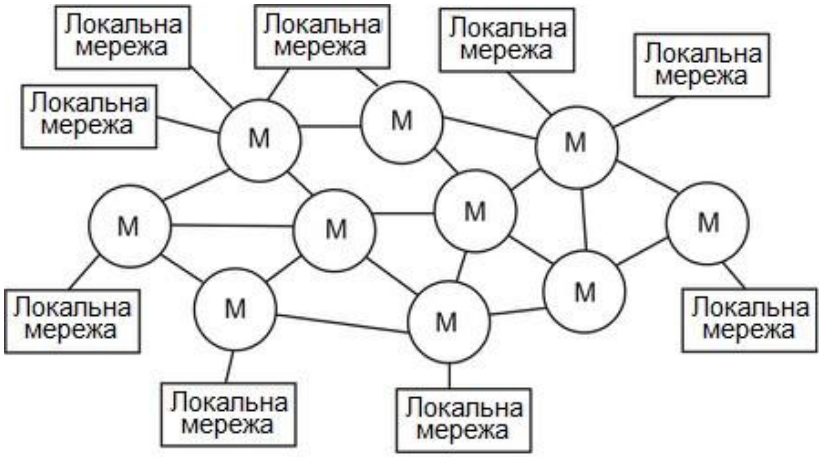


Рисунок 2.49 – Топологія хмара, що утворена з’єднаннями маршрутизаторів

Маршрутизатори обробляють адресну інформацію, що відноситься до структури дейтаграми IP, яка вкладена в область даних кадру, а та в свою чергу в пакет 1 рівня. (рис.2.50). Тому кажуть, що вони працюють з дейтаграммами, або ретранслюють дейтаграми. Маршрутизатор аналізує мережеву IP-адресу дейтаграми.

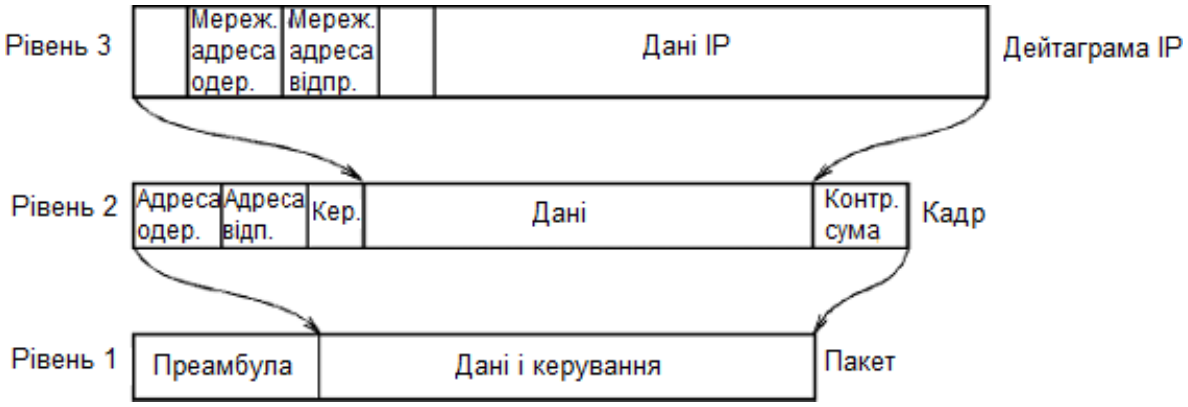


Рисунок 2.50 – Інкапсуляція дейтаграми в кадр

2.3.2 Додаткові функції мостів та комутаторів. Перспективи розвитку маршрутизаторів

Віртуальні локальні мережі VLAN. VLAN (Virtual Local Area Network) – група пристроїв, що мають можливість взаємодіяти між собою

безпосередньо на канальному рівні, хоча фізично при цьому вони можуть бути підключені до різних мережевих комутаторів. І навпаки, пристрої, що знаходяться в різних VLAN, невидимі один для одного на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв'язок між цими пристроями можливий тільки на мережевому і більш високих рівнях.

VLAN можуть бути налаштовані на комутаторах, маршрутизаторах, інших мережевих пристроях і на хостах. Розглянемо налаштування VLAN на комутаторі, до якого підключені 4 хости: A, B, C і D. На комутаторі налаштовані два VLAN, всі порти налаштовані як нетеговані (access-порти в термінології Cisco) у відповідних VLAN (рис.2.51).

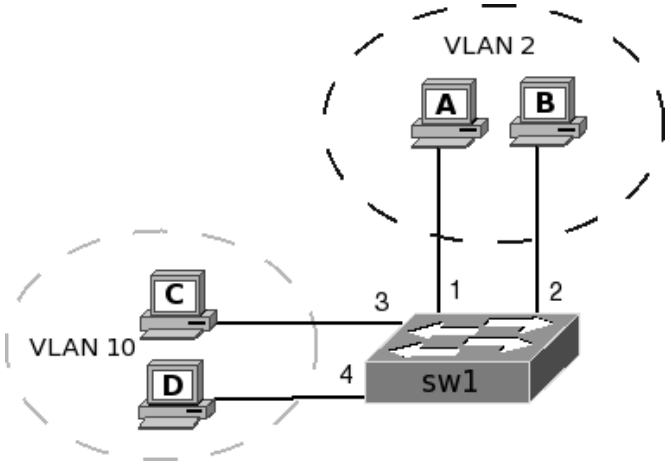


Рисунок 2.51 – Приклад мережі, в якій хости знаходяться в різних VLAN на одному комутаторі

Після цього на комутаторі існують дві таблиці комутації для VLAN 2 (табл.2.11) і для VLAN 10 (табл.2.12). Всі базові механізми комутатора залишаються точно такими ж, як і до поділу на VLAN, але вони використовуються тільки в межах відповідного VLAN.

Таблиця 2.11

Таблиця комутації для VLAN 2 для схеми мережі, представленої на рис. 2.51

Порт комутатора	MAC – адреса хоста
1	A
2	B

Таблиця 2.12

Таблиця комутации для VLAN 10 для схеми мережі, представленої на рис. 2.51

Порт комутатора	MAC – адреса хоста
3	C
4	D

Наприклад, якщо хост з VLAN 10 відправляє широкомовний кадр, то він буде відправлений тільки на порти в цьому VLAN. Виходить, що нетеговані порти це «звичайні» порти комутатора. Це просто можливість повідомити комутатору про те, якому VLAN належать порти. Потім комутатор використовує цю інформацію при передачі кадрів.

Як правило, реально в таблиці комутації в комутаторах вказується порт, MAC-адреса і VLAN. Тобто, для зазначеного прикладу таблиця комутації буде така, як приведена в табл.2.13. Однак далі для спрощення використовується запис таблиці комутації у вигляді відповідності між портами і MAC-адресами.

Таблиця 2.13

Реальна таблиця комутації комутатора в схемі мережі, представленої на рис. 2.51

Порт комутатора	VLAN	MAC – адреса хоста
1	2	A
2	2	B
3	10	C
4	10	D

Розглянемо приклад налаштування VLAN на різних комутаторах. До мережі, наведеної на рис.2.51 додається ще один комутатор і хости в VLAN 2. Для початку доданий комутатор sw2 і два хости E і F в VLAN 2 (рис.2.52).

Якщо розглядати два комутатора окремо, то виходить, що на комутаторі sw1 залишилася колишня таблиця комутації, а на комутаторі sw2 таблиця така, як в табл. 2.14 (поки що комутатори пов'язані).

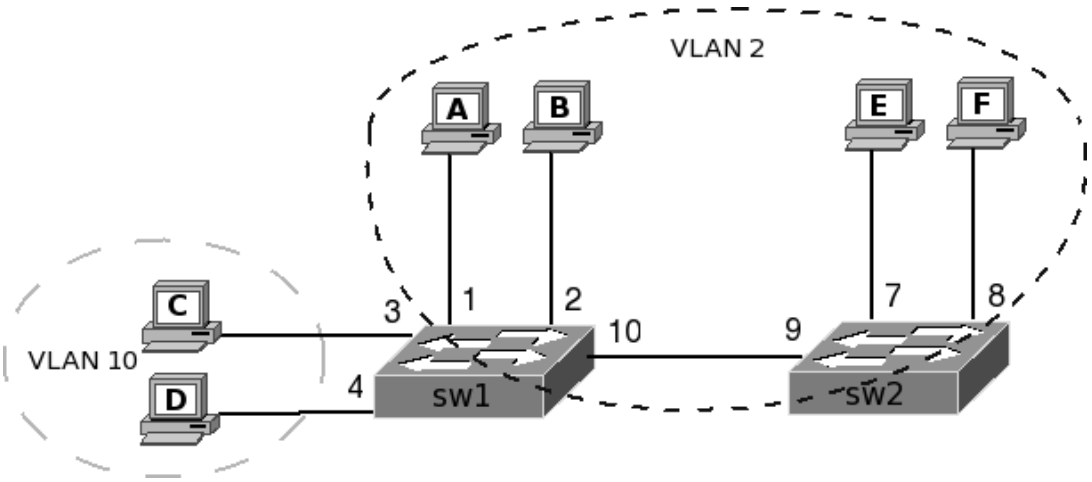


Рисунок 2.52 – Приклад мережі, в якій хости знаходяться в різних VLAN на різних комутаторах

Таблиця 2.14

Таблиця комутації для комутатора sw2 за умови, що комутатор sw1 і sw2 пов'язані

Порт комутатора	MAC – адреса хоста
7	E
8	F

Тепер необхідно щоб хости A, B, E, F «побачили» один одного. Вони повинні знаходитися в одному VLAN. Тобто, необхідно якимось чином вказати комутатору, що ще на одному порту є хости у відповідному VLAN.

Для зазначеного прикладу досить додати на комутаторі sw1 порт 10 в VLAN 2, а на комутаторі sw2 порт 9 в VLAN 2. Належність до VLAN вказується налаштуванням порту нетегованим в VLAN 2 (поки що). Після цього на комутаторах в таблицях комутації додадуться нові порти і відповідні MAC-адреси хостів (табл.2.15 і 2.16).Тепер чотири хости на різних комутаторах знаходяться в одному широкомовному сегменті.

Таблиця 2.15

Таблиця комутации sw1 для VLAN 2

Порт комутатора	MAC – адреса хоста
1	A
2	B
10	E
10	F

Таблиця 2.16

Таблиця комутации sw2 для VLAN 2

Порт комутатора	MAC – адреса хоста
7	E
8	F
9	A
9	B

Додамо до другого комутатора хости в VLAN 10 як показано на рис. 2.53. До комутатора sw2 додані два хости G і H в VLAN 10. Для того щоб хости C і D в VLAN 10, могли обмінюватися інформацією з хостами VLAN 10 доданий лінк між комутаторами. Таблиці комутації sw1 і sw2 для VLAN 10 наведені в табл.2.17 і 2.18.

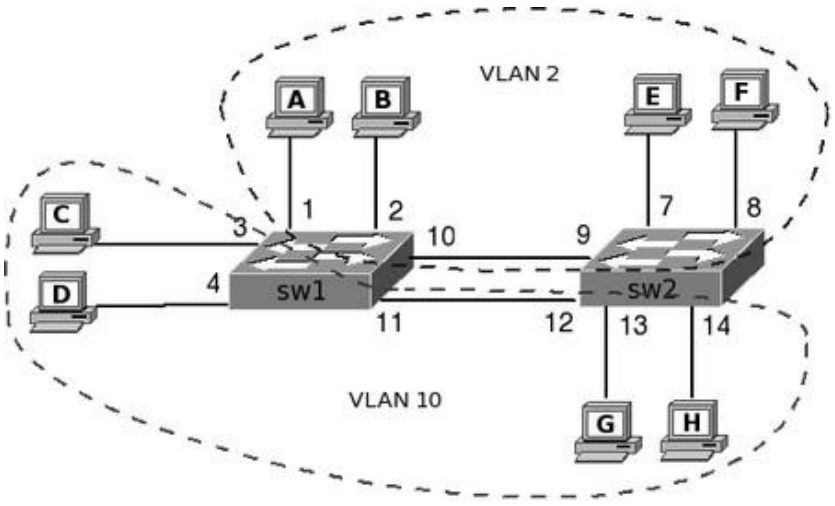


Рисунок 2.53 – Модифікована схема мережі з VLAN 2 і VLAN 10 на двох комутаторах

Таблиця 2.17

Таблиця комутації sw1 для VLAN 10

Порт комутатора	MAC – адреса хоста
3	C
4	D
11	G
11	H

Таблиця 2.18

Таблиця комутації sw2 для VLAN 10

Порт комутатора	MAC – адреса хоста
13	G
14	H
12	C
12	D

Коли необхідно передати трафік одного-двох VLAN між комутаторами, то схема, яка використовувалася вище, виглядає нормально. Однак, коли кількість VLAN зростає, то схема явно стає дуже незручною, оскільки для кожного VLAN треба буде додавати лінк між комутаторами для того, щоб об'єднати хости в один широкомовний сегмент.

Для вирішення цієї проблеми використовуються *теговані порти*.

Тегований порт дозволяє комутатору передати трафік декількох VLAN через один порт і зберегти при цьому інформацію про те, в межах якого саме VLAN передається фрейм.

Створимо тегований порт між комутаторами (рис. 2.54). На комутаторах sw1 і sw2 порти 21 і 22, відповідно, це теговані порти.

Для того, щоб комутатори розуміли до якого VLAN належить кадр і використовували відповідну таблицю комутації для його обробки, виконується *тегування кадру*.

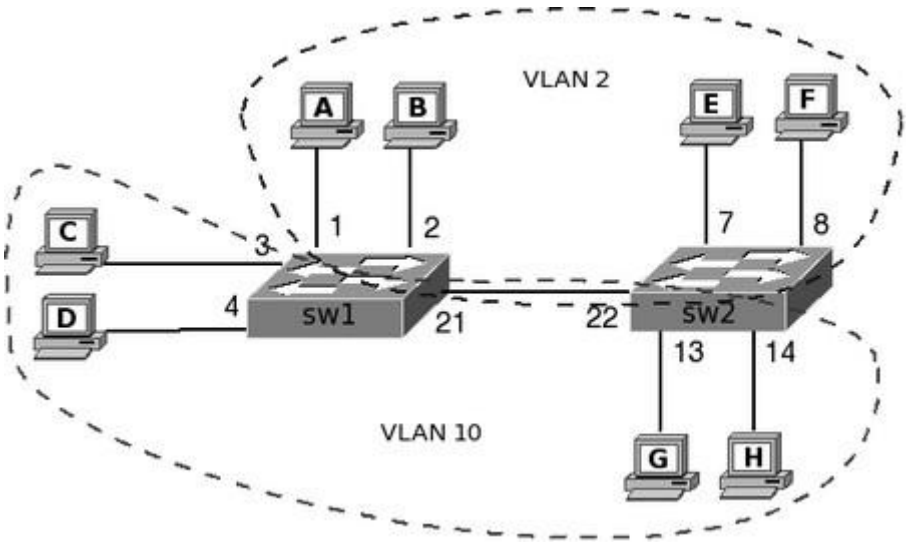


Рисунок 2.54 – Схема VLAN 2 і VLAN 10 з тегованим портом між комутаторами

Наприклад, якщо хост E передає фрейм хосту A, то комутатор sw2 перевіряє свою таблицю і бачить, що хост A доступний через порт 22. Так як порт налаштований як тегований, то коли кадр виходить з порту 22 в ньому проставляється тег, який вказує, якому VLAN належить цей кадр. В даному випадку проставляється тег з VLAN 2.

Комутатор sw1 отримує тегований фрейм через тегований порт 21 (рис.2.55). Для того щоб визначити на якій порт його передавати далі sw1 використовує таблицю комутації для VLAN 2 (тому що цей VLAN був вказаний в тезі). На комутаторі sw1 порт 21 повинен бути налаштований як тегований для того щоб комутатор не відкидав теговані фрейми, а зчитував інформацію тега. І відповідно щоб він також позначав фрейм тегом, коли буде передаватися трафік комутатора sw2.

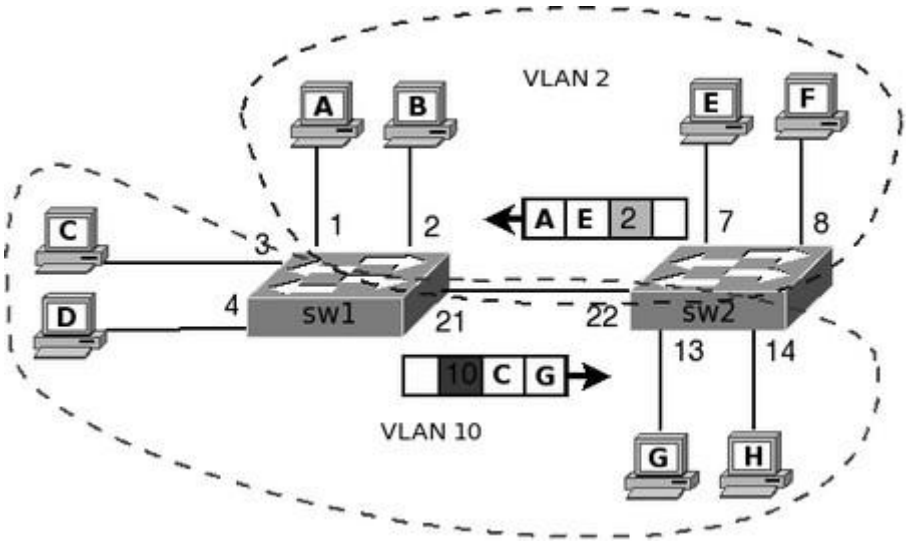


Рисунок 2.55 – Схема передачі тегованого фрейму

Решта портів комутатора залишаються нетегованими. І для хостів операція тегування, яку виконують комутатори, абсолютно прозора. Хости нічого не знають про тегі і отримують звичайні кадри.

Тобто, порти комутатора, що підтримують VLAN, (з деякими припущеннями) можна розділити на дві множини:

1) Теговані порти (або транкові порти, trunk-порти в термінології Cisco).

2) Нетеговані порти (або порти доступу, access-порти в термінології Cisco).

Теговані порти потрібні для того, щоб через один порт була можливість передати кілька VLAN і, відповідно, отримувати трафік

декількох VLAN на один порт. Інформація про приналежність трафіку VLAN, як було сказано вище, вказується в спеціальному тезі. Без тега комутатор не зможе розрізнити трафік різних VLAN.

Якщо порт нетегований в якомусь VLAN, то трафік цього VLAN передається без тега. На Cisco нетегованим порт може бути тільки в одному VLAN, на деяких інших комутаторах (наприклад, ZyXEL, D-Link і Planet) даного обмеження нема.

Існують два підходи до призначення порту певного VLAN:

– Статичне призначення – коли приналежність порту VLAN задається адміністратором в процесі настройки;

– Динамічне призначення – коли приналежність порту VLAN визначається в ході роботи комутатора за допомогою процедур, описаних у спеціальних стандартах, таких, наприклад, як 802.1X.

Ієрархічна модель мережі (Hierarchical internetworking model) – трирівнева модель організації корпоративної мережі (рис.2.56), яка вперше була запропонована інженерами Cisco Systems.

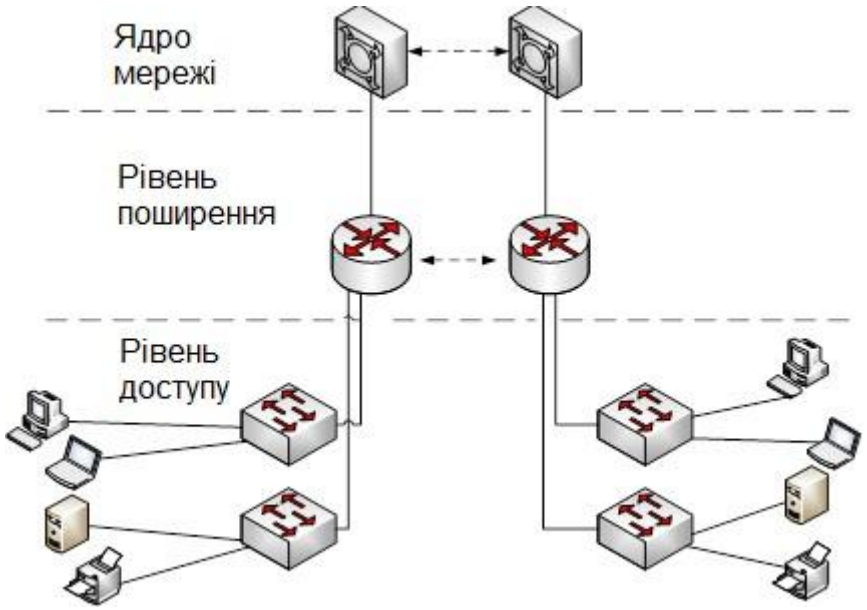


Рисунок 2.56 – Ієрархічна модель мережі

Відповідно до цієї моделі, мережа розбивається на три логічних рівня:

1) *ядро мережі (Core layer)* – високопродуктивні пристрої, головне призначення – швидкий транспорт;

2) *рівень поширення (Distribution layer)* – забезпечує застосування політик безпеки, QoS, агрегацію і маршрутизацію в VLAN, визначає широкомовні домени;

3) *рівень доступу (Access-layer)*, як правило, комутатори 2 рівня, призначення – підключення кінцевих пристроїв, маркування трафіку для QoS, захист від кілець в мережі (STP) і широкомовних штормів, забезпечення живлення для PoE пристроїв.

Ієрархічна модель мережі має багато переваг в порівнянні з «плоскою мережею»:

– спрощується розуміння організації мережі;

– модель передбачає модульність, що означає простоту нарощування потужностей саме там, де необхідно;

– легше знайти і ізолювати проблему;

– підвищена відмовостійкість за рахунок дублювання пристроїв та/або з'єднань;

– розподіл функцій щодо забезпечення працездатності мережі за різними пристроям.

Контрольні питання й завдання

1. Опишіть основні типи і характеристики коаксіальних і SPT та UPT кабелів. Чим різняться їхні конструкції?
2. Опишіть пристрій і експлуатаційні характеристики волоконно-оптичного кабелю.
3. Дайте визначення пропускної здатності лінії зв'язку. Зв'язок між пропускною здатністю та смугою пропущення лінії. Формула Шеннона. Формула Найквіста.
4. Методи цифрового кодування. Потенційні коди. У чому проявляється недолік потенційних кодів? Яким образом можна їх поліпшити?
5. Дайте характеристику методам логічного кодування. Яким способом логічне кодування сприяє поліпшенню потенційних кодів?
6. Дайте характеристику методам виявлення помилок. У чому полягають недоліки методу контролю за паритетом? Перерахуйте достоїнства методу циклічного надлишкового контролю.
7. Приведіть діаграми роботи методу "ковзного вікна".

8. У чому полягає подібність і відмінність між маркерним пріоритетним доступом до кільця в технологіях Token Ring і FDDI?
9. Дайте характеристику технології Token Ring: метод доступу, формати кадрів і фізичний рівень.
10. Опишіть особливості фізичного рівня технології FDDI.
11. Які особливості підключення вузлів до кільця FDDI? Яким образом способом забезпечується висока відказостійкість технології FDDI?
12. Назвіть зміни які відбулися у швидкості, формату кадра і методі доступа сучасних технологій сімейства Ethernet.
13. Які обмеження підключення мостів і комутаторів існують? Яким чином вони виконуються?
14. Назвіть відмінності між мостом і комутатором? Комутатором і маршрутизаторм?
15. Призначення віртуальних локальних мереж VLAN. Чим відрізняються теговані і нелеговані порти?

3 ОБ’ЄДНАНІ МЕРЕЖІ. ЗАСОБИ АНАЛІЗУ ТА КЕРУВАННЯ МЕРЕЖАМИ

3.1 Протоколи середнього та високого рівнів

3.1.1 Об’єднання мереж на основі мережевого рівня

Протокол IP – головний мережевий протокол стеку TCP/IP вирішує завдання доставки повідомлень між вузлами складеної мережі і відноситься до протоколів без встановлення з'єднання. Якщо модуль IP з якої-небудь причини не може доставити дейтаграмму, вона знищується. При цьому модуль IP може відправити комп'ютеру-відправнику цієї дейтаграми повідомлення про помилку; такі повідомлення відправляються за допомогою протоколу ICMP, що є невід'ємною частиною модуля IP. Більше ніяких засобів контролю коректності даних, підтвердження їхньої доставки, забезпечення правильного порядку проходження дейтаграм, попереднього встановлення з'єднання між комп'ютерами протокол IP не має. Це завдання покладене на транспортний рівень.

Важливою особливістю протоколу IP є його здатність виконувати динамічну фрагментацію пакетів при передачі їх між мережами з різними, максимально припустимими значеннями поля даних кадрів MTU (блок даних максимальної довжини). *Фрагментація* - це розподіл поля даних вихідного пакета на частини і оформлення цих частин у вигляді пакетів меншого розміру – фрагментів. Фрагментація виконується коли неможливо передати пакет у наступну за маршрутом мережу через те, що його розмір перевершує максимально припустимий розмір одиниці переданих даних MTU у цій мережі. Всі фрагменти переміщуються складеною мережею незалежно один від одного, тому деякі з них можуть прийти не в тому порядку, в якому їх відправляли, або зовсім загубитися. Протокол IP повинен забезпечувати відновлення вихідного пакета даних у вузлі призначення (або на проміжних маршрутизаторах) незалежно від того, скільки фрагментів потрібно було для його доставки до місця призначення. При збірці встановлюється таймер, що обмежує час очікування фрагментів. Якщо хоча б один фрагмент не дійде до вузла призначення вчасно, то всі фрагменти відкидаються.

Структура IP - пакета складається із заголовка і поля даних. Заголовок звичайно має довжину 20 байт і являє собою наступну структуру (рис.3.1).

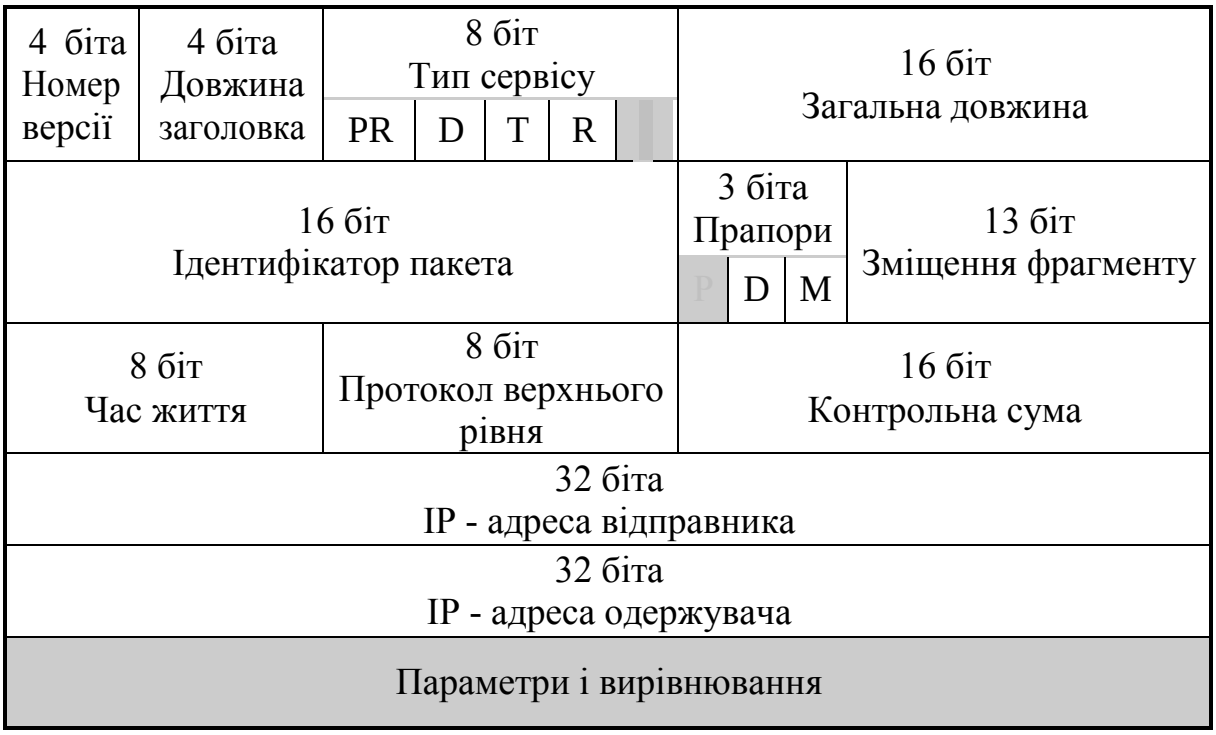


Рисунок 3.1 – Структура заголовка IP-пакета

Поле *Номер версії (Version)* – довжина 4 біти, містить версію протоколу IP (IPv4 або IPv6).

Поле *Довжина заголовка (IHL) IP-пакета* – довжина 4 біти, вказує значення довжини заголовка (у 32-бітових словах). Звичайно заголовок має довжину в 20 байт (п'ять 32-бітових слів). Найбільший заголовок займає 60 байтів за рахунок використання поля *Параметри (IP Options)*.

Поле *Тип сервісу (Type of Service)* займає один байт і вказує пріоритетність пакета та вид критерію вибору маршруту. Перші три біти цього поля утворюють підполе пріоритету пакета (Precedence). Пріоритет може мати значення від найнижчого – 0 (нормальний пакет) до найвищого – 7 (пакет керуючої інформації). Маршрутизатори і комп'ютери можуть брати до уваги пріоритет пакета і обробляти більш важливі пакети в першу чергу. Поле Тип сервісу містить також три біти, що визначають критерій вибору маршруту. Установлений біт D (delay) говорить про те, що маршрут повинен вибиратися для мінімізації затримки доставки даного пакета, біт T – для максимізації пропускної здатності, а біт R – для максимізації надійності доставки.

Поле *Загальна довжина (Total Length)* – довжина 2 байти, визначає загальну довжину пакета з урахуванням заголовка і поля даних. Максимальна довжина пакета становить 65 535 байт.

Поле *Ідентифікатор пакета (Identification)* – довжина 2 байти, використовується для розпізнавання пакетів, що утворилися шляхом фрагментації вихідного пакета. Всі фрагменти повинні мати однакове значення цього поля.

Поле *Прапори (Flags)* – довжина 3 біти, містить ознаки, пов'язані із фрагментацією. Установлений біт DF (Do not Fragment) забороняє маршрутизатору фрагментувати даний пакет, а встановлений біт MF (More Fragments) говорить про те, що даний пакет є проміжним (не останнім) фрагментом. Біт, що залишився, зарезервований.

Поле *Зміщення фрагменту (Fragment Offset)* – довжина 13 біт, задає зміщення у байтах поля даних цього пакета від початку загального поля даних вихідного пакета, підданого фрагментації. Використовується при збірці/розбиранню фрагментів пакетів при передачах їх між мережами з різними величинами MTU. Зміщення повинно бути кратне 8 байтам.

Поле *Час життя (Time to Live)* займає один байт і означає граничний строк, протягом якого пакет може переміщатися мережею. Час життя даного пакета виміряється у секундах, задається джерелом передачі та зменшується на 1 для кожного переходу (hop). Якщо параметр часу життя стане нульовим до того, як пакет досягне одержувача, цей пакет буде знищений, при цьому генерується і передається відправникові повідомлення ICMP.

Ідентифікатор *Протокол верхнього рівня (Protocol)* займає один байт і вказує, якому протоколу верхнього рівня належать дані після заголовка (наприклад, 6 – TCP, 17 – UDP, або 1 – ICMP).

Поле *Контрольна сума (Header Checksum)* займає 2 байти і розраховується тільки за вмістом заголовка. Оскільки деякі поля заголовка міняють своє значення в процесі передачі пакета мережею (наприклад, час життя), контрольна сума перевіряється і повторно розраховується при кожній обробці IP-заголовка. Якщо контрольна сума невірна, то пакет буде відкинутий, як тільки помилка буде виявлена.

Поля *IP-адрес відправника (Source IP Address)* і *IP-адрес одержувача (Destination IP Address)* мають однакову довжину - 32 біта і однакову структуру.

Поле *Параметри (IP Options)* є необов'язковим і використовується звичайно тільки при налагодженні мережі. Це поле складається з декількох підполей, кожне з яких може бути одного з восьми визначених типів. У цих підполях можна вказувати точний маршрут проходження маршрутизаторів, реєструвати прохідні пакети маршрутизаторів, поміщати дані системи безпеки, а також часові оцінки.

Поле *Вирівнювання (Padding)* використовується для того, щоб переконатися у тому, що IP-заголовок закінчується на 32-бітній границі. Вирівнювання здійснюється нулями.

Як видно із представленої структури заголовок IP-пакета містить IP-адресу одержувача, що далі використовується маршрутизаторами для визначення оптимального маршруту в мережі. Для просування пакетів вони використовують *таблиці маршрутизації*.

3.1.2 Протоколи маршрутизації

Головне призначення маршрутизаторів локальних комп'ютерних мереж – вибір маршруту проходження пакетів на основі таблиць маршрутизації. В таблицях маршрутизації вказується напрямок передачі пакета для конкретної мережі, групи мереж (CIDR) або для всіх невідомих мереж (маршрут «за замовчуванням»). Приймаючи рішення про передачу кожного пакета мережевий пристрій переглядає свою локальну таблицю маршрутизації і вибирає підходящий напрямок.

Для повноцінного функціонування комп'ютерної мережі необхідно забезпечити коректне конфігурування таблиць маршрутизації всіх мережевих пристроїв. Якщо в конфігурації мережі відбуваються які-небудь зміни, то вони повинні бути внесені в усі таблиці, які ці зміни зачіпають. Очевидно, що в мережах, в яких зміни конфігурації відбуваються часто, необхідно забезпечити автоматичну реконфігурацію таблиць маршрутизації.

Для автоматичної настройки своїх таблиць маршрутизатори повинні регулярно обмінюватися ними. Для цього розроблені спеціальні протоколи. Незважаючи на те що маршрутизація включає в себе два етапи: формування таблиць і вибір маршрутів, протоколи обміну таблицями часто називають *протоколами динамічної маршрутизації*.

Обмінюючись таблицями маршрутизації і формуючи свою власну таблицю маршрутизатор вибирає до кожної з відомих йому мереж найкращий маршрут. Очевидно, що найкращим маршрутом між двома

точками є найкоротший маршрут – маршрут, який має найменшу відстань. Відстань між мережами в різних протоколах вимірюється по-різному. У будь-якому випадку відстань між мережами складається з характеристик всіх каналів передачі інформації, які необхідно подолати, щоб досягти необхідну мережу.

Характеристику каналу, що використовується для визначення відстані, називають *метрикою*.В якості метрики може використовуватися середнє арифметичне значення або показник пропускної здатності і/або надійність каналу. У деяких протоколах вводиться додаткова метрика, що характеризує недосяжність мережі. Також може використовуватися нульова метрика, що характеризує безпосереднє підключення маршрутизатора до мережі. Зазвичай, чим менше метрика, тим менше відстань.

Головне завдання протоколів маршрутізації – формування узгоджених таблиць маршрутизації. *Узгоджена таблиця* – це така таблиця, яка забезпечує передачу даних між мережами за кінцеве число кроків (*хопів*). При змінах в мережі таблиці стають неузгодженими, тобто передача даних між деякими мережами виявляється неможливою.

Час, протягом якого таблиці приводяться в узгоджений стан називається *часом конвергенції* (або *збіжності алгоритму*).

Класифікація протоколів динамічної маршрутизації. Маршрутизатор, використовуючи протоколи динамічної маршрутизації, збирають інформацію від своїх сусідів (маршрутизаторів, що мають безпосереднє підключення) про топології мережі зв'язків, обробляють її і формують своє «бачення» конфігурації мережі.

У сформованій таким чином таблиці маршрутизації кожному маршруту виставляється період часу, протягом якого він буде існувати на даному маршрутизаторі. Це робиться, в першу чергу для того, щоб гарантувати, що якщо маршрутизатор, який повідомив про існування цієї мережі з яких-небудь причин більше не буде підтверджувати цей факт, то маршрут буде визнаний неіснуючим (і видалений з таблиці).

Протоколи динамічної маршрутизації можна розділити на два великих класи: *централізовані* та *розподілені*.

У першому випадку в мережі вибирається один з маршрутизаторів, який формує у себе таблицю маршрутів і поширює її між іншими маршрутизаторами мережі. Інші маршрутизатори, при цьому, не

виконують ніяких побудов таблиць маршрутизацій, а лише використовують отриману таблицю.

У розподілених алгоритмах все маршрутизатори перебувають у рівних умовах і кожен з них самостійно будує таблицю маршрутизації. Очевидно, що надійність розподілених алгоритмів маршрутизації вище, ніж у централізованих (в них при виході з ладу центрального маршрутизатора вся мережа виявляється непрацездатною).

Розподілені протоколи динамічної маршрутизації можна розділити на два класи: *дистанційно-векторні алгоритми (Distance Vector Algorithm, DVA)* та *алгоритми станів зв'язків (Link State Algorithm, LSA).*

У дистанційно-векторних алгоритмах кожен маршрутизатор регулярно розсилає вектор, в якому вказує відстань до всіх (або деяких) відомих йому мереж всім своїм сусідам. Формування таблиць маршрутизації засновано на *алгоритмі Беллмана-Форда-Мура*. Отримавши вектор кожен маршрутизатор збільшує значення відстаней з урахуванням відстані «до себе» і формує свою таблицю маршрутизації, вибираючи найкращий маршрут до кожної мережі. Зрештою, кожен маршрутизатор дізнається через сусідні маршрутизатори інформацію про всі наявні мережі і про відстані до них.

Дистанційно-векторні алгоритми застосовні для невеликих мереж. Обмеження пов'язане з тим, що зі збільшенням кількості мереж, про які необхідно передавати інформацію обсяг трафіку і час конвергенції алгоритму різко збільшуються.

До дистанційно-векторного відносяться протоколи: *RIP, IGRP, BGP, AODV* і ін.

В алгоритмах, заснованих на стані зв'язків, кожен маршрутизатор розсилає інформацію тільки про мережі, до яких він має безпосередній зв'язок. В результаті кожен маршрутизатор самостійно будує топологію мережі і вибирає найменші відстані до кожної мережі. Для розрахунку відстаней використовується *алгоритм Дейкстри*.

До протоколів, заснованим на станах каналів зв'язків, відносяться *IS-IS, OSPF, NLSP, OLSR* і ін.

Деякі протоколи маршрутизації реалізують як елементи дистанційно-векторних алгоритмів, так і алгоритмів на основі станів каналів. Прикладом таких протоколів можна назвати – *EIGRP*.

Протокол RIP (Routing Information Protocol) відноситься до дистанційно-векторного протоколу динамічної маршрутизації. Вважається,

що він найпоширеніший протокол в невеликих комп'ютерних мережах. Вперше протокол був запропонований в 1969 році як основний для мережі ARPANET.

В якості метрики протокол використовує ціле число з діапазону від 0 до 15. Число 16 задає нескінченну довжину маршруту. Зазвичай для каналів використовуються поодинокі метрики, в результаті вважається, що максимальна довжина маршруту, тобто кількість переходів (маршрутизаторів) між двома будь-якими мережами, не може бути більше 15.

За замовчуванням кожен маршрутизатор широкомовно розсилає свій вектор в мережу кожен 30 секунд. Протокол працює на прикладному рівні моделі OSI, використовує в якості транспорту протокол UDP і за службою, що реалізує протокол RIP, закріплений порт номер 520.

Існує три версії цього протоколу з власними форматами пакетів:

– RIP версії 1. Забезпечує передачу інформації про мережі, що описуються класовим способом. Протокол описаний в RFC 10582;

– RIP версії 2. Підтримує маски мереж змінної довжини і авторизацію маршрутизаторів. Протокол описаний в RFC 24533;

– RIPng. Підтримує IP версії 6.

Протоколом передбачається дві команди (поле «команда» пакета RIP): запит вектора і відповідь вектора. Також в пакеті RIP наступними полями вказуються: версія протоколу, що використовується, ідентифікатор системи адресації вузлів (для TCP/IP заданий код 2) і значення вектора. Одним пакетом може передаватися вся таблиця або її частина (якщо вона містить інформацію про більш ніж 25 мереж).

Команда запиту використовується маршрутизатором для отримання таблиць маршрутизації від своїх сусідів за власною ініціативою. Потреба використання цієї команди може виникнути в момент включення маршрутизатора (або початку роботи на ньому демона RIP) або в разі пошкодження поточної таблиці.

Команда відповіді використовується для формування відповіді на запит або для регулярного поширення свого вектора.

Формат елемента вектора залежить від версії протоколу. Всі версії першим полем вказують тип адресації вузлів, що використовується в мережі. Для стандарту TCP/IP заданий тип з номером 2. У версії 1 кожен елемент містить ідентифікатор мережі (відповідає одному з класів мережі)

і метрику (відстань до мережі). У версії 2 вказуються поля «маска підмережі», «адреса маршрутизатора » (next hop), а також вказується тип маршруту (домен маршрутизації):«зовнішній» або «внутрішній». Зовнішній маршрут запозичений граничним маршрутизатором із інформації іншого протоколу маршрутизації.

Маршрутизатор, що працює за протоколом версії 2, здатний обробляти інформацію, відправлену в форматі протоколу версії 1.

Робота маршрутизатор, що підтримує протокол RIP, виконується в декілька етапів.

1) Створення мінімальної таблиці. На цьому етапі маршрутизатор формує початковий вектор, в який включає інформацію про всі мережі, до яких він має безпосереднє підключення. Кожен комутатор таку таблицю формує самостійно.

2) Розсилка власної таблиці своїм сусідам. Після того, як сформований локальний вектор він регулярно розсилається через все інтерфейси маршрутизатора (які беруть участь у формуванні топології мережі).

3) Отримання і обробка векторів від своїх сусідів. Отримавши вектор від свого сусіда, маршрутизатор збільшує значення метрик з урахуванням метрики каналу, через який надійшло RIP-повідомленя.

В результаті обробки вектора маршрутизатор може виявити кілька шляхів до якої-небудь мережі. У підсумкову таблицю маршрутизатор включає тільки один найкращий маршрут до кожної мережі. Найкращим вважається маршрут, який має найменше значення метрики і йде через маршрутизатор, з найбільшим значенням мережевої адреси (ідентифікатора маршрутизатора).

Далі етапи 2 і 3 виконуються циклічно. В результаті періодичної розсилки, отриманню і обробці векторів за кінцевий час маршрутизатор отримує робочу таблицю маршрутизації.

Важливою здатністю протоколів динамічної маршрутизації є можливість автоматичного реагування на зміни, що відбулися в топології мережі. Якщо який-небудь маршрутизатор виявляє, що якісь з його інтерфейсів переходять в неробочий стан, то він змінює власну таблицю маршрутизації і розсилає змінений вектор за всіма своїми робочим інтерфейсам.

У разі, якщо відбулися які-небудь зміни до існуючих маршрутів, то вони вказуються в новому векторі і доводяться до відома всіх маршрутизаторів.

Ситуація зникнення будь-яких маршрутів складніше. Формат пакета дозволяє передати інформацію тільки про існуючі маршрути і ніяк не дозволяє повідомити про їх зникнення.

Для виключення інформації про будь-який маршрут використовується два механізми:

– таймер життя (TTL) маршруту в динамічної таблиці маршрутизації;

– передача маршруту з метрикою, відповідної нескінченної відстані до мережі.

Механізм TTL маршруту передбачає наявність в таблиці маршрутизації додаткового поля, що вказує скільки часу вказаний маршрут буде вважатися чинним. Якщо протягом цього часу ніхто не почув ні від одного з сусідів інформації про існування цього маршруту, то маршрут позначається як недійсний. Якщо отримано повідомлення з таким маршрутом, то таймер TTL починає відраховуватися заново.

Час життя маршруту вибирається кратним часу розсилки RIP повідомлень по мережі. За замовчуванням TTL дорівнює 180 секундам (6-ти кратний період розсилки повідомлень).

Використання TTL для маршрутів працює добре, але вимагає великого інтервалу часу для реагування на зміни в мережі. Припустимо, що один з маршрутизаторів мережі з якої-небудь причини перестав розсилати інформацію про маршрути, які проходили через нього. Його сусідні маршрутизатори переведуть всі ці маршрути в недійсне стан через 180 секунд. Їхні сусіди переведуть маршрути в недійсне стан вже через 360 секунд і так далі.

Щоб прискорити процес сходження маршрутизатори, які продовжують розсилати свої вектори і виявляють, що будь-якої маршрут стає недійсним продовжують розсилати інформацію про нього, але ставлять йому метрику 16 (тобто вказують, що маршрут недосяжний). В результаті час реакції маршрутизаторів скорочується.

Отримавши повідомлення про недосяжність деякої мережі маршрутизатор змінює свій вектор тільки в тому випадку, якщо спочатку він дізнався про цей маршрут від того ж маршрутизатора. Якщо інформацію про недосяжність маршруту прийшла від іншого сусіда, то

вона ігнорується (тобто у власній таблиці є маршрут з кращим значенням вектора).

Протокол OSPF. Популярним протоколом динамічної маршрутизації в локальних мережах є протокол *Open Shortest Path First (OSPF)*. Протокол був розроблений IETF в 1988 році. Остання версія протоколу представлена в RFC 23284. Протокол OSPF має менший час збіжності, ніж протокол RIP. Крім того, OSPF спочатку враховує опис мереж за допомогою масок змінної довжини (VLSM). Протокол OSPF відноситься до протоколів стану каналів. Основна ідея протоколів цього класу полягає в тому, що маршрутизатори розсилають інформацію про стан своїх каналів і ретранслюють повідомлення про стан каналів інших маршрутизаторів. В результаті кожен маршрутизатор відповідає тільки за власні канали, але має інформацію про стан каналів всіх своїх сусідів.

Зібравши інформацію від своїх сусідів маршрутизатор самостійно будує своє бачення топології мережі і вибирає найкоротший маршрути до всіх відомих йому мереж. Пошук маршруту в OSPF проводиться за допомогою алгоритму Дейкстра. Слід зазначити, що протокол OSPF підтримує три типи мереж: широкомовні (Ethernet, Token Ring), точка-точка (T1, E1) і мережі з множинним доступом (Frame Relay). Далі розглядається робота протоколу OSPF тільки в широкомовних мережах.

Для функціонування протоколу OSPF кожен маршрутизатор збирає інформацію про стан своїх каналів зв'язків, сусідніх маршрутизаторів і каналів зв'язків, наявних у сусідніх маршрутизаторів. Стан каналу – це опис мережевого інтерфейсу і його відносин з сусідніми маршрутизаторами. Опис інтерфейсу включає, наприклад, його IP-адресу, маску, тип мережі, до якої він підключений, маршрутизатори, підключені до цієї мережі і т.п. В результаті кожен маршрутизатор збирає у себе інформацію про всі мережі.

Колекція всіх станів каналів являє собою базу даних станів каналів. Мета роботи OSPF – забезпечити повну синхронізацію баз даних станів каналів на всіх маршрутизаторах мережі. В результаті кожен маршрутизатор розрахує свою таблицю маршрутизації.

Кожен маршрутизатор несе відповідальність тільки за власні канали. Якщо він виявляє будь-які зміни в них, то він повідомляє про це всім своїм сусідам. Повідомлення, за допомогою яких поширюється інформація про стан каналів, називаються *оголошеннями про стан зв'язків* (*Link State*

Advertisement, LSA). LSA поширюються усім сусідам за допомогою спеціальної групової адреси – 224.0.0.5.

Для скорочення обсягів переданої службової інформації і часу збіжності алгоритму пошуку найкоротших шляхів протокол OSPF передбачає поділ мережі на непересічні області – *зони* (*Area*). Маршрутизатор, інтерфейси яких належать до різних областей OSPF називаються *прикордонними* (*Area border router, ABR*). Маршрутизатор, все інтерфейси якого знаходяться в одній зоні називається *внутрішнім* (*Internal router, IR*).

Щоб скоротити обсяги переданої по мережі службової інформації і часу її поширення до всіх маршрутизаторів зони всередині кожної зони будується топологія зв'язків маршрутизаторів. Всі маршрутизатори встановлюють зв'язок один з одним. Один з маршрутизаторів мережі вибирається *головним* (*призначеним, Designated Router, DR*). Основним завданням цього маршрутизатора є ведення еталонної бази даних станів каналів. Всі маршрутизатори регулярно повідомляють один одному про своє існування. Про всі зміни в своїх каналах зв'язків і про те, що будь-якої комутатор припинив надсилати інформацію про своє існування маршрутизатори зони повідомляють своєму DR, а він уже повідомляє про це іншим маршрутизаторам зони.

Головний маршрутизатор зони визначається шляхом виборів в початковій стадії функціонування протоколу OSPF. Критерієм вибору є пріоритет маршрутизатора і його ідентифікатор. Ідентифікатором маршрутизатора, за замовчуванням, є його найбільша (в числовому виразі) IP адреса. Головним вибирається маршрутизатор, який має найбільше значення пріоритету і ідентифікатора. Вибори головного маршрутизатора ініціюються або в разі відмови DR, або за його ініціативою.

Очевидно, що централізація управління мережі негативно позначається на її надійності. Тому в мережі додатково вибирають *резервний головний маршрутизатор* (*Backup Designated Router, BDR*), який зберігає копію еталонної бази зв'язків каналів і починає працювати в разі виходу з ладу DR. Маршрутизатор DR і BDR обмінюються еталонною базою використовуючи спеціальну групову адресу – 224.0.0.6. Запасний BDR вибирається аналогічно DR.

В алгоритмі OFPS метрика каналу зв'язку обернено пропорційна його пропускної здібності. Формула для розрахунку метрики: метрика = 100 000 000 / пропускна здатність в біт/с. Наприклад, вартість передачі

даних через 10-ти мегабітний канал Ethernet – $10^8/10^7 = 10$, вартість передачі даних через канал T1 – $10^8/1544000 = 64$.

Метрика каналу може здаватися адміністратором вручну.

Основна робота маршрутизатора при реалізації алгоритму OSPF полягає в моніторингу станів каналів зв'язків і інформуванні сусідніх маршрутизаторів про зміни в них.

Для контролю станів каналів зв'язків все маршрутизатори регулярно обмінюються невеликими службовими повідомленнями. Отримавши таке повідомлення від свого сусіда маршрутизатор вважає, що його сусід є працездатним і ніяких змін з його каналами зв'язків не відбулося. Переставши отримувати такі повідомлення або виявивши зміни в своїх каналах зв'язків маршрутизатор «б'є на сполох» і повідомляє про це всіх своїх сусідів (через DR). Ці ж службові повідомлення використовуються для «знайомства» маршрутизаторів.

Отримавши повідомлення від невідомого сусіда, що відноситься до тієї ж зоні, маршрутизатор встановлює з ним двосторонній зв'язок (тобто вони запам'ятовують інформацію один про одного, визначають свої ролі у відношенні один до одного і синхронізують LSADB). Вважається, що сусід відноситься до тієї ж зоні, якщо повідомлення було отримано через допустимий інтерфейс і в повідомленні вказані правильні значення службових полів.

Протокол працює на мережевому рівні (має свій код - 89). Інформація передається або в режимі Юнікаст (конкретному маршрутизатора) або многоадресной розсилкою в групах: 224.0.0.5 (всі OSPF маршрутизатори мережі) і 224.0.0.6 (всі маршрутизатори, які мають роль DR або BDR). Існує три версії протоколу, перші дві з яких підтримують IP версії 4, а третя - IP версії 6.

3.1.3 Протоколи транспортного рівня

Завданням протоколів транспортного рівня є забезпечення прозорої (наскрізної) доставки даних (end-to-end delivery service) між двома прикладними процесами. Процес, що одержує або відправляє дані за допомогою транспортного рівня, ідентифікується на цьому рівні номером, що називається *номером порту*. Таким чином, роль адреси відправника і одержувача на транспортному рівні виконує номер порту (або простіше - *порт*).

Аналізуючи заголовок свого пакета, отриманого від мережевого рівня, транспортний протокол визначає за номером порта одержувача, якому спрямовані дані, і передає ці дані відповідному прикладному процесу (можливо, після перевірки їх на наявність помилок і т.п.).

Номера портів можна призначати процесам довільно, але для полегшення взаємодії між різними програмами прикладного рівня прийняті угоди про номери портів, які закріплені за певними службами Internet. За *загальнодоступними службами*, такими як FTP, telnet, HTTP, DNS і ін. централізовано закріплені стандартні *привласнені (assigned) номера*. Для інших додатків і служб номера портів виділяються локальною операційною системою. Такі номери називають *динамічними (dynamic)*. У форматі повідомлення протоколу TCP під номер порту виділяється 16 біт, тому максимально можливим номером порту є число 65535.

Немає ніякої залежності між призначенням номерів портів для додатків, що використовують протокол TCP, і додатків, що працюють із протоколом UDP. Перші одержують номери, які називаються портами TCP, другі – портами UDP.

Протоколи TCP і UDP ведуть для кожного номера порту дві черги: черга пакетів, що надходять у даний порт з мережі, і черга пакетів, що відправляються даним портом у мережу. Процедура прийому даних протоколом TCP (або UDP), що надходять від декількох прикладних служб, називається *мультиплексуванням*. Зворотна процедура розподілу протоколом TCP (або UDP) пакетів, що надходять від мережевого рівня, між набором служб, ідентифікованих номерами портів, називається *демультиплексуванням* (рис. 3.2).

Протокол TCP. Будь-який канал зв'язку в TCP визначається двома числами – ця комбінація називається *сокетом (socket)*. Таким чином, сокет визначається IP-адресою вузла і номером порту, що використовується програмним забезпеченням TCP. При з'єднанні будь-яка машина однозначно визначена IP-адресою, а кожний процес – портом, тому з'єднання між двома процесами однозначно визначається сокетом. Наприклад, якщо кілька машин пошлють запити на з'єднання, у яких зазначені однакові порти джерела і одержувачі, плутанини із з'єднаннями не виникає, тому що IP-адреси у всіх машин різні, отже, кожне з'єднання буде однозначно визначено своїм сокетом.

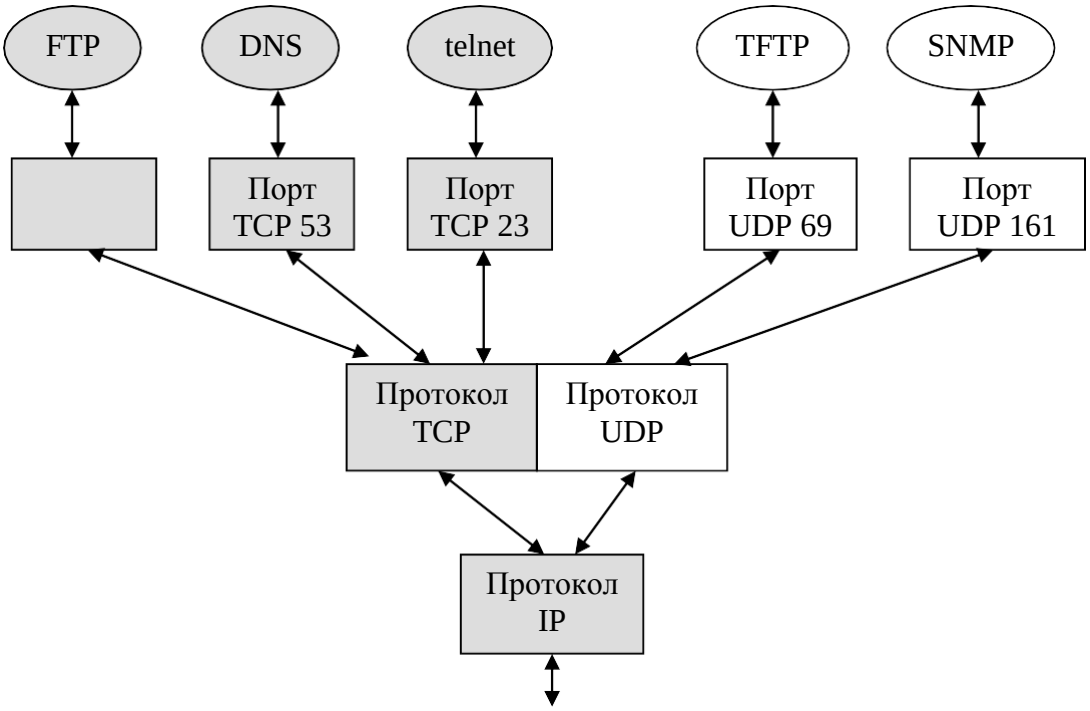


Рисунок 3.2 – Мультиплексування та демультиплексування на транспортному рівні

Таким чином, процес обміну даними за протоколом TCP починається з передачі запиту на встановлення з'єднання від машини-відправника до машини-одержувача. У запиті міститься ціле число – номер сокета**.** У відповідь одержувач посилає номер свого сокета. Номера сокетів відправника і одержувача однозначно визначають з'єднання. Після встановлення з'єднання TCP починає передавати сегменти повідомлення. На більш низькому IP-рівні відправника сегменти розбиваються на одну або декілька дейтаграм. Пройшовши через мережу, дейтаграми надходять до одержувача, де IP-рівень знову збирає з них сегменти і передає їх TCP. TCP збирає всі сегменти в повідомлення. Від TCP повідомлення надходить до процесу-одержувача, де обробляється протоколом прикладного рівня.

Інформація, що надходить до протоколу TCP у рамках логічного з'єднання від протоколів більш високого рівня, розглядається протоколом TCP як неструктурований *потік* байтів. Дані, що надходять, буферизуються засобами TCP. Для передачі на мережевий рівень із буфера "вирізається" деяка безперервна частина даних, що називається *сегментом***.** Два взаємодіючих пристроя задають порядковий номер для кожного переданого сегмента, і цей номер записується в заголовок TCP. Порядковий номер не тільки показує місце розташування сегмента в потоці

сегментів, але й указує на довжину даних, що містяться в ньому. Одержавши сегмент вузол перевіряє порядковий номер і переконується в тому, що отримано правильний сегмент у правильній черговості. Якщо вузол призначення приймає сегмент, він передає підтвердження передавальному вузлу (так звану *позитивну квитанцію*). Квитанція не тільки свідчить про успішний прийом, але й містить порядковий номер наступного сегмента, передачу якого очікує приймаючий вузол.

Кількість байтів даних, переданих у сегменті, називається *ковзним вікном (sliding window)*, оскільки ця кількість може збільшуватися або зменшуватися в процесі обміну інформацією із взаємної згоди між взаємодіючими вузлами. Розмір ковзного вікна визначається, вузлами динамічно, при цьому враховуються два фактори: поточний мережевий трафік і розмір буфера (звичайно в пам'яті), що в даний час може виділити кожний вузол для зберігання сегментів, які очікують обробки даним вузлом.

Заголовок TCP (рис.3.3) має мінімальну довжину 20 байтів.

Порт TCP відправника				Порт TCP одержувача
Порядковий номер				
Підтверджений номер				
Зміщення			Прапори/ керування	Розмір вікна
Контрольна сума				Покажчик терміновості
Параметри і заповнення				
Дані				

Рисунок 3.3 – Структура заголовка TCP

Поле *Порт TCP відправника (Source Port)* – 16-розрядний номер порту TCP на передавальному пристрої.

Поле *Порт TCP одержувача (Destination Port)* – 16-розрядний номер порту TCP на приймаючому пристрої.

Поле *Порядковий номер (Sequence Number)* – 32-розрядний послідовний номер, що призначається кожному сегменту в процесі передачі даних. З його допомогою протокол TCP забезпечує надійність прийому всіх сегментів. Порядковий номер також використовується для виявлення дублікатів і для розташування сегментів у потрібному порядку

після того, як вони були передані за різними мережевими маршрутами або каналами.

Поле *Підтверджений номер (Acknowledgement Number)* – число, що підтверджує одержання сегмента, і передається протоколом TCP вихідному вузлу після перевірки порядкового номера сегмента. Якщо підтверджений номер не відправляється назад, то виконується повторна передача сегмента.

Поле *Зміщення (Offset)* або *Довжина заголовка (Header Length)* займає 4 біти і містить число, що визначає довжину заголовка. З його допомогою можна швидко визначити початок даних, переданих у сегменті.

Поле *Прапори/керування (Flags/control)* займає 6 бітів. Два прапори в цьому полі використовуються для позначення початку *(SYN)* і кінця *(FIN)* повного потоку даних. Інші 4 прапори є керуючою інформацією (наприклад, для розрива з'єднання або для відображення активності поля покажчика терміновості).

Поле *Розмір вікна (Window)* займає 2 байти і використовується одержувачем для передачі відправникові інформації про те, який обсяг даних він готовий прийняти в одному сегменті TCP.

Поле *Контрольна сума (Checksum)* – 16-розрядний *циклічний надлишковий код (CRC)*, що обчислюється шляхом додавання всіх полів заголовка та поля даних (сума всіх полів TCP-сегмента). Загальна CRC-сума записується в сегмент передавальним вузлом. Приймаючий вузол також обчислює контрольну суму і порівнює отримане значення зі значенням, записаним у поле сегмента. Якщо значення розрізняються, то сегмент відкидається і приймаючий вузол запитує повторну передачу.

Поле *Покажчик терміновості (Urgent Pointer)* – це 16-розрядне поле заголовка, що представляє собою попередження для приймаючого вузла про те, що передаються термінові дані. Воно також указує на кінець термінових даних у послідовності сегментів, що пересилаються. Призначення цього поля – заздалегідь дати інформацію про те, скільки даних ще буде передано в логічно зв'язаній послідовності з декількох сегментів.

Поле *Параметри (Options)* – поле сегмента, що може містити додаткову інформацію про передані дані, а також додаткові прапори.

Поле *Заповнення (Padding)* – поле, що використовується в тих випадках, коли додаткові дані відсутні або їх занадто мало, щоб забезпечити необхідну довжину заголовка, що повинна бути кратна 32.

Підтвердження протоколу TCP можуть створити в мережі помітний додатковий трафік, особливо, якщо середній розмір ковзного вікна відносно малий. Саме тому деякі типи додатків, для яких не потрібен рівень надійності, що забезпечується протоколом TCP (за допомогою механізмів упорядкування та підтвердження), використовують протокол *User Datagram Protocol (UDP).*

Протокол UDP є більш простим транспортним протоколом, чим протокол TCP. Завданням протоколу UDP є передача даних між прикладними процесами без гарантій доставки, тому його пакети можуть бути загублені, продубльовані або прийти не в тому порядку, у якому вони були відправлені.

Структура заголовка UDP представлена на рис.3.4.

Порт UDP відправника (2 байта)	Порт UDP одержувача (2 байта)	Контрольна сума (2 байта)	Довжина повідомлення (2 байта)

Рисунок 3.4– Структура заголовка протокола UDP

Поле *Порт UDP відправника (Source Port)* – номер порту процеса-відправника.

Поле *Порт UDP одержувача (Destination Port)* – номер порту процеса-одержувача.

Поле *Контрольна сума (Cheksum)* – контрольна сума. Контрольна сума одержується у результаті математичних обчислень над вмістом сегмента (також як і в TCP-заголовку), якщо UDP-пакет має непарну довжину, то при обчисленні контрольної суми до нього додається нульовий октет. Потім аналогічні обчислення виконуються одержувачем. Розбіжність двох результатів означає, що в процесі пересилання відбулася помилка.

Поле *Довжина повідомлення (Length)* – довжина UDP-пакета разом із заголовком в октетах. Забезпечує додаткову можливість для перевірки правильності повідомлення.

Після заголовка безпосередньо ідуть користувальницькі дані, передані модулю UDP прикладним рівнем за один виклик. Протокол UDP розглядає ці дані як цілісне повідомлення; він ніколи не розбиває

повідомлення для передачі в декількох пакетах і не поєднує кілька повідомлень для пересилання в одному пакеті.

Додатки, у яких реалізований власний, досить надійний, механізм обміну повідомленнями, заснований на встановленні з'єднання, для безпосередньої передачі даних по мережі віддають перевагу менш надійному, але більш швидкому засобу транспортування, у якості якого і виступає протокол UDP. Із цієї причини він добре підходить для додатків, критичних за часом, – таких, як передача голосових даних Voi (Voice over IP) і відеоконференцій у реальному часі. Протокол UDP може бути використаний і в тому випадку, коли гарна якість каналів зв'язку забезпечує достатній рівень надійності і без застосування додаткових прийомів типу встановлення логічного з'єднання та квитування переданих пакетів.

Приклади прикладних процесів, що використовують протокол UDP: NFS (Network File System – мережева файлова система), TFTP (Trivial File Transfer Protocol – простий протокол передачі файлів), SNMP (Simple Network Management Protocol – простий протокол керування мережею), DNS (Domain Name Service – доменна служба імен).

3.1.4 Організація сервісних служб в мережі Інтернет

Протоколи TCP/IP призначені для роботи з безліччю прикладних протоколів, що забезпечують передачу електронної пошти, емуляцію терміналів, передачу файлів і виконання інших завдань. Нижче перераховані деякі з основних протоколів і прикладних служб, що входять у стек TCP/IP:

– протокол Telnet;

– протоколи File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) і Network File System (NFS);

– протокол Simple Mail Transfer Protocol (SMTP);

– протокол Hypertext Transfer Protocol (HTTP).

Далі перераховані протоколи і додатки розглядаються більш докладно .

Протокол Telnet – один із самих ранніх прикладних протоколів стека TCP/IP, що забезпечує емуляцію терміналів. *Термінал* – це пристрій, що складається з монітора та клавіатури і використовується для взаємодії з хост- комп'ютерами (звичайно мейнфреймами або міні-комп'ютерами), на яких виконуються програми. Програми запускаються на хості, оскільки термінали, як правило, не мають власного процесора.

При емуляції терміналів використовуються програмні засоби, за допомогою яких деякий комп'ютер (наприклад, персональний) може функціонувати як термінал. Протокол Telnet дозволяє клієнтові підключитися до хост-комп'ютеру, при цьому реакція хоста буде такою ж, як і при підключенні термінала.

Протокол Telnet використає надійний транспорт TCP, оскільки він повинен підтримувати надійний, стабільний зв'язок. За замовчуванням Telnet використовує порт TCP 23 на передавальному і приймаючому вузлах.

Протокол Telnet функціонує поверх TCP/IP і має дві важливі особливості, відсутні в інших емуляторах: він присутній практично в кожній реалізації стека TCP/IP, а також є відкритим стандартом (тобто кожний виробник або розроблювач легко може, реалізувати його). Для деяких реалізацій Telnet потрібно, щоб хост був конфігурований як Telnet-сервер. Протокол Telnet підтримується багатьма робочими станціями, що працюють під керуванням MS-DOS, UNIX і будь-яких версій Windows. Багато фахівців користуються Telnet, що дозволяє їм працювати на деякому хості, розташованому на видаленні сотень тисяч кілометрів.

Протоколи FTP, TFTP і NFS. Стек TCP/IP містить три протоколи для передачі файлів: *File Transfer Protocol (FTP)*, *Trivial File Transfer Protocol (TFTP)* і *Network File System (NFS)*. За допомогою протоколу FTP можна, працюючи на комп'ютері в одному місці, підключитися до хост-комп'ютеру, розташованому в іншому місці, і скачати один або кілька файлів (при цьому, звичайно, потрібно знати ім'я облікового запису і пароль для віддаленого хоста.).

Перевага FTP у порівнянні із протоколами TFTP і NFS полягає в тому, що FTP використовує два порти TCP: 20 і 21. Порт 21 – це керуючий порт для команд FTP, які визначають спосіб передачі даних. Наприклад, команда get служить для одержання файлу, а команда put використовується для пересилання файлу деякому хосту. FTP підтримує передачу двійкових або текстових (ASCII) файлів, для чого застосовуються команди binary і ascii. Порт 20 служить тільки для передачі даних, що задаються командами FTP. Деякі команди FTP перераховані в табл. 2.1.

FTP призначений для передачі файлів цілком, що робить його зручним засобом для пересилання через глобальну мережу файлів великого розміру. FTP не дозволяє передати частину файлу або деякі записи усередині файлу. Оскільки дані інкапсульовані в пакети TCP, комунікації з використанням FTP є надійними і забезпечуються механізмом служб із встановленням

з'єднання. При FTP-комунікаціях виконується передача одного потоку даних, наприкінці якого потрібна ознака кінця файлу (EOF).

Таблиця 2.1

Приклади команд FTP

Команда	Опис
ascii	Передавати файли у форматі ASCII Binary
binary	Передавати файли у двійковому виді
bye або quit	Завершити сеанс передачі файлів і вийти з режиму FTP
close	Завершити сеанс передачі файлів
delete	Видалити файл на іншому комп'ютері
dir или Is	Вивести зміст каталогу на іншому комп'ютері
get	Одержати файл із іншого комп'ютера
help	Відобразити опис деякої команди FTP
put	Послати файл на інший комп'ютер
pwd	Вивести поточне ім'я каталогу іншого комп'ютера
send	Переслати файл на інший комп'ютер

TFTP – це файловий протокол стека TCP/IP, призначений для таких завдань, як передача з деякого сервера файлів, що забезпечують завантаження бездискової робочої станції. Протокол TFTP не встановлює з'єднань і орієнтований на пересилання невеликих файлів у тих випадках, коли поява комунікаційних помилок не є критичним і немає особливих вимог до безпеки. Відсутність з'єднань при роботі TFTP пояснюється тим, що він функціонує поверх протоколу UDP (через порт UDP 69), а не з використанням TCP. Це означає, що в процесі передачі даних відсутні підтвердження пакетів або не задіяні служби із встановленням з'єднань, що гарантують успішну доставку пакетів у пункт призначення.

Альтернативою FTP є програмні засоби Network File System (NFS) (мережева файлова система), розроблені компанією Sun Microsystems. Для їхньої роботи використовується запропонована компанією специфікація віддалених викликів процедур через порт TCP 111. NFS установлюється як на передавальні, так і на приймаючі вузли, і тому NFS-програми одного комп'ютера можуть запускати NFS-програми на іншому комп'ютері.

Система NFS, що часто використовуються в UNIX-системах, передає дані у вигляді потоку записів, а не як послідовність цілих файлів. Як і FTP, NFS є протоколом із встановленням з'єднання і працює поверх протоколу TCP. NFS особливо підходить для комп'ютерів, що обробляють великі обсяги транзакцій з використанням записів, що зберігаються у файлах або базах даних. Також NFS можна застосовувати в тих випадках, коли файли даних розподілені між декількома серверами.

Протокол SMTP (Simple Mail Transfer Protocol) призначений для передачі повідомлень електронної пошти між мережевими системами. За допомогою цього протоколу операційні системи можуть пересилати електронну пошту поверх протоколу TCP.

SMTP використовує порт TCP з номером 25. При роботі з SMTP не потрібно знати ім'я облікового запису і пароль для віддаленої системи. Усе, що потрібно, – це адреса електронної пошти приймаючого вузла. SMTP може пересилати тільки текстові файли, тому файли в інших форматах повинні бути конвертовані в текстовий вид, тільки після цього їх можна помістити в Smtp- повідомлення (хоча існує *стандарт MIME (Multipurpose Internet Mail Extensions),* що доповнює SMTP і дозволяє включати в стандартні повідомлення SMTP мультимедійні дані).

Повідомлення, що пересилаються за допомогою SMTP, мають дві частини: адресний заголовок і тіло повідомлення (текст). Адресний заголовок може бути дуже довгим, оскільки він містить адреси всіх SMTP-вузлів, через які передавалося повідомлення, а також мітку часу для кожного пересильного вузла. Якщо приймаючий вузол недоступний, SMTP чекає якийсь час, а потім намагається переслати повідомлення знову. У випадку невдачі (якщо приймаючий вузол так і не став доступним протягом заданого періоду часу) повідомлення вертається відправникові.

SMTP відповідає стандартам TCP/IP, але не є сумісним із протоколом X.400, що описує системи електронної пошти. SMTP пересилається поверх протоколу TCP, що забезпечує надійність поштового зв'язку, завдяки наявності служб із встановленням з'єднання. Для розгортання SMTP потрібні SMTP-сумісні додатки електронної пошти як на передавальному, так і на приймаючих вузлах. SMTP-додатки вибирають деякий сервер як основний поштовий шлюз, що з'єднує робочі станції і обробляє чергу поштових повідомлень, що зберігаються в деякому файловому каталозі. Ця черга служить поштовим доменом для всіх користувачів, що підключаються до даного сервера. Клієнти можуть зареєструватися на сервері і одержати свої

повідомлення, а сервер може також перенаправляти повідомлення іншим клієнтам.

На ранніх порах існування електронної пошти Інтернету користувачам доводилося підключатися до сервера, щоб прочитати свої повідомлення. Поштові програми звичайно працювали в текстовому режимі і були не дуже зручні для багатьох користувачів. Тому були розроблені протоколи, які дозволяли доставляти повідомлення електронної пошти прямо на робочі станції користувачів. Ці протоколи також виявилися дуже зручними для користувачів, що працюють за різними комп'ютерами. У цей час для завантаження повідомлень з поштових серверів на персональні комп'ютери користувачів найчастіше використовують два протоколи – *POP (Post Office Protocol - протоколи поштового відділення)* та *IMAP (Internet Mail Access Protocol - протокол доступу до електронної пошти в Internet)*.

Поточним стандартом протоколу *POP* є *POP3* (порт 110). Протокол обміну поштовою інформацією POP3 призначений для одержання пошти з поштових скриньок користувачів на їхні робочі місця за допомогою програм-клієнтів. Якщо за допомогою протоколу SMTP користувачі відправляють кореспонденцію через Internet, то за допомогою протоколу POP3 користувачи можуть тільки одержувати кореспонденцію зі своїх поштових скриньок на поштовому сервері в локальні файли.

Через свою простоту протокол POP3 часто має обмежені можливості. Наприклад, він може працювати тільки з однією поштовою скринькою, і тільки в автономному режимі, тобто завантажені повідомлення повинні віддалятися із сервера (хоча багато реалізацій дозволяють залишати повідомлення на сервері).

Протокол *IMAP* могутніший чим POP. Остання його версія *IMAP4* працює на порту TCP з номером 143. IMAP4 має ряд переваг: посилена аутентифікація, підтримка декількох поштових скриньок, поліпшена підтримка автономного і підключеного режимів роботи.

Підтримка підключеного режиму дозволяє прийняти із сервера частини повідомлень, проводить пошук і завантажувати повідомлення за певними критеріями й т.д. IMAP4 також дозволяє користувачам і користувальницьким агентам переміщати повідомлення між папками на сервері і видаляти деякі повідомлення. IMAP4 краще підходить для мобільних користувачів, що працюють за декількома комп'ютерами, і для користувачів з декількома поштовими скриньками. Головний недостаток

IMAP4 - це, що він не одержав широкого поширення серед постачальників послуг Інтернету.

У залежності от користувальницького агента, MTA і конкретних потреб користувача можна використати один із двох протоколів або обоє відразу.

Протоколи WWW, HTTP. World Wide Web (WWW) – це найвідоміша та найпопулярніша служба Інтернету («Всесвітня павутина»). Це глобальна розподілена по всьому світу інформаційна гіпертекстова мультимедійна система. Вона дозволила з'єднати в одну систему інформацію різних видів, яка зберігається на різних комп'ютерах. WWW призначена для інтерактивного пошуку інформації. Інформація в WWW розповсюджується у вигляді Web-сторінок (Web-документів). В основі WWW лежать два поняття: *формат документів HTML* та *гіпертекстові посилання.*

Web-сервери служать постачальниками інформаційного вмісту Web. Одержавши запит від клієнта, web-сервер надає запитані дані в тій або іншій формі. Документи на Web-серверах звичайно представлені у форматі HTML. *Hyper Text Markup Language (HTML)* – це мова розмітки гіпертекстів, що використовується для подання інформації в World Wide Web. HT у HTML позначає Hyper Text, основну концепцію розміщення інформації в WWW. Hyper Text або *hyperlinks (гіперпосилання)*, містить зв'язки (URL) усередині текстового документа, які дозволяють користувачеві швидко переходити від однієї частини документа до іншої або до іншого документа. *Гіпертекст* – це текст із виділеними фрагментами, що відіграють роль посилань, активізація яких призведе до виконання певних дій, наприклад, виведення графічного зображення, відтворення звуку, відкриття нового документа тощо. Дії, які асоціюються з певними гіперпосиланнями, можуть виконуватися автоматично. Частіше для активізації гіперпосилання потрібне втручання користувача. Посилання (гіперзв'язки) в документах виділяють іншим кольором та підкреслюють. Завдяки гіпертексту Web-сторінки набувають властивості інтерактивності.

Якщо HTML-файл знаходиться на web-сервері і до нього відкрито доступ, то говорять, що електронний документ опубліковано. Адресою публікації є адреса сервера, до якої додається шлях пошуку файлу з документом на самому сервері. Web-сторінка – це один електронний документ (він може бути малим та достатньо великим), яка відіграє роль

мінімальної одиниці подання інформації в просторі WWW. Гіперпосилання дозволяють зв'язати докупи Web-документи, які присвячені одній темі, їх тоді називають Web-вузлом (Web-сайтом).

Клієнтські функції в Web виконуються *браузерами*. Браузери містять програмні засоби, необхідні для взаємодії з web-сервером, а також перетворення і відображення інформації, що повертається сервером. До основних браузеров належать: Google Chrome, Mozilla Firefox, Internet Explorer, Opera.

Керуючими конструкціями мови HTML є теги. Теги являють собою ключові слова, укладені в кутові дужки. Ключові слова - це звичайні слова англійської мови, що позначають ту або іншу команду, що повинна бути застосована до тексту, обрамленого тегами. Таким чином, HTML документ являє собою звичайний ASCII-текст, у якому за допомогою тегів позначається приєднана до файлу графіка, відео, аудіо інформація або коди, що виконуються Web - браузером, наприклад Java Script. Вся ця інформація зберігається у файлах на WWW-сервері. Коли браузер одержує доступ до HTML документа, він спочатку інтерпретує закодовану в HTML-файлі інформацію, а потім представляє для користувача всю інформацію в графічному або текстовому виді.

Обмін даними між web-сервером і браузером здійснюється на базі протоколу *HTTP (Hypertext Transfer Protocol, Протокол передачі гіпертексту)*, що являє собою протокол прикладного рівня сімейства протоколів TCP/IP. Протокол HTTP найпоширеніший прикладний протокол стека TCP/IP. Коли користувач відвідує різні WWW сайти за допомогою браузера, браузер взаємодіє з Web-серверами, використовуючи саме протокол HTTP. Щораз при переході по гіперзв'язку від одного ресурсу до іншого браузер звертається до HTTP для доступу до сервера, що зберігає необхідну інформацію. HTTP забезпечує високопродуктивний механізм тиражування інформації мультимедійних систем незалежно від типу подання даних. Цей протокол побудований за об'єктно-орієнтованою технологією і може використовуватися для рішення різних завдань, наприклад, роботи із серверами імен або керування розподіленими інформаційними системами. На даний момент існує кілька версій протоколу HTTP. В 1996 році була стандартизована версія 1.1, що у даний момент підтримується більшістю серверів у мережі Інтернет. У цих версіях використовується повний запит, і значно розширений набір методів. Зокрема можна не тільки одержувати файли із сервера, але і передавати

файли на сервер, видаляти їх із сервера (природно, при наявності певних прав), передавати різними способами інформацію спеціальним программам, працюючим на сервері, а також управляти параметрами з'єднання, кеширування, виду, типу та кодування ресурсу й т.д.

Ідентифікація сторінок і інших ресурсів в Web здійснюється за допомогою уніфікованих покажчиків інформаційних ресурсів, або *URL (Uniform Resource Locators)*.

Цей сервіс складається із трьох частин:

– *Схема.* Ідентифікує тип сервісу, через який можна одержати доступ до сервісу, наприклад FTP або WWW-сервер.

– *Адреса.* Ідентифікує адресу (хост) ресурсу, наприклад, www.w3c.org

– *Ім'я або шлях доступу.* Ідентифікує повний шлях до ресурсу на обраному хості, який варто використати для доступу до ресурсу, наприклад, /Protocols/index.html.

Існує два типи адрес: *абсолютний URL* і *відносний URL.*

Абсолютний URL містить повну адресу об'єкта і протокол, тобто всі три вищенаведені частини. Наприклад, файл index.html, розташований у каталозі Protocols на сервері www.w3c.org, буде мати наступний абсолютний URL http:// www.w3c.org/ Protocols/ index.html.

Це означає, що буде використатися тип доступу через HTTP, схема доступу відділена двокрапкою ":" і вказує на використання протоколу HTTP. Наступні два слэша відокремлюють наступну адресу сервера www.w3c.org, далі йде шлях до файлу і сам файл. Абсолютний URL завжди повинен починатися зі схеми доступу. Якщо шлях до файлу і ім'я файлу відсутні, то передбачається, що звернення відбувається до кореневого каталогу сервера "/".

Відносний URL використовує URL поточного документа, запитаного HTTP клієнтом. Застосовуючи ту ж схему, HTTP клієнт реконструює URL, змінюючи тільки деякі імена і розширення файлів. Вказівка перед відносним URL ".." значить перехід на вищий рівень каталогів, а вказівка слеша - ігнорує всі каталоги і додає зазначений далі шлях безпосередньо до адреси сервера.

Крім того, URL ресурс може містити не тільки ім'я ресурсу, але й параметри, необхідні для його роботи. Ім'я ресурсу відділене від рядка параметрів символом "?". Рядок параметрів складається з лексем, поділюваних символом "&". Кожна така лексема складається з імені

параметра і його значення, розділених символом "=". Символи, що не входять у набір символів ASCII, заміняються знаком "%" і шістнадцятковим значенням цього символу. Наприклад, символ "?" заміняється на "%3F". Оскільки символ пробілу зустрічається в рядку параметрів досить часто, то він замінюється не на "%20", а на символ "+" (якщо ж у рядку параметрів зустрічається символ "+", то він замінюється на "%2B"). Для зазначеного ресурсу весь рядок параметрів є одним строковим параметром, тому тип, черговість або унікальність імен окремих параметрів рядки не істотні.

Наприклад:

http://www.mail.ru/users/mail.cgi?login=vasia&folder=my%20inbox

Протокол HTTP побудований за моделлю "запит/відповідь". Іншими словами, клієнт встановлює з'єднання із сервером і відправляє запит. У ньому зазначений тип запиту, URL, версія протоколу HTTP і зміст запиту: інформація клієнта (параметри) і, можливо супроводжуюча інформація або тіло повідомлення. Сервер HTTP після обробки запита повертає відповідь, що містить: версію підтримуваного протоколу, код обробки запиту або код помилки та інформацію, що повертається за запитом. Інформація тіла повідомлень, як клієнта, так і сервера повинна бути представлена в MIME-форматі (стандарт MIME дозволяє передавати дані у форматах, відмінних від простого тексту: звуки, відео, зображення, додатка та ін.).

HTTP-з'єднання ініціюється клієнтом. У найпростішому випадку, з'єднання являє собою потік даних між клієнтом - ініціатором з'єднання та сервером. Однак досить часто в з'єднанні може брати участь проміжний агент або Proxy сервер. Proxy сервер - це проміжний агент, що приймає запит клієнта та, залежно від своїх настроювань, змінює частину або все повідомлення запиту і передає переформатований запит запитуваному серверу. У момент прийняття запитів proxy може працювати як сервер, а при передачі запитів - як клієнт. Крім того, proxy може підтримувати внутрішній кеш запитів і відповідей. Кеш зберігає відповіді серверів і повертає їх за запитом клієнта, не передаючи запит безпосередньо запитаному серверу. Тим самим зменшується час з'єднання, і збільшується продуктивність роботи з віддаленими та повільними серверами. Однак далеко не всі відповіді можуть кешуватися. Деякі запити можуть містити параметри, що накладають обмеження на роботу кеша.

HTTP – це протокол прикладного рівня, що працює поверх транспортного протоколу TCP. Однак, як усякий протокол прикладного

рівня, може працювати на будь-якому іншому транспортному протоколі, орієнтованому на встановлення з'єднання. За замовчуванням HTTP протокол використовує TCP порт 80. На відміну від інших прикладних протоколів, що забезпечують нерозривне з'єднання поки не відбудеться помилка або не буде поданий сигнал до завершення з'єднання, HTTP працює по-іншому. HTTP-з'єднання повинно відкриватися клієнтом перед кожним запитом і закриватися сервером після відправлення відповіді. Ні браузер (клієнт), ні сервер не зберігають інформацію навіть про останнє з'єднання. Такий стиль роботи дозволяє серверу швидше переходити до обслуговування інших клієнтів, що збільшує ефективність його роботи. Однак при одержанні гіпертекстових документів, які містять вбудовані графічні об'єкти або інші асоційовані об'єкти, за короткий проміжок часу браузер відправляє кілька запитів до того самого сервера. У цьому випадку знижується ефективність роботи та збільшується завантаження мережі за рахунок великої кількості службових TCP пакетів, призначених для відкриття й закриття з'єднання. Тому в специфікації HTTP 1.1 постійні з'єднання стали використовуватися за замовчуванням. Крім цього в HTTP 1.1 при використанні постійних з'єднань може бути використана конвеєрна обробка запитів. При цьому клієнт може відправити кілька запитів, не чекаючи відповіді на кожний, а потім одержати кілька відповідей від сервера. Слід також зазначити, що навіть при використанні постійних з'єднань, сервер всеж розриває з'єднання із клієнтом, якщо після закінчення деякого таймаута не одержує від нього ніяких даних. Таймаут звичайно становить порядка декількох десятків секунд. Тому, незважаючи на можливість використання постійних з'єднань, протокол HTTP всеж відрізняється від інших прикладних протоколів стека TCP/IP, у яких з'єднання звичайно закривається з боку клієнта.

3.2 Функції та архітектура систем керування мережами

Для підтримки мережі в працездатному стані необхідний постійний контроль над її роботою. Використання засобів контролю дозволяє адміністратору виявити і усунути будь-яку загрозу нормальному функціонуванню мережі.

Процес контролю роботи мережі ділиться на два етапи - моніторинг і аналіз.

На етапі моніторингу виконується простіша процедура - процедура збору первинних даних про роботу мережі: статистики по циркулює в

мережі пакетів різних протоколів, стан портів комунікаційних пристроїв і т.п.

Далі виконується етап аналізу, більш складний і інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з раніше отриманими даними і вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі.

Всі засоби, що застосовуються для моніторингу та аналізу обчислювач-них мереж, можна розділити на кілька великих класів: системи управління мережею, засоби управління системою, вбудовані системи діагностики і управління, аналізатори протоколів, обладнання для діагностики і сертифікації кабельних систем, експертні системи, багатофункціональні пристрої аналізу і діагностики.

Системи управління мережею - це централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік, циркулюючому в мережі.

Ці системи не тільки здійснюють моніторинг і аналіз мережі, а й виконують в автоматичному чи напівавтоматичному режимі дії з управління мережею - включення і відключення портів пристроїв, зміна параметрів адресних таблиць комутаторів і маршрутизаторів і т.п.

Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView. Відповідно до рекомендацій стандартів можна виділити ряд функцій засобів управління системою.

Крім моніторингу та аналізу роботи мережі, необхідних для отримання вихідних даних для настройки мережі, до них відносяться управління конфігурацією і безпекою, які потрібні для налаштування і оптимізації мережі: • Управління конфігурацією мережі і ім'ям - полягає в конфігурації компонентів мережі, включаючи їх місце розташування , мережеві адреси і ідентифікатори, управління параметрами мережевих операційних систем.

Обробка помилок - це виявлення, визначення і усунення по-наслідків збоїв і відмов в роботі мережі.

Аналіз продуктивності - допомагає на основі накопиченої статистичної інформації оцінювати час відповіді системи і величину трафіку, а також планувати розвиток мережі.

Управління безпекою - включає в себе контроль доступу і збереження цілісності даних. У функції входить процедура аутентифікації,

перевірки привілеїв, підтримка ключів шифрування, управління повноваженнями.

Облік роботи мережі - включає реєстрацію і управління використовуваними ресурсами і пристроями.

Створення списку мережевих програм, що полегшує їх установку і модернізацію, отримання даних про використання додатків, вирішення питань ліцензування.

Розподіл і установка програмного забезпечення. Після завершення обстеження адміністратор може створити пакети розсилки про-граммного забезпечення.

Віддаленого аналізу продуктивності і виникаючих проблем.

Адміністратор може дистанційно керувати мишею, клавіатурою і бачити екран будь-якого ПК, що працює в мережі під управлінням тієї чи іншої мережевої операційної системи. Інструменти моніторингу вбудовані в багато сучасні операційні системи. Вони застосовні для визначення базових показників продуктивності або діагностування та усунення неполадок в мережі.

За допомогою програми System Monitor Windows можна вимірювати продуктивність багатьох системних компонентів, зокрема виводити на екран показання лічильників мережевих інтерфейсів, наприклад загальна кількість байтів або пакетів в секунду, кількість переданих і прийнятих байтів або пакетів в секунду. Ця програма дозволяє виводити дані в графічному форматі і складати по ним звіти. Вимірювання можна переглядати в реальному часі, оновлювати автоматично або на вимогу. Можна конфігурувати оповіщення, тобто встановити автоматичне повідомлення адміністратора при настанні деякої події, наприклад, якщо задані параметр продуктивності досягне верхнього або нижнього рівня. Моніторинг дозволяє правильно планувати продуктивність мережі.

Аналізатори протоколів є програмні або апаратно-програмні системи, які обмежуються функціями моніторингу і аналізу трафіку в мережах.

Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують повне декодування захоплених пакетів, тобто перетворюють їх з довічного формату до вигляду, придатного для аналізу людиною.

Існують такі аналізатори, які надають статистичну інформацію про перехоплених пакетах, дають результати аналізу неполадок в з'єднаннях, аналіз продуктивності, виявлення вторгнень. За допомогою комплексу Sniffer, в який входить великий набір різноманітних засобів, що дозволяють виконувати фільтрацію пакетів, генерувати завантаження мережі, яка полегшує тестування нових пристроїв і додатків. Його можна використовувати для моделювання мережевого навантаження, визначення часу відповіді і т.д.

В програми Sniffer вбудовані такі утиліти TCP / IP, як ping, tracert, перегляду DNS і ін. Процес аналізу протоколів включає захоплення циркулюючих в мережі пакетів, що реалізують той чи інший мережевий протокол, і вивчення вмісту цих пакетів.

Грунтуючись на результатах аналізу, можна здійснювати обґрунтоване і зважене зміна будь-яких компонентів мережі, оптимізацію її продуктивності, пошук і усунення неполадок. Аналізатор протоколів є або самостійне спеціалізоване пристрій, або персональний комп'ютер, зазвичай переносний класу Notebook, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням.

Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережного адаптера і декодирующего одержувані дані, і додаткового програмного коду, що залежить від топології досліджуваної мережі.

Програми управління мережами більш повні, в них включені не тільки компоненти моніторингу, а й багато інших засобів. Прикладами засобів управління системою є такі продукти, як SystemManagementServer (SMS) компанії Microsoft, Manage Wise компанії Novell або LANDeskManager фірми Intel.

Програма SMS представляє собою потужний засіб управління мережами, за допомогою якої можна отримувати списки устаткування і програмного забезпечення. До складу SMS включена повна версія програми Network Monitor фірми Microsoft. Вона призначена для аналізу роботи процедур протоколів. Наприклад, вона застосовується для моніторингу використання пропускної здатності мережі, вимірювання кількості кадрів в секунду і отримання додаткової статистичної інформації про роботу мережі, а також розпізнавання імен та пошуку маршрутизаторів.

Програма має вбудовані засоби поширення програмного забезпечення. Скорочена версія програми поставляється в складі Windows. Програма OpenView компанії Hewlett Packard містить інструменти управління великими і середніми мережами, до складу яких входять тисячі серверів і більше 5000 робочих станцій. Для управління невеликими мережами використовується, наприклад, програма Network Monitor Suite (NMS) компанії Lanware і ViewLAN компанії NuLink, робота яких заснована на протоколах SNMP і CMIP. Програма надає такі можливості, як повторний запуск службових програм, складання розкладів і перезавантаження серверів. Протокол SNMP використовується для отримання від мережевих пристроїв інформації про їх статус, продуктивності і характеристиках, які зберігаються в базі даних мережевих пристроїв MIB (Management Information Base).

Агент в протоколі SNMP - це обробляє елемент, який забезпечує менеджерам, розміщеним на керуючих станціях мережі, доступ до значень змінних MIB, і тим самим дає їм можливість реалізовувати функції з управління та нагляду за пристроєм. Вбудовані системи діагностики і управління виконуються у вигляді програмно-апаратних модулів, що встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи.

Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Як правило, вбудовані модулі управління одночасно виконують роль SNMP-агентів, що поставляють дані про стан пристрою для систем управління.

Існує кілька стандартів на бази даних керуючої інформації. Основними є стандарти MIB-I і MIB-II, а також версія бази даних для віддаленого управління RMONMIB. Крім цього, існують стандарти для спеціальних MIB пристроїв конкретного типу (наприклад, MIB для концентраторів або MIB для модемів), а також приватні MIB конкретних фірм-виробників обладнання. Новітнім додаванням до функціональних можливостей SNMP є специфікація RMON, яка забезпечує віддалене взаємодія з базою MIB. До появи RMON протокол SNMP не міг використовуватися віддаленим чином, він допускав лише локальне управління пристроями.

База RMONMIB володіє поліпшеним набором властивостей для віддаленого управління. Об'єкти RMONMIB включають додаткові

лічильники помилок в пакетах, гнучкіші засоби аналізу графічних трендів і статистики, більш потужні засоби фільтрації для захоплення і аналізу окремих пакетів. Агенти RMONMIB більш інтелектуальні порівняно з агентами MIB-I або MIB-II і виконують значну частину роботи по обробці інформації про пристрій, яку раніше виконували менеджери.

Ці агенти можуть розташовуватися всередині різних комунікаційних пристроїв, а також бути виконані у вигляді окремих програмних модулів, що працюють на універсальних ПК і ноутбуках (прикладом може служити LANalyzer Novell). Устаткування для діагностики і сертифікації кабельних систем. Умовно це устаткування можна поділити на чотири основні групи: мережеві монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультиметри). Мережеві монітори (звані також мережевими аналізаторами) призначені для тестування кабелів різних категорій. Слід розрізняти мережеві монітори і аналізатори протоколів. Мережеві монітори збирають дані тільки про статистичні показники трафіку - середньої інтенсивності загального трафіку мережі, середньої інтенсивності потоку пакетів з певним типом помилки і т.п. Мережеві аналізатори - це великогабаритні і дорогі (понад $ 20000) прилади, призначені для використання в лабораторних умовах спеціально навченим технічним персоналом і дозволяють вимірювати різні електромагнітні характеристики кабелю.

Призначення пристроїв для сертифікації кабельних систем, безпосередньо випливає з їх назви. Сертифікація виконується відповідно до вимог одного з міжнародних стандартів на кабельні системи. Кабельні сканери використовуються для діагностики мідних кабельних систем. Ціна на ці прилади варіюється від $ 1000 до $ 3000. Для визначення місця розташування несправності кабельної системи (обриву, короткого замикання, неправильно встановленого роз'єму і т.д.) використовується метод «кабельного радара». Суть цього методу полягає в тому, що сканер випромінює в кабель короткий електричний імпульс і вимірює час затримки до приходу відбитого сигналу. За полярності відображеного імпульсу визначається характер пошкодження кабелю (коротке замикання або обрив). В правильно встановленому і підключеному кабелі відбитий імпульс зовсім відсутній.

Тестери кабельних систем - найбільш прості і дешеві прилади для діагностики кабелю. Вони дозволяють визначити безперервність кабелю, однак, на відміну від кабельних сканерів, не дають відповіді на питання

про те, в якому місці стався збій. Експертні системи акумулюють людські знання про виявлення причин аномальної роботи мереж і можливі способи приведення мережі в працездатний стан.

Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу та аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів. Найпростішим варіантом експертної системи є контекстно-залежна help-система. Більш складні експертні системи являють собою так звані бази знань, що володіють елементами штучного інтелекту. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron. В останні роки, у зв'язку з повсюдним поширенням локальних мереж виникла необхідність розробки недорогих портативних приладів, які суміщають функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів і навіть деяких можливостей ПЗ мережевого управління. Як приклад такого роду пристроїв можна привести Compas компанії MicrotestInc або LANMeter компанії FlukeCorp.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АМ	амплітудна модуляція
ВІС	велика інтегральна схема
ДХ	довгі хвилі
ЕОМ	електронно-обчислювальна машина
ІС	інформаційна система
КМ	комп'ютерна мережа
КХ	короткі хвилі
ЛОМ	локальна обчислювальна мережа
НВЧ	надвисокі частоти
ОС	обчислювальна система
ПЕОМ	персональна ЕОМ
ПК	персональний комп'ютер
РС	робоча станція
СУБД	система управління базами даних
СХ	середні хвилі
УКХ	ультракороткі хвилі
ЧМ	частотна модуляція
ЦКП	центр комутації пакетів
AM	Amplitude Modulation
AMI	Bipolar Alternate Mark Inversion
ANSI	American National Standard Institute
ARP	Address Resolution Protocol
ASCII	American National Standard Code For Information Interchange
ATM	Asynchronous Transfer Mode
AUI	Attached Unit Interface
CGI	Common Gateway Interface
CRC	Cyclic Redundancy Checksum
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DA	Dual Attachment
DAC	Dual Attachment Concentrator
DAS	Dual Attachment Station
DCE	Data Circuit - terminating Equipment
DEC	Digital Equipment Corporation
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DSE	Data Switching Equipment
DTE	Data Terminal Equipment
DWDM	Dense Wave Division Multiplexing
DIS	Distributed Information Systems
FCS	Frame Check Sequence
FM	Frequency Modulation

FOIRL	Fiber Optic Inter-Repeater Link
FTAM	File Transfer Access Method
FTP	File Protocol
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IMAP	Internet Mail Access Protocol
IP	Internet Protocol
IPX/SPX	Internet Packet Exchange/ Sequenced Packet Exchange
IS	Information System
ISO	International Organization for Standardization
LAN	Local Area Networks
LD	Laser Diode
LED	Light Emitting Diode
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Networks
MAU	Multistation Access Unit
MIB	Management Information Base
MMF	Multi Mode Fiber
MS	Message Store
MSAU	Multi-Station Access Unit
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit
MIME	Multipurpose Internet Mail Extensions
NBF	NetBEUI Frame
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	Network Information Center
NRZ	Non Return to Zero
NRZI	Non Return to Zero with ones Inverted
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
PDV	Path Delay Value
POP	Post Office Protocol
PPP	Point-to-Point Protocol
RARP	Reverse Address Resolution Protocol
RG	Radio Grade
RIP	Routing Internet Protocol

SA	Single Attachment
SAC	Single Attachment Concentrator
SAP	Service Access Point
SAS	Single Attachment Station
SDH	Synchronous Digital Hierarchy
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
TELNET	Terminal Network
TFTP	Trivial File Transfer Protocol
TRT	Token Rotation Time
TTL	Time-to-Live
UA	User Agent
UDP	User Datagram Protocol
URL	Uniform Resource Locators
UTP	Unshielded Twisted Pair
WAN	Wide Area Networks
WWW	World Wide Web
WINS	Windows Internet Naming Service

Навчальне електронне видання

КУЗНІЧЕНКО СВІТЛАНА ДМИТРІВНА

КОМП’ЮТЕРНІ МЕРЕЖІ

Конспект лекцій

Видавець і виготовлювач
Одеський державний екологічний університет
вул. Львівська, 15, м. Одеса, 65016
тел./факс: (0482) 32-67-35
E-mail: info@odeku.edu.ua
Свідоцтво суб’єкта видавничої справи
ДК № 5242 від 08.11.2016