МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Комп'ютерні мережі 1.

Локальні комп'ютерні мережі

Методичні вказівки до комп'ютерного практикуму

Для студентів напряму підготовки
6.050102 «Комп'ютерна інженерія»
кафедри обчислювальної техніки
всіх форм навчання

Рекомендовано
Вченою радою факультету
інформатики та обчислювальної
техніки НТУУ «КПІ»
Протокол № 10 від 28.05 2012р.

Київ
НТУУ «КПІ»
2012

Комп'ютерні мережі 1.Локальні комп'ютерні мережі. Методичні вказівки до комп'ютерного практикуму. [Текст] / Уклад.: О.Ю. Кулаков, Р.Ю.Берест – К.: НТУУ «КПІ», 2012. – 164 с.

Методичні вказівки призначені для студентів напряму підготовки 6.050102 «Комп'ютерна інженерія» кафедри обчислювальної техніки всіх форм навчання. В посібнику наведена тематика практичних занять, основні теоретичні відомості, завдання для лабораторних робіт, список рекомендованої літератури, контрольні питання.

Укладач О.Ю. Кулаков, к.т.н.
Р.Ю.Берест

Рецензент Муха І.П., к.т.н., доц.
кафедри АСОІУ

За редакцією укладачів

ЗМІСТ

ВСТУП

Дисципліна «Комп'ютерні мережі» призначена для вивчення основних принципів, методів та засобів побудови комп'ютерних мереж, зокрема структурної організації локальних та глобальних мереж, мереж з асинхронним режимом передавання інформації, архітектури мережевих операційних систем та мережевих технологій.

Практична частина курсу складається з восьми лабораторних робіт і призначена для отримання практичних навичок використання існуючих мережевих технологій для побудови локальних та глобальних комп'ютерних мереж. Всі лабораторні роботи виконуються в системі автоматизованого проектування NetCrackerPro, призначеної для побудови та моделювання інформаційно-обчислювальних мереж та оцінки їх технічних параметрів. Роботи послідовно логічно впорядковані за складністю та охоплюють всі теми, що вивчаються в курсі.

Матеріал для кожної лабораторної роботи містить мету, основні теоретичні відомості, загальне завдання, варіанти індивідуальних завдань, список питань для самоперевірки, зміст звіту про виконання лабораторних робіт, а також список рекомендованих інформаційних джерел для підготовки та виконання лабораторних робіт.

Комп’ютерний практикум № 1

ВИВЧЕННЯ ПАКЕТУ NETCRACKER PRO

Мета та основні завдання роботи: познайомитись з основними можливостями пакету NetCracker Pro і отримати навики побудови комп’ютерних мереж.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Коротке керівництво по використанню програми NetCracker Pro.

Програма NetCracker призначена для проектування і моделювання комп'ютерних мереж. Для проектування структури мережі програма надає можливість вибору необхідного устаткування з вбудованої бази даних, а також додавання в базу даних і конфігурації нового обладнання різних типів. Користувач розміщує обрані компоненти на складальному полі, задає структуру і тип зв'язків між ними, визначає тип програмного забезпечення та характер трафіку між вузлами мережі. Далі є можливість вказати перелік аналізованих характеристик і вид відображення статистичної інформації та виконати імітаційне моделювання спроектованої мережі.

На рисунку 1 наведений типовий вид вікна програми NetCracker. Панель перегляду компонент, що маються в базі даних, розміщується звичайно в лівій частині вікна і включається з допомогою команди View->Bars->Browser Pane. Панель вміщує декілька закладок.

Закладка Project Hierarchy призначена для відображення структури документів створюваного проекту мережі.

Закладка Devices призначена для відображення бази даних пристроїв. Список пристроїв має декілька видів відображення:

Types (Типи) – пристрої в списку групуються по типах. Далі в кожній групі можуть виділятись підтипи пристроїв по функціональних признаках. Після цього пристрої розділяються по виробниках.

Vendors (Виробники) – пристрої в списку групуються по виробниках. Далі в кожній групі виділяються підгрупи, що відповідають типу пристроїв.

User (Користувацькі) – пристрої, що визначаються користувачем. В свою чергу також можуть групуватись по типах або виробниках.

Закладка Compatible Devices призначена для відображення списку сумісних пристроїв.

В нижній частині вікна програми звичайно розміщується панель пристроїв, яка може бути відображена з допомогою команди View->Bars->Image Pane. Дана панель призначена для відображення приладів з вибраної групи.

В правій верхній частині головного вікна програми розміщується основне вікно, що представляє собою набірне поле. В ньому необхідно розміщувати компоненти, що використовуються при проектуванні структури мережі.

Для налаштування структури мережі необхідно розмістити в полі набору пристрої, що використовуються і з'єднати їх лініями зв'язку. Для розміщення пристрою в полі набору необхідно, користуючись панеллю переглянути список пристроїв, вибрати відповідний клас і тип пристрою. Після цього потрібно вибрати пристрій в панелі пристроїв, перетягнути його в набірне поле і розмістити в потрібному місці. Для дублювання розміщеного пристрою потрібно вибрати потрібний пристрій і виконати команду Edit-> Duplicate. Команда Edit-> Replicate дозволяє розмістити в складальному полі потрібну кількість пристроїв. Для цього в діалоговому вікні потрібно вказати кількість пристроїв і натиснути кнопку Replicate. Перемикач Organize дозволяє вибрати найбільш зручний варіант розміщення пристроїв в полі набору. Для видалення пристрою з набірного поля необхідно вибрати пристрій і виконати команду Delete з меню Edit або з контекстного меню.

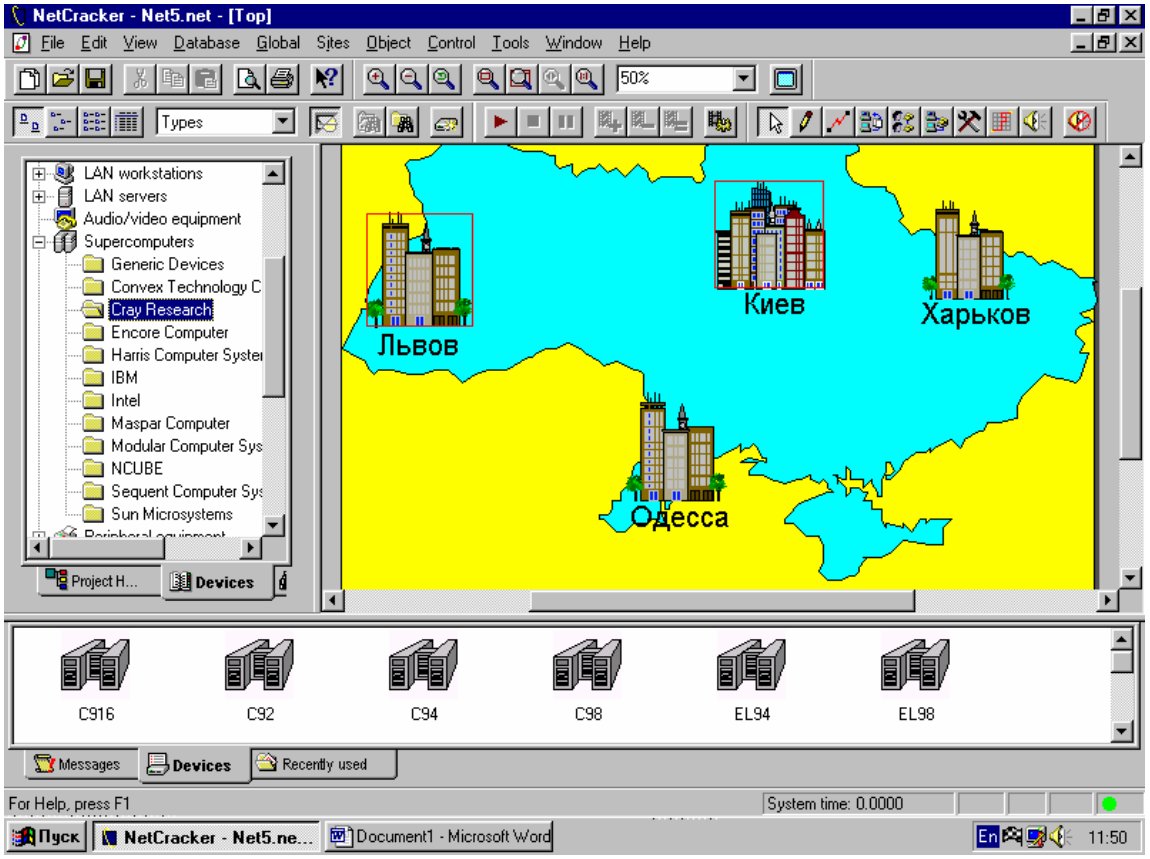


Рисунок 1-типовий вид вікна програми NetCracker

Для відображення реальної структури мережі організації бажано використовувати такі класи компонент, як City (Місто), Building (Будівля), Campus (Університет), Floor (Поверх) і Room (Кімната). Кожний з цих об’єктів має своє поле набору, розкрити яке можна за допомогою команди Expand з меню Object або з контекстного меню. В новому вікні, що відкривається при виконанні даної команди, можна побудувати ту частину мережі, яка відповідає даному об’єкту.

При виборі різних пристроїв, що використовуються для побудови мережі, перш за все необхідно враховувати такі параметри:

Необхідна кількість портів

Необхідний тип портів

Пропускну здатність

Підтримувані транспортні протоколи

Підтримувані протоколи маршрутизації

Кількість слотів.

Багато пристроїв вимагають установки певних компонентів для виконання ними необхідних функцій. Так, наприклад, багато робочі станції поставляються без мережевих карт. В такому разі, їх потрібно встановити. Для цього треба знайти потрібний пристрій, і перетягнути його на потрібний об'єкт. Слід враховувати кількість слотів і їх тип при встановленні додаткового обладнання. Наприклад, якщо пристрій не містить портів MCA, то встановити в нього мережеву карту, розраховану на шину MCA, буде неможливо. Також, якщо в пристрої немає вільних слотів, встановити в нього що-небудь буде важко. Для перегляду та редагування параметрів пристроїв використовуються команди Properties, Open, Configuration, Configure Ports з меню Object або команди Configuration і Properties з контекстного меню. Для налаштування зв'язків між пристроями (а точніше між їх інтерфейсами або портами) необхідно скористатися кнопкою Link Devices на панелі режимів покажчика миші (включається командою View-> Bars-> Modes). Після вибору даної кнопки необхідно вказати один з з'єднуваних пристроїв і, не відпускаючи кнопку миші, розтягнути зв'язок до другого пристрою. Після цього з'являється діалогове вікно Link Assistant, в якому проводиться подальше конфігурування параметрів з'єднання. Спочатку надається можливість визначити з'єднувані порти пристроїв і зв'язати їх, виконавши клацання по кнопці Link. Після цього стає доступною секція Link Settings, в якій настроюються параметри даного з'єднання, наприклад, використовуваний протокол (Ethernet 10Base-T), тип середовища передачі (Twisted Pair - вита пара), пропускна здатність середовища (10 Мб / с), довжина з'єднання (до 100 м). У більшості випадків ці параметри фіксовані і змінюватися не можуть, хоча іноді є можливість вибору з декількох значень. Наприклад, при з'єднанні двох оптоволоконних модемів пропускна здатність може бути обрана зі списку значень: T3, E3, DSn, Ocn, STSn, STMn (для аналогового модему: 2400, 9600, 14400, 28800 і т. д.). Тип з'єднання в даному випадку єдиний - frame relay (ретрансляція кадрів). Середовище передачі теж фіксоване - fiber-optic cable (оптоволокно). При з'єднанні пристроїв, що мають порт ISDN, список типів з'єднань дещо ширший - ISDN BRI, ISDN PRI, point-to-point leased line (виділена лінія), dial-up analog line (аналогова телефонна лінія).

Після введення структури мережі і топології зв’язків визначається склад і розміщення використовуваного програмного забезпечення. Для цього необхідно в списку компонентів вибрати категорію Network and enterprise software, в ній знайти необхідне програмне забезпечення і помістити його на відповідний об’єкт в мережі.

Наступним кроком визначається трафік між вузлами мережі. Для налаштування трафіку необхідно скористатись кнопкою Set Traffic на панелі режимів вказівника миші для переходу в відповідний режим. Після цього необхідно послідовно вибрати пари абонентських станцій (АС) мережі, між якими буде заданий трафік. Порядок кліків на АС визначає направлення передачі – спочатку відмічається джерело, потім приймач. В результаті з’являється діалогове вікно Profiles, яке дозволяє задати тип і основні характеристики трафіку. Тип трафіку вибирається з списку Profiles List, причому вказується по принципу "запити клієнта до серверу", тобто в якості приймача може виступати тільки та АС, на якій функціонує відповідне програмне забезпечення (HTTP/FTP Server, SQL server, File Server). Деякі типи трафіку складають виключення з даного правила, наприклад, Small office, LAN peer-to-peer traffic, InterLAN traffic і інші. Для налаштування характеристик трафіку між вказаними АС необхідно натиснути кнопку Advanced. В діалоговому вікні, що зявилось Traffic from (АС-джерело) to (АС-приймач) задаються закон розподілу і діапазон значень для розміру запиту (Transaction Size) і інтервалу між запитами (Time Between Transactions), а також тип протоколу прикладного рівня (Application Layer Protocol). При необхідності добавити новий тип трафіку, видалити або змінити параметри існуючих типів слідує скористатись кнопками Add, Remove, Edit і Rename діалогового вікна Profiles. Колір, яким при моделюванні будуть відображатися пакети, що належать даному типу трафіка, відображається в стовбці Color. Характеристики типів трафіка, що використовуються по замовчуванню, можна змінити також і з допомогою команди Global->Profiles. Також є можливість використовувати команду Global->Data Flow для конфігурації потоків даних в мережі.

Для вказівки аналізованих характеристик слід скористатися командою Statistics з контекстного меню або Define Statistics з меню Object. У діалоговому вікні Statistical Items можна задати тип характеристики і спосіб відображення статистичної інформації в процесі моделювання. Це діалогове вікно буде різним для різних типів об'єктів, тобто може змінюватися перелік характеристик, а також деякі способи відображення інформації можуть бути недоступні. Для одного об'єкту (вибраного пристрою, з'єднання або потоку даних) можна вибирати кілька способів відображення інформації (індикатор, число, графік).

Після цього вже можна робити імітаційне моделювання роботи мережі. Для управління процесом моделювання використовуються команди пункту меню Control. Команда Start використовується для запуску, Pause для призупинення і Stop для повної зупинки процесу моделювання. Команди Simulation Faster і Simulation Slower призначені для зміни швидкості моделювання, тоді як команди Animation Faster, Animation Slower, Animation Default призначені для зміни швидкості візуалізації процесу. Команда Animation Setup дозволяє в діалоговому режимі вибрати найбільш підходящі параметри для інтенсивності, швидкості та розміру пакетів і дзвінків. Деякі з перерахованих команд можна виконати за допомогою кнопок, розташованих на панелях інструментів Zoom і Control.

Для перегляду узагальнених результатів моделювання використовується команда Associated Data Flow з меню Object або з контекстного меню. В результаті виконання даної команди у вікні відображається статистика по процентному співвідношенню кількості пакетів для вхідних (Incoming Traffic) і вихідних дзвінків (Outgoing Traffic).

За допомогою команд, що містяться в пункті меню Tools-> Reports, можна створити звіти, узагальнюючі результати виконаної роботи.

ЗАВДАННЯ НА РОБОТУ

1. Використовуючи пакет NetCracker, побудувати локальну мережу технології Ethernet з наступними параметрами:

- Кількість робочих станцій $N_{PC} = MOD_4(N_B) + 2$;
- Кількість серверів $N_C = MOD_3(N_B) + 1$;
- Тип середовища передачі $T_{СП} = MOD_3(N_B)$

Тип трафіку: LAN peer-to-peer traffic; FTP; E-Mail (SMTP); HTTP.

Де N_B - варіант (порядковий номер студента в журналі групи).

$T_{СП}$	0	1	2
Середовище передачі	Вита пара	Кооксіальний кабель	Оптоволокно

2. Провести імітаційне моделювання роботи мережі і зібрати статистику: середня загрузка вузлів, каналів передачі даних; середня затримка; кількість прийнятих, відкинутих пакетів.

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

Які мережеві пристрої використовуються для побудови мережі Ethernet 10BASE T?

Які мережеві пристрої використовуються для побудови мережі Ethernet 10BASE 5?

ЛІТЕРАТУРА

NetCracker Professional Tutorial

Комп'ютерний практикум № 2

ВИВЧЕННЯ ОБЛАДНАННЯ І КАБЕЛЬНОЇ СИСТЕМИ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ. ЕТАЛОНА МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ.

Мета роботи: познайомитись з багаторівневою організацією мережевої взаємодії систем; з основними апаратними засобами локальних обчислювальних мереж, отримати навики вибору обладнання і кабельної системи для побудови локальної обчислювальної мережі.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Еталонна модель взаємодії відкритих систем.

На початку 80-х років ряд міжнародних організацій по стандартизації – ISO, ITU-T і деякі інші – розробили модель, яка відіграла значну роль в розвитку мереж. Ця модель називається *еталонною моделлю взаємодії відкритих систем (Open System Interconnection, OSI)* або моделлю OSI. Модель OSI визначає різні рівні взаємодії систем, дає їм стандартні імена і вказує, які функції повинен виконувати кожний рівень. Модель OSI була розроблена на основі великого досвіду, отриманого при створенні комп'ютерних мереж, в основному глобальних, в 70-ті роки. Повний опис цієї моделі займає більше 1000 сторінок тексту.

В моделі OSI засоби взаємодії діляться на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережевий, канальний и фізичний. Кожний рівень має справу з одним певним аспектом взаємодії мережевих пристроїв.

Модель OSI описує тільки системні засоби взаємодії, що реалізуються операційною системою, системними утилітами, системними апаратними засобами. Модель не включає засоби взаємодії прикладних програм кінцевих користувачів. Свої власні протоколи взаємодії прикладні програми реалізують, звертаючись до системних засобів.

Програма може взяти на себе функції деяких верхніх рівнів моделі OSI. Наприклад, деякі СКБД мають вбудовані засоби віддаленого доступу до файлів. В цьому випадку програма, виконуючи доступ до віддалених ресурсів, не використовує системну файлову службу; вона обходить верхні рівні моделі OSI і звертається напряму до системних засобів, що відповідають за транспортування повідомлень по мережі, які розміщуються на нижніх рівнях моделі OSI.

На рисунку 2.1 представлений приклад взаємодії процесів А та В, що перебувають, відповідно, на комп'ютерах 1 і 2. Програма зв'язана з процесом А звертається із запитом до прикладного рівня, наприклад до файлової служби. На підставі цього запиту програмне забезпечення прикладного рівня формує

повідомлення стандартного формату. Звичайне повідомлення складається з заголовка і поля даних. Заголовок містить службову інформацію, яку необхідно передати через мережу прикладному рівню машини-адресата, щоб повідомити йому, яку роботу треба виконати. В даному випадку заголовок повинен містити інформацію про місце знаходження файлу і про тип операції, яку необхідно над ним виконати. Поле даних повідомлення може бути порожнім або містити будь-які дані, наприклад ті, які необхідно записати у віддалений файл. Але для того щоб доставити цю інформацію за призначенням, належить вирішити ще багато задач, відповідальність за які несуть нижчі рівні.

Після формування повідомлення прикладний рівень направляє його вниз по стеку представницькому рівню. Протокол представницького рівня на основі інформації, отриманої з заголовка прикладного рівня, виконує необхідні дії і добавляє до повідомлення власну службову інформацію – заголовок представницького рівня, в якому містяться вказівки для протоколу представницького рівня машини-адресата. Отримане в результаті повідомлення передається вниз сеансовому рівню, який в свою чергу додає свій заголовок, і так далі. (Деякі реалізації протоколів поміщують службову інформацію не тільки спочатку повідомлення у вигляді заголовка, але і в кінці, у вигляді так званого «кінцевика».) Нарешті, повідомлення досягає нижнього, фізичного рівня, який саме і передає його по лініях зв’язку машині-адресату. До цього моменту повідомлення «обростає» заголовками всіх рівнів.

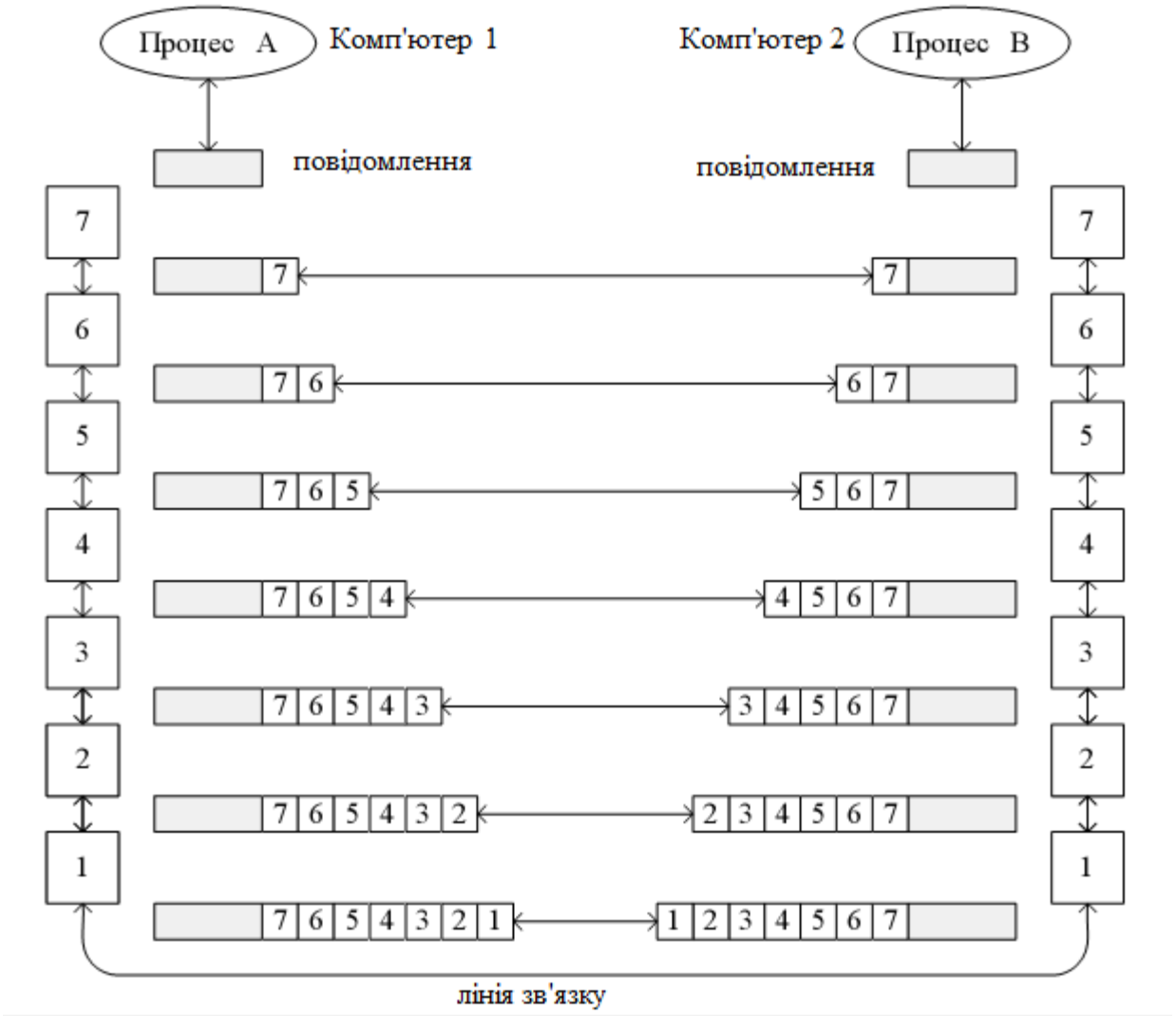


Рисунок 2.1. Модель взаємодії відкритих систем ISO/OSI

Коли повідомлення по мережі поступає на машину-адресат, воно приймається її фізичним рівнем і послідовно переміщується вверх з рівня на рівень. Кожний рівень аналізує і обробляє заголовок свого рівня, виконуючи відповідні даному рівню функції, а після цього видаляє цей заголовок і передає повідомлення вищому рівню.

Нарівні з терміном повідомлення (message) існують і інші терміни, що використовуються мережевими спеціалістами для позначення одиниць даних в процедурах обміну. В стандартах ISO для позначення одиниць даних, з якими мають справу протоколи різних рівнів, використовується загальна назва протокольний блок даних (*Protocol Data Unit, PDU*). Для позначення блоків даних певних рівнів часто використовуються спеціальні назви: кадр (frame), пакет (packet), дейтаграма (datagram), сегмент (segment).

Рівні моделі OSI

Фізичний рівень

Фізичний рівень (*Physical layer*) має справу з відправкою бітів по фізичних каналах зв'язку, таким, наприклад, як коаксіальний кабель, вита пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як полоса пропускання, перешкодозахищеність, хвильовий опір і інші. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад, крутизна фронтів імпульсів, рівні напруги або струму сигналу, що передається, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх приладах, що підключені до мережі. Зі сторони комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 10-Base-T технології Ethernet, яка визначає в якості використовуваного кабелю неекрановану виту пару категорії 3 з хвильовим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегменту 100 метрів, манчестерський код для представлення даних в кабелі, а також деякі інші характеристики середовища і електричних сигналів.

Канальний рівень

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, в яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайнята. Тому одним із завдань канального рівня (Data Link layer) є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення і корекції помилок. Для цього на канальному рівні біти групуються в набори, звані кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру, поміщаючи спеціальну послідовність біт в початок і кінець кожного кадру, для його виділення, а також

обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить по мережі, одержувач знову обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр вважається правильним і приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка. Канальний рівень може не тільки виявляти помилки, але і виправляти їх за рахунок повторної передачі пошкоджених кадрів. Необхідно відзначити, що функція виправлення помилок не є обов'язковою для канального рівня, тому в деяких протоколах цього рівня вона відсутня, наприклад, в Ethernet і Frame Relay.

У протоколах канального рівня, що використовуються в локальних мережах, закладена певна структура зв'язків між комп'ютерами і способи їх адресації. Хоча канальний рівень і забезпечує доставку кадру між будь-якими двома вузлами локальної мережі, він це робить тільки в мережі з абсолютно певною топологією зв'язків, саме тією топологією, для якої він був розроблений. До таких типових топологій, що підтримуються протоколами канального рівня локальних мереж, відносяться загальна шина, кільце і зірка, а також структури, отримані з них за допомогою мостів і комутаторів. Прикладами протоколів канального рівня є протоколи Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

В локальних мережах протоколи канального рівня використовуються комп’ютерами, мостами, комутаторами и маршрутизаторами. В комп’ютерах функції канального рівня реалізуються спільними зусиллями мережевих адаптерів і їх драйверів.

У глобальних мережах, які рідко володіють регулярною топологією, канальний рівень часто забезпечує обмін даними тільки між двома сусідніми комп'ютерами, сполученими індивідуальною лінією зв'язку. Прикладами протоколів «точка-точка» (як часто називають такі протоколи) можуть служити широко поширені протоколи PPP і LAP-B. У таких випадках для доставки повідомлень між кінцевими вузлами через всю мережу використовуються засоби і мережевого рівня. Саме так організовані мережі X.25. Іноді в глобальних мережах функції канального рівня в чистому вигляді виділити важко, оскільки в одному і

тому ж протоколі вони об'єднуються з функціями мережевого рівня. Прикладами такого підходу можуть служити протоколи технологій ATM і Frame Relay.

В цілому канальний рівень являє собою досить потужний і закінчений набір функцій по пересилці повідомлень між вузлами мережі. В деяких випадках протоколи канального рівня виявляються самодостатніми транспортними засобами і можуть допускати роботу поверх них безпосередньо протоколів прикладного рівня або програм, без залучення коштів мережевого і транспортного рівнів. Наприклад, існує реалізація протоколу управління мережею SNMP безпосередньо поверх Ethernet, хоча стандартно цей протокол працює поверх мережевого протоколу IP і транспортного протоколу UDP. Природно, що застосування такої реалізації буде обмеженим - вона не підходить для складних мереж різних технологій, наприклад Ethernet і X.25, і навіть для такої мережі, в якій у всіх сегментах застосовується Ethernet, але між сегментами існують петлевидні зв'язки. А ось в двохсегментній мережі Ethernet, об'єднаній мостом, реалізація SNMP над канальним рівнем буде цілком працездатна.

Тим не менш для забезпечення якісного транспортування повідомлень в мережах будь-яких топологій і технологій функцій канального рівня виявляється недостатньо, тому в моделі OSI рішення цієї задачі покладається на два наступних рівня – мережевий і транспортний.

Мережевий рівень

Мережевий рівень (*Network layer*) служить для утворення єдиної транспортної системи, що об’єднує декілька мереж, причому ці мережі можуть використовувати зовсім різні принципи передачі повідомлень між кінцевими вузлами і володіти довільною структурою зв’язків. Функції мережевого рівня достатньо різноманітні.

Протоколи канального рівня локальних мереж забезпечують доставку даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією, наприклад топологією ієрархічної зірки. Це дуже жорстке обмеження, яке не дозволяє будувати мережі з розвиненою структурою, наприклад, мережі, що об'єднують декілька мереж підприємства в єдину мережу, або високонадійні

мережі, в яких існують надмірні зв'язки між вузлами. Можна було б ускладнювати протоколи канального рівня для підтримки петлевидних надлишкових зв'язків, але принцип поділу обов'язків між рівнями призводить до іншого рішення. Щоб з одного боку зберегти простоту процедур передачі даних для типових топологій, а з іншого допустити використання довільних топологій, вводиться додатковий мережевий рівень.

На мережевому рівні сам термін *мережа* наділяють специфічним значенням. В даному випадку під мережею розуміється сукупність комп'ютерів, що з'єднані між собою в відповідності з одною з стандартних типових топологій і використовують для передачі даних один з протоколів канального рівня, визначений для цієї топології.

Всередині мережі доставка даних забезпечується відповідним канальним рівнем, а ось доставкою даних між мережами займається мережевий рівень, який і підтримує можливість правильного вибору маршруту передачі даних навіть в тому випадку, коли структура зв'язків між складовими мережами має характер, відмінний від прийнятого в протоколах канального рівня. Мережі з'єднуються між собою спеціальними пристроями, званими маршрутизаторами. *Маршрутизатор* - це пристрій, який збирає інформацію про топологію міжмережевих з'єднань і на її підставі пересилає пакети мережевого рівня в мережу призначення. Щоб передати повідомлення від відправника, що знаходиться в одній мережі, одержувачу, що знаходиться в іншій мережі, треба здійснити деяку кількість транзитних передач між мережами, або хопів (від hop - стрибок), кожний раз вибираючи відповідний маршрут. Таким чином, маршрут являє собою послідовність маршрутизаторів, через які проходить пакет.

Проблема вибору найкращого шляху називається *маршрутизацією*, і її рішення є однією з головних задач мережевого рівня. Ця проблема ускладнюється тим, що самий короткий шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту; воно залежить від пропускної здатності каналів зв'язку і інтенсивності трафіка, яка може змінюватися з плином часу. Деякі алгоритми маршрутизації намагаються пристосуватися до зміни

навантаження, в той час як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися і за іншими критеріями, наприклад надійності передачі.

У загальному випадку функції мережевого рівня ширші, ніж функції передачі повідомлень по зв'язках з нестандартною структурою, які розглянуті на прикладі об'єднання декількох локальних мереж. Мережевий рівень вирішує також задачі узгодження різних технологій, спрощення адресації у великих мережах і створення надійних і гнучких бар'єрів на шляху небажаного трафіка між мережами.

Блок даних мережевого рівня прийнято називати *пакетами* (packets). При організації доставки пакетів на мережевому рівні використовується поняття «номер мережі». У цьому випадку адреса одержувача складається з старшої частини - номера мережі і молодшої - номеру вузла в цій мережі. Всі вузли однієї мережі повинні мати одну і ту ж старшу частину адреси, тому терміну «мережа» на мережевому рівні можна дати й інше, більш формальне визначення: мережа - це сукупність вузлів, мережева адреса яких містить один і той же номер мережі.

На мережевому рівні визначаються два види протоколів. Перший вид – *мережеві протоколи (routed protocols)* – реалізують просування пакетів через мережу. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережевого рівня. Однак часто до мережевого рівня відносять и інший вид протоколів, що називаються протоколами обміну маршрутною інформацією або просто *протоколами маршрутизації (routing protocols)*. З допомогою цих протоколів маршрутизатори збирають інформацію про топології міжмережевих з’єднань. Протоколи мережевого рівня реалізуються програмними модулями операційної системи, а також програмними і апаратними засобами маршрутизаторів.

На мережевому рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, що використовується на мережевому рівні, в локальну адресу мережі. Такі протоколи часто називають *протоколами роздільної здатності адрес – Address Resolution Protocol, ARP*. Іноді їх відносять

не до мережевого рівня, а до канального, хоча тонкості класифікації не змінюють їх сутності. Прикладами протоколів мережевого рівня являються протокол міжмережевої взаємодії IP стека TCP/IP і протокол міжмережевого обміну пакетами IPX стека Novell.

Транспортний рівень

На шляху від відправника до одержувача пакети можуть бути спотворені або загублені. Хоча деякі програми мають власні засоби обробки помилок, існують і такі, які вважають за краще відразу мати справу з надійним з'єднанням. Транспортний рівень (*Transport layer*) забезпечує програмам або верхнім рівням стеку - прикладному і сеансовому - передачу даних з тим ступенем надійності, яка їм потрібна. Модель OSI визначає п'ять класів сервісу, що надаються транспортним рівнем. Ці види сервісу відрізняються якістю послуг, що надаються: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне - здатність до виявлення і виправлення помилок передачі, таких як спотворення, втрата і дублювання пакетів.

Вибір класу сервісу транспортного рівня визначається, з одного боку, тим, якою мірою задача забезпечення надійності вирішується самими програмами і протоколами більш високих, ніж транспортний, рівнів, а з іншого боку, цей вибір залежить від того, наскільки надійною є система транспортування даних в мережі, що забезпечується рівнями, розташованими нижче транспортного - мережевим, канальним і фізичним. Так, наприклад, якщо якість каналів передачі зв'язку дуже висока і вірогідність виникнення помилок, не виявлених протоколами більш низьких рівнів, невелика, то розумно скористатися одним з полегшених сервісів транспортного рівня, не обтяжених численними перевірками, квитуванням і іншими прийомами підвищення надійності. Якщо ж транспортні засоби нижніх рівнів від початку дуже ненадійні, то доцільно звернутися до найбільш розвиненого сервісу транспортного рівня, який працює, використовуючи максимум засобів для виявлення та усунення помилок, - за допомогою

попереднього встановлення логічного з'єднання, контролю доставки повідомлень по контрольних сумах і циклічній нумерації пакетів , встановлення тайм-аутів доставки і т. п.

Блок даних транспортного рівня прийнято називати *дейтаграмами (datagram)*.

Як правило, всі протоколи, починаючи з транспортного рівня и вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережевих операційних систем. В якості прикладу транспортних протоколів можна привести протоколи TCP і UDP стека TCP/IP і протокол SPX стеку Novell.

Протоколи нижніх чотирьох рівнів узагальнено називають мережевим транспортом або транспортною підсистемою, так як вони повністю рішають задачу транспортування повідомлень з заданим рівнем якості в складових мережах з довільною топологією і різними технологіями. Інші три верхні рівні вирішують задачі надання прикладних сервісів на основі наявної транспортної підсистеми.

Сеансовий рівень

Сеансовий рівень (*Session layer*) забезпечує управління діалогом: фіксує, яка з сторін являється активною в даний момент, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у випадку відмови можна було вернутися назад до останньої контрольної точки, а не починати все з початку. На практиці небагато програм використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто об’єднують з функціями прикладного рівня і реалізують в одному протоколі.

Представницький рівень

Представницький рівень (*Presentation layer*) має справу з формою представлення інформації, що передається по мережі, не міняючи при цьому її змісту. За рахунок рівня представлення інформація, що передається прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. З допомогою засобів даного рівня протоколи прикладних рівнів можуть подолати

синтаксичні відмінності в представлення даних або ж відмінності в кодах символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватись шифрування і дешифрування даних, завдяки якому секретність обміну даними забезпечується зразу для всіх прикладних служб. Прикладом такого протоколу являється протокол Secure Socket Layer (SSL), який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень

Прикладний рівень (*Application layer*) – це в дійсності просто набір різноманітних протоколів, з допомогою яких користувачі мережі отримують доступ до ресурсів, що розділяються, таким як файли, принтери або гіпертекстові Web-сторінки, а також організують свою сумісну роботу, наприклад, з допомогою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, звичайно називається *повідомленням (message).*

Існує дуже велика різноманітність служб прикладного рівня, наприклад, декілька найбільш поширених реалізацій файлових служб: NCP в операційній системі Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP и TFTP, що входять в стек TCP/IP.

Типовий склад обладнання локальної мережі

Фрагмент комп'ютерної мережі (рисунок 2.2) включає основні типи комунікаційного обладнання, що застосовується для утворення локальних мереж і з'єднання їх через глобальні зв'язки один з одним. Для побудови локальних зв'язків між комп'ютерами використовуються різні види кабельних систем, мережеві адаптери, концентратори (повторювачі), мости, комутатори і маршрутизатори. Для підключення локальних мереж до глобальних зв'язків використовуються спеціальні виходи (WAN-порти) мостів і маршрутизаторів, а також апаратура передачі даних по довгих лініях – DSL модеми (при роботі по аналогових лініях) або ж прилади підключення до цифрових каналів (ТА – термінальні адаптери мереж ISDN, пристрої обслуговування цифрових виділених каналів типу CSU/DSU і т.п.).

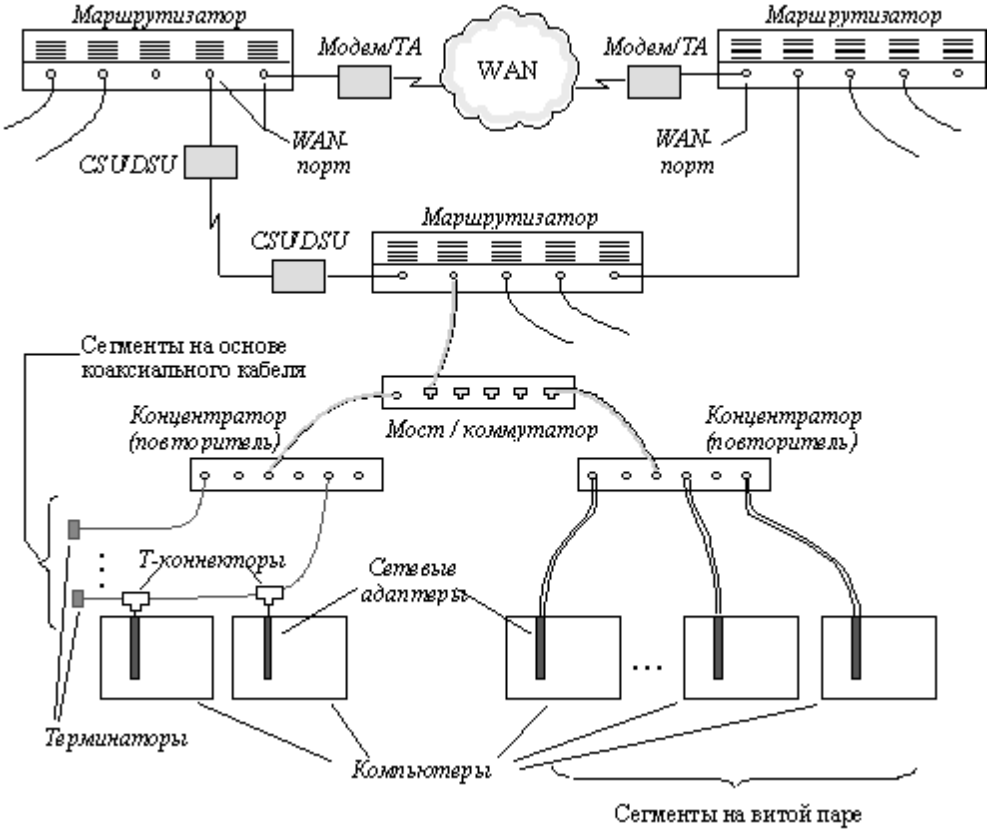


Рисунок 2.2 Фрагмент мережі

Роль кабельної системи

Для побудови локальних зв'язків в комп'ютерних мережах використовуються різні види кабелів - коаксіальний кабель, кабель на основі екранованої (STP - Shielded twisted pair) і неекранованої (UTP - Unshielded twisted pair) витої пари і оптоволоконний кабель. Найбільш популярним видом середовища передачі даних на невеликі відстані (до 100 м) стає неекранована вита пара, яка включена практично в усі сучасні стандарти і технології локальних мереж і забезпечує пропускну здатність до 1000 Мб / с (на кабелях категорії 5е). Оптоволоконний кабель широко застосовується як для побудови локальних мереж, так і для утворення магістралей глобальних мереж. Оптоволоконний кабель може забезпечити дуже високу пропускну здатність каналу (до декількох десятків Гб / с) і передачу на значні відстані (до декількох десятків кілометрів без проміжного посилення сигналу).

В якості середовища передачі даних в комп'ютерних мережах використовуються також електромагнітні хвилі різних частот – КВ, УКВ, СВЧ.

Згідно з дослідженнями, 70% часу простоїв обумовлено проблемами, що

виникають внаслідок низької якості кабельних систем, що застосовуються. Тому так важливо правильно побудувати фундамент мережі – кабельну систему. Останнім часом в якості такої надійної основи все частіше використовується структурована кабельна система.

Структурована кабельна система (Structured Cabling System, SCS) – це набір комутаційних елементів (кабелів, роз'ємів, конекторів, кросових панелей і шаф), а також методика їх сумісного використання, яка дозволяє створювати регулярні, легко розширювані структури зв'язків в комп'ютерних мережах.

Переваги структурованої кабельної системи:

• Універсальність. Структурована кабельна система при продуманій організації може стати єдиним середовищем для передачі комп'ютерних даних у локальній комп'ютерній мережі, організації локальної телефонної мережі, передачі відеоінформації і навіть передачі сигналів від датчиків пожежної безпеки або охоронних систем. Це дозволяє автоматизувати багато процесів з контролю, моніторингу та управління господарськими службами і системами життєзабезпечення.

• Збільшення строку служби. Строк старіння добре структурованої кабельної системи може складати 8-10 років.

• Зменшення вартості додавання нових користувачів і зміни їх місць розміщення. Вартість кабельної системи в основному визначається не вартістю кабелю, а вартістю робіт з його прокладанні. Тому більш вигідно провести одноразову роботу з прокладання кабелю, можливо з великим запасом по довжині, ніж кілька разів виконувати прокладку, нарощуючи довжину кабелю. Це допомагає швидко і дешево змінювати структуру кабельної системи при переміщеннях персоналу або зміні програм.

• Можливість легкого розширення мережі. Структурована кабельна система являється модульною, тому її легко нарощувати, дозволяючи легко и ціною малих затрат переходити на більш досконале обладнання, що задовольняє потребам до систем комунікацій, які ростуть.

• Забезпечення більш ефективного обслуговування. Структурована

кабельна система полегшує обслуговування і пошук несправностей в порівнянні з шинною кабельною системою.

• Надійність. Структурована кабельна система має підвищену надійність, оскільки звичайно виробництво всіх її компонентів і технічний супровід виконується однією фірмою-виробником.

Мережеві адаптери

Мережевий адаптер (*Network Interface Card, NIC*) – це периферійний пристрій комп'ютера,що безпосередньо взаємодіє із середовищем передачі даних, яке прямо або через інше комунікаційне обладнання зв'язує його з іншими комп'ютерами. Цей пристрій вирішує задачі надійного обміну двійковими даними, що представлені відповідними електромагнітними сигналами, по зовнішніх лініях зв'язку. Як і будь-який контролер комп'ютера, мережевий адаптер працює під управлінням драйвера операційної системи і розподіл функцій між мережевим адаптером і драйвером може змінюватись від реалізації до реалізації.

У перших локальних мережах мережевий адаптер з сегментом коаксіального кабелю представляв собою весь спектр комунікаційного обладнання, за допомогою якого організовувалася взаємодія комп'ютерів. Мережевий адаптер комп'ютера-відправника безпосередньо по кабелю взаємодіяв з мережевим адаптером комп'ютера-одержувача. У більшості сучасних стандартів для локальних мереж передбачається, що між мережевими адаптерами взаємодіючих комп'ютерів встановлюється спеціальне комунікаційний пристрій (концентратор, міст, комутатор або маршрутизатор), який бере на себе деякі функції з управління потоком даних.

Мережевий адаптер звичайно виконує наступні функції:

• Оформлення інформації, що передається у вигляді кадру певного формату. Кадр включає кілька службових полів, серед яких є адреса комп'ютера призначення і контрольна сума кадру, по якій мережевий адаптер станції призначення робить висновок про коректність доставленої по мережі інформації.

• Отримання доступу до середовища передачі даних. У локальних мережах

в основному застосовуються колективні між групою комп'ютерів канали зв'язку (загальна шина, кільце), доступ до яких надається за спеціальним алгоритмом (найбільш часто застосовуються метод випадкового доступу або метод з передачею маркера доступу по кільцю). В останніх стандартах і технологіях локальних мереж намітився перехід від використання колективного середовища передачі даних до використання індивідуальних каналів зв'язків комп'ютера з комунікаційними пристроями мережі, як це завжди робилося в телефонних мережах, де телефонний апарат пов'язаний з комутатором АТС індивідуальною лінією зв'язку. Технологіями, які використовують індивідуальні лінії зв'язку, є 100VG-AnyLAN, ATM і комутуючі модифікації традиційних технологій - switching Ethernet, switching Token Ring і switching FDDI. При використанні індивідуальних ліній зв'язку у функції мережевого адаптера часто входить встановлення з'єднання з комутатором мережі.

• Кодування послідовності біт кадру послідовністю електричних сигналів при передачі даних і декодування при їх прийомі. Кодування має забезпечити передачу вихідної інформацію по лініях зв'язку з певною смугою пропускання і певним рівнем перешкод таким чином, щоб приймаюча сторона змогла розпізнати з високим ступенем ймовірності надіслану інформацію. Так як в локальних мережах використовуються широкосмугові кабелі, то мережеві адаптери не використовують модуляцію сигналу, необхідну для передачі дискретної інформації по вузькосмугових лініях зв'язку (наприклад, телефонних каналах тональної частоти), а передають дані за допомогою імпульсних сигналів. Представлення ж двійкових 1 і 0 може бути різним.

• Перетворення інформації з паралельної форми в послідовну і назад. Ця операція зв’язана з тим, що для спрощення проблеми синхронізації сигналів і здешевлення ліній зв’язку в обчислювальних мережах інформація передається в послідовній формі, біт за бітом, а не побайтно, як всередині комп’ютера.

• Синхронізація бітів, байтів і кадрів. Для стійкого прийому переданої інформації необхідна підтримка постійного синхронізму приймача і передавача інформації. Мережевий адаптер використовує для вирішення цього завдання

спеціальні методи кодування, які не використовують додаткової шини з тактовими синхросигналами. Ці методи забезпечують періодичну зміну стану переданого сигналу, яке використовується тактовим генератором приймача для підстроювання синхронізму. Крім синхронізації на рівні бітів, мережевий адаптер вирішує задачу синхронізації і на рівні байтів, і на рівні кадрів.

Мережеві адаптери розрізняються за типом і розрядності використовуваної в комп'ютері внутрішньої шини даних - ISA, EISA, PCI, MCA.

Мережеві адаптери розрізняються також за типом використовуваної мережевої технології - Ethernet, Token Ring, FDDI і т.п. Як правило, конкретна модель мережевого адаптера працює за певною мережевою технологією (наприклад, Ethernet). У зв'язку з тим, що для кожної технології зараз є можливість використання різних середовищ передачі даних (той же Ethernet підтримує коаксіальний кабель, неекрановану виту пару і оптоволоконний кабель), мережевий адаптер може підтримувати як одну, так і одночасно кілька середовищ. У випадку, коли мережевий адаптер підтримує тільки одне середовище передачі даних, а необхідно використовувати інше, застосовуються медіаконвертори.

Фізична структуризація локальної мережі. Повторювачі і концентратори

Для побудови простої односегментної мережі достатньо мати мережеві адаптери і кабель підходящого типу. Але навіть в цьому простому випадку часто використовуються додаткові пристрої – повторювачі сигналів, що дозволяють подолати обмеження на максимальну довжину кабельного сегменту.

Основна функція повторювача (*repeater*), як це слідує з його назви – повторення (і підсилення) сигналів, що поступають на один із його портів, на всіх інших портах (Ethernet) або на наступному в логічному кільці порту (Token Ring, FDDI) синхронно з сигналами-оригіналами. Повторювач покращує електричні характеристики сигналів і їх синхронність, і за рахунок цього появляється можливість збільшувати загальну довжину кабелю між самими віддаленими в мережі станціями.

Багатопортовий повторювач часто називають концентратором (hub, concentrator), що відображає той факт, що даний пристрій реалізує не тільки

функцію повторення сигналів, але і концентрує в одному центральному пристрої функції об’єднання комп’ютерів в мережу. Практично у всіх сучасних мережевих стандартах концентратор являється необхідним елементом мережі, що з’єднує окремі комп’ютери в мережу.

Відрізки кабелю, що з’єднують два комп’ютери або якісь два інших мережевих пристрої, називаються фізичними сегментами. Таким чином, концентратори і повторювачі, які використовуються для додавання нових фізичних сегментів, являються засобом фізичної структуризації мережі.

Концентратори утворюють з окремих фізичних відрізків кабелю загальне середовище передачі даних - логічний сегмент (рисунок 2.3). Логічний сегмент також називають доменом колізій, оскільки при спробі одночасної передачі даних будь-яких двох комп'ютерів цього сегмента, що хоча б і належать різним фізичним сегментам, виникає блокування передавальної середовища. Слід особливо підкреслити, що яку б складну структуру не утворювали концентратори, наприклад, шляхом ієрархічного з'єднання, всі комп'ютери, підключені до них, утворюють єдиний логічний сегмент, в якому будь-яка пара взаємодіючих комп'ютерів повністю блокує можливість обміну даними для інших комп'ютерів.

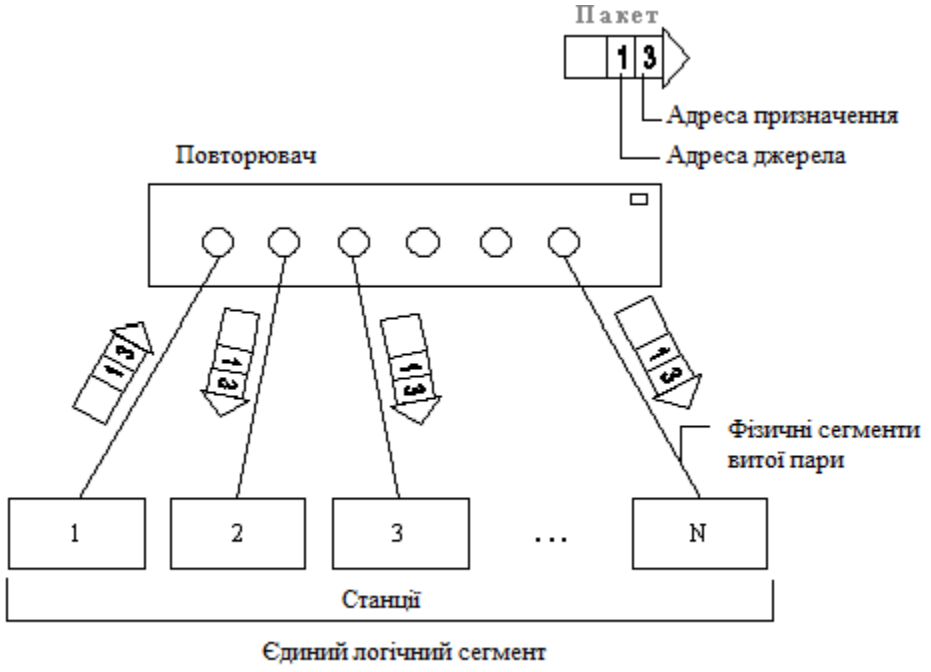


Рисунок 2.3. Повторювач Ethernet синхронно повторяє біти кадру на всіх своїх портах

Поява пристроїв, що централізують з'єднання між окремими мережевими

пристроями, потенційно дозволяє поліпшити керованість мережі та її експлуатаційні характеристики (модифікованість, ремонтопридатність і т.п.). З цією метою розробники концентраторів часто вбудовують в свої пристрої, крім основної функції повторювача, ряд допоміжних функцій, вельми корисних для поліпшення якості мережі.

Різні виробники концентраторів реалізують в своїх пристроях різні набори допоміжних функцій, але найбільш часто зустрічаються наступні:

• Об'єднання сегментів з різними фізичними середовищами (наприклад, коаксіальний кабель, вита пара і оптоволокно) в єдиний логічний сегмент.

• Автосегментація портів – автоматичне відключення порта при його некоректній поведінці (пошкодження кабелю, інтенсивна генерація пакетів помилкової довжини і т.п.).

• Підтримка між концентраторами резервних зв'язків, які використовуються при відмові основних.

• Захист даних, що передаються по мережі, від несанкціонованого доступу (наприклад, шляхом спотворення поля даних в кадрах, що повторяються на портах, що не містять комп'ютера з адресою призначення).

Підтримка засобів управління мережами – протоколу SNMP, баз керівної інформації MIB.

Логічна структуризація мережі. Мости і комутатори

Незважаючи на появу нових додаткових можливостей, основною функцією концентраторів залишається передача пакетів по загальному роздільному середовищі. Колективне використання багатьма комп'ютерами загальної кабельної системи в режимі поділу часу призводить до істотного зниження продуктивності мережі при інтенсивному трафіку. Загальне середовище перестає справлятися з потоком кадрів, що передаються, та в мережі виникає черга комп'ютерів, які очікують доступу. Це явище характерне для всіх технологій, які використовують колективні середовища передачі даних, незалежно від використовуваних алгоритмів доступу (хоча найбільш потерпають від перевантажень трафіку мережі Ethernet з методом випадкового доступу до середовища).

Тому мережі, побудовані на основі концентраторів, не можуть розширюватися в необхідних межах - при певній кількості комп'ютерів в мережі або при появі нових програм завжди відбувається насичення передавального середовища, і затримки в її роботі стають неприпустимими. Ця проблема може бути вирішена шляхом логічної структуризації мережі за допомогою мостів, комутаторів і маршрутизаторів.

Міст (bridge), а також його швидкодіючий функціональний аналог - комутатор (switch), ділить загальне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання кількох фізичних сегментів (відрізків кабелю) за допомогою одного або декількох концентраторів. Кожний логічний сегмент підключається до окремого порту комутатора/моста (рисунок 2.4). При надходженні кадру на який-небудь з портів комутатор/міст повторює цей кадр, але не на всіх портах, як це робить концентратор, а тільки на тому порту, до якого підключений сегмент, що містить комп'ютер-адресат.

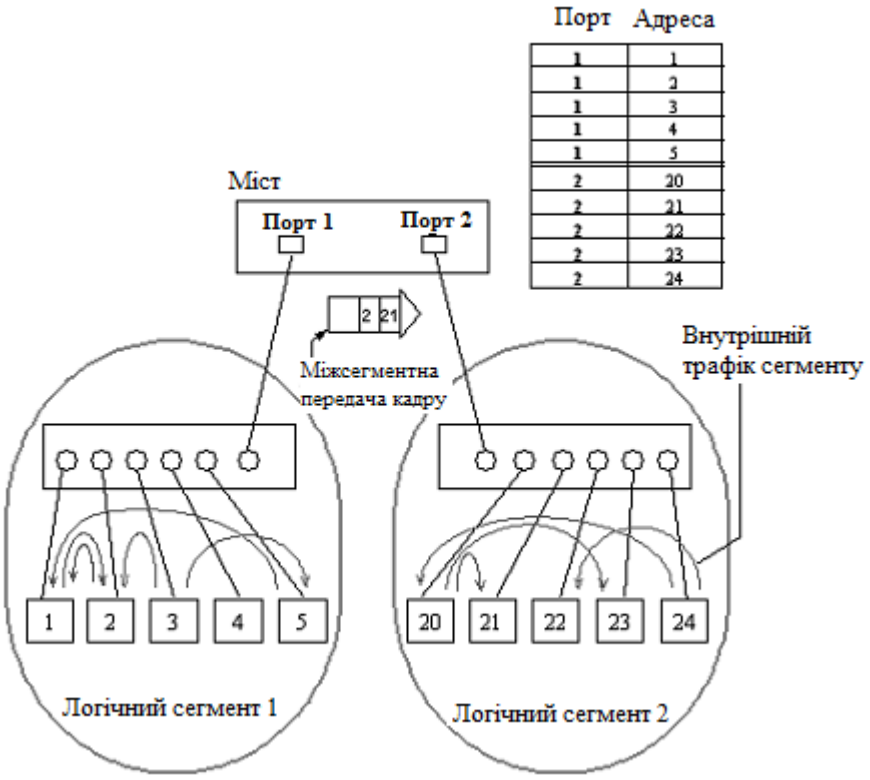


Рисунок 2.4. Розділення мережі на логічні сегменти

При роботі комутатора/ моста середовище передачі даних кожного логічного сегмента залишається спільним тільки для тих комп'ютерів, які підключені до

цього сегменту безпосередньо. Комутатор/ міст здійснює зв'язок середовищ передачі даних різних логічних сегментів. Він передає кадри між логічними сегментами тільки при необхідності, тобто тільки тоді, коли взаємодіючі комп'ютери знаходяться в різних сегментах.

Розподіл мережі на логічні сегменти покращує продуктивність мережі, якщо в мережі є групи комп'ютерів, які переважно обмінюються інформацією між собою. Якщо ж таких груп немає, то введення в мережу комутаторів/мостів може тільки погіршити загальну продуктивність мережі, так як прийняття рішення про те, чи потрібно передавати кадр з одного сегмента в інший, вимагає додаткового часу. Однак навіть у мережі середніх розмірів такі групи, як правило, є. Тому поділ її на логічні сегменти дає виграш в продуктивності - трафік локалізується в межах груп, і навантаження на їх колективні кабельні системи істотно зменшується.

Комутатори/мости приймають рішення про те, на який порт потрібно передати кадр, аналізуючи адресу призначення, поміщену в кадрі, а також на підставі інформації про належність того чи іншого комп'ютера до певного сегменту, підключеному до одного з портів комутатора/моста, тобто на підставі інформації про конфігурацію мережі. Для того щоб зібрати і обробити інформацію про конфігурацію підключених до нього сегментів, комутатор/міст повинен пройти стадію "навчання", тобто самостійно виконати деяку попередню роботу з вивчення трафіку, що проходить по ньому. Визначення приналежності комп'ютерів сегментами можливо за рахунок наявності в кадрі не тільки адреси призначення, а й адреси джерела, що згенерувало кадр. Використовуючи інформацію про адресу джерела, комутатор/міст встановлює відповідність між номерами портів та адресами комп'ютерів. В процесі вивчення мережі комутатор/міст просто передає кадри, що з’являються на входах його портів, на всі інші порти, працюючи деякий час повторювачем. Після того, як комутатор/міст дізнається про приналежність адрес сегментам, він починає передавати кадри між портами тільки в разі міжсегментної передачі. Якщо, вже після завершення навчання, на вході комутатора раптом з'явиться кадр з невідомою адресою

призначення, то цей кадр буде повторений на всіх портах.

Комутатори/мости, що працюють описаним способом, зазвичай називаються прозорими (transparent), оскільки поява таких комутаторів/мостів у мережі зовсім не помітна для її кінцевих вузлів. Це дозволяє не змінювати їх програмне забезпечення при переході від простих конфігурацій, що використовують тільки концентратори, до більш складних, сегментованих.

Існує й інший клас комутаторів/мостів, що передають кадри між сегментами на основі повної інформації про міжсегментні маршрути. Цю інформацію записує в кадр станція-джерело кадру, тому говорять, що такі пристрої реалізують алгоритм маршрутизації від джерела (source routing). При використанні комутаторів/мостів з маршрутизацією від джерела кінцеві вузли повинні бути в курсі ділення мережі на сегменти і мережеві адаптери, в цьому випадку повинні в своєму програмному забезпеченні мати компонент, який займається вибором маршруту кадрів.

За простоту принципу роботи прозорого комутатора/моста доводиться розплачуватися обмеженнями на топологію мережі, побудованої з використанням пристроїв даного типу - такі мережі не можуть мати замкнутих маршрутів - петель. Комутатор/ міст не може правильно працювати в мережі з петлями, при цьому мережа засмічується зацикленими пакетами та її продуктивність знижується.

Для автоматичного розпізнавання петель в конфігурації мережі розроблений алгоритм покриваючого дерева (Spanning Tree Algorithm, STA). Цей алгоритм дозволяє комутаторам/мостам адаптивно будувати дерево зв'язків, коли вони вивчають топологію зв'язків сегментів за допомогою спеціальних тестових кадрів. При виявленні замкнутих контурів деякі зв'язки оголошуються резервними. Комутатор/міст може використовувати резервний зв'язок тільки при відмові якогось основного. В результаті мережі, побудовані на основі комутаторів/мостів, що підтримують алгоритм покриваючого дерева, володіють деяким запасом надійності, але підвищити продуктивність за рахунок використання декількох паралельних зв'язків у таких мережах не можна.

Маршрутизатори

Маршрутизатор (*router*) дозволяє організувати в мережі надлишкові зв’язки, що утворюють петлі. Він справляється з цією задачею за рахунок того, що приймає рішення про передачу пакетів на основі більш повної інформації про граф зв’язків в мережі, ніж міст або комутатор. Маршрутизатор має у своєму розпорядженні базу топологічної інформації, яка говорить йому, наприклад, про те, між якими підмережами загальної мережі є зв'язки і в якому стані (працездатному чи ні) вони знаходяться. Маючи таку карту мережі, маршрутизатор може вибрати один з декількох можливих маршрутів доставки пакета адресату. В даному випадку під маршрутом розуміють послідовність проходження пакетом маршрутизаторів. Наприклад, на рисунку 2.5 для зв'язку станцій L2 мережі LAN1 і L1 мережі LAN6 є два маршрути: M1-M5-M7 і M1-M6-M7.

На відміну від комутатора/моста, який не знає, як пов'язані сегменти один з одним за межами його портів, маршрутизатор бачить всю картину зв'язків підмереж один з одним, тому він може вибрати правильний маршрут і при наявності декількох альтернативних маршрутів. Рішення про вибір того чи іншого маршруту приймається кожним маршрутизатором, через який проходить повідомлення.

Для того, щоб скласти карту зв'язків у мережі, маршрутизатори обмінюються спеціальними службовими повідомленнями, в яких міститься інформація про ті зв'язки між підмережами, про які вони знають (ці підмережі підключені до них безпосередньо або ж вони дізналися цю інформацію від інших маршрутизаторів).

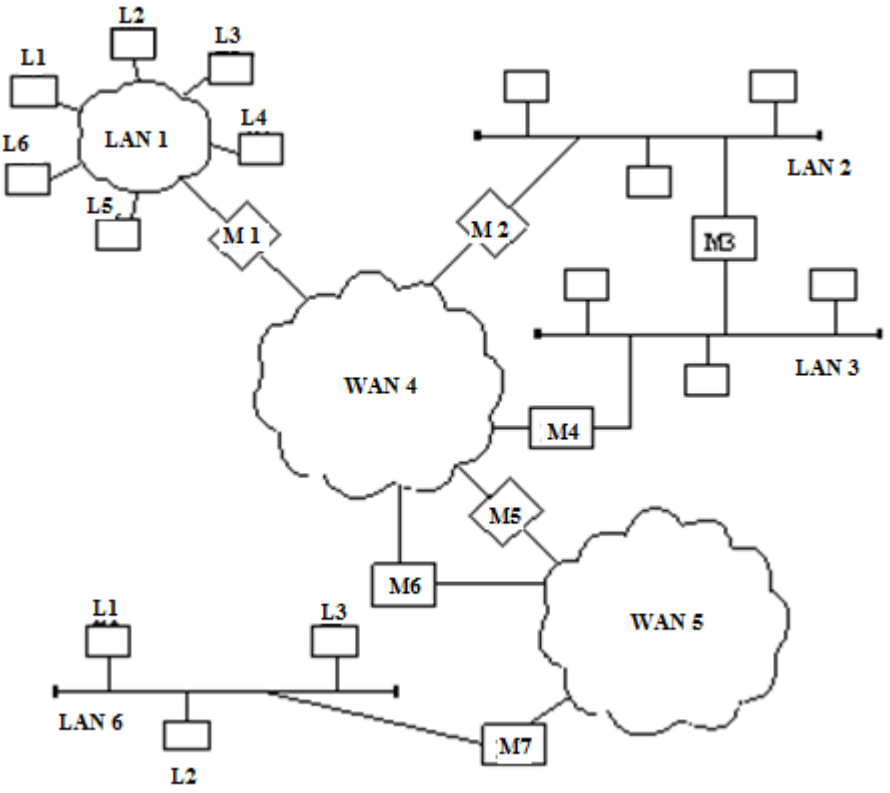


Рисунок 2.5. Структура інтермережі, побудованої на основі маршрутизаторів:

M1, M2, ... , M7 - маршрутизатори

LAN1, LAN2, LAN3, WAN4, WAN5, LAN6 – унікальні номери мереж в єдиному форматі

L1, L2, ... - локальні номери вузлів (дублюються, різний формат)

Побудова графа зв'язків між підмережами і вибір оптимального по якомусь критерію маршруту на цьому графі являють собою складну задачу. При цьому можуть використовуватися різні критерії вибору маршруту - найменша кількість проміжних вузлів, час, вартість або надійність передачі даних.

Маршрутизатори дозволяють об'єднувати мережі з різними принципами організації в єдину мережу, яка в цьому випадку часто називається інтермережа (internet). Назва інтермережа підкреслює ту особливість, що утворене за допомогою маршрутизаторів об'єднання комп'ютерів представляє собою сукупність декількох мереж, що зберігають велику ступінь автономності, ніж кілька логічних сегментів однієї мережі. У кожній з мереж, що утворюють інтермережу, зберігаються властиві їм принципи адресації вузлів і протоколи обміну інформацією. Тому маршрутизатори можуть об'єднувати не тільки локальні мережі з різною технологією, а й локальні мережі з глобальними.

Маршрутизатори не тільки об'єднують мережі, але і надійно захищають їх один від одного. Причому ця ізоляція здійснюється набагато простіше і надійніше, ніж за допомогою комутаторів/мостів. Наприклад, при вступі кадру з неправильною адресою комутатор/міст зобов'язаний повторити його на всіх своїх портах, що робить мережу незахищеною від некоректно працюючого вузла. Маршрутизатор ж у такому випадку просто відмовляється передавати "неправильний" пакет далі, ізолюючи дефектний вузол від іншої мережі.

Крім того, маршрутизатор надає адміністратору зручні засоби фільтрації потоку повідомлень за рахунок того, що сам розпізнає багато із полів службової інформації в пакеті і дозволяє їх іменувати зрозумілим адміністратору чином. Потрібно зауважити, що деякі комутатори/мости також здатні виконувати функції гнучкої фільтрації, але ставити умови фільтрації адміністратор мережі повинен сам у двійковому форматі, що досить складно.

Крім фільтрації, маршрутизатор може забезпечувати пріоритетний порядок обслуговування буферизованих пакетів, коли на підставі деяких ознак пакетам надаються переваги при виборі з черги.

В результаті, маршрутизатор виявляється складним інтелектуальним пристроєм, побудованим на базі одного, а іноді й кількох потужних процесорів. Такий спеціалізований мультипроцесор працює, як правило, під управлінням спеціалізованої операційної системи.

Функціональна відповідність видів комунікаційного обладнання рівням моделі OSI

Кращим способом для розуміння відмінностей між мережевими адаптерами, повторювачами, комутаторами/мостами і маршрутизаторами являється розгляд їх роботи в термінах моделі OSI. Співвідношення між функціями цих пристроїв і рівнями моделі OSI показано на рисунку 2.6.

Повторювач, який регенерує сигнали, за рахунок чого дозволяє збільшувати довжину мережі, працює на фізичному рівні.

Мережевий адаптер працює на фізичному і канальному рівнях. До фізичного рівня відноситься та частина функцій мережевого адаптера, яка пов'язана з

прийомом і передачею сигналів по лінії зв'язку, а отримання доступу до поділюваного середовища передачі, розпізнавання MAC-адреси комп'ютера - це вже функція канального рівня.

Мости виконують велику частину своєї роботи на канальному рівні. Для них мережа представляється набором MAC-адрес пристроїв. Вони витягають ці адреси з заголовків, доданих до пакетів на канальному рівні, і використовують їх під час обробки пакетів для ухвалення рішення про те, на який порт відправити той або інший пакет. Мости не мають доступу до інформації про адреси мереж, що відноситься до більш високого рівня. Тому вони обмежені у прийнятті рішень про можливі шляхи або маршрути переміщення пакетів по мережі.

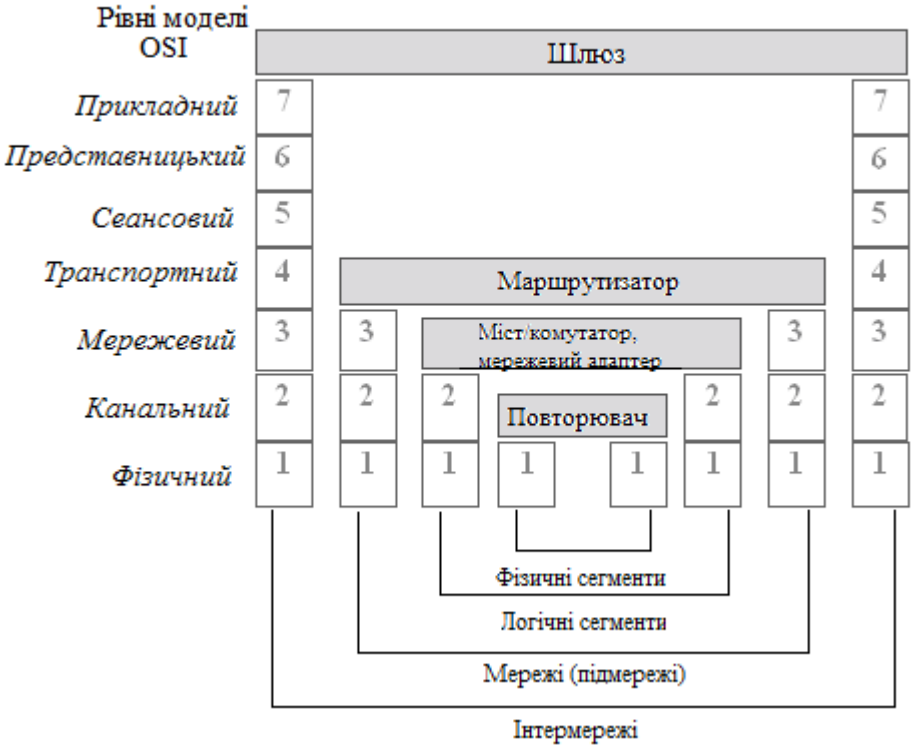


Рисунок 2.6. Відповідність функцій комунікаційного обладнання моделі OSI

Маршрутизатори працюють на мережевому рівні моделі OSI. Для маршрутизаторів мережа - це набір мережевих адрес пристроїв і безліч мережевих шляхів. Маршрутизатори аналізують усі можливі шляхи між будь-якими двома вузлами мережі і вибирають найкоротший з них. При виборі можуть прийматися до уваги і інші фактори, наприклад, стан проміжних вузлів і ліній зв'язку,

пропускна спроможність ліній або вартість передачі даних.

Для того, щоб маршрутизатор міг виконувати покладені на нього функції йому повинна бути доступна більш розгорнута інформація про мережу, ніж та, яка доступна мосту. У заголовку пакета мережевого рівня крім мережевої адреси є дані, наприклад, про критерій, який повинен бути використаний при виборі маршруту, про час життя пакета в мережі, про те, якому протоколу верхнього рівня належить пакет.

Завдяки використанню додаткової інформації, маршрутизатор може здійснювати більше операцій з пакетами, ніж комутатор/міст. Тому програмне забезпечення, необхідне для роботи маршрутизатора, є більш складним.

На рисунку 2.6 показаний ще один тип комунікаційних пристроїв - шлюз, який може працювати на будь-якому рівні моделі OSI. Шлюз (gateway) - це пристрій, що виконує трансляцію протоколів. Шлюз розміщується між взаємодіючими мережами і служить посередником, що переводить повідомлення, що надходять з однієї мережі, у формат іншої мережі. Шлюз може бути реалізований як тільки програмними засобами, встановленими на звичайному комп'ютері, так і на базі спеціалізованого комп'ютера. Трансляція одного стека протоколів в інший представляє собою складну інтелектуальну задачу, що вимагає максимально повної інформації про мережу, тому шлюз використовує заголовки всіх трансльованих протоколів.

ЗАВДАННЯ НА РОБОТУ

1. Використовуючи пакет NetCracker, вивчити склад і функціональні характеристики стандартного набору локальних мереж.

2. У відповідний розділ бази даних компонент додати опис нового елементу із вказаними характеристиками (табл. 2.1-2.4).

Таблиця 2.1. Варіанти завдань.

№ Варіанту	Тип адаптера	Тип концентратора	Тип комутатора
1	1	1	1
2	2	2	2
3	3	3	1
4	4	1	2
5	5	2	1
6	1	3	2
7	2	1	1
8	3	2	2
9	4	3	1
10	5	1	2
11	1	2	1
12	2	3	2
13	3	1	1
14	4	2	2
15	5	3	1

Таблиця 2.2 Типи мережевих адаптерів.

№	Виробник	Модель	Швидкість передачі, Мб/с	Тип слоту розширення	Тип середовища передачі	Макс. відстань до концентратора, м
1	DLink	DFE538TX	10/100	PCI	Ethernet, UTP, TX	100
2	Intel	EtherExpress 100+ TX	10/100	PCI	Ethernet, UTP, TX	100
3	IBM	EtherJet 100+ TX	10/100	PCI	Ethernet, UTP, TX	100
4	3Com	3C905B-TX	10/100	PCI	Ethernet, UTP, TX	100
5	3Com	FastEtherlink 3C980C	10/100	PCI	Ethernet, UTP, TX	100

Таблиця 2.3. Типи концентраторів.

№	Виробник	Модель	Тип портів	Кількість портів	Швидкість передачі, Мб/с
1	DLink	DFE 916Dx	Ethernet, TX	16	10/100
2	3COM	3C16750A	Ethernet, TX	8	10/100
3	Allied Telesyn	AT-FH7024E	Ethernet, TX	24	10/100

Таблиця 2.4. Типи комутаторів.

№	Виробник	Модель	Тип портів	Кількість портів	Швидкість передачі, Мб/с
1	Allied Telesyn	AT-8316SX	Ethernet, TX	16	10/100
2	Cisco	Catalist 3512-XL	Ethernet, TX	12	10/100

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

Визначте основні причини представлення Еталонної моделі у вигляді багаторівневої структури?
Визначте призначення канального рівня?
Визначте призначення мережевого рівня?
Визначте призначення представницького рівня?
Визначте призначення прикладного рівня?
Визначте призначення сеансового рівня?
Визначте призначення транспортного рівня?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Кулаков Ю.А., Омелянский С. В. Компьютерные сети. Выбор, установка, использование и администрирование – К.: Юниор, 1999.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 2-е издание – СПб.: Питер, 2003.

Комп’ютерний практикум № 3

ПОБУДОВА ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ETHERNET. МЕТОДИ ДОСТУПУ В ЛОКАЛЬНИХ МЕРЕЖАХ

Мета роботи: отримати навики вибору обладнання, кабельної системи для побудови інфраструктури локальної обчислювальної мережі рівня підприємства на основі технології Ethernet.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

У мережах Ethernet використовується метод доступу до середовища передачі даних, що називається методом колективного доступу з розпізнаванням несучої і виявленням колізій (carrier-sense-multiply-access with collision detection, CSMA / CD).

Цей метод застосовується виключно в мережах з логічною загальною шиною (до яких відносяться і радіомережі, що породили цей метод). Всі комп'ютери такої мережі мають безпосередній доступ до загальної шини, тому вона може бути використана для передачі даних між будь-якими двома вузлами мережі. Одночасно всі комп'ютери мережі мають можливість негайно (з урахуванням затримки поширення сигналу по фізичному середовищу) одержати дані, які будь-який з комп'ютерів почав передавати на загальну шину. Простота схеми підключення - це один з факторів, що визначили успіх стандарту Ethernet. Кажуть, що кабель, до якого підключені всі станції, працює в режимі колективного доступу (Multiply Access, MA).

Всі дані, що передаються по мережі, поміщаються в кадри певної структури і забезпечуються унікальною адресою станції призначення.

Щоб отримати можливість передавати кадр, станція повинна переконатися, що колективне середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, яка також називається несучою частотою (carrier-sense, CS). Ознакою незайнятості середовища є відсутність на ній несучої частоти, яка при манчестерському способі кодування рівна 5-10 МГц, залежно від послідовності одиниць і нулів, переданих в даний момент.

Якщо середовище вільне, то вузол 1 має право почати передачу кадру. Усі станції, підключені до кабелю, можуть розпізнати факт передачі кадру, і та станція, яка впізнає власну адресу в заголовках кадру, записує його вміст у свій внутрішній буфер, обробляє отримані дані, передає їх вгору по своєму стеку, а потім посилає по кабелю кадр-відповідь. Адреса станції джерела міститься у вихідному кадрі, тому станція-одержувач знає, кому потрібно послати відповідь.

Вузол 2 під час передачі кадру вузлом 1 також намагався почати передачу свого кадру, однак виявив, що середовище зайняте - на ній присутня несуча частота, - тому вузол 2 змушений чекати, поки вузол 1 не припинить передачу кадру.

Після закінчення передачі кадру усі вузли мережі зобов'язані витримати технологічну паузу (Inter Packet Gap) у 9,6 мкс. Ця пауза, що називається також міжкадровим інтервалом, 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, так як середовище вільне. Через затримки поширення сигналу по кабелю не всі вузли строго одночасно фіксують факт закінчення передачі кадру вузлом 1.

Виникнення колізії

При описаному підході можлива ситуація, коли дві станції одночасно намагаються передати кадр даних по загальному середовищу. Механізм прослуховування середовища і пауза між кадрами не гарантують відсутність виникнення такої ситуації, коли дві або більше станції одночасно вирішують, що середовище вільне, і починають передавати свої кадри. Кажуть, що при цьому відбувається *колізія (collision)*, тому що вміст обох кадрів зіштовхується на загальному кабелі і відбувається спотворення інформації - методи кодування, використовувані в Ethernet, не дозволяють виділяти сигнали кожної станції із загального сигналу.

Колізія - це нормальна ситуація в роботі мереж Ethernet. Для виникнення колізії не обов'язково, щоб кілька станцій почали передачу абсолютно одночасно, така ситуація малоймовірна. Набагато ймовірніше, що колізія виникає через те, що один вузол починає передачу раніше іншого, але до другого вузла сигнали першого просто не встигають дійти до того часу, коли другий вузол вирішує почати передачу свого кадру. Тобто колізії - це наслідок розподіленого характеру мережі.

Щоб коректно обробити колізію, усі станції одночасно спостерігають за

виникаючими на кабелі сигналами. Якщо передані і спостережувані сигнали відрізняються, то фіксується *виявлення колізії (collision detection, CD)*. Для збільшення імовірності якнайшвидшого виявлення колізії всіма станціями мережі станція, яка знайшла колізію, перериває передачу свого кадру (у довільному місці, можливо, і не на межі байта) і підсилює ситуацію колізії посилкою в мережу спеціальної послідовності з 32 біт, званої *jam-послідовністю*.

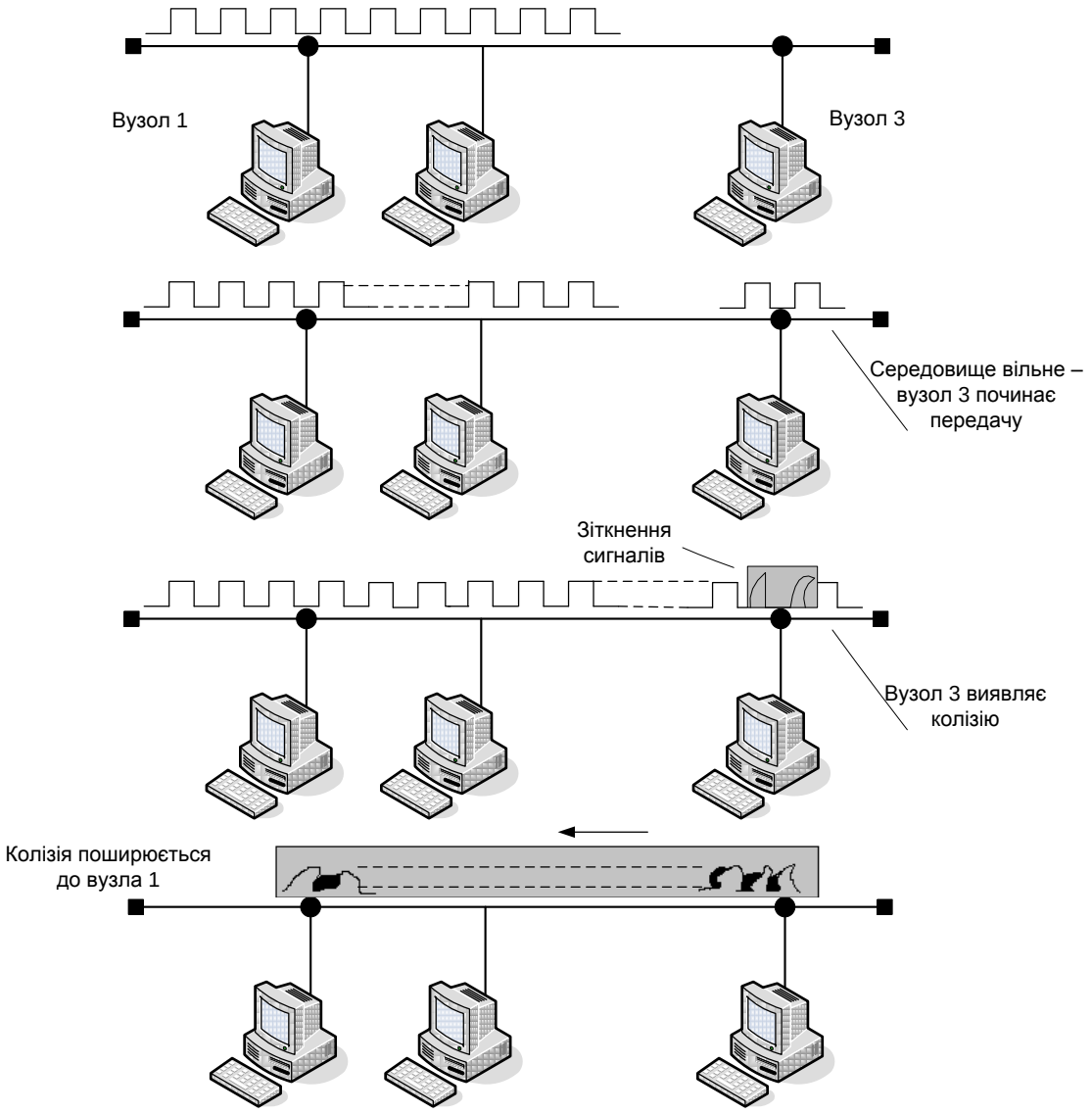


Схема виникнення та поширення колізії

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

Слід зазначити, що метод доступу CSMA/CD взагалі не гарантує станції, що вона коли-небудь зможе отримати доступ до середовища. Звичайно, при невеликому завантаженні мережі ймовірність такої події невелика, але при коефіцієнті використання мережі, що наближається до 1, така подія стає дуже ймовірною. Цей недолік методу випадкового доступу - плата за його надзвичайну простоту, яка зробила технологію Ethernet самою недорогою. Інші методи доступу - маркерний доступ мереж Token Ring і FDDI, метод Demand Priority мереж 100VG-AnyLAN - вільні від цього недоліку.

Специфікації фізичного середовища Ethernet

Історично перші мережі технології Ethernet були створені на коаксіальному кабелі діаметром 0,5 дюйма. Надалі були визначені й інші специфікації фізичного рівня для стандарту Ethernet, що дозволяють використовувати різні середовища передачі даних. Метод доступу CSMA/CD і всі тимчасові параметри залишаються одними і тими ж для будь-якої специфікації фізичного середовища технології Ethernet 10 Мбіт/с.

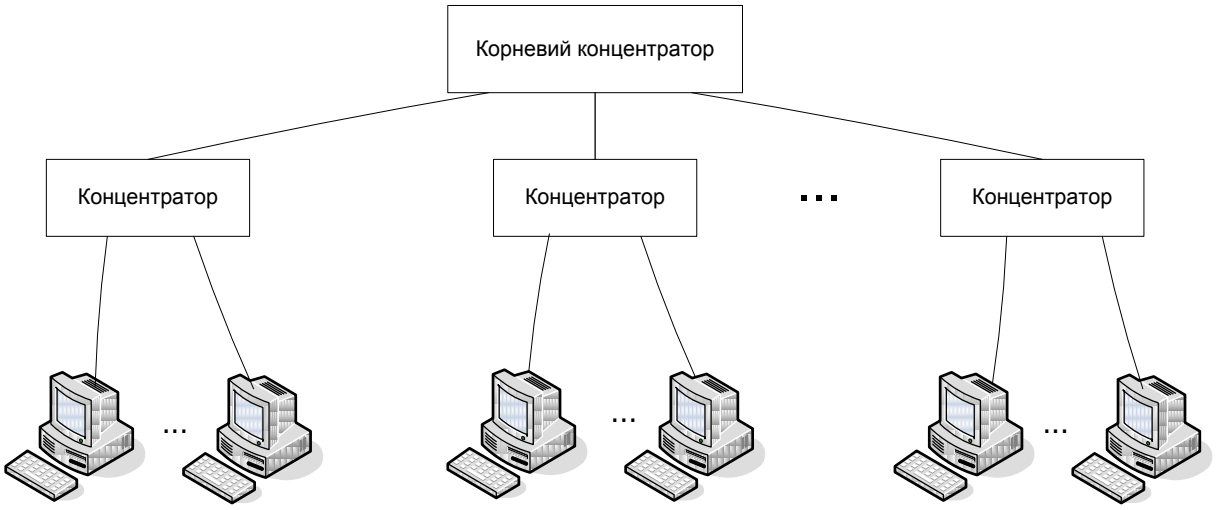
Фізичні специфікації технології Ethernet на сьогоднішній день включають наступні середовища передачі даних.

l0Base-5 - коаксіальний кабель діаметром 0,5 дюйма, що називається «товстим» коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента - 500 метрів (без повторювачів). Допускається підключення до одного сегмента не більш 100 вузлів, причому відстань між вузлами не повинна бути менше 2,5 м. Стандарт дозволяє використання в мережі не більше 4 повторювачів і, відповідно, не більше 5 сегментів кабелю. При максимальній довжині сегмента кабелю в 500 м це дає максимальну довжину мережі l0Base-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, так що максимальна конфігурація мережі являє собою два навантажених крайніх сегмента, які з'єднуються ненавантаженими сегментами ще з одним

центральним навантаженим сегментом. Правило застосування повторювачів у мережі Ethernet l0Base-5 зветься «правило 5-4-3». 5 сегментів, 4 повторювача, 3 навантажених сегмента. Обмежене число повторювачів пояснюється додатковими затримками поширення сигналу, які вони вносять. Застосування повторювачів збільшує час подвійного поширення сигналу, яке для надійного розпізнавання колізій не повинно перевищувати час передачі кадру мінімальної довжини.

l0Base-2 - коаксіальний кабель діаметром 0,25 дюйма, так званий «тонкий» коаксіал. Має хвильовий опір 50 Ом. Максимальна довжина сегмента - 185 метрів (без повторювачів). Максимальна кількість станцій, що підключаються до одного сегмента - 30. Мінімальна відстань між станціями - 1м. Стандарт також передбачає використання повторювачів, застосування яких також повинно відповідати «правилу 5-4-3». В цьому випадку мережа буде мати максимальну довжину в 5х185 = 925 м.

l0Base-T (IEEE 802.3L) - кабель на основі неекранованої витої пари (Unshielded Twisted Pair, UTP). Багатопарний кабель на основі неекранованої витої пари категорії 3 (категорія визначає смугу пропускання кабелю, величину перехресних наведень NEXT і деякі інші параметри його якості). Утворює зіркоподібну топологію на основі концентратора. Відстань між концентратором і кінцевим вузлом - не більше 100 м. Для забезпечення синхронізації станцій при реалізації процедур доступу CSMA/CD і надійного розпізнавання станціями колізій у стандарті визначено максимальне число концентраторів між будь-якими двома станціями мережі, а саме 4. Це правило носить назву «правило 4-х хабів" і воно замінює «правило 5-4-3», що застосовується до коаксіальним мереж. Загальна кількість станцій у мережі 10Base-T не повинна перевищувати загальної межі в 1024, і для даного типу фізичного рівня цю кількість дійсно можна досягти. Для цього досить створити дворівневу ієрархію концентраторів, розташувавши на нижньому рівні достатню кількість концентраторів із загальною кількістю портів 1024. Кінцеві вузли потрібно підключити до портів концентраторів нижнього рівня. Правило 4-х хабів при цьому виконується - між будь-якими кінцевими вузлами буде рівно 3 концентратора.



Максимальна довжина мережі в 2500 м тут розуміється як максимальна відстань між будь-якими двома кінцевими вузлами мережі (часто застосовується також термін «максимальний діаметр мережі»). Очевидно, що якщо між будь-якими двома вузлами мережі не повинно бути більше 4-х повторювачів, то максимальний діаметр мережі 10Base-T складає 5 * 100 = 500 м.

l0Base-F - волоконно-оптичний кабель. Топологія аналогічна топології стандарту l0Base-T. Є кілька варіантів цієї специфікації - FOIRL (відстань до 1000 м), l0Base-FL (відстань до 2000 м), l0Base-FB (відстань до 2000 м).

Число 10 у зазначених вище назвах позначає бітову швидкість передачі даних цих стандартів - 10 Мбіт/с, а слово Base - метод передачі на одній базовій частоті 10 МГц (на відміну від методів, що використовують кілька несучих частот, які називаються Broadband - широкосмуговими). Останній символ в назві стандарту фізичного рівня позначає тип кабелю.

Параметри специфікацій фізичного рівня для стандарту Ethernet

Специфікація фізичного рівня	10BASE-5	10BASE-2	10BASE-T	10BASE-F
Швидкість передачі даних, Мб/с	10	10	10	10
Передача даних	Вузькосмугова	Вузькосмугова	Вузькосмугова	Вузькосмугова

Тип середовища передачі	Коаксіальний кабель діаметром 0,5" ("товстий" коаксіал)	Коаксіальний кабель діаметром 0,2" ("тонкий" коаксіал)	Неекранована вита пара категорії 3,4,5 (UTP cat3)	Волоконно-оптичний кабель
Топологія	Шина	Шина	Зірка	Зірка
Максимальна довж. сегменту, м	500	185	100	2000
Максимальна кількість абонентів в сегменті	100	30	1024	1024
Максимальний діаметр мережі, м	2500	925	500	2500
Максимальна кількість повторювачів	4	4	4	4

Технологія Fast Ethernet: стандарт IEEE 802.3u

Класичний 10-мегабітний Ethernet влаштовував більшість користувачів на протязі близько 15 років. Однак на початку 90-х років почала відчуватися його недостатня пропускна здатність. Для комп'ютерів на процесорах Intel 80286 чи 80386 з шинами ISA (8 Мбайт / с) або EISA (32 Мбайт / с) пропускна здатність сегмента Ethernet складала 1/8 чи 1/32 каналу «Пам'ять-диск», і це добре узгоджувалося зі співвідношенням обсягів даних, що обробляються локально, і даних, що передавались по мережі. Для більш потужних клієнтських станцій із шиною PCI (133 Мбайт / с) ця частка впала до 1/133, що було явно недостатньо. Тому багато сегментів 10-мегабітного Ethernet стали перевантаженими, реакція серверів у них значно впала, а частота виникнення колізій істотно зросла, ще більш знижуючи корисну пропускну здатність.

Назріла необхідність в розробці «нового» Ethernet, тобто технології, яка була б такою ж ефективною по співвідношенню ціна/якість при продуктивності 100 Мбіт/с. В результаті пошуків і досліджень фахівці розділилися на два табори, що зрештою привело до появи двох нових технологій - Fast Ethernet і l00VG-AnyLAN. Вони відрізняються ступенем наступності з класичним Ethernet.

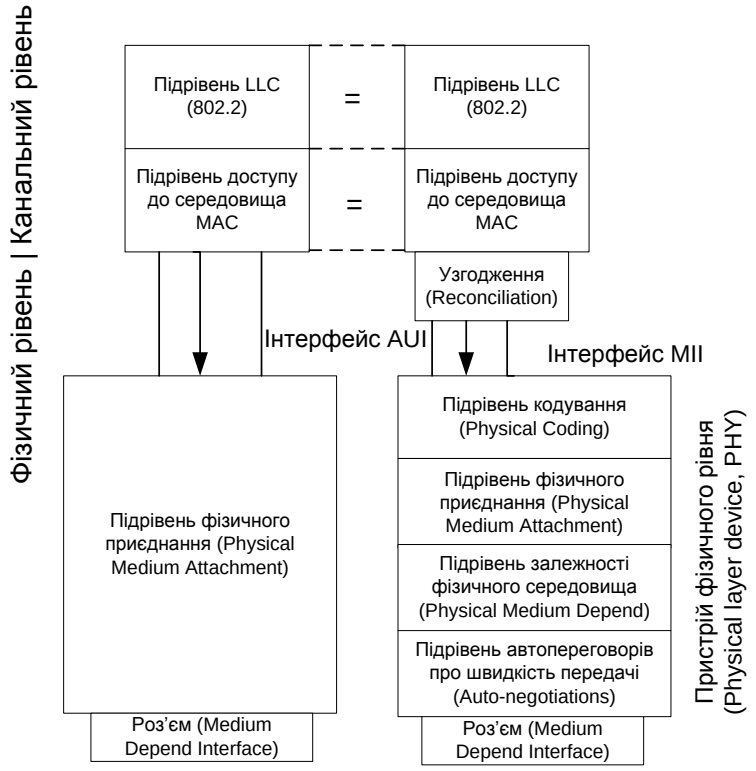
Фізичний рівень технології Fast Ethernet

Всі відмінності технології Fast Ethernet від Ethernet зосереджені на фізичному рівні. Рівні MAC і LLC в Fast Ethernet залишилися абсолютно тими ж. Тому розглядаючи технологію Fast Ethernet, ми будемо вивчати тільки кілька варіантів її фізичного рівня.

Більш складна структура фізичного рівня технології Fast Ethernet викликана тим, що в ній використовуються три варіанти кабельних систем:

- волоконно-оптичний багатомодовий кабель, використовуються два волокна;
- вита пара категорії 5, використовуються дві пари;
- вита пара категорії 3, використовуються чотири пари.

Коаксіальний кабель, що дав світові першу мережу Ethernet, в число дозволених середовищ передачі даних нової технології Fast Ethernet не потрапив. Це загальна тенденція багатьох нових технологій, оскільки на невеликих відстанях вита пара категорії 5 дозволяє передавати дані з тією ж швидкістю, що і коаксіальний кабель, але мережа виходить більш дешевою і зручною в експлуатації. На великих відстанях оптичне волокно володіє набагато більш широкою смугою пропускання, ніж коаксіал, а вартість мережі виходить ненабагато вище, особливо якщо врахувати високі витрати на пошук і усунення несправностей у великій кабельній коаксіальній системі.



Відмінності технології Fast Ethernet від технології Ethernet

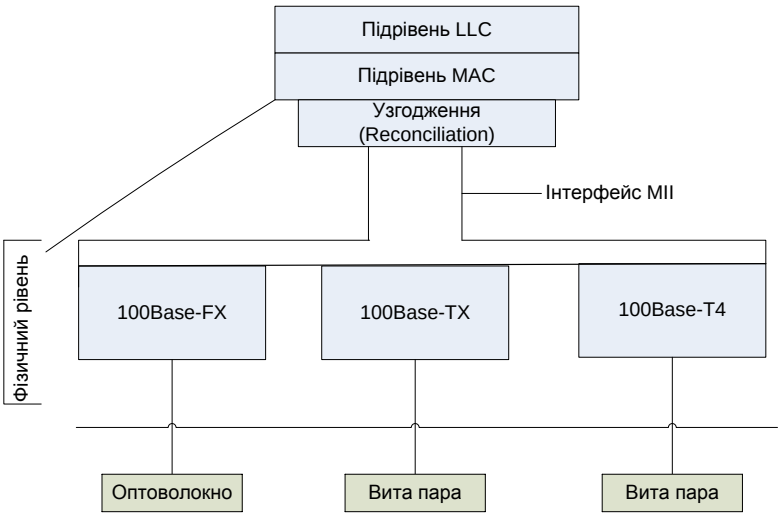
Відмова від коаксіального кабелю привела до того, що мережі Fast Ethernet завжди мають ієрархічну деревоподібну структуру, побудовану на концентраторах, як і мережі l0Base-T/l0Base-F. Основною відмінністю конфігурацій мереж Fast Ethernet є скорочення діаметра мережі приблизно до 200 м, що пояснюється зменшенням часу передачі кадру мінімальної довжини в 10 разів за рахунок збільшення швидкості передачі в 10 разів у порівнянні з 10-мегабітним Ethernet.

Проте ця обставина не дуже перешкоджає побудові великих мереж на технології Fast Ethernet. Справа в тому, що середина 90-х років відзначена не тільки широким розповсюдженням недорогих високошвидкісних технологій, але і бурхливим розвитком локальних мереж на основі комутаторів. При використанні комутаторів протокол Fast Ethernet може працювати в повнодуплексному режимі, в якому немає обмежень на загальну довжину мережі, а залишаються тільки обмеження на довжину фізичних сегментів, що з'єднують сусідні пристрої (адаптер - комутатор або комутатор - комутатор). Тому при створенні магістралей локальних мереж великої протяжності технологія Fast Ethernet також активно

застосовується, але тільки в повнодуплексному варіанті, спільно з комутаторами.

У порівнянні з варіантами фізичної реалізації Ethernet (а їх налічується шість), в Fast Ethernet відмінності кожного варіанту від інших глибші - змінюється як кількість провідників, так і методи кодування. А так як фізичні варіанти Fast Ethernet створювалися одночасно, а не еволюційно, як для мереж Ethernet, то була можливість детально визначити ті підрівні фізичного рівня, які не змінюються від варіанту до варіанту, і ті підрівні, які специфічні для кожного варіанту фізичного середовища.

Офіційний стандарт 802.3и установив три різних специфікації для фізичного рівня Fast Ethernet и дав їм наступні назви:



Структура фізичного рівня Fast Ethernet

- 100Base-TX для двухпарного кабелю на неекранованій витій парі UTP категорії 5 або екранованій витій парі STP Type 1;
- 100Base-T4 для четирьохпарного кабелю на неекранованій витій парі UTP категорії 3, 4 або 5;
- 100Base-FX для багатомодового оптоволоконного кабелю, використовуються два волокна.

Для всіх трьох стандартів справедливі наступні твердження і характеристики.

- Формати кадрів технології Fast Ethernet не відрізняються від форматів кадрів технологій

10-мегабітного Ethernet.

Міжкадровий інтервал (IPG) рівний 0,96 мкс, а бітовий інтервал рівний 10 нс. Всі часові параметри алгоритму доступу (інтервал відстрочки, час передачі кадру мінімальної довжини і т. п.), виміряні в бітових інтервалах, залишились колишніми, тому зміни в розділи стандарту, що стосується рівня MAC, не вносились.

Ознакою вільного стану середовища являється передача по ньому символу Idle, що відповідає надлишковому коду (а не відсутність сигналів, як в стандартах Ethernet 10 Мбіт/с). Фізичний рівень включає три елементи:

- рівень узгодження (reconciliation sublayer);
- незалежний від середовища інтерфейс (Media Independent Interface, MII);
- пристрій фізичного рівня (Physical layer device, PHY).

Фізичний рівень 100Base-FX - багатомодове оптоволокно, два волокна

Ця специфікація визначає роботу протоколу Fast Ethernet по багатомодовому оптоволокну в напівдуплексному і повнодуплексному режимах на основі добре перевіреної схеми кодування FDDI. Як і в стандарті FDDI, кожен вузол з'єднується з мережею двома оптичними волокнами, що йдуть від приймача (Rx) і від передавача (Tx).

Між специфікаціями l00Base-FX і l00Base-TX є багато спільного, тому загальні для двох специфікацій властивості будуть даватися під узагальненою назвою l00Base-FX/TX.

У той час як Ethernet зі швидкістю передачі 10 Мбіт/с використовує манчестерське кодування для представлення даних при передачі по кабелю, в стандарті Fast Ethernet визначено інший метод кодування - 4B/5B. Цей метод вже показав свою ефективність у стандарті FDDI і без змін перенесений в специфікацію l00Base-FX/TX. При цьому методі кожні 4 біта даних підрівня MAC (що називаються символами) представляються 5 бітами. Надлишковий біт дозволяє застосувати потенційні коди при поданні кожного з п'яти біт у вигляді електричних або оптичних імпульсів. Існування заборонених комбінацій символів

дозволяє відбраковувати помилкові символи, що підвищує стійкість роботи мереж з l00Base-FX/TX.

Після перетворення 4-бітових порцій кодів MAC в 5-бітові порції фізичного рівня їх необхідно представити у вигляді оптичних або електричних сигналів в кабелі, що з'єднує вузли мережі. Специфікації l00Base-FX і l00Base-TX використовують для цього різні методи фізичного кодування - NRZI і MLT-3 відповідно (як і в технології FDDI при роботі через оптоволокно і виту пару).

Фізичний рівень 100Base-TX - вита пара DTP Cat 5 або STP Type 1, дві пари

В якості середовища передачі даних специфікація l00Base-TX використовує кабель UTP категорії 5 або кабель STP Type 1. Максимальна довжина кабелю в обох випадках - 100 м.

Основні відмінності від специфікації l00Base-FX - використання методу MLT-3 для передачі сигналів 5-бітових порцій коду 4B/5B по витій парі, а також наявність функції автопереговорів (Auto-negotiation) для вибору режиму роботи порту. Схема автопереговорів дозволяє двом з'єднаним фізично пристроям, які підтримують декілька стандартів фізичного рівня, що відрізняються бітовою швидкістю і кількістю витих пар, вибрати найбільш вигідний режим роботи. Зазвичай процедура автопереговорів відбувається при приєднанні мережного адаптера, який може працювати на швидкостях 10 і 100 Мбіт/с, до концентратора або комутатора.

Описана нижче схема Auto-negotiation сьогодні є стандартом технології l00Base-T. До цього виробники застосовували різні власні схеми автоматичного визначення швидкості роботи взаємодіючих портів, які не були сумісні. Прийняту як стандарт схему Auto-negotiation запропонувала спочатку компанія National Semiconductor під назвою NWay.

Всього в даний час визначено 5 різних режимів роботи, які можуть підтримувати пристрої l00Base-TX або 100Base-T4 на витих парах;

- l0Base-T - 2 пари категорії 3;
- l0Base-T full-duplex - 2 пари категорії 3;
- l00Base-TX - 2 пари категорії 5 (або Type 1ASTP);

• 100Base-T4 - 4 пари категорії 3;

• 100Base-TX full-duplex - 2 пари категорії 5 (або Type 1A STP).

Режим l0Base-T має найнижчий пріоритет при переговорному процесі, а повнодуплексний режим 100Base-T4 - найвищий. Переговорний процес відбувається при включенні живлення пристрою, а також може бути ініційований в будь-який момент модулем управління пристрою.

Пристрій, що почав процес auto-negotiation, посилає своєму партнеру пачку спеціальних імпульсів Fast Link Pulse burst (FLP), в якому міститься 8-бітове слово, кодує пропонований режим взаємодії, починаючи з самого пріоритетного, підтримуваного даним вузлом.

Якщо вузол-партнер підтримує функцію auto-negotiation і також може підтримувати запропонований режим, він відповідає пачкою імпульсів FLP, в якій підтверджує даний режим, і на цьому переговори закінчуються. Якщо ж вузол-партнер може підтримувати менш пріоритетний режим, то він вказує його у відповіді, і цей режим вибирається в якості робочого. Таким чином, завжди вибирається найбільш пріоритетний загальний режим вузлів.

Вузол, який підтримує тільки технологію l0Base-T, кожні 16 мс посилає манчестерські імпульси для перевірки цілісності лінії, що зв'язує його із сусіднім вузлом. Такий вузол не розуміє запит FLP, який робить йому вузол з функцією Auto-negotiation, і продовжує посилати свої імпульси. Вузол, що отримав у відповідь на запит FLP тільки імпульси перевірки цілісності лінії, розуміє, що його партнер може працювати тільки за стандартом l0Base-T, і встановлює цей режим роботи і для себе.

Фізичний рівень 100Base-T4 - вита пара UTP Cat 3, чотири пари

Специфікація 100Base-T4 була розроблена для того, щоб можна було використовувати для високошвидкісного Ethernet наявну проводку на витій парі категорії 3. Ця специфікація дозволяє підвищити загальну пропускну здатність за рахунок одночасної передачі потоків біт по всіх 4 парах кабелю.

Специфікація 100Base-T4 з'явилася пізніше інших специфікацій фізичного рівня Fast Ethernet. Розробники цієї технології в першу чергу хотіли створити

фізичні специфікації, найбільш близькі до специфікацій l0Base-T і l0Base-F, які працювали на двох лініях передачі даних: двох парах або двох волокнах. Для реалізації роботи по двох витих парах довелося перейти на більш якісний кабель категорії 5.

У той же час розробники конкуруючої технології l00VG-AnyLAN спочатку зробили ставку на роботу по витій парі категорії 3; найголовніша перевага полягала не стільки у вартості, а в тому, що вона була вже прокладена в переважній кількості будівель. Тому після випуску специфікацій l00Base-TX і l00Base-FX розробники технології Fast Ethernet реалізували свій варіант фізичного рівня для витої пари категорії 3.

Замість кодування 4B/5B в цьому методі використовується кодування 8B/6T, яке має більш вузький спектр сигналу і при швидкості 33 Мбіт/с укладається в смугу 16 Мгц витої пари категорії 3 (при кодуванні 4B/5B спектр сигналу в цю смугу не вкладається) . Кожні 8 біт інформації рівня MAC кодуються 6-ма трійковими цифрами (ternary symbols), тобто цифрами, які мають три стани. Кожна трійкова цифра має тривалість 40 нс. Група з 6-ти трійкових цифр потім передається на одну з трьох передавальних кручених пар, незалежно і послідовно.

Четверта пара завжди використовується для прослуховування несучої частоти з метою виявлення колізії. Швидкість передачі даних по кожній з трьох передавальних пар дорівнює 33,3 Мбіт/с, тому загальна швидкість протоколу 100Base-T4 складає 100 Мбіт/с. У той же час через прийнятий спосіб кодування швидкість зміни сигналу на кожній парі дорівнює всього 25 Мбод, що і дозволяє використовувати виту пару категорії 3.

Специфікація IEEE 802.3u визначає наступні максимальні довжини сегментів.

Стандарт	Тип кабелю	Максимальна довжина сегменту
100Base-TX	Категорія 5 UTP	100 м
100Base-FX	Багатомодове оптоволокно 62,5/125 мкм	412 м (півдуплекс) 2 км (повний дуплекс)
100Base-T4	Категорія 3, 4 або 5 UTP	100 м

Технологія Gigabit Ethernet: стандарт IEEE 802.3z.

Загальна характеристика стандарту

Досить швидко після появи на ринку продуктів Fast Ethernet мережеві інтегратори й адміністратори відчули певні обмеження при побудові корпоративних мереж. У багатьох випадках сервери, підключені по 100-мегабитному каналу, перевантажували магістралі мереж, що працюють також на швидкості 100 Мбіт/с - магістралі FDDI і Fast Ethernet. Відчувалася потреба в наступному рівні ієрархії швидкостей. У 1995 році більш високий рівень швидкості могли надати тільки комутатори ATM, а за відсутності в той час зручних засобів міграції цієї технології в локальні мережі (хоча специфікація LAN Emulation - LANE була прийнята на початку 1995 року, практична її реалізація була попереду) впроваджувати їх в локальну мережу майже ніхто не наважувався. Крім того, технологія ATM відрізнялася дуже високим рівнем вартості.

Тому логічним виглядав наступний крок, зроблений IEEE, - через 5 місяців після остаточного прийняття стандарту Fast Ethernet в червні 1995 року дослідницькій групі по вивченню високошвидкісних технологій IEEE було наказано зайнятися розглядом можливості вироблення стандарту Ethernet із ще більш високою бітовою швидкістю.

Перша версія стандарту була розглянута в січні 1997 року, а остаточно стандарт 802.3z був прийнятий 29 червня 1998 року на засіданні комітету IEEE 802.3. Роботи з реалізації Gigabit Ethernet на витій парі категорії 5 були передані спеціальному комітету 802.3ab, який вже розглянув кілька варіантів проекту цього стандарту, причому з липня 1998 року проект придбав досить стабільний характер. Остаточне ухвалення стандарту 802.3ab очікувався у вересні 1999 року. Основна ідея розробників стандарту Gigabit Ethernet складається в максимальному збереженні ідей класичної технології Ethernet при досягненні бітової швидкості в 1000 Мбіт/с.

Так як при розробці нової технології природно очікувати деяких технічних новинок, що йдуть у загальному руслі розвитку мережних технологій, то важливо

відзначити, що Gigabit Ethernet, так само як і його менш швидкісні побратими, на рівні протоколу *не буде* підтримувати:

- якість обслуговування;
- надлишкові зв'язки;
- тестування працездатності вузлів і обладнання (в останньому випадку - за виключенням тестування зв'язка порт - порт, як це робиться для Ethernet l0Base-T і l0Base-F і Fast Ethernet).

Всі три названі властивості рахуються досить перспективними і корисними в сучасних мережах, а особливо в мережах найближчого майбутнього. Чому ж автори Gigabit Ethernet відмовляються от них?

З приводу якості обслуговування коротко можна відповісти так: «сила є - розуму не треба». Якщо магістраль мережі буде працювати зі швидкістю що в 20 000 разів перевищує середню швидкість мережної активності клієнтського комп'ютера і в 100 разів перевищує середню мережеву активність сервера з мережевим адаптером 100 Мбіт/с, то про затримки пакетів на магістралі в багатьох випадках можна не піклуватися взагалі. При невеликому коефіцієнті завантаження магістралі 1000 Мбіт/с черги в комутаторах Gigabit Ethernet будуть невеликими, а час буферизації і комутації на такій швидкості складає одиниці і навіть частки мікросекунд.

Ну а якщо все ж магістраль завантажиться на достатню величину, то пріоритет чутливого до затримок або вимогливому до середньої швидкості трафіку можна надати за допомогою техніки пріоритетів у комутаторах - відповідні стандарти для комутаторів уже прийняті (вони будуть розглядатися в наступному розділі). Зате можна буде користуватися досить простою (майже як Ethernet) технологією, принципи роботи якої відомі практично всім мережевим фахівцям.

Головна ідея розробників технології Gigabit Ethernet полягає в тому, що існує і буде існувати дуже багато мереж, в яких висока швидкість магістралі і можливість призначення пакетам пріоритетів у комутаторах будуть цілком достатні для забезпечення якості транспортного обслуговування всіх клієнтів

мережі. І тільки в тих рідкісних випадках, коли і магістраль досить завантажена, і вимоги до якості обслуговування дуже жорсткі, потрібно застосовувати технологію ATM, яка дійсно за рахунок високої технічної складності дає гарантії якості обслуговування для всіх основних видів трафіку.

Надлишкові зв'язки і тестування устаткування не будуть підтримуватися технологією Gigabit Ethernet через те, що з цими завданнями добре справляються протоколи більш високих рівнів, наприклад Spanning Tree, протоколи маршрутизації і т. п. Тому розробники технології вирішили, що нижній рівень просто повинен швидко передавати дані, а більш складні і більш рідкісні завдання (наприклад, пріоритезація трафіка) повинні передаватися верхнім рівням.

Що ж спільного є в технології Gigabit Ethernet у порівнянні з технологіями Ethernet і Fast Ethernet?

• Зберігаються всі формати кадрів Ethernet.

• Як і раніше будуть існувати напівдуплексна версія протоколу, що підтримує метод доступу CSMA/CD, і повнодуплексна версія, що працює з комутаторами. З приводу збереження напівдуплексної версії протоколу сумніви були ще у розробників Fast Ethernet, так як складно змусити працювати алгоритм CSMA/CD на високих швидкостях. Однак метод доступу залишився незмінним у технології Fast Ethernet, і його вирішили залишити в новій технології Gigabit Ethernet. Збереження недорогого рішення для роздільних середовищ дозволить застосувати Gigabit Ethernet у невеликих робочих групах, що мають швидкі сервери і робочі станції.

• Підтримуються всі основні види кабелів, що використовуються в Ethernet і Fast Ethernet:

Волоконно-оптичний, вита пара категорії 5, коаксіал.

Проте розробникам технології Gigabit Ethernet для збереження наведених вище властивостей довелося внести зміни не тільки у фізичний рівень, як це було у випадку Fast Ethernet, а й в рівень MAC.

Перед розробниками стандарту Gigabit Ethernet стояло кілька важко вирішуваних проблем. Однією з них було завдання забезпечення прийнятного

діаметра мережі для напівдуплексного, режиму роботи. У зв'язку з обмеженнями, що накладаються методом CSMA/CD на довжину кабелю, версія Gigabit Ethernet для поділюваного середовища допускала би довжину сегмента усього в 25 метрів при збереженні розміру кадрів і всіх параметрів методу CSMA/CD незмінними. Так як існує велика кількість застосувань, коли потрібно підвищити діаметр мережі хоча б до 200 метрів, необхідно було якимось чином вирішити цю задачу за рахунок мінімальних змін у технології Fast Ethernet.

Інший складним завданням було досягнення бітової швидкості 1000 Мбіт/с на основних типах кабелів. Навіть для оптоволокна досягнення такої швидкості представляє деякі проблеми, тому що технологія Fibre Channel, фізичний рівень якої був взятий за основу для оптоволоконної версії Gigabit Ethernet, забезпечує швидкість передачі даних всього в 800 Мбіт / с (бітова швидкість на лінії дорівнює в цьому випадку приблизно 1000 Мбіт/с, але при методі кодування 8B/10B корисна бітова швидкість на 25% менше швидкості імпульсів на лінії).

І нарешті, найскладніше завдання - підтримка кабелю на витій парі. Таке завдання на перший погляд здається нерозв'язним - адже навіть для 100-мегабітних протоколів довелося використовувати досить складні методи кодування, щоб укласти спектр сигналу в смугу пропускання кабелю. Однак успіхи фахівців з кодування, що проявилися в останній час в нових стандартах модемів, показали, що завдання має шанси на рішення. Щоб не гальмувати прийняття основної версії стандарту Gigabit Ethernet, що використовує оптоволокно і коаксіал, був створений окремий комітет 802.3ab, який займається розробкою стандарту Gigabit Ethernet на витій парі категорії 5.

Всі ці задачі були успішно розв’язані:

Специфікації фізичного середовища стандарту 802.3z

В стандарті 802.3z визначені наступні типи фізичного середовища:

- одномодовий волоконно-оптичний кабель;
- багатомодовий волоконно-оптичний кабель 62,5/125;
- багатомодовый волоконно-оптичний кабель 50/125;
- подвійний коаксіал з хвильовим опором 75 Ом.

Багатомодовий кабель

Для передачі даних по традиційному для комп'ютерних мереж багатомодовому волоконно-оптичному кабелю стандарт визначає застосування випромінювачів, що працюють на двох довжинах хвиль: 1300 і 850 нм. Застосування світлодіодів з довжиною хвилі 850 нм пояснюється тим, що вони набагато дешевші, ніж світлодіоди, які працюють на хвилі 1300 нм, хоча при цьому максимальна довжина кабелю зменшується, так як загасання багатомодового оптоволокна на хвилі 850 м більше ніж у два рази вище, ніж на хвилі 1300 нм. Однак можливість здешевлення надзвичайно важлива для такої в цілому дорогої технології, як Gigabit Ethernet.

Для багатомодового оптоволокна стандарт 802.3z визначив специфікації l000Base-SX і l000Base-LX.

У першому випадку використовується довжина хвилі 850 нм (S означає Short Wavelength, коротка хвиля), а в другому - 1300 нм (L - від Long Wavelength, довга хвиля).

Для специфікації l000Base-SX гранична довжина оптоволоконного сегменту для кабелю 62,5/125 залишає 220 м, а для кабелю 50/125 - 500 м. Очевидно, що ці максимальні значення можуть досягатися тільки для повнодуплексної передачі даних, так як час подвійного обороту сигналу на двох відрізках 220 м рівний 4400 bt, що перевершує межу 4095 bt навіть без урахування повторювача і мережевих адаптерів. Для напівдуплексної передачі максимальні значення сегментів оптоволоконного кабелю завжди повинні бути менше 100 м. Наведені відстані в 220 і 500 м розраховані для гіршого за стандартом випадку смуги пропускання багатомодового кабелю, що знаходиться в межах від 160 до 500 МГц/км. Реальні кабелі зазвичай мають значно кращі характеристики, що знаходяться між 600 і 1000 МГц/км. В цьому випадку можна збільшити довжину кабелю приблизно до 800 м.

Одномодовий кабель

Для специфікації l000Base-LX в якості джерела випромінювання завжди застосовується напівпровідниковий лазер з довжиною хвилі 1300 нм.

Основна область застосування l000Base-LX - це одномодове оптоволокно. Максимальна довжина кабелю для одномодового волокна дорівнює 5000 м.

Специфікація l000Base-LX може працювати і на багатомодовому кабелі. В цьому випадку гранична відстань виходить невелика - 550 м. Це пов'язано з особливостями розповсюдження когерентного світла в широкому каналі багатомодового кабелю. Для приєднання лазерного трансівера до багатомодового кабелю необхідно використовувати спеціальний адаптер.

Твінаксіальний кабель

Як середовище передачі даних використовується високоякісний твінаксіальний кабель (Twinax) з хвильовим опором 150 Ом (2х75 Ом). Дані надсилаються одночасно по парі провідників, кожен з яких оточений екрануючою спліткою. При цьому виходить режим напівдуплексної передачі. Для забезпечення повнодуплексної передачі необхідні ще дві пари коаксіальних провідників. Почав випускатися спеціальний кабель, який містить чотири коаксіальних провідника - так званий Quad-кабель. Він зовні нагадує кабель категорії 5 і має близький до нього зовнішній діаметр і гнучкість. Максимальна довжина твінаксіального сегмента становить всього 25 метрів, тому це рішення підходить для обладнання, розташованого в одній кімнаті.

Gigabit Ethernet на витій парі категорії 5

Як відомо, кожна пара кабелю категорії 5 має гарантовану полосу пропускання до 100 МГц. Для передачі по такому кабелю даних зі швидкістю 1000 Мбіт/с було вирішено організувати паралельну передачу одночасно по всіх 4 парах кабелю (так, як і в технології l00VG-AnyLAN).

Це відразу зменшило швидкість передачі даних по кожній парі до 250 Мбіт / с. Однак і для такої швидкості необхідно було придумати метод кодування, який мав би спектр не вище 100 МГц. Крім того, одночасне використання чотирьох пар на перший погляд позбавляє мережу можливість розпізнавати колізії.

Для кодування даних був застосований код PAM5, що використовує 5 рівнів потенціалу: -2, -1, 0, +1, +2. Тому за один такт по одній парі передається 2,322 біт

інформації. Отже, тактову частоту замість 250 МГц можна знизити до 125 МГц. При цьому якщо використовувати не всі коди, а передавати 8 біт за такт (по 4 парам), то витримується необхідна швидкість передачі в 1000 Мбіт / с і ще залишається запас невикористовуваних кодів, так як код PAM5 містить 54 = 625 комбінацій, а якщо передавати за один такт по всіх чотирьох парах 8 біт даних, то для цього потрібно всього 28 = 256 комбінацій. Решта комбінацій приймач може використовувати для контролю прийнятої інформації і виділення правильних комбінацій на фоні шуму. Код PAM5 на тактовій частоті 125 МГц укладається в смугу 100 МГц кабелю категорії 5.

Для розпізнавання колізій і організації повнодуплексного режиму розробники специфікації 802.3ab застосували техніку, яка використовується при організації дуплексного режиму на одній парі проводів у сучасних модемах і апаратурі передачі даних абонентських закінчень ISDN. Замість передачі по різних парах проводів або рознесення сигналів двох одночасно працюючих назустріч передавачів по діапазону частот обидва передавача працюють назустріч один одному по кожній з 4-х пар в одному і тому ж діапазоні частот, так як використовують один і той же потенційний код PAM5. Схема гібридної розв'язки H дозволяє приймачу і передавачу одного і того ж вузла використовувати одночасно виту пару і для прийому і для передачі (так само, як і в трансиверах коаксіального Ethernet).

Для відділення сигналу від свого власного приймач віднімає з результуючого сигналу відомий йому свій сигнал. Природно, що це не проста операція і для її виконання використовуються спеціальні цифрові сигнальні процесори - DSP (Digital Signal Processor). Така техніка вже пройшла перевірку практикою, але в модемах і мережах ISDN вона застосовувалася зовсім на інших швидкостях.

При напівдуплексному режимі роботи одержання зустрічного потоку даних вважається колізією, а для повнодуплексного режиму роботи - нормальною ситуацією.

З огляду на те що роботи по стандартизації специфікації Gigabit Ethernet на

неекранованої витої пари категорії 5 підходять до кінця, багато виробників і споживачі сподіваються на позитивний результат цієї роботи, так як в цьому випадку для підтримки технології Gigabit Ethernet не потрібно буде замінювати вже встановлену проводку категорії 5 на оптоволокно або проводку категорії 7.

Висновки

Технологія Gigabit Ethernet добавляє нову, 1000 Мбіт/с, ступінь в ієрархії швидкостей сімейства Ethernet. Ця ступінь дозволяє ефективно будувати великі локальні мережі, в яких потужні сервери і магістралі нижніх рівнів мережі працюють на швидкості 100 Мбіт/с, а магістраль Gigabit Ethernet об’єднує їх, забезпечуючи достатньо великий запас пропускної здатності.

Розробники технології Gigabit Ethernet зберегли велику ступінь спадкоємності з технологіями Ethernet і Fast Ethernet. Gigabit Ethernet використовує ті ж формати кадрів, що і 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 в напівдуплексному режимі розробники технології пішли на збільшення мінімального розміру кадру з 64 до 512 байт. Дозволяється також передавати декілька 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, який визначає використання в якості фізичного середовища трьох типів кабелю: багатомодового оптоволоконного (відстань до 500 м), одномодового оптоволоконного (відстань до 5000 м) і подвійного коаксіального (twinax), за яким дані передаються одночасно за двома мідним екранованим провідникам на відстань до 25 м.

Для розробки варіанту Gigabit Ethernet на UTP категорії 5 була створена спеціальна група 802.3ab, яка вже розробила проект стандарту для роботи з 4-м парам UTP категорії 5. Прийняття цього стандарту очікується найближчим часом.

Технологія 10 Gigabit Ethernet: стандарт IEEE 802.3ae

Специфікація стандарту IEEE 802.3ae являється подальшим розвитком оптичних специфікацій Gigabit Ethernet і на канальному рівні моделі OSI немає ніяких змін, чого не скажеш про специфікації на реалізацію фізичного рівня.

Відповідно до моделі OSI протокол Ethernet є стандартом 2-го рівня. 10 Gigabit Ethernet використовує на 2-му рівні протокол IEEE 802.3 Ethernet Media Access Control (MAC) і має будову кадру Ethernet з відповідними обмеженнями за його мінімальної і максимальної довжини.

Так само як і гігабітні специфікації 1000Base-X і 1000Base-T залишилися вірними моделі Ethernet, 10 Gigabit Ethernet продовжує природну еволюцію Ethernet по швидкості і відстані передачі. Оскільки це повнодуплексна технологія і виключно оптична, вона не потребує використання алгоритму CSMA/CD з виявленням колізій і контролем доступу до середовища передачі, які необхідні для менш швидкісних напівдуплексних систем. В інших же аспектах 10 Gigabit Ethernet відповідає усталеній моделі Ethernet.

Пристрої фізичного рівня (PHY), з'єднують середовище передачі з пристроєм канального рівня, 2-го відповідно до моделі OSI. Архітектура Ethernet розділяє фізичний рівень на Physical Media Dependent (PMD) і Physical Coding Sublayer (PCS) підрівні. Оптичний трансивер, таким чином, є пристроєм PMD підрівня, а на підрівні PCS проводиться кодування (64/66 біт) і здійснюються функції перетворення в послідовний сигнал.

Специфікація IEEE 802.3ae визначає два типи фізичного рівня: LAN PHY і WAN PHY. В WAN PHY додані деякі додаткові функції у порівнянні з LAN PHY. Вони повністю визначаються підрівнем PCS. Також існує кілька різновидів реалізації PMD.

Як показує досвід попередніх версій Ethernet, вартість 10 гігабітних комунікацій має великий потенціал для її зменшення з ходом розвитку сучасних технологій. На відміну від телекомунікаційних 10 гігабітних лазерів, в «коротких» каналах 10 Gigabit Ethernet можна використовувати дешеву неохолоджувану оптику і, в деяких випадках, лазери поверхневого випромінювання з

вертикальними резонаторами (VCSEL), у яких є значний запас до здешевлення. На додаток до цього хорошим стимулом до здешевлення є агресивна ситуація на ринку мікросхем для телекомунікації, який пропонує високоінтегровані рішення.

Одним із завдань робочої групи IEEE 802.3ae було забезпечення можливості використовувати існуючі волоконно-оптичні лінії для використання 10 Gigabit Ethernet обладнанням. Таке рішення було викликане привабливістю використання для нової технології вже прокладених оптичних кабелів, призначених для мереж SDH / SONET. Саме це, в сукупності з останніми розробками в області напівпровідникових лазерів, дозволить значно розширити вплив мереж Ethernet і особливо на ринку обладнання для операторів послуг передачі даних.

З появою високошвидкісних специфікацій Gigabit Ethernet з можливістю передачі даних на відстані до 70 км стало доступним використання Ethernet як протокол передачі в операторських мережах масштабу міста. Завдяки цьому оператор може запропонувати своїм клієнтам послуги з організації корпоративних мереж Ethernet, які значно ефективніші в роботі і зручніші в обслуговуванні, ніж мережі Frame-Relay, і тому більш вигідні. Використання протоколу Ethernet в таких мережах за рахунок однорідності протоколу передачі значно зменшує витрати на обладнання, підтримку, навчання персоналу.

При використанні об'єднання локальних мереж через традиційні MAN мережі, дані від комутаторів мережі проходять через обладнання ATM та мультиплексори SDH в кожній точці підключення до MAN мережі, що, крім витрат на обладнання і внесення затримки на обробку кадрів, несе ще й значні витрати на конфігурування та підтримку роботи всієї системи.

Крім зменшення вартості і збільшення швидкості передачі даних перехід до побудови операторських мереж на основі Ethernet дозволяє використовувати всі ті інтелектуальні функції, які зараз широко використовуються в локальних мережах: пріоритизація трафіку і забезпечення якості обслуговування. Завдяки цьому стає реальним наскрізне використання цих функцій від одного користувача мережі до іншого без необхідності додаткових проміжних операцій, що дозволяє надавати розширений в порівнянні зі звичайними MAN мережами набір послуг.

ЗАВДАННЯ НА РОБОТУ

1. Використовуючи пакет NetCracker, вивчити склад і функціональні характеристики типового обладнання локальних мереж на основі технології Ethernet.

2. У відповідності з варіантом завдання побудувати мережу підприємства з використанням технологій Ethernet і Fast Ethernet, виходячи з розрахунку мінімізації вартості проектованої мережі.

3. Для отриманої моделі мережі задати необхідні типи потоків даних між робочими станціями і серверами і провести імітаційне моделювання роботи мережі.

4. Проаналізувати середню загрузку мережевого обладнання і середовища передачі даних і час відповіді для потоку даних. Вказати ділянки мережі, вразливі до перегрузок, і визначити засоби підвищення надійності функціонування мережі.

Таблиця 3.1. Варіанти завдань.

№ варіанту	Тип інфраструктури	Тип трафіку
1	1	2
2	2	3
3	3	4
4	4	1
5	1	3
6	2	4
7	3	1
8	4	2
9	1	4
10	2	1
11	3	2
12	4	3
13	1	1
14	2	2
15	3	3

Таблиця 3.2. Тип інфраструктури.

№ варіанту	Кількість будівель	Відстань між будівлями	Кількість поверхів	Кількість кімнат на поверсі

1	2	300	4	3
2	2	250	3	3
3	3	200	3	3
4	3	150	2	3

Таблиця 3.3. Тип модельованого трафіку.

№ варіанту	Кількість файлових серверів	Кількість HTTP-серверів	Кількість FTP-серверів	Кількість серверів баз даних
1	3	1	2	2
2	3	2	1	2
3	2	1	2	3
4	2	2	1	3

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

Коротка характеристика технології Ethernet.

Правила побудови мереж Ethernet і Fast Ethernet.

Вкажіть причину збільшення мінімального розміру кадру в Gigabit Ethernet до 512 байт?

Допустима довжина мережі з множинним методом доступу з контролем несучої і виявленням колізій?

Що позначають цифри 5 і 2 в назві стандарту Ethernet 10BASE 5 і Ethernet 10BASE 2?

Який метод доступу до передавального середовища використовується в мережі Ethernet?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Кулаков Ю.А., Омелянский С. В. Компьютерные сети. Выбор, установка, использование и администрирование – К.: Юниор, 1999.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы,

технологии, протоколы. 2-е издание – СПб.: Питер, 2003.

3. IEEE Standard for Information Technology. Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications – IEEE Std 802.3, 2000 Edition.

Комп'ютерний практикум № 4

ПОБУДОВА ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ TOKEN RING І FDDI

Мета роботи: отримати навики вибору обладнання, кабельної системи для побудови інфраструктури локальної обчислювальної мережі рівня підприємства на основі технологій Token Ring і FDDI.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Стандарти Token Ring і IEEE 802.5

Мережа Token Ring спочатку була розроблена компанією IBM в 1970 році. Вона як і раніше являється основною технологією IBM для локальних мереж, уступаючи по популярності серед аналогічних технологій тільки Ethernet/IEEE 802.3. Стандарт IEEE 802.5 практично ідентичний і повністю сумісний з стандартом Token Ring IBM. Стандарт IEEE 802.5 був фактично створений по прикладу Token Ring IBM, і продовжує відслідковувати її розробку. Термін "Token Ring" часто використовується як при посиланні на мережу Token Ring IBM, так і на мережу IEEE 802.5.

В табл. 4.1 представлені узагальнені характеристики мереж Token Ring і IEEE 802.5.

Таблиця 4.1 - характеристики мереж Token Ring і IEEE 802.5.

	IBM Token Ring	IEEE 802.5
Швидкість передачі даних, Мб/с	4 або 16	4 або 16
Кількість станцій в сегменті	260 (STP) 72 (UTP)	250
Фізична топологія	Зірка	Не визначено
Тип середовища передачі	Вита пара	Не визначено
Максимальна довжина кабелю між станцією і концентратором, м	100 (STP) 45 (UTP)	100
Передача сигналу	В основній полосі частот	В основній полосі частот
Метод доступу до середовища передачі	Маркерний	Маркерний
Спосіб кодування	Манчестерський	Манчестерський

Token Ring і IEEE 802.5 являються найбільш яскравими прикладами мереж, що використовують маркерний метод доступу до середовища передачі. В цьому випадку по мережі передається невеликий блок даних, що називається маркером. Володіння маркером гарантує право передачі даних. Якщо станції, що отримала маркер, не потрібно виконувати передачу даних, маркер переправляється наступній станції в кільці. Кожна станція може утримувати маркер на протязі певного максимального часу.

Якщо у станції, що отримала вільний маркер, є дані для передачі, вона захоплює маркер, змінює у нього один біт (в результаті чого маркер перетворюється в послідовність "початок блоку даних"), доповнює інформацією, яку він хоче передати і відсилає цю інформацію наступній в кільці станції. Коли інформаційний блок циркулює по кільцю, маркер в мережі відсутній (якщо тільки кільце не забезпечує "раннього звільнення маркера" - *early token release*), тому інші станції, які бажають передати інформацію, змушені чекати. Отже, в мережах Token Ring не може бути колізій. Якщо забезпечується раннє звільнення маркера, то новий маркер може бути випущений після завершення передачі блоку даних.

Інформаційний блок передається по кільцю, поки не досягне станції призначення, яка копіює інформацію для подальшої обробки. Після цього блок

передається далі по кільцю, поки не досягне відправника, який повинен видалити цей блок. Відправник може перевірити блок, що повернувся, щоб переконатися, що він був доставлений станції призначення.

На відміну від мереж, що використовують метод доступу CSMA/CD (наприклад, Ethernet), мережі з передачею маркера є детермінованими мережами. Це означає, що можна обчислити максимальний час, який пройде, перш ніж будь-яка кінцева станція зможе передавати дані. Ця характеристика, а також деякі характеристики надійності, роблять мережу Token Ring ідеальною для застосувань, коли, по-перше, затримка передачі повинна бути передбачена і, по-друге, важлива стійкість функціонування мережі. Прикладами таких застосувань є середовище автоматизованих станцій на промислових підприємствах.

Особливості фізичного рівня в мережах Token Ring

Станції мережі IBM Token Ring безпосередньо підключаються до багатостанційного пристрою доступу (*multistation access unit, MSAU*), які можуть бути об'єднані за допомогою кабелів, утворюючи одну велику кільцеву мережу (рис. 4.1). Кабелі-перемички з'єднують MSAU з суміжними MSAU. Кабелі-пелюстки підключають MSAU до станцій. У складі MSAU є шунтуючі реле для виключення станцій з кільця.

Мережі Token Ring використовують складну систему пріоритетів, яка дозволяє деяким станціям з високим пріоритетом, призначеним користувачем, більш часто користуватися мережею. Блоки даних Token Ring містять два поля, які управляють пріоритетом: поле пріоритетів і поле резервування.

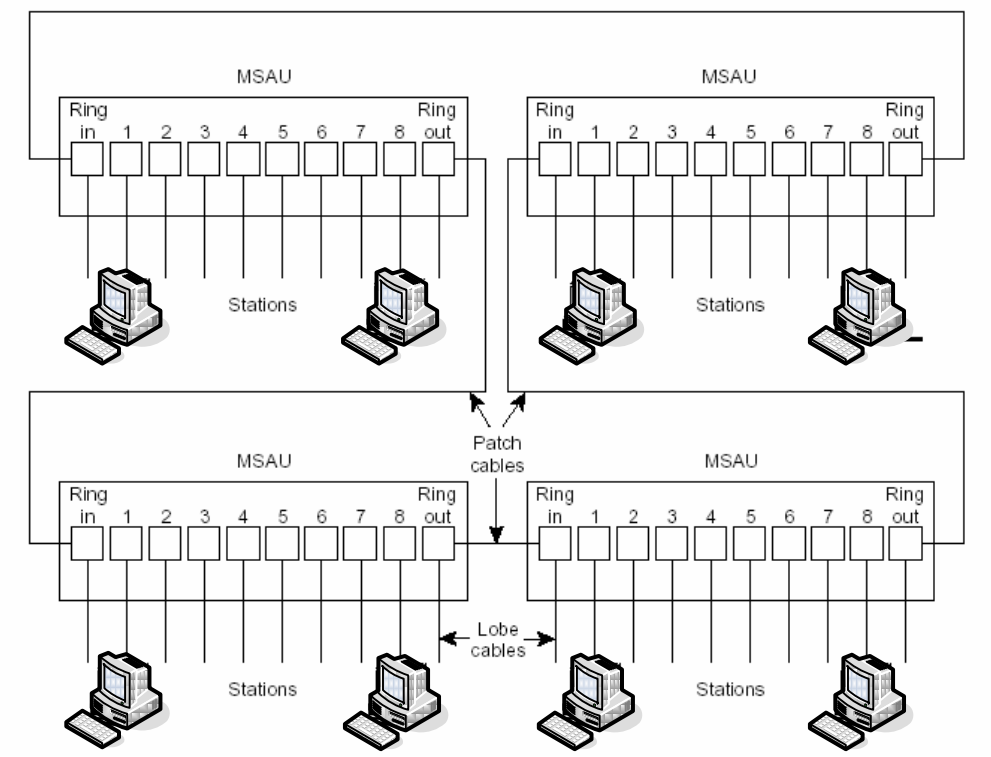


Рис. 4.1- мережа Token Ring

Тільки станції з пріоритетом, який дорівнює або вище величини пріоритету, що міститься в маркері, можуть заволодіти ним. Після того, як маркер захоплений і змінений (в результаті чого він перетворився в інформаційний блок), тільки станції, пріоритет яких вище пріоритету передавальної станції, можуть зарезервувати маркер для наступного проходу по мережі. При генерації наступного маркера в нього включається більш високий пріоритет даної резервуючої станції. Станції, які підвищують рівень пріоритету маркера, повинні відновити попередній рівень пріоритету після завершення передачі.

Мережі Token Ring використовують декілька механізмів виявлення та усунення несправностей в мережі. Так, в мережі вибирається "активний монітор" (*active monitor*), в ролі якого може виступати будь-яка станція. Ця станція діє як централізоване джерело синхронізуючої інформації для інших станцій кільця і виконує різноманітні функції для підтримки кільця. Однією з таких функцій є видалення з кільця постійно циркулюючих блоків даних. Якщо пристрій, що відправив блок даних, відмовив, то цей блок може постійно циркулювати по кільцю. Це може завадити іншим станціям передавати власні блоки даних і

фактично блокує мережу. Активний монітор може виявляти і видаляти такі блоки і генерувати новий маркер.

Зіркоподібна топологія мережі IBM Token Ring також сприяє підвищенню загальної надійності мережі. Так як вся інформація мережі Token Ring проглядається активними MSAU, ці пристрої можна запрограмувати так, щоб вони перевіряли наявність проблем і при необхідності вибірково видаляли станції з кільця.

Застосування сигналізуючого (*beaconing*) алгоритму в мережі Token Ring дає можливість виявляти і усувати деякі несправності мережі. Якщо яка-небудь станція виявить серйозну проблему в мережі (наприклад, обрив кабелю), вона висилає сигнальний блок даних. Сигнальний блок даних вказує домен несправності, в який входять станція, що повідомляє про несправності, її найближчий активний сусід, що знаходиться вище за течією потоку інформації (*nearest active upstream neighbor, NAUN*), і все, що знаходиться між ними. Сигналізація ініціалізує процес, що називається автореконфігурацією (*autoreconfiguration*), в ході якого вузли, розташовані в межах домену, що відмовив, автоматично виконують діагностику, намагаючись реконфігурувати мережу навколо зони, що відмовила. У фізичному плані MSAU може виконати це за допомогою електричної реконфігурації.

Стандарт FDDI

Стандарт FDDI (*Fiber Distributed Data Interface*) був випущений комітетом ANSI X3T9.5 в середині 80-х років. В цей період вимоги, що пред'являлись зі сторони швидкодіючих робочих станцій, почали перевищувати можливості існуючих локальних мереж (в основному Ethernet і Token Ring). Виникла необхідність в новому стандарті для локальних мереж, який задовольнив би вимоги нових робочих станцій і розподілених обчислювальних систем. Разом з цим, все більше значення виділяється проблемі надійності мережі, оскільки багато з критичних по призначенню прикладних задач були перенесені з великих комп'ютерів в мережі.

Стандарт FDDI визначає мережу з швидкістю передачі даних 100 Мб/с, з

двійним кільцем і передачею маркера (рис. 4.2). Трафік по двійному кільцю рухається в протилежних напрямках. В фізичному вираженні кільце складається з двох або більше двоточкових з'єднань між суміжними станціями. Одно з двох кілець FDDI називається первинним кільцем, друге - вторинним кільцем. Первинне кільце використовується для передачі даних, в той час як вторинне кільце звичайно являється дублюючим.

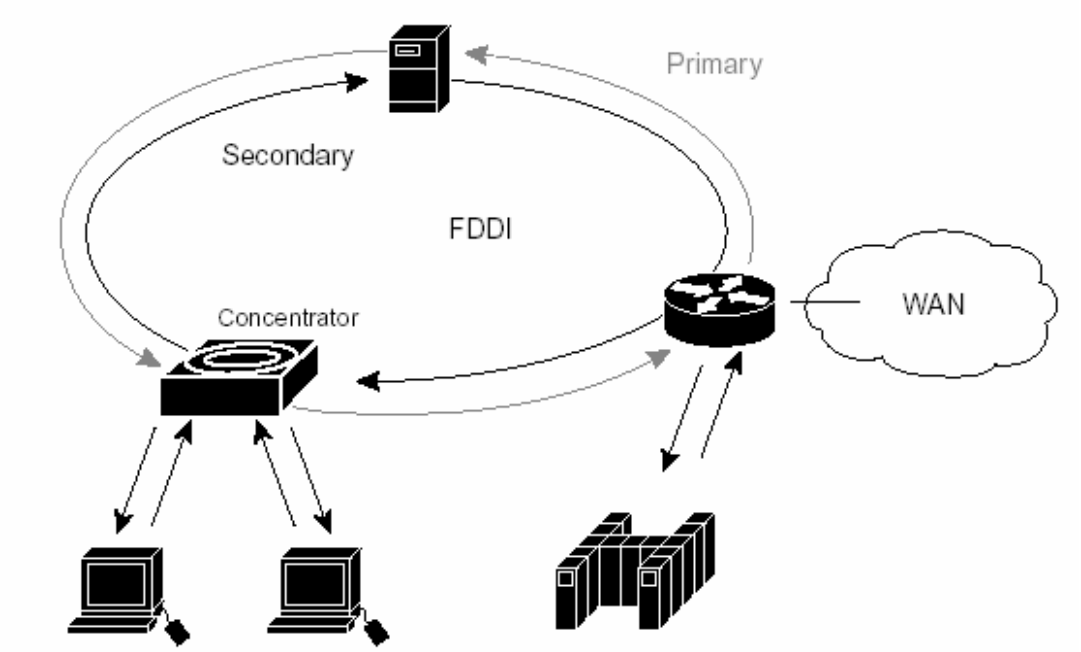


Рис. 4.2 – мережа з двійним кільцем і передачею маркера

В якості середовища передачі використовується волоконно-оптичний кабель. Оптоволокно забезпечує ряд переваг у порівнянні з більш широко вживаними мідними провідниками, включаючи захист даних (не випромінює електричні сигнали, які можна перехоплювати), надійність (стійке до електричних перешкод) і швидкість (потенційна пропускна здатність набагато вища, ніж у мідного кабелю). Стандарт FDDI визначає два типи використовуваного оптичного волокна: одномодове (іноді зване мономодовим) і багатомодове. Моди - це світлова хвиля, що входить в оптичне волокно під певним кутом. Одномодове волокно дозволяє поширюватися через оптичне волокно тільки одній моді, в той час як багатомодове одночасно кільком. Так як безліч мод світла, що поширюються по оптичному кабелю, можуть проходити різні відстані (в

залежності від кута входу), і, отже, досягати пункт призначення в різний час (явище, зване модальною дисперсією), одномодовий світловод здатний забезпечувати більшу смугу пропускання та передачу сигналу на великі відстані, ніж багатомодові світловоди. Завдяки цим характеристикам одномодові світлопроводи часто використовуються в якості основи великомасштабних мереж, в той час як багатомодовий світловод часто використовується в мережах рівня робочих груп. В багатомодовому світловоді в якості генераторів світла використовуються діоди, що випромінюють світло (LED), в той час як в одномодовому світловоді зазвичай застосовуються лазери.

Слідує відмітити, що існує також стандарт, іменований CDDI (*Copper Distributed Data Interface*) або TPDDI (*Twisted-Pair Distributed Data Interface*), аналогічний FDDI, але такий, що визначає в якості середовища передачі виту пару.

Основні характеристики мережі FDDI наведені в табл. 4.2.

Таблиця 4.2 - Основні характеристики мережі FDDI

	FDDI	CDDI
Швидкість передачі даних, Мб/с	100	100
Кількість станцій в кільці	500	250
Фізична топологія	Змішана (кільцева, деревовидна)	Деревовидна
Тип середовища передачі	Оптоволокно	Вита пара (STP Type 1, UTP cat 5)
Максимальна відстань між станціями, м	2000	200
Метод доступу до середовища передачі	Маркерний	Маркерний
Спосіб кодування	4B/5B	4B/5B

Особливості фізичного рівня стандарту FDDI

Відмінною рисою мереж FDDI є використання пристроїв з різним типом підключення до фізичного середовища передачі:

- станції з одиночним підключенням (Single-attachment station, SAS)
- станції з подвійним підключенням (Dual-attachment station, DAS)
- концентратори

Станції з одиночним підключенням приєднуються тільки до одного (первинного) кільця за допомогою концентратора. Перевагою такого способу підключення станції до мережі є те, що стан станції не впливає на роботу всього кільця, навіть при фізичному відключенні від середовища або виключенні живлення.

Станції з подвійним підключенням містять два порти, іменовані A і B, і забезпечують з'єднання з первинним і вторинним кільцем. Як далі буде показано, станції з подвійним підключенням визначають структуру подвійного кільця і впливають на працездатність всієї мережі.

Концентратори мережі FDDI, також іменовані як *концентратори з подвійним підключенням* (*Dual-attached concentrator, DAC*), є базовими елементами мережі. Вони підключаються безпосередньо до первинного і вторинного кільця і забезпечують контроль відмов або відключення живлення станцій з одиночним підключенням, тим самим запобігаючи розрив кільця.

На рис. 4.3 представлена типова конфігурація FDDI, що включає всі типи вузлів.

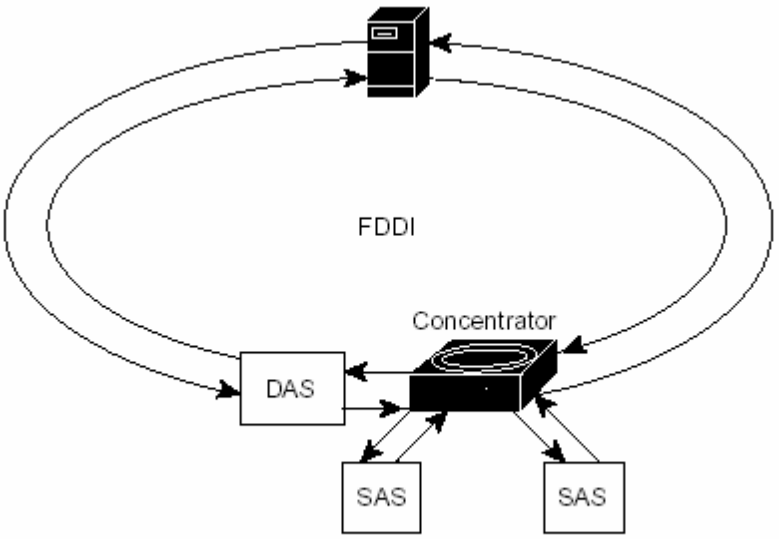


Рис. 4.3 - типова конфігурація FDDI

Наявність подвійної кільцевої мережі підвищує надійність функціонування всієї мережі. Якщо яка-небудь станція, підключена до подвійної кільцевої мережі,

відмовляє, або у неї відключається живлення, або пошкоджений мережний кабель, то подвійна кільцева мережа автоматично "згортається" в одне кільце, як показано на рис.4.4. При відмові станції 3, зображеної на малюнку, подвійне кільце автоматично згортається в станціях 2 і 4, утворюючи одинарне кільце. Хоча станція 3 більше не підключена до кільця, мережа продовжує працювати для решти станцій.

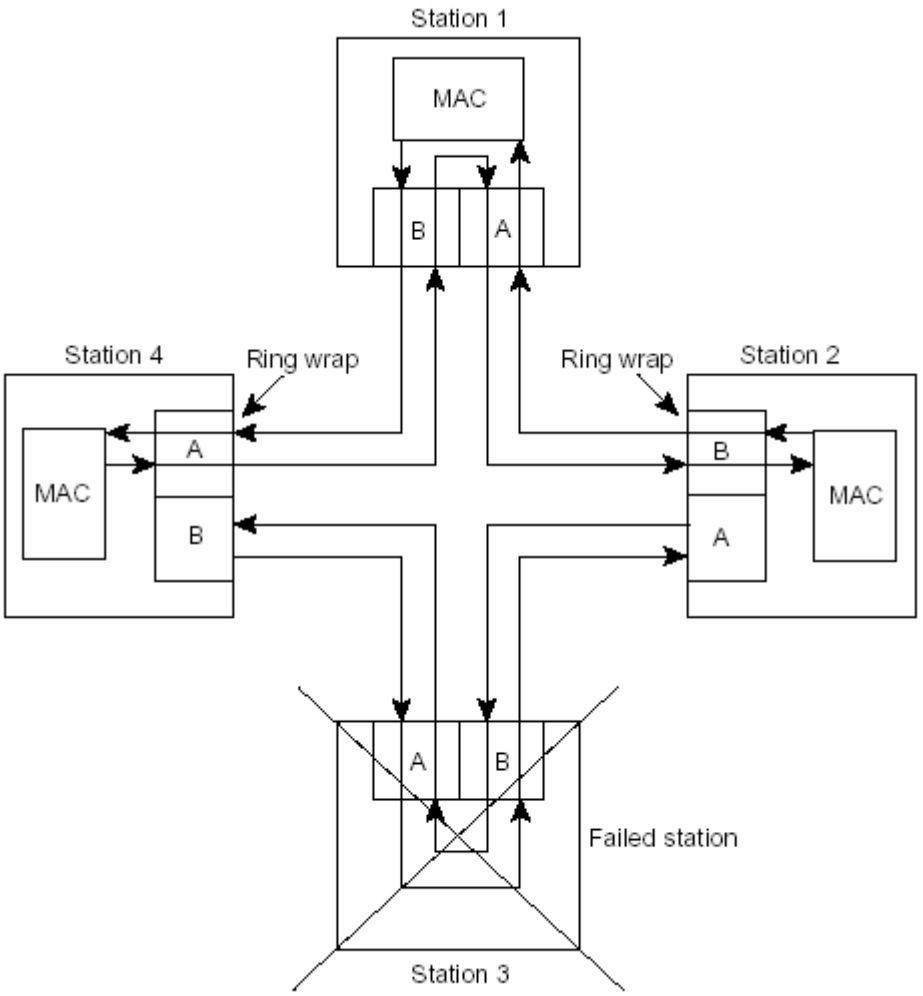


Рис. 4.4

На рис. 4.5 показано, як FDDI усуває пошкодження середовища передачі. В даному прикладі кільце згортається між станціями 3 і 4.

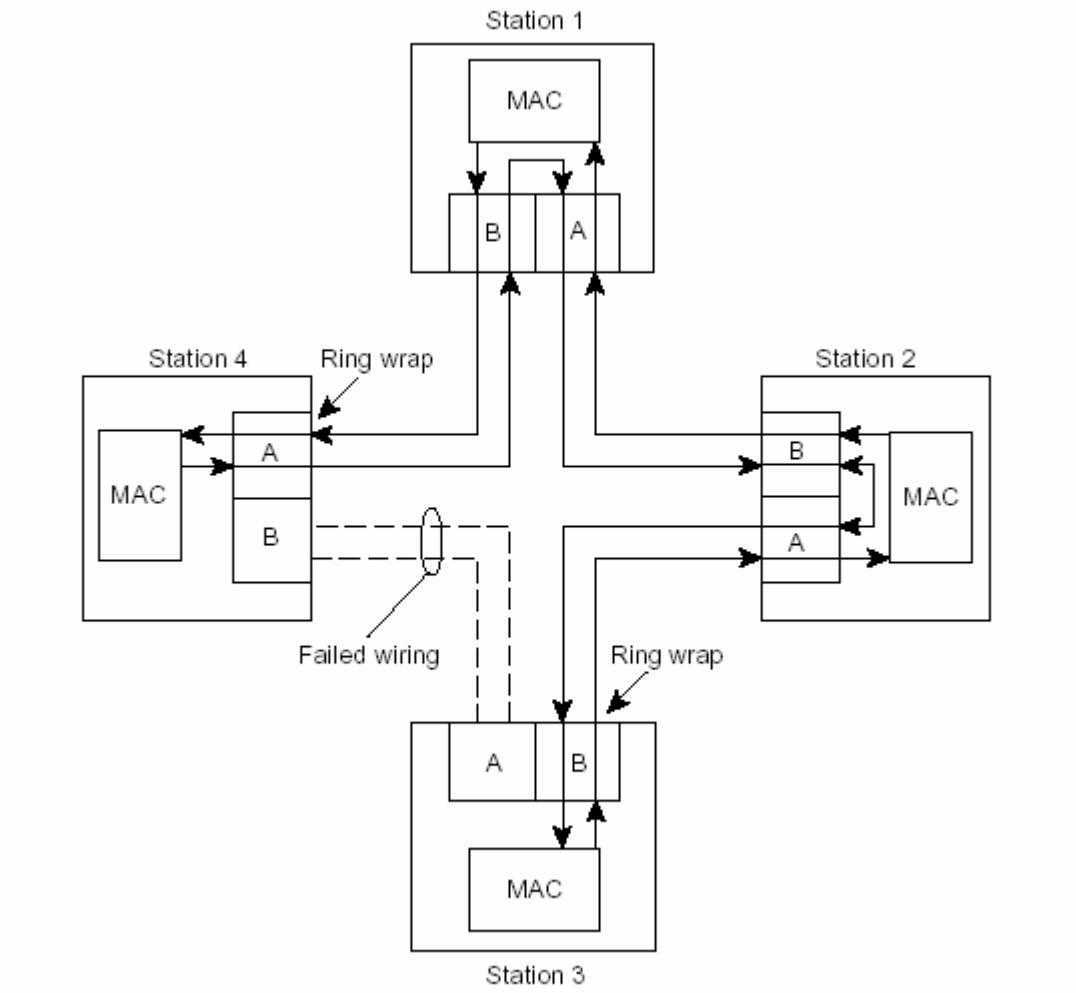


Рис. 4.5 – реконфігурація кільця при відмові станцій

У міру збільшення розмірів мереж FDDI зростає ймовірність збільшення числа відмов кільцевої мережі. Якщо мають місце дві відмови кільцевої мережі, то кільце буде згорнуто в обох випадках, що призводить до фактичної сегментації кільця на два окремих кільця, які не можуть повідомлятись одне з одним. Наступні відмови викличуть додаткову сегментацію кільця. Для запобігання сегментації кільця можуть бути використані оптичні шунтуючі перемикачі, які виключають станції, що відмовили, з кільця (рис. 4.6).

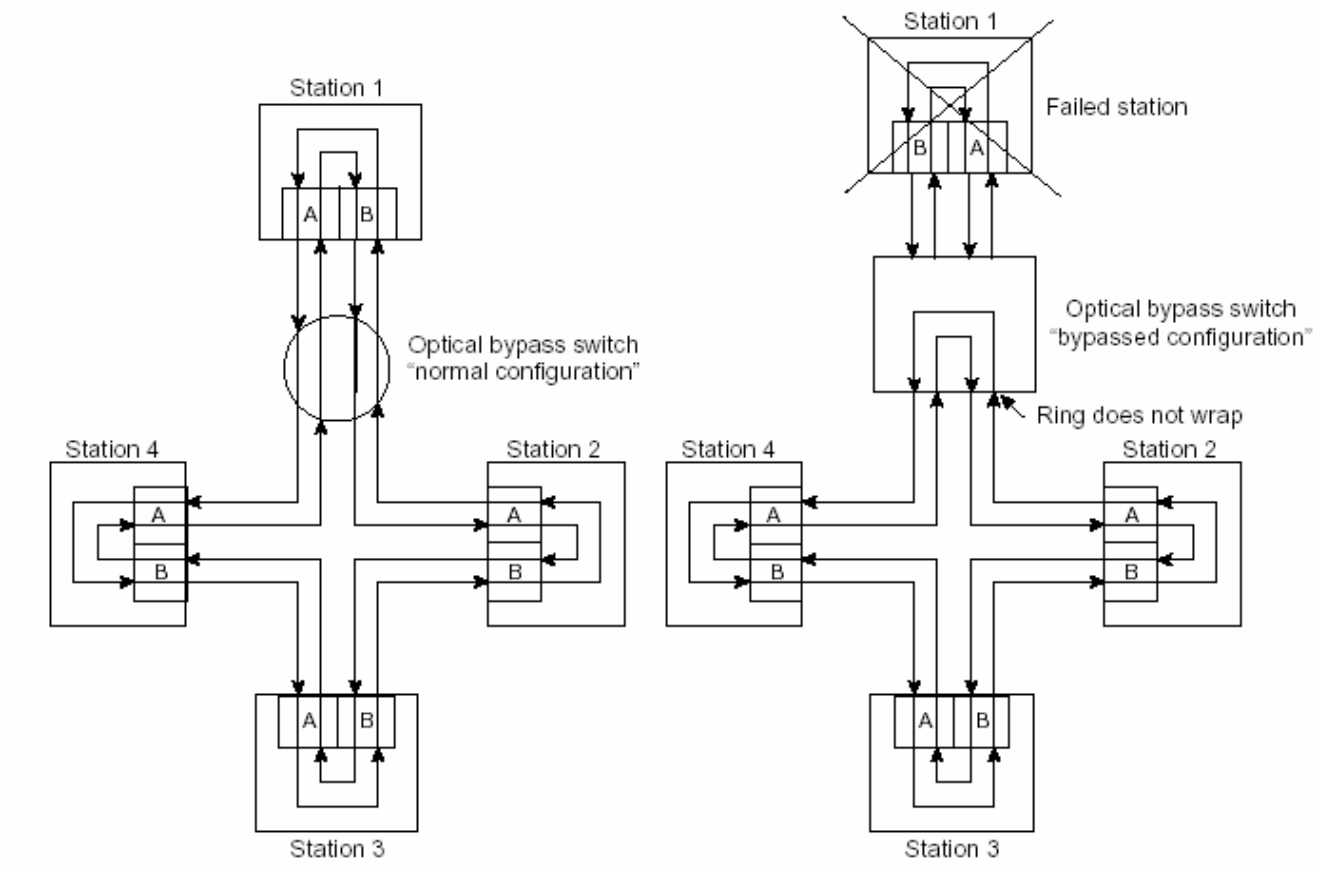


Рис. 4.6 - запобігання сегментації кільця

Пристрої, критичні до відмов, такі як маршрутизатори або шлюзи, а також серверні системи, можуть використовувати іншу техніку підвищення відмовостійкості, звану двухадаптерним підключенням (*dual homing*), для того, щоб забезпечити додаткову надмірність і підвищити ступінь працездатності. При двухадаптерному підключенні критичний до відмов пристрій приєднується до двох концентраторів одночасно. Одна пара каналів концентраторів вважається активною, інша пара - пасивною. Пасивний канал знаходиться в режимі підтримки до тих пір, поки не буде встановлено, що основний канал (або концентратор, до якого він підключений) відмовив. Якщо це відбувається, то пасивний канал автоматично активується.

Таким чином, мережі, що використовують технологію FDDI, відрізняються наступними важливими властивостями:

- висока ступінь відмовостійкості

- велика протяжність
- висока швидкість передачі даних
- гнучкий механізм розподілу пропускної здатності мережі і призначення пріоритетів станціям
- можливість максимального використання пропускної здатності мережі

Але при цьому FDDI залишається однією з найбільш дорогих технологій, що і звужує область її застосування. Тому найчастіше FDDI використовується для побудови високошвидкісних магістральних мереж будівель, підприємств, міст, а також для забезпечення доступу до високопродуктивних корпоративних серверів. Багато з сучасних корпоративних мереж будуються з використанням технології FDDI в поєднанні з більш дешевими технологіями Token Ring, Ethernet і Fast Ethernet. У зв'язку з широким розповсюдженням дешевших технологій, застосування FDDI для створення невеликих локальних мереж рівня робочих груп представляється недоцільним.

ЗАВДАННЯ НА РОБОТУ

1. Використовуючи пакет NetCracker, вивчити склад і функціональні характеристики типового обладнання локальних мереж на основі технологій Token Ring і FDDI.
2. У відповідності з варіантом завдання побудувати мережу підприємства з використанням технологій Token Ring и FDDI.
3. Для отриманої моделі мережі задати необхідні типи потоків даних між робочими станціями і серверами і провести імітаційне моделювання роботи мережі.
4. Проаналізувати середню загрузку мережевого обладнання і середовища передачі даних і час відповіді для потоку даних. Вказати ділянки

мережі, вразливі до перевантажень, і визначити засоби підвищення надійності функціонування мережі.

Таблиця 4.2. Варіанти завдань.

№ варіанту	Тип інфраструктури	Тип трафіку
1	1	2
2	2	3
3	3	4
4	4	1
5	1	3
6	2	4
7	3	1
8	4	2
9	1	4
10	2	1
11	3	2
12	4	3
13	1	1
14	2	2
15	3	3

Таблиця 4.3. Тип інфраструктури.

№ варіанту	Кількість будівель	Відстань між будівлями	Кількість поверхів	Кількість кімнат на поверсі
1	2	300	4	3
2	2	250	3	3
3	3	200	3	3
4	3	150	2	3

Таблиця 4.4. Тип модельованого трафіку.

№ варіанту	Кількість файлових серверів	Кількість HTTP-серверів	Кількість FTP-серверів	Кількість серверів баз даних
1	3	1	2	2
2	3	2	1	2
3	2	1	2	3
4	2	2	1	3

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

Коротка характеристика технології Token Ring.

Особливості мереж стандарту FDDI.

Засоби структуризації мереж на базі стандарту IEEE 802.5.

Типи обладнання мереж FDDI.

Засоби забезпечення відмовостійкості в мережах Token Ring и FDDI.

Яке передавальне середовище є основним в мережі FDDI?

Який метод доступу до передавальної середовищі використовується в мережі Token Ring (стандарт IEEE-802.5.)?

Яку конфігурацію має мережа Token Ring в загальному випадку?

Яку функцію виконує концентратор мережі Token Ring?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Буров Є. Комп'ютерні мережі – Л.: БаК, 1999.
2. Кулаков Ю.А., Омелянский С. В. Компьютерные сети. Выбор, установка, использование и администрирование – К.: Юниор, 1999.
3. Кульгин М. Технологии корпоративных сетей – СПб.: Питер, 2000.
4. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: функции, выбор, разработка – М.: ЭКОМ, 1998.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы – СПб.: Питер, 1999.
6. CISCO Internetworking technology overview – Cisco, 1999.
7. IEEE Standard for Information Technology. Part 5: Token ring access method and physical layer specifications – IEEE Std 802.5, 1998 Edition.

Комп'ютерний практикум № 5

Побудова корпоративної мережі з використанням стека протоколів TCP/IP

Мета роботи: вивчити принципи розподілу адресного простору з мережах TCP/IP, отримати навики формування підмереж, визначення маски підмережі; вивчити способи маршрутизації даних.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Стек протоколів TCP/IP є найбільш популярним на сьогоднішній день, оскільки забезпечує можливість взаємодії як локальних, так і глобальних мереж. Найбільш широке розповсюдження отримав стек протоколів TCP/IP версії 4. До складу даного стеку входить безліч протоколів, найбільш відомими з яких є *протокол управління передачею* (Transmission Control Protocol, TCP) і *протокол міжмережевої взаємодії* (Internet Protocol, IP). Враховуючи тенденцію швидкого зростання мережі Internet, в основу якої покладено TCP/IP, розроблений стек протоколів TCP/IP версії 6, що використовується поки що не в таких значних масштабах. Основу нової версії стека протоколів складає *протокол міжмережевої взаємодії нового покоління* (IP new generation, IPng або IPv6). У даній роботі буде розглянуто тільки TCP/IP версії 4. Протокол міжмережевої взаємодії (IP) є протоколом мережевого рівня. Цей протокол визначає спосіб адресації мереж і окремих вузлів і забезпечує підтримку маршрутизації потоків даних.

Кожному вузлу мережі TCP/IP (хосту) призначається 32-розрядна логічна адреса, іменована IP-адресою і складається в загальному випадку з двох полів - адреса (номер) мережі та адресу (номер) вузла. Адреса мережі унікально ідентифікує кожну мережу і призначається централізовано. Якщо мережа підключена до Internet, адреса мережі може бути отримана

безпосередньо в Мережевому інформаційному центрі (Internet Network Information Center, InterNIC) або ж призначена регіональним провайдером послуг Internet (ISP), який отримав блок адрес у InterNIC. Адреса хоста вибирається адміністратором мережі, але повинна бути унікальною в межах мережі. Для запису IP-адреси найчастіше використовується десяткова форма запису з розділенням крапками (dotted decimal notation), відповідно до якої кожен октет представляється десятковим числом в діапазоні від 0 до 255, наприклад, 1.2.3.4. Загальний формат IP-адреси представлений на рис. 5.1.

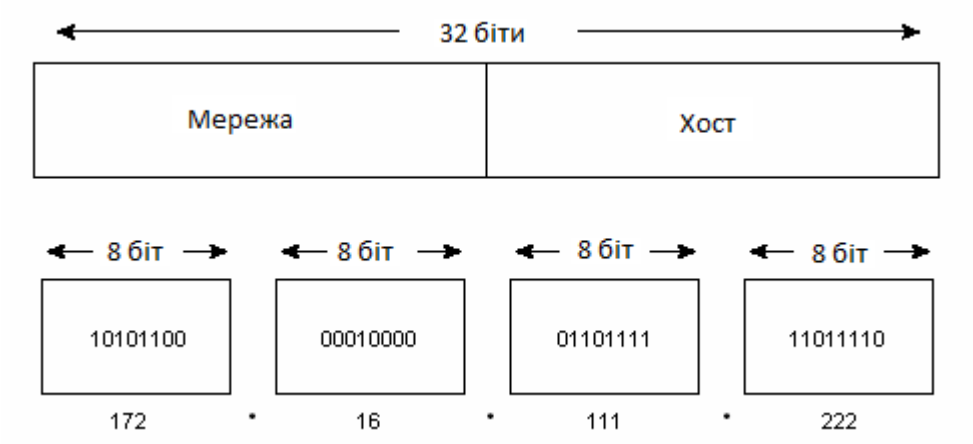


Рис. 5.1- Загальний формат IP-адреси

Для виділення з IP-адреси номера мережі і номера вузла спочатку були визначені 5 класів адрес – класи A, B, C, D і E. Для загального користування були доступні тільки класи A, B і C. Клас D призначався для використання в мережах з груповою адресацією, клас E був зарезервований для подальшого використання. Формат адреси для мережі класів A, B і C представлений на рис. 5.2.

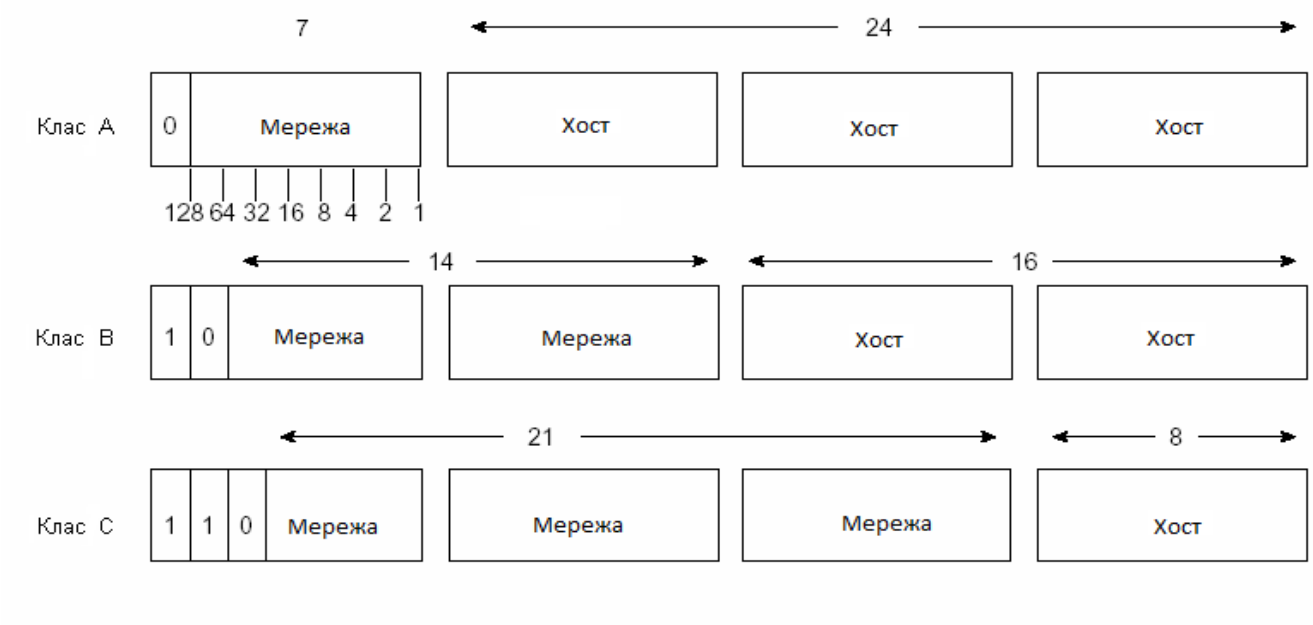


Рис.5. 2 - Формат адреси для мережі класів A, B і C

Клас IP-адреси, а, отже, і співвідношення між розмірностями полів номера мережі і номера вузла, можуть бути легко визначені по старших бітах першого октету. Основні характеристики мереж різних класів наведені в табл. 5.1.

Табл. 5.1 - Основні характеристики мереж різних класів

Клас адреси	**Формат адреси**	**Старші біти**	**Діапазон адрес**	**Кількість біт в адресі сети / хоста**	**Кількість мереж**	**Кількість хостів в мережі**
A	C.X.X.X	0	1.0.0.0 - 126.0.0.0	7/24	126	16 777 214
B	C.C.X.X	10	128.1.0.1 - 191.254.0.0	14/16	16384	65 543
C	C.C.C.X	110	192.0.0.0 - 223.255.254.0	22/8	4194304	254
D	Не визначено	1110	224.0.0.0 - 239.255.255.255	Не визначено	Не визначено	Не визначено
E	Не визначено	1111	224.0.0.0 - 254.255.255.255	Не визначено	Не визначено	Не визначено

Деякі IP-адреси мають спеціальне призначення і не можуть бути використані для вузлів в реальних мережах (табл. 5.2).

Табл. 5.2

Тип адреси		Призначення
Всі нулі	0.0.0.0	Даний вузол
[Номер мережі].[Всі нулі]	192.168.1.0	Дана мережа
[Всі нулі].[Номер вузла]	0.0.0.1	Вузол даної мережі
Всі одиниці	255.255.255.255	Всі вузли даної мережі
[Номер мережі].[Всі одиниці]	192.168.1.255	Всі вузли вказаної мережі
127.[будь-яке число]	127.0.0.1	"Петля" (loopback)

Для використання в приватних (внутрішніх) мережах зарезервовані три блоки IP-адресів: 10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.1.0 – 192.168.255.255

Ці адреси призначені для внутрішнього використання і можуть призначатися вузлам в будь-якій мережі без попереднього узгодження з будь-якою організацією. Очевидно, що ці адреси не є унікальними в межах глобальної мережі, тому не можуть бути використані для адресації хостів з інших мереж. Зовнішні мережеві шлюзи і маршрутизатори відкидають всі пакети, що відправляються хостами, у яких є тільки внутрішні адреси.

IP-мережа може бути розбита на дрібніші фрагменти, звані підмережами. Кожна підмережа представляється як звичайна IP-мережа, що надає велику гнучкість схемі розподілу адрес, дозволяє більш ефективно витрачати адреси і уникнути їх порожньої витрати. Перевагою використання підмереж є також те, що для зовнішнього світу мережа організації представляється як єдине ціле, завдяки чому ховається її реальна внутрішня структура.

Для створення номера підмережі виділяється деяка частина розрядів з поля номера вузла. Розмірність поля номера підмережі змінюється в залежності від необхідної кількості підмереж і кількості вузлів в кожній з них. Для виділення номера підмережі використовується маска підмережі (subnet

mask). Формат маски підмережі аналогічний формату IP-адреси. Однак, маска підмережі в двійковому поданні завжди містить послідовність "1" в тій частині, яка відповідає номеру мережі і підмережі, і послідовність "0" в тій частині, яка відповідає номеру вузла (рис.5.3).

Рис.5.3. - Формат маски підмережі

Для мереж класів A, B і C у випадку відсутності підмереж використовуються маски 255.0.0.0, 255.255.0.0 і 255.255.255.0 відповідно. При необхідності використання підмереж потребується визначити кількість розрядів в полях номера підмережі і номера вузла. Замітимо, що номери підмереж, що складаються з всіх "0" або "1", використовувати, як правило, не рекомендується. Для розрахунку можна скористатись одним з наступних способів:

1. Виходячи з необхідності, задається кількість підмереж Ns . Довжина поля номерв під мережі визначається по формулі $n_s = \lceil log_2(N_s + 2) \rceil$. Поле номеру вузла буде мати розмірність $n_h = 32 - (n_n - n_s)$ розрядів, де nn - довжина поля номера мережі. Отже, максимальна кількість хостів в кожній під мережі рівна $N_h = 2^{n_h} - 2$.
2. Виходячи з необхідності, задається максимальна кількість вузлів в кожній під мережі Nh. Довжина поля номера вузла визначається по формулі $n_h = \lceil log_2(N_h + 2) \rceil$. Поле номеру під мережі буде мати розмірність $n_s = 32 - (n_n - n_h)$ розрядів, де n_n – довжина поля номеру мережі. Отже, максимальна кількість під мереж рівна $N_s = 2^{n_s} - 2$

В даному випадку передбачається, що у всіх підмережах використовуються однакові (рівні) маски. Це може виявитися неприйнятним в тому випадку, коли кількість вузлів в різних підмережах істотно відрізняється. Для усунення цього недоліку можуть бути використані нерівні маски або маски змінної довжини (variable length subnet mask). В цьому випадку процес розбиття мережі на підмережі виконується в кілька етапів, коли на першому етапі розбивається базова мережа, а в подальшому отримані підмережі в свою чергу розбиваються на підмережі.

Наприклад, припустимо, що мережі організації надано IP-адресу 172.16.0.0. Необхідно визначити 10 підмереж однакового розміру. У такому випадку для створення номера підмережі буде потрібно виділити 4 біта з поля номера вузла, що дозволить адресувати до 16 підмереж. Маска для кожної підмережі буде задаватися у вигляді 255.255.240.0. Кожна підмережа дозволяє адресувати 16382 вузла. Адреси підмереж наведені в табл.5.3.

Табл. 5.3 - Адреси підмереж

№	Адреса підмережі	Адреса широкомовної передачі для підмережі
1.	172.16.0.0	172.16.15.255
2.	172.16.16.0	172.16.31.255
3.	172.16.32.0	172.16.47.255
4.	172.16.48.0	172.16.63.255
5.	172.16.64.0	172.16.79.255
6.	172.16.80.0	172.16.95.255
7.	172.16.96.0	172.16.111.255
8.	172.16.112.0	172.16.127.255
9.	172.16.128.0	172.16.143.255
10.	172.16.144.0	172.16.159.255
11.	172.16.160.0	172.16.175.255
12.	172.16.176.0	172.16.191.255

13.	172.16.192.0	172.16.207.255
14.	172.16.208.0	172.16.223.255
15.	172.16.224.0	172.16.239.255
16.	172.16.240.0	172.16.255.255

В іншому випадку, припустимо, організації надано адресу 192.168.1.0. Адреси необхідно розподілити між п'ятьма взаємопов'язаними мережами, у трьох з яких є 50 вузлів, в двох, що залишилися по 30. Очевидно, що, використовуючи рівні маски підмережі, не можна отримати рішення, яке задовольняє умовам завдання. Тому необхідно скористатися масками змінної довжини. На першому етапі при використанні маски підмережі 255.255.255.192 мережа розбивається на чотири підмережі, в кожній з яких може перебувати до 64 хостів (табл. 5.4).

Таб.5.4

№	Адреса підмережі	Маска підмережі	Адреса широкомовної передачі для підмережі
1.	192.168.1.0	255.255.255.192	192.168.1.63
2.	192.168.1.64	255.255.255.192	192.168.1.127
3.	192.168.1.128	255.255.255.192	192.168.1.191
4.	192.168.1.192	255.255.255.192	192.168.1.255

Після цього одна з отриманих підмереж з допомогою маски 255.255.255.224 розбивається ще на дві підмережі по 32 вузла в кожній (табл. 5.5).

Таб.5.5

№	Адреса підмережі	Маска підмережі	Адреса широкомовної передачі для підмережі
1.	192.168.1.0	255.255.255.192	192.168.1.63
2.	192.168.1.64	255.255.255.192	192.168.1.127
3.	192.168.1.128	255.255.255.192	192.168.1.191
4.	192.168.1.192	255.255.255.224	192.168.1.223

5.	192.168.1.224	255.255.255.224	192.168.1.255

У даному прикладі задіяні підмережі, номери яких в двійковому поданні містять всі "0" і "1", що може виявитися неприйнятним при наявності апаратних або програмних маршрутизаторів, що не підтримують безкласову маршрутизацію.

Важливою функцією мережевого рівня є управління процесом маршрутизації пакетів, що передаються через мережу. Для з'єднання джерела і одержувача повинен бути встановлений маршрут або набір маршрутів. Зазвичай маршрути фіксуються в кожному вузлі за допомогою записів у відповідній таблиці маршрутів, що показує за яким виходить каналу повинен направлятися даний пакет. Алгоритми вибору маршрутів, що застосовуються для встановлення відповідних шляхів і формування таблиць маршрутів, грунтуються на обліку міри вартості кожного маршруту. Вартість може бути величиною фіксованою й визначатися такими параметрами, як довжина лінії, швидкість передачі або ширина смуги (пропускна здатність), безпека, оцінювана затримка при передачі сигналу і т.п.

Пристрої, які вирішують це завдання, називаються маршрутизаторами (router). Маршрутизатори об'єднують окремі мережі в загальну складову мережу. Внутрішня структура кожної мережі в даному випадку значення не має. До кожного маршрутизатора можуть бути приєднані декілька мереж (принаймні дві). У складних складових мережах майже завжди існує декілька альтернативних маршрутів для передачі пакетів між двома кінцевими вузлами. Маршрут - це шлях (послідовність маршрутизаторів), який повинен пройти пакет від відправника до пункту призначення. Маршрутизатор вибирає маршрут на підставі свого уявлення про поточну конфігурації мережі та відповідного критерію вибору маршруту. Звичайно як критерій виступає час проходження маршруту, яке в локальних мережах збігається з довжиною

маршруту, вимірюваної в кількості пройдених вузлів маршрутизації (в глобальних мережах приймається в розрахунок і час передачі пакета по кожній лінії зв'язку).

У мережі Internet, найбільш розвиненою на справжній момент мережі дейтаграммного типу, деякі маршрутизатори використовуються для переміщення інформації через одну конкретну групу мереж, що знаходяться під одним і тим же адміністративним початком і управлінням (такий об'єкт називається автономною системою - autonomous system). Маршрутизатори, що використовуються для обміну інформацією в межах автономних систем, називаються внутрішніми (interior routers); вони використовують різні протоколи внутрішніх шлюзів (Interior Gateway Protocol, IGP) для виконання цього завдання. Маршрутизатори, які переміщують інформацію між автономними системами, називаються зовнішніми (exterior routers); для цього вони використовують протоколи зовнішньої маршрутизації (Exterior Gateway Protocol, EGP).

Для накопичення інформації про поточну конфігурації мережі маршрутизатори обмінюються маршрутною інформацією між собою по спеціальному протоколу. Протоколи цього типу називаються протоколами обміну маршрутною інформацією (або протоколами маршрутизації). Протоколи обміну маршрутною інформацією слід відрізняти від протоколів мережного рівня, оскільки вони служать для обміну службовою інформацією, тоді як протоколи мережевого рівня призначені для передачі даних користувача, аналогічно протоколам канального рівня.

Для доставки пакетів протоколу обміну маршрутною інформацією використовується протокол мережевого рівня, так як тільки він може передати інформацію між маршрутизаторами, які у різних мережах. Пакет протоколу обміну маршрутною інформацією поміщається в поле даних пакета мережного рівня. За допомогою протоколів обміну маршрутною інформацією

маршрутизатори складають карту міжмережевих зв'язків тієї чи іншої міри детальності і приймають рішення про те, якому наступному вузлу потрібно передати пакет.

Протоколи обміну маршрутною інформацією стека TCP/IP є адаптивними, в свою чергу їх можна розділити на дві групи:

- протоколи вектора відстаней (distance vector);
- протоколи станів зв'язків (link state).

Протоколи, що використовують алгоритм вектора відстаней, наказують кожному маршрутизатору періодично і широкомовно розсилати по мережі вектор відстаней від себе до всіх відомих йому мереж. Під відстанню зазвичай розуміється число проміжних маршрутизаторів, через які пакет повинен пройти перш, ніж потрапить у відповідну мережу (hop). Може використовуватися і інша метрика, що враховує не тільки число проміжних пунктів, а й час проходження пакетів по зв'язку між сусідніми маршрутизаторами. Отримавши вектор від сусіднього маршрутизатора, кожний маршрутизатор додає до нього інформацію про відомі йому інші мережі, про які він дізнався безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектора по мережі. Зрештою кожен маршрутизатор дізнається інформацію про наявні в інтермережі мережі і про відстань до них через сусідні маршрутизатори.

Алгоритми вектора відстаней добре працюють тільки в невеликих мережах. У великих мережах вони засмічують лінії зв'язку інтенсивним широкомовним трафіком, до того ж зміни конфігурації можуть відпрацьовуватися з цього алгоритму не завжди коректно, тому що маршрутизатори не мають точного уявлення про топологію зв'язків у мережі, а мають у своєму розпорядженні тільки узагальнену інформацію - вектор дистанцій, до того ж отриману через посередників. Робота маршрутизатора в

даному випадку нагадує роботу моста, так як точної топологічної картини мережі такий маршрутизатор не має.

Найбільш поширеним протоколом, заснованим на алгоритмі вектора відстаней, є протокол RIP (Routing Information Protocol - протокол інформації маршрутизації), описаний в RFC 1058. Це один з найстаріших протоколів обміну маршрутною інформацією, проте він до цих пір надзвичайно поширений в обчислювальних мережах. Існують різновиди протоколу RIP для різних мереж і різних стеків протоколів.

Згідно з протоколом RIP всі мережі мають номери (спосіб утворення номера залежить від використовуваного в мережі протоколу мережевого рівня), а всі маршрутизатори - ідентифікатори. Вектор відстаней являє собою набір пар чисел, відповідних номерами мереж і відстаням до них. Вектори відстаней ітераційно поширюються маршрутизаторами по мережі, і через кілька кроків кожен маршрутизатор має дані про досяжні для нього мережі і про відстані до них. Якщо зв'язок з якою-небудь мережею обривається, то маршрутизатор відзначає цей факт тим, що привласнює елементу вектора, відповідному відстані до цієї мережі, максимально можливе значення, яке має спеціальний зміст - "зв'язку немає". Таким значенням в протоколі RIP є число 16.

Кожен запис даних у таблиці маршрутизації RIP містить необхідну інформацію, включаючи кінцевий пункт призначення, наступне пересилання на шляху до цього пункту призначення і метрику. У таблиці маршрутизації може знаходитися також і інша інформація, у тому числі різні таймери, пов'язані з даним маршрутом. Типова таблиця маршрутизації RIP показана на рис. 5.4.

Distination	Next hop	Distance	Timers	Flags
Network A	Router 1	3	11, 12, 13	x, y
Network B	Router 2	5	11, 12, 13	x, y
Network C	Router 1	2	11, 12, 13	x, y
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

Рис.5.4 - Типова таблиця маршрутизації RIP

RIP зберігає тільки найкращі маршрути до пункту призначення. Якщо нова інформація забезпечує кращий маршрут, то ця інформація замінює стару маршрутну інформацію. Зміни в топології мережі можуть викликати зміни в маршрутах, приводячи до того, наприклад, що який-небудь новий маршрут стає кращим маршрутом до конкретного пункту призначення. Коли мають місце зміни в топології мережі, то ці зміни відображаються в повідомленнях про коректування маршрутизації. Наприклад, коли який-небудь маршрутизатор виявляє відмова одного з каналів або іншого маршрутизатора, він повторно обчислює свої маршрути і відправляє повідомлення про коригування маршрутизації. Кожен маршрутизатор, що приймає повідомлення про оновлення маршрутизації, в якому міститься зміна, коригує свої таблиці і поширює цю зміну.

RIP визначає ряд характеристик, призначених для більш стабільної роботи в умовах швидко мінливої топології мережі. У їх число входить обмеження числа пересилань, тимчасові утримування змін (hold-downs), розщеплені горизонти (split-horizons) і коригування відміни (poison reverse updates).

Обмеження кількості пересилок

RIP дозволяє максимальне число пересилань, рівне 15. Будь-якому пункту призначення, що знаходиться далі, ніж на відстані 15 пересилань, присвоюється ярлик "недосяжного". Максимальне число пересилань RIP в

значній мірі обмежує його застосування у великих об'єднаних мережах, проте сприяє запобіганню появи проблеми, іменованої рахунком до нескінченності (count to infinity), що приводить до зациклення маршрутів в мережі. Проблема рахунку до нескінченності представлена на рис. 5.5.

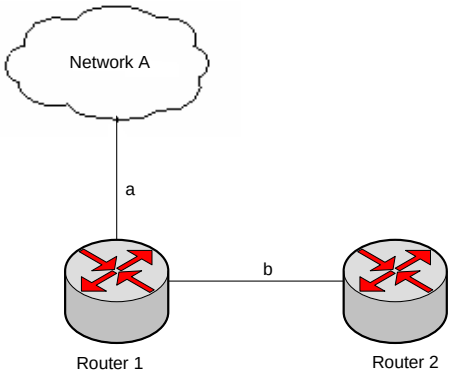


Рис.5.5

Розглянемо, що станеться, якщо на рис. 3 канал а маршрутизатора 1 (R1), що зв'язує його з мережею А, відмовить. R1 перевіряє свою інформацію і виявляє, що маршрутизатор 2 (R2) пов'язаний з мережею А каналом завдовжки в одну пересилку. Так як R1 знає, що він безпосередньо з'єднаний з R2, то він оголошує про маршрут з двох пересилань до мережі А і починає спрямовувати весь трафік в мережу А через R2. Це призводить до утворення маршрутної петлі. Коли R2 виявляє, що R1 може тепер досягти мережі А за два пересилання, він змінює запис своїх власних даних в таблиці маршрутизації, щоб показати, що він має тракт довжиною в 3 пересилання до мережі А. Ця проблема, а також дана маршрутна петля триватимуть нескінченно, або до тих пір, поки не буде нав'язана якась зовнішня гранична умова. Цією граничною умовою є максимальне число пересилань RIP. Коли число пересилань перевищить 15, даний маршрут маркується як недосяжний. Через деякий час цей маршрут видаляється з таблиці.

Часові утримування змін

Часові утримування змін використовуються для того, щоб перешкодити

регулярним повідомленням про коригування незаконно відновити в правах маршрут, який виявився зіпсованим. Коли якийсь маршрут відмовляє, сусідні маршрутизатори виявляють це. Потім вони обчислюють нові маршрути і відправляють повідомлення про оновлення маршрутизації, щоб інформувати своїх сусідів про зміни в маршруті. Ця діяльність призводить до появи цілої хвилі корекцій маршрутизації, які фільтруються через мережу.

Наведені в дію коректування неодночасно прибувають в усі пристрої мережі. Тому можливо, що який-небудь пристрій, який ще не отримав інформацію про яку-небудь відмову в мережі, може відправити регулярне повідомлення про коригування (у якому маршрут, який тільки що відмовив, все ще числиться справним) в інший пристрій, яке щойно отримало повідомлення про цю відмову в мережі. В цьому випадку цей інший пристрій тепер буде мати (і можливо, рекламувати) неправильну маршрутну інформацію.

Команди про часове утримування вказують маршрутизаторам, щоб вони на деякий час притримали будь-які зміни, які можуть вплинути на тільки що віддалені маршрути. Цей період утримування зазвичай розраховується таким чином, щоб він був більше періоду часу, необхідного для внесення будь-якої зміни про маршрутизації на всю мережу. Утримання змін запобігає появі проблеми рахунку до нескінченності.

Розщеплені горизонти

Розщеплені горизонти використовують перевагу того факту, що ніколи не буває корисним надсилати інформацію про якийсь маршрут назад в тому напрямку, з якого прийшла ця інформація. Для ілюстрації цього положення розглянемо рис.5. 6.

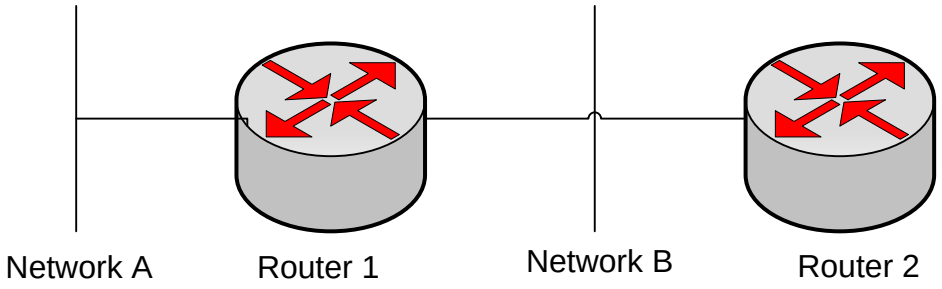


Рис.5.6

Маршрутизатор 1 (R1) спочатку оголошує, що він має в своєму розпорядженні якийсь маршрут до мережі А. Маршрутизатору 2 (R2) немає підстав включати цей маршрут у своє коригування, що відсилається назад маршрутизатору R1, так як R1 ближче до мережі А. Правило розщепленого горизонту свідчить , що R2 має виключити (потрапити на) цей маршрут за будь-яких коректуваннях, які він відправляє в R1.

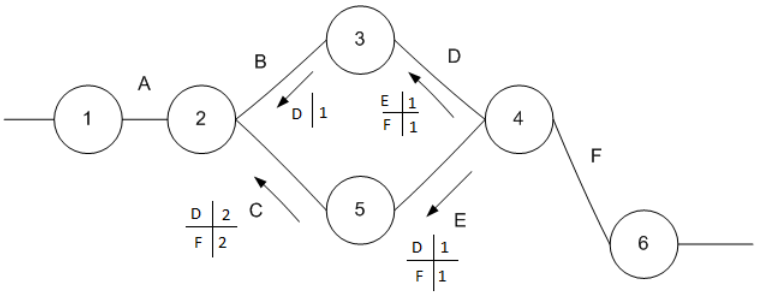
Правило розщепленого горизонту допомагає запобігти маршрутних петел між двома вузлами. Наприклад, розглянемо випадок, коли відмовляє інтерфейс R1 з мережею А. При відсутності розщеплених горизонтів R2 продовжує інформувати R1 про те, що він може потрапити в мережу А через R1. Якщо R1 не має достатнього інтелекту, то він дійсно може вибрати маршрут, пропонований R2, в якості альтернативи для свого прямого зв'язку, що відмовив, що призводить до утворення петлі маршрутизації. І хоча тимчасове утримання змін має запобігати цьому, застосування розщепленого горизонту забезпечує додаткову стабільність алгоритму.

Коректування відміни маршруту

У той час як завданням розщеплених горизонтів є запобігання утворення маршрутних петель між сусідніми маршрутизаторами, коректування скасування призначені для усунення більших маршрутних петель. В основі їх дії лежить положення про те, що збільшення значення показників маршрутизації звичайно вказує на наявність маршрутних петель. В цьому випадку відправляються коректування скасування для видалення даного

маршруту і поміщення його в стан тимчасового утримування.

На рис.5.7 наведено приклад мережі, що складається з шести маршрутизаторів, що мають ідентифікаційні номери від 1 до 6, і з шести мереж від A до F, утворених прямими зв'язками типу "точка-точка".



Початкова інформація в вузлі 2:

Мережа	Відстань	
A	1	
B	1	-
C	1	-

Після 2-х ітерацій:

A	1	-
B	1	-
C	1	-
D	2	2
E	2	2
D	3	3
F	3	3

Рис.5.7

На малюнку приведена початкова інформація, що міститься в таблиці маршрутизації маршрутизатора 2, а також стан після двох ітерацій обміну маршрутними пакетами протоколу RIP. Після певного числа ітерацій маршрутизатор 2 буде знати про відстані до всіх мереж інтермережі, причому у нього може бути кілька альтернативних варіантів відправки пакета до мережі призначення. Нехай у нашому прикладі мережею призначення є мережа D.

При необхідності відправити пакет в мережу D маршрутизатор переглядає свою базу даних маршрутів і вибирає порт, який має найменшу відстані до мережі призначення (в даному випадку порт, що зв'язує його з маршрутизатором 3).

Для адаптації до зміни стану зв'язків і обладнання з кожним записом таблиці маршрутизації пов'язаний таймер. Якщо за час тайм-ауту не прийде нове повідомлення, яке підтверджує цей маршрут, то він видаляється з маршрутної таблиці.

Протокол RIP використовує евристичний алгоритм Беллмана-Форда, і рішення, знайдене з його допомогою є не оптимальним, а близьким до оптимального. Перевагою протоколу RIP є його обчислювальна простота, а недоліками - збільшення трафіку при періодичній розсилці широкомовних пакетів і неоптимальність знайденого маршруту.

На рис. 5.8 показаний випадок нестійкої роботи мережі по протоколу RIP при зміні конфігурації - відмові лінії зв'язку маршрутизатора М1 з мережею 1. При працездатному стані цього зв'язку в таблиці маршрутів кожного маршрутизатора є запис про мережу з номером 1і відповідною відстанню до неї.

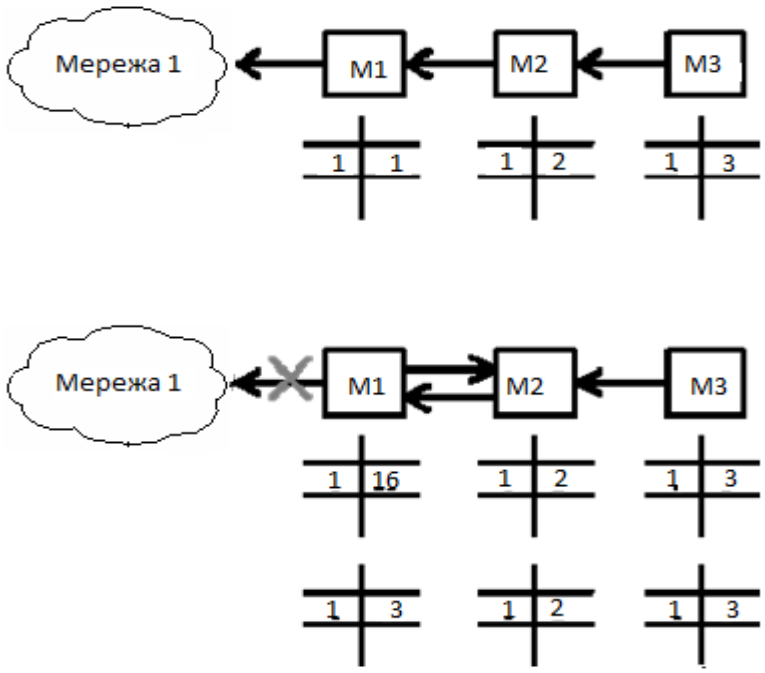


Рис.5.8 - випадок нестійкої роботи мережі по протоколу RIP

При обриві зв'язку з мережею 1 маршрутизатор М1 відзначає, що відстань до цієї мережі прийняло значення 16. Проте отримавши через деякий час від маршрутизатора М2 маршрутне повідомлення про те, що від нього до мережі 1 відстань складає 2 пересилання, маршрутизатор М1 нарощує цю відстань на 1 і відзначає, що мережа 1 досяжна через маршрутизатор 2. У результаті пакет, призначений для мережі 1, буде циркулювати між маршрутизаторами М1 і М2 до тих пір, поки не закінчиться час зберігання

запису про мережу 1 в маршрутизаторі 2, і він не передасть цю інформацію маршрутизатору М1.

Для виключення подібних ситуацій маршрутна інформація про відому маршрутизатора мережі не передається тому маршрутизатору, від якого вона прийшла.

Існують і інші , більш складні випадки нестабільної поведінки мереж, що використовують протокол RIP, при змінах в стані зв’язків або маршрутизаторів мережі.

Алгоритми стану зв'язків забезпечують кожен маршрутизатор інформацією, достатньою для побудови точного графу зв'язків мережі. Всі маршрутизатори працюють на підставі однакових графів, що робить процес маршрутизації більш стійким до змін конфігурації. Широкомовна розсилка використовується тут тільки при змінах стану зв'язків, що відбувається в надійних мережах не так часто.

Для того, щоб зрозуміти, в якому стані знаходяться лінії зв'язку, підключені до його портів, маршрутизатор періодично обмінюється короткими пакетами зі своїми найближчими сусідами. Цей трафік також широкомовний, але він циркулює тільки між сусідами і тому не так засмічує мережу.

Протоколом, заснованим на алгоритмі стану зв'язків, в стеку TCP/IP є протокол OSPF (Open Shortest Path First), що володіє багатьма особливостями, орієнтованими на застосування у великих гетерогенних мережах.

Протокол OSPF обчислює маршрути в IP-мережах, зберігаючи при цьому інші протоколи обміну маршрутною інформацією.

Безпосередньо пов'язані (тобто досяжні без використання проміжних маршрутизаторів) маршрутизатори називаються "сусідами". Кожен маршрутизатор зберігає інформацію про те, в якому стані на його думку знаходиться сусід. Маршрутизатор покладається на сусідні маршрутизатори і передає їм пакети даних тільки в тому випадку, якщо він впевнений, що вони

повністю працездатні. Для з'ясування стану зв'язків маршрутизатори-сусіди досить часто обмінюються короткими повідомленнями HELLO.

Для розповсюдження по мережі даних про стан зв'язків маршрутизатори обмінюються повідомленнями іншого типу. Ці повідомлення називаються оголошеннями про зв'язки маршрутизатора (router links advertisement), або, точніше, про стан зв'язків. OSPF-маршрутизатори обмінюються не тільки своїми, але й чужими оголошеннями про зв'язки, отримуючи в кінці кінців інформацію про стан всіх зв'язків мережі. Ця інформація і утворює граф зв'язків мережі, який, природно, один і той же для всіх маршрутизаторів мережі.

Крім інформації про сусідів, маршрутизатор в своєму оголошенні перераховує IP-підмережі, з якими він пов'язаний безпосередньо, тому після отримання інформації про граф зв'язків мережі, обчислення маршруту до кожної мережі проводиться безпосередньо з цього графу за алгоритмом Дейкстри. Більш точно, маршрутизатор обчислює шлях не до конкретної мережі, а до маршрутизатора, до якого ця мережа підключена. Кожен маршрутизатор має унікальний ідентифікатор, який передається в оголошенні про стани зв'язків. Такий підхід дає можливість не витрачати IP-адреси на зв'язку типу "точка-точка" між маршрутизаторами, до яких не підключені робочі станції.

Маршрутизатор обчислює оптимальний маршрут до кожної адресованої мережі, але запам'ятовує тільки перший проміжний маршрутизатор з кожного маршруту. Таким чином, результатом обчислень оптимальних маршрутів є список рядків, в яких вказується номер мережі і ідентифікатор маршрутизатора, якому потрібно переслати пакет для цієї мережі. Зазначений список маршрутів і є маршрутною таблицею, але обчислений він на підставі повної інформації про граф зв'язків мережі, а не часткової інформації, як в протоколі RIP.

Описаний підхід призводить до результату, який не може бути досягнутий при використанні протоколу RIP або інших дистанційно-векторних алгоритмів. RIP припускає, що всі підмережі певної IP-мережі мають один і той же розмір, тобто, що всі вони можуть потенційно мати однакове число IP-сайтів, адреси яких не перекриваються. Більш того, класична реалізація RIP вимагає, щоб виділені лінії "точка-точка" мали IP-адресу, що призводить до додаткових витрат IP-адрес.

У OSPF такі вимоги відсутні: мережі можуть мати різне число хостів і можуть перекриватися. Під перекриттям розуміється наявність декількох маршрутів до однієї і тієї ж мережі. У цьому випадку адреса мережі в пакеті, що прийшов може співпасти з адресою мережі, що привласнена декільком портам.

Якщо адреса належить декільком підмережам в базі даних маршрутів, то маршрутизатор, що просуває пакет, використовує найбільш специфічний маршрут, тобто адресу підмережі, що має довшу маску.

Наприклад, якщо робоча група відгалужується від головної мережі, то вона має адресу головної мережі поряд з більш специфічним адресою, обумовленим маскою підмережі. При виборі маршруту до хоста в підмережі цієї робочої групи маршрутизатор знайде два шляхи, один для головної мережі і один для робочої групи. Так як останній більш специфічний, то він і буде обраний. Цей механізм є узагальненням поняття "маршрут за умовчанням", що використовується в багатьох мережах.

Використання підмереж з різною кількістю хостів є цілком природним. Наприклад, якщо в будівлі або кампусі на кожному поверсі є локальні мережі, і на деяких поверхах комп'ютерів більше, ніж на інших, то адміністратор може вибрати розміри підмереж, що відображають очікувані вимоги кожного поверху, а не відповідають розміру найбільшою підмережі.

В протоколі OSPF підмережі діляться на три категорії:

- "хост-мережа", що представляє собою під мережу з однієї адреси,
- "тупикова мережа", яка представляє собою під мережу, що підключена тільки до одного маршрутизатора,
- "транзитна мережа", яка представляє собою підмережу, що підключена до більш ніж до одного маршрутизатора .

Транзитна мережа є для протоколу OSPF особливим випадком. У транзитній мережі кілька маршрутизаторів є взаємно і одночасно досяжними. У широкомовних локальних мережах, таких як Ethernet або Token Ring, маршрутизатор може послати одне повідомлення, яке отримають всі його сусіди. Це зменшує навантаження на маршрутизатор, коли він посилає повідомлення для визначення існування зв'язку або оновлені оголошення про сусідів. Однак, якщо кожен маршрутизатор буде перераховувати всіх своїх сусідів у своїх оголошеннях про сусідів, то оголошення займуть багато місця в пам'яті маршрутизатора. При визначенні шляху за адресами транзитної підмережі може виявитися багато надлишкових маршрутів до різних маршрутизаторів. На обчислення, перевірку і відбраковування цих маршрутів піде багато часу.

Коли маршрутизатор починає працювати в перший раз (тобто інсталюється), він намагається синхронізувати свою базу даних зі всіма маршрутизаторами транзитної локальної мережі, які за визначенням мають ідентичні бази даних. Для спрощення та оптимізації цього процесу в протоколі OSPF використовується поняття "виділеного" маршрутизатора, який виконує дві функції.

По-перше, виділений маршрутизатор і його резервний "напарник" є єдиними маршрутизаторами, з якими новий маршрутизатор буде синхронізувати свою базу. Синхронізувавши базу з виділеним маршрутизатором, новий маршрутизатор буде синхронізований з усіма маршрутизаторами даної локальної мережі.

По-друге, виділений маршрутизатор робить оголошення про мережеві зв'язки, перераховуючи своїх сусідів по підмережі. Інші маршрутизатори просто оголошують про свій зв'язок з виділеним маршрутизатором. Це робить оголошення про зв'язки (яких багато) більш короткими, розміром з оголошення про зв'язки окремої мережі.

Для початку роботи маршрутизатора OSPF потрібен мінімум інформації - IP-конфігурація (IP-адреси і маски підмереж), деяка інформація за замовчуванням (default) і команда на включення. Для багатьох мереж інформація за замовчуванням дуже схожа. У той же час протокол OSPF передбачає високий ступінь програмованості.

Інтерфейс OSPF (порт маршрутизатора, що підтримує протокол OSPF) є узагальненням підмережі IP. Подібно підмережі IP, інтерфейс OSPF має IP-адресу і маску підмережі. Якщо один порт OSPF підтримує більше, ніж одну підмережу, протокол OSPF розглядає ці підмережі так, як якщо б вони були на різних фізичних інтерфейсах, і обчислює маршрути відповідно.

Інтерфейси, до яких підключені локальні мережі, називаються широкомовними (broadcast) інтерфейсами, так як вони можуть використовувати широкомовні можливості локальних мереж для обміну сигнальної інформацією між маршрутизаторами. Інтерфейси, до яких підключені глобальні мережі, не підтримують широкомовлення, але забезпечують доступ до багатьох вузлів через одну точку входу, наприклад мережі X.25 або frame relay, називаються нешироковомовними інтерфейсами з множинним доступом або NBMA (non-broadcast multi-access). Вони розглядаються аналогічно широкомовним інтерфейсам за винятком того, що широкомовна розсилка емулюється шляхом посилки повідомлення кожному сусідові. Так як виявлення сусідів не є автоматичним, як в широкомовних мережах, NBMA-сусіди повинні здаватися при конфігуруванні вручну. Як на широкомовних, так і на NBMA-інтерфейсах можуть бути задані пріоритети

маршрутизаторів для того, щоб вони могли вибрати виділений маршрутизатор.

Інтерфейси «точка-точка», на подобі PPP, дещо відрізняються від традиційної IP-моделі. Хоча вони і можуть мати IP-адреси і підмаски, але необхідності в цьому немає.

У простих мережах досить визначити, що пункт призначення досяжний і знайти маршрут, який буде задовільним. У складних мережах зазвичай є кілька можливих маршрутів. Іноді хотілося б мати можливості щодо встановлення додаткових критеріїв для вибору шляху: наприклад, найменша затримка, максимальна пропускна здатність або найменша вартість (у мережах з оплатою за пакет). З цих причин протокол OSPF дозволяє адміністратору призначати кожному інтерфейсу певне число, зване метрикою, щоб надати потрібний вплив на вибір маршруту.

Число, яке використовується в якості метрики шляху, може бути призначено довільним чином за бажанням адміністратора. Але за умовчанням як метрика використовується час передачі біта в 10-ти наносекундних одиницях (10 Мб/с Ethernet призначається значення 10, а лінії 56 Кб/с - число 1785). Обчислюється протоколом OSPF метрика шляху є сумою метрик всіх прохідних в дорозі зв'язків; це дуже груба оцінка затримки шляху. Якщо маршрутизатор виявляє більше, ніж один шлях до віддаленої підмережі, то він використовує шлях з найменшою вартістю шляху.

У протоколі OSPF використовується кілька часових параметрів, і серед них найбільш важливими є інтервал повідомлення HELLO і інтервал відмови маршрутизатора (router dead interval).

HELLO - це повідомлення, яким обмінюються сусідні, тобто безпосередньо пов'язані маршрутизатори підмережі, з метою встановити стан лінії зв'язку і стан маршрутизатора-сусіда. У повідомленні HELLO маршрутизатор передає свої робочі параметри і говорить про те, кого він розглядає як своїх найближчих сусідів. Маршрутизатори з різними робочими

параметрами ігнорують повідомлення HELLO один одного, тому невірно сконфігуровані маршрутизатори не будуть впливати на роботу мережі. Кожен маршрутизатор шле повідомлення HELLO кожному своєму сусідові по крайній мірі один раз протягом інтервалу HELLO. Якщо інтервал відмови маршрутизатора закінчується без отримання повідомлення HELLO від сусіда, то вважається, що сусід непрацездатний, і поширюється нове оголошення про мережеві зв'язки, щоб в мережі стався перерахунок маршрутів.

Завдання на роботу

1. У відповідності з варіантом завдання побудувати мережу підприємства з використанням засобів маршрутизації потоків даних, забезпечивши резервування основних каналів зв’язку.
2. Виконати розподіл IP-адресів між вузлами побудованої мережі.
3. Для отриманої моделі мережі задати необхідні типи потоків даних між робочими станціями і серверами і виконати імітаційне моделювання роботи мережі.
4. Проаналізувати середнє завантаження мережевого комунікаційного обладнання і середовища передачі даних, порівняти інтенсивності потоків службових даних при використанні різних протоколів обміну маршрутною інформацією. Вказати ділянки мережі, Указать участки сети, вразливі до перенавантажень, і визначити засоби підвищення надійності функціонування мережі.

Таблиця 5.1. Варіанти завдань.

№ варіанту	Тип інфраструктури	Тип трафіку
1	1	2
2	2	3
3	3	4
4	4	1
5	5	3

6	6	4
7	7	1
8	8	2
9	1	4
10	2	1
11	3	2
12	8	3
13	5	1
14	6	2
15	7	3

Таблиця 5.2. Тип інфраструктури.

№ варіанту	**Кількість підмереж**	**Кількість вузлів в підмережі**	**Надані адреси**
1	4	60, 40, 30, 30	192.168.11.0
2	5	100, 100, 50, 50, 50	172.22.0.0
3	6	12, 14, 30, 60, 60, 60	192.168.13.0
4	4	60, 60, 50, 50	172.24.0.0
5	5	30, 30, 60, 60, 60	192.168.15.0
6	4	30, 30, 120, 160	172.26.0.0
7	4	30, 30, 60, 120	192.168.17.0
8	6	30, 30, 60, 60, 60, 120	172.28.0.0

Таблиця 5.3. Тип модельованого трафіку.

№ варіанту	Кількість файлових серверів	Кількість HTTP-серверів	Кількість FTP-серверів	Кількість серверів баз даних
1	3	1	2	2
2	3	2	1	2
3	2	1	2	3
4	2	2	1	3

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

Правила розподілу адрес в мережах IP.

Класифікація IP-адрес, поняття маски підмережі.

Використання нерівних масок підмереж.

Задача маршрутизації, способи маршрутизації.

Протоколи маршрутизації стека TCP/IP

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Буров Є. Комп'ютерні мережі – Л.: БаК, 1999.
2. Кулаков Ю.А., Омелянский С. В. Компьютерные сети. Выбор, установка, использование и администрирование – К.: Юниор, 1999.
3. Кульгин М. Технологии корпоративных сетей – СПб.: Питер, 2000.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы – СПб.: Питер, 1999.
5. CISCO Internetworking technology overview – Cisco, 1999.

Комп’ютерний практикум № 6

АДРЕСАЦІЯ І МАРШРУТИЗАЦІЯ В МЕРЕЖАХ TCP/IP

Мета роботи: практично засвоїти роботу з утилітами TCP/IP, визначити налаштування для підключення до локальної мережі і до мережі Internet з використанням утиліти ping, дослідити топології фрагментів мережі Internet з використанням утиліти tracert.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Типи адресів: фізична(MAC-адреса), мережева(IP-адреса) і символьна (DNS-ім'я)

Кожний комп'ютер в мережі TCP/IP має адреси трьох рівнів:

Локальна адресу вузла, яка визначається технологією, за допомогою якої побудована окрема мережа, у яку входить даний вузол. Для вузлів, що входять в локальні мережі, це MAC-адреса мережного адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками обладнання 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.

- IP-адреса, що складається з 4 байт, наприклад, 109.26.17.100. Ця адреса використовується на мережному рівні. Вона призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі й номера вузла. 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. Зазвичай провайдери послуг Internet одержують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Розподіл IP-адреси на поле номера мережі і номери вузла - гнучкі, і границя між цими полями може встановлюватися досить довільно. Вузол може входити в кілька IP-мереж. У цьому випадку вузол повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережне з'єднання.
- Символьний ідентифікатор-ім'я, наприклад, SERV1.IBM.COM. Ця

адреса призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домену. Така адреса, іменована також DNS-ім'ям, використовується на прикладному рівні, наприклад, в протоколах FTP або telnet.

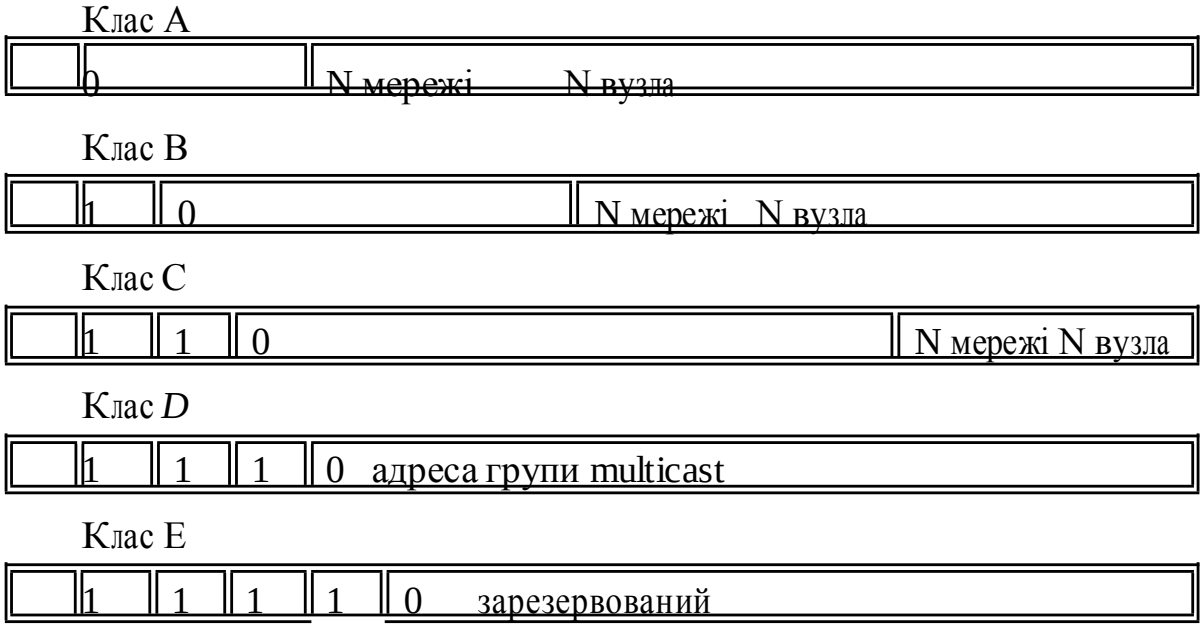
Три основні класи IP-адрес

IP-адреса має довжину 4 байти і звичайно записується у вигляді чотирьох чисел, що представляють значення кожного байту в десятковій формі, і розділені точками, наприклад:

128.10.2.30 – традиційна десяткова форма представлення адреси,

10000000 00001010 00000010 00011110 – двійкова форма представлення цієї ж адреси.

Далі показана структура IP-адреси в залежності від класу мережі



Адреса складається з двох логічних частин – номера мережі і номера вузла в мережі. Яка частина адреси відноситься до номеру мережі, а яка до номеру вузла, визначається значеннями перших бітів адреси:

- Якщо адреса починається з 0, то мережу відносять до класу A, і номер мережі займає один байт, інші 3 байти інтерпретуються як номер вузла в мережі.

Мережі класу А мають номери в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей, про що буде сказано нижче.) В мережах класу А кількість вузлів повинна бути більше 2^{16}, але не перевищувати 2^{24}.

- Якщо перші два біти адреси рівні 10, то мережа відноситься до класу В і є мережею середніх розмірів з числом вузлів 2^8 - 2^{16}. У мережах класу В під адресу мережі і під адресу вузла відводиться по 16 біт, тобто по 2 байти.
- Якщо адреса починається з послідовності 110, то це мережа класу С з кількістю вузлів не більше 2^8. Під адресу мережі відводиться 24 біти, а під адресу вузла – 8 біт.
- Якщо адреса починається з послідовності 1110, то він є адресою класу D і позначає особливу, групову адресу - multicast. Якщо в пакеті як адреса призначення вказана адреса класу D, то такий пакет повинен отримати всі вузли, яким визначено цю адресу.
- Якщо адреса починається з послідовності 11110, то це адреса класу Е, вона зарезервована для майбутніх застосувань.

В таблиці наведені діапазони номерів мереж, що відповідають кожному класу мереж.

Клас	Найменша адреса	Найбільша адреса
A	01.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Відображення символьних адрес на IP-адреси: служба DNS

DNS (Domain Name System) - це розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів у мережі Internet. Служба DNS

призначена для автоматичного пошуку IP-адреси за відомим символьним іменем вузла. Специфікація DNS визначається стандартами RFC 1034 і 1035. DNS вимагає статичної конфігурації своїх таблиць, що відображають імена комп'ютерів в IP-адресу.

Протокол DNS є службовим протоколом прикладного рівня. Цей протокол несиметричний – у ньому визначені DNS-сервери і DNS-клієнти. DNS-сервери зберігають частину розподіленої бази даних про відповідність символьних імен і IP-адрес. Ця база даних розподілена по адміністративних доменах мережі Internet. Клієнти сервера DNS знають IP-адреси сервера DNS свого адміністративного домену і по протоколу IP передають запит, у якому повідомляють символьне ім’я і просять повернути відповідну йому IP-адресу.

Якщо дані про запрошену відповідність зберігаються в базі даного DNS-сервера, то він відразу посилає відповідь клієнту, якщо ж ні - то він надсилає запит DNS-сервера іншого домену, який може сам обробити запит, або передати його іншому DNS-серверу. Всі DNS-сервери з'єднані ієрархічно, відповідно до ієрархії доменів мережі Internet. Клієнт опитує ці сервери імен, поки не знайде потрібні відображення. Цей процес прискорюється через те, що сервери імен постійно кешують інформацію, що надається за запитами. Клієнтські комп'ютери можуть використовувати у своїй роботі IP-адреси декількох DNS-серверів, для підвищення надійності своєї роботи.

База даних DNS має структуру дерева, іменованого доменним простором імен, у якому кожний домен (вузол дерева) має ім'я і може містити піддомени. Ім'я домену ідентифікує його положення в цій базі даних стосовно батьківського домену, причому крапки в імені відокремлюють частини, відповідні вузлам домену.

Корінь бази даних DNS управляється центром Internet Network Information Center. Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Імена цих доменів повинні слідувати міжнародному

стандарту ISO 3166. Для позначення країн використовуються трьохбуквені і двохбуквенні абревіатури, а для різних типів організацій використовуються наступні абревіатури:

- com – комерційні організації (наприклад, Microsoft.com)
- edu – освітні (наприклад, mit.edu)
- gov – урядові організації (наприклад, nsf.gov)
- org – некомерційні організації (наприклад, fidonet.org)
- net – організації, що підтримують мережі (наприклад, nsf.net)

Кожен домен DNS адмініструється окремою організацією, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Кожен домен має унікальне ім'я, а кожен з піддоменів має унікальне ім'я усередині свого домена. Ім'я домену може містити до 63 символів. Кожен хост в мережі Internet однозначно визначається своїм повним доменним ім'ям (*fully qualified domain name, FQDN*), яке включає імена всіх доменів по напрямку від хоста до кореня. Приклад повного DNS-імені: server.aics.acs.cctpu.edu.ru

Автоматизація процесу призначення IP-адрес вузлам мережі – протокол DHCP

IP-адреси можуть призначатися адміністратором мережі вручну. Це являє для адміністратора тяжку процедуру. Ситуація ускладнюється ще тим, що багато користувачів не володіють достатніми знаннями для того, щоб конфігурувати свої комп'ютери для роботи в інтермережі і тому повинні покладатися на адміністраторів.

Протокол *Dynamic Host Configuration Protocol (DHCP)* був розроблений для того, щоб звільнити адміністратора від цих проблем. Основним призначенням DHCP є динамічне призначення IP-адресів. Однак, крім динамічного, DHCP може підтримувати і більш прості способи ручного й автоматичного статичного призначення адрес.

У ручній процедурі призначення адрес активну участь приймає адміністратор, який надає DHCP-серверу інформацію про відповідність IP-адрес фізичним адресами або іншим ідентифікаторам клієнтів. Ці адреси повідомляються клієнтам у відповідь на їх запити до DHCP-сервера.

При автоматичному статичному способі DHCP-сервер присвоює IP-адресу (і, можливо, інші параметри конфігурації клієнта) з пулу (набору) наявних IP-адрес без втручання оператора. Межі пулу адрес, що призначаються, задає адміністратор при конфігуруванні DHCP-сервера. Між ідентифікатором клієнта і його IP-адресою, як і раніше, як при ручному призначенні, існує постійна відповідність. Воно встановлюється в момент первинного призначення сервером DHCP IP-адреси клієнта. При всіх наступних запитах сервер повертає ту ж саму IP-адресу.

При динамічному розподілі адрес DHCP-сервер видає адресу клієнту на обмежений час, що дає можливість згодом повторно використовувати IP-адреси іншими комп'ютерами. Динамічне розділення адрес дозволяє будувати IP-мережу, кількість вузлів у якої набагато перевищує кількість наявних у розпорядженні адміністратора IP-адрес.

Системні утиліти мережевої діагностики

В склад TCP/IP входять діагностичні утиліти, що призначені для перевірки конфігурації стеку і тестування мережевого з’єднання.

Утиліта	Використання
arp	Виводить для перегляду і зміни таблицю трансляції адресів, що використовуються протоколом дозволу адресів ARP (Address Resolution Protocol – визначає локальну адресу по
hostname	Виводить ім’я локального хосту. Використовується без параметрів.
ipconfig	Виводить значення для поточної конфігурації стеку TCP/IP: IP-адресу, маску під мережі, адресу шлюзу по замовчуванню, адресу WINS (Windows Internet Naming Service) і DNS

nbtstat	Виводить статистику і поточну інформацію по NetBIOS, установленому поверх TCP/IP. Використовується для перевірки стану NetBIOS.
netstat	Виводить статистику і поточну інформацію по з'єднанню TCP/IP.
nslookup	Виконує перевірку записів і доменних псевдонімів хостів, доменних сервісів хостів, а також інформації операційної системи, шляхом запитів до серверів DNS.
ping	Виконує перевірку правильності конфігурування TCP/IP і перевірку зв'язку з віддаленим хостом.
route	Модифікує таблиці маршрутизації IP. Відображає вміст таблиці, добавляє і видаляє маршрути IP.
tracert	Виконує перевірку маршруту до віддаленого комп'ютера шляхом відправки ехо-пакетів протоколу ICMP (Internet Control Message Protocol). Виводить маршрут проходження пакетів на віддалений комп'ютер.

Утиліта ipconfig

При усуненні несправностей і проблем в мережі TCP/IP слід спочатку перевірити правильність конфігурації TCP/IP. Для цього використовується утиліта ipconfig.

Ця команда корисна на комп'ютерах, що працюють з DHCP (Dynamic Host Configuration Protocol), так як дає користувачам можливість визначити, яка конфігурація мережі TCP/IP і які величини були встановлені з допомогою DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметри:

all видає весь список параметрів. Без цього ключа відображається тільки IP-адреса, маска і шлюз по замовчуванню;

renew[adapter] обновляє параметри конфігурації DHCP для вказаного мережевого адаптера;

release[adapter] звільняє виділену DHCP IP-адресу; adapter – ім'я мережевого адаптера;

displaydns виводить інформацію про вміст локального кешу клієнта

DNS, що використовується для дозволу доменних імен.

Таким чином, утиліта ipconfig дозволяє виявнити, чи ініціалізована конфігурація і чи не дублюються IP-адреси:

- якщо конфігурація ініціалізована, то появляється IP-адреса, маска, шлюз;
- якщо IP-адреси дублюються, то маска мережі буде 0.0.0.0;

якщо при використанні DHCP комп'ютер не зміг отримати IP-адресу, то вона буде рівна 0.0.0.0 .

Наприклад, при виконанні команди ipconfig ми можемо отримати наступні результати.

>ipconfig

Налаштування протоколу *IP* для *Windows*

Підключення по локальній мережі *2 – Ethernet* адаптер:

DNS-суфікс цього підключення . . *: voliacable.com IP*-адреса . . *: 82.144.223.226*

Маска підмережі . . . . . *: 255.255.252.0*

Основний шлюз . . . . . *: 82.144.220.1*

Утиліта ping

Утиліта ping (Packet Internet Groper) є одним з головних засобів, що використовуються для налагодження мереж, і служить для примусового виклику відповіді конкретної машини. Вона дозволяє перевіряти роботу програм TCP/IP на віддалених машинах, адреси пристроїв в локальній мережі, адресу і маршрут для віддаленого мережевого пристрою. У виконанні команди ping беруть участь система маршрутизації, схеми дозволу адрес і мережеві шлюзи. Це утиліта низького рівня, яка не вимагає наявності серверних процесів на перевіреній машині, тому успішний результат при проходженні запиту зовсім не означає, що виконуються якісь сервісні програми високого рівня, а говорить про те, що

мережа знаходиться в робочому стані, живлення машини, що перевіряється, включене, і машина не відмовила ("не висить").

У Windows утиліта ping є в комплекті поставки і являє собою програму, що запускається з командного рядка.

Запити утиліти ping передаються по протоколу ICMP (Internet Control Message Protocol). Отримавши такий запит, програмне забезпечення, що реалізує протокол IP у адресата, посилає ехо-відповідь. Якщо машина, що перевіряється, в момент отримання запиту була завантажена більш пріоритетною роботою (наприклад, обробкою і перенаправленням великого обсягу трафіку), то відповідь буде відправлена не відразу, а як тільки закінчиться виконання більш пріоритетного завдання. Тому слід врахувати, що затримка, розрахована утилітою ping, викликана не тільки пропускною здатністю каналу передачі даних до машини, що перевіряється, а й завантаженістю цієї машини.

Ехо-запити відправляються задану кількість разів (ключ -n). По замовчуванню, передається чотири запити, після чого виводяться статистичні дані.

Зверніть увагу: оскільки з утиліти ping починається хакерська атака, деякі сервери з метою безпеки можуть не відправляти ехо-відповіді (наприклад, www.microsoft.com). Не чекайте марно, введіть команду переривання (CTRL+C).

Формат команди: ping [-t][-a][-n][-l][-f][-i TTL][-v TOS]

[-r][][ім'я машини][[-j списокВузлів]|[-k списокВузлів]][-w]

Параметри утиліти ping

Ключі	Функції
-t	Відправка пакетів на вказаний вузол до команди
-a	Визначення імені вузла по IP-адресі
-n	Кількість запитів що відправляються
-l	Розмір буферу відправки
-f	Установка прапору, що забороняє фрагментацію пакету
-i TTL	Задання часу життя пакету (поле "Time To Live")

На практиці більшість опцій в форматі команди можна опустити, тоді в

командному рядку може бути: ping ім'я вузла (для за циклювання виводу інформації про з'єднання використовується опція –t; для виводу інформації n разів використовується опція –n кількість разів).

Наприклад, при виконанні команди ping www.google.com.ua ми отримаємо наступні результати

ping google.com.ua

Обмін пакетами з www.google.com.ua [216.239.39.99] по 32 байти:

Відповідь від 216.239.39.99: число байт=32 час=154мс TTL=236
Відповідь від 216.239.39.99: число байт=32 час=156мс TTL=236
Відповідь від 216.239.39.99: число байт=32 час=156мс TTL=236
Відповідь від 216.239.39.99: число байт=32 час=171мс TTL=236

Статистика *Ping для 216.239.39.99:*
Пакетів: відправлено = 4, отримано = 4, втрачено = 0 (0% втрат),
Приблизний час прийому-передачі в мс:
Мінімальний = 154 мсек, Максимальний = 171 мсек, Середній = 159 мсек

ping –n 20 peak.mountin.net

Обмін пакетами *з peak.mountin.net [207.227.119.2] по 32 байт:*
Перевищено інтервал очікування для запиту.
Відповідь від 207.227.119.2: число байт=32 час=734мс TTL=231
Відповідь від 207.227.119.2: число байт=32 час=719мс TTL=231
Відповідь від 207.227.119.2: число байт=32 час=688мс TTL=231
Перевищено інтервал очікування для запиту.
Відповідь від 207.227.119.2: число байт=32 час=719мс TTL=231
Відповідь від 207.227.119.2: число байт=32 час=1015мс TTL=231
Перевищено інтервал очікування для запиту.

Відповідь від 207.227.119.2: число байт=32 час=703мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=688мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=782мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=688мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=688мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=688мс TTL=231

Перевищено інтервал очікування для запиту.

Відповідь від 207.227.119.2: число байт=32 час=687мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=735мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=672мс TTL=231

Відповідь від 207.227.119.2: число байт=32 час=704мс TTL=231

Статистика *Ping для 207.227.119.2:*

Пакетів: відправлено = 20, отримано = 16, втрачено = 4 (20% втрат),

Приблизний час прийому-передачі в мс:

Мінімальний = 672 мсек, Максимальний = 1015 мсек, Середній = 580 мсек

Приклад визначення імені вузла по IP-адресі

ping –a 194.67.57.26

Обмін пакетами з mail.ru [194.67.57.26] по 32 байти: …

Утиліта tracert

Утиліта tracert дозволяє виявляти послідовність маршрутизаторів, через які проходить IP-пакет па шляху до пункту свого призначення.

Формат команди: tracert ім'я_машини.

Ім'я машини може бути іменем вузла або IP-адресою машини. Вихідна інформація представляє собою список машин, починаючи з першого шлюзу і закінчуючи пунктом призначення.

Наприклад, при виконанні команди tracert www.google.com.ua ми отримаємо наступні результати

>tracert www.google.com.ua

Трасування маршруту до *www.l.google.com [66.249.93.104]*
з максимальною кількістю стрибків 30:

1 *45 ms 31 ms 31 ms c7-2.sub-5.volia.net [82.144.220.1]*
2 *15 ms 15 ms 31 ms gig0-1-5.diamond.volia.net [82.144.192.225]*
3 *187 ms 46 ms 31 ms datagroup-gw.volia.net [80.91.180.69]*
4 *77 ms 93 ms 93 ms peer-sprint-r.newline.net.ua [80.91.180.6]*
5 *106 ms 77 ms 61 ms sl-bb20-fra-6-1.sprintlink.net [217.147.96.68]*
6 *77 ms 77 ms 62 ms sl-bb21-par-4-0.sprintlink.net [213.206.129.149]*
7 *187 ms 77 ms 62 ms sle-franc1-3-0.sprintlink.net [213.206.131.42]*
8 *77 ms 77 ms 93 ms 193.251.128.117*
9 *124 ms 93 ms 93 ms 193.251.132.73*
10 *93 ms 93 ms 109 ms 193.251.249.62*
11 *93 ms 108 ms77 ms 216.239.46.48*
12 *93 ms 124 ms 109 ms 64.233.175.248*
13 *124 ms 93 ms 93 ms 216.239.43.89*
14 *109 ms 109 ms 109 ms 66.249.94.54*
15 *109 ms 93 ms 109 ms 66.249.94.50*
16 *187 ms 109 ms93 ms 66.249.93.104*

Трасування завершено.

Пакети надсилаються по три на кожен вузол. Для кожного пакета на екрані відображається величина інтервалу часу між відправленням пакета й одержанням відповіді. Символ * означає, що відповідь на цей пакет не був

отриманий. Якщо вузол не відповідає, то при перевищенні інтервалу очікування відповіді видається повідомлення «Перевищений інтервал очікування для запиту». Інтервал очікування відповіді може бути змінений за допомогою опції -w команди tracert.

Примітка:

Деякі маршрутизатори просто мовчки знищують пакети з вичерпаним часом очікування і не будуть видні утиліті tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] ім'я_цільового_хосту

Параметри:

-d вказує, що не потрібно розпізнавати адреси для імен хостів;

-h maximum_hopsвказує максимальну кількість хопів для того, щоб шукати ціль;

-j host-list вказує нежорстку статичну маршрутизацію у відповідності host-list;

-w timeout вказує, що потрібно очікувати відповідь на кожний ехо-пакет задану кількість мсек.

Команда tracert працює шляхом установки поля часу життя (числа переходів) вихідного пакета таким чином, щоб цей час минав до досягнення пакетом пункту призначення. Коли час життя закінчиться, поточний шлюз відправить повідомлення про помилку на машину-джерело. Кожне прирощення поля часу життя дозволяє пакету пройти на один маршрутизатор далі.

Примітка:

Для виводу інформації в файл використовуйте символ перенаправлення потоку виводу «>». Даний символ справедливий і для утиліт ping і tracert.

Приклад:

tracert 195.208.164.1 > tracert.txt

Звіт про трасування маршруту до вказаного вузла буде поміщений в файл tracert.txt.

Утиліта ARP.

Основна задача протоколу ARP - трансляція IP-адрес у відповідні локальні адреси. Для цього ARP-протокол використовує інформацію з ARP-таблиці (ARP-кешу). Якщо необхідний запис в таблиці не знайдений, то протокол ARP відправляє широкомовний запит до всіх комп'ютерів локальної підмережі, намагаючись знайти власника даної IP-адреси. У кеші можуть міститися два типи записів: статичні і динамічні. Статичні записи вводяться вручну і зберігаються в кеші постійно. Динамічні записи поміщаються в кеш в результаті виконання широкомовних запитів. Для них існує поняття часу життя. Якщо протягом певного часу (за замовчуванням 2 хв.) Запис не був затребуваний, то він видаляється з кешу.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметри:

-s занесення в кеш статичних записів;

-d видалення з кешу запису для визначеної IP-адреси;

-a перегляд вмісту кешу для всіх мережевих адаптерів локального комп’ютера;

inet_addr - IP-адреса;

eth_addr - MAC-адреса.

Утиліта netstat.

Утиліта netstat дозволяє отримати статичну інформацію по деяким з протоколів стека (TCP, UDP, IP, ICMP), а також виводить відомості про поточні мережеві з'єднання. Особливо вона корисна на брандмауерах, з її допомогою можна виявити порушення безпеки периметра мережі.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметри:

-a виводить список всіх мережевих з'єднань і портів локального комп'ютера, що прослуховуються;

-e виводить статистику для Ethernet-інтерфейсів (наприклад, кількість отриманих і відправлених байтів);

-n виводить інформацію по всіх поточних з'єднаннях (наприклад, TCP) для всіх мережевих інтерфейсів локального комп'ютера. Для кожного з'єднання виводиться інформація про IP-адреси локального і віддаленого інтерфейсів разом з номерами використовуваних портів;

-s виводить статичну інформацію для протоколів UDP, TCP, ICMP, IP.

Ключ «/more» дозволяє переглянути інформацію посторінково;

-r виводить вміст таблиці маршрутизації.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

1. Вивчіть методичні вказівки до лабораторної роботи.

2. Виконайте вправи.

3. Оформіть звіт по лабораторній роботі, описавши виконання вправ і давши короткі відповіді на контрольні запитання.

4. Виведіть на екран довідкову інформацію по утилітам ipconfig, ping, tracert, hostname. Для цього в командному рядку введіть ім'я утиліти без параметрів або з /?. Вивчіть ключі, що використовуються при запуску утиліт.

5. Виведіть на екран ім'я локального хоста за допомогою команди hostname.

6. Перевірте конфігурацію TCP/IP за допомогою утиліти ipconfig. Заповніть таблицю:

Ім’я хосту	Ws21
IP-адреса	192.168.12.21
Маска підмережі	255.255.255.0
Основний шлюз	192.168.12.1
Чи використовується DHCP (адреса DHCP-сервера)	No
Опис адаптера	PCI FAST ETHERNET realtek rtl8139
Фізична адреса мережевого адаптера	00-c0-26-2b-66-fe
Адреса DNS-сервера	No
Адреса WINS-сервера	No

7. Перевірте правильність установки і конфігурування TCP / IP на локальному комп'ютері. Перевірте, чи правильно доданий в мережу локальний комп'ютер і чи не дублюється IP-адреса.

8. Перевірте функціонування шлюзу, пославши 5 exo-пакетів довжиною 64 байта.

9. За допомогою команди ping перевірте перераховані нижче адреси і для кожного з них зазначте час відгуку. Спробуйте збільшити час відгуку.

a) www.nau.edu.ua

b) www.rambler.ru

c) www.mit.edu Задайте різну довжину пакетів, що відсилаються. Запишіть часи проходження пакетів для всіх випадків.

10. За допомогою команди tracert перевірте для перерахованих нижче адрес, через які проміжні вузли йде сигнал. Позначте їх:

a) www.nau.edu.ua

b) www.rambler.ru

11. За допомогою утиліти arp перегляньте ARP-таблицю локального комп'ютера.

12. Виконайте команду tracert www.nau.edu.ua. Запишіть адреси та імена проміжних вузлів, через які здійснюється трасування маршруту.

13. Виконайте команду tracert www.rambler.ru > c: \ temp \ mytrace.txt

14. Проаналізуйте отриманий файл mytrace.txt. Оцініть часи затримок пакетів трасування в дорозі.

15. Виконайте команду tracert www.mit.edu > c: \ temp \ mytrace.txt

16. Проаналізуйте отриманий файл і визначте вузли, пов'язані між собою супутниковим каналом.

17. Виконайте команду tracert і ping до Мельбурнського (www.mbs.unimelb.edu.au), Токійського (www.tufs.ac.jp) і Владивостоцького (www.vvsu.ru) університетів. Порівняйте часи доступу.

18. Викличте браузер Internet Explorer (подвійним клацанням миші на значку на робочому столі)

19. В поле адреси (Uniform Resource Location - URL) наберіть NOC.CARAVAN.RU. Це сайт російського сервера, що виконує деякі функції мережевого операційного центру (Network Operation Center - NOC).

20. Знайдіть на цьому сайті в розділі Caravan Looking Glass. операції Ping і Traceroute. Тепер ви можете зробити трасування маршруту з Інтернету до вашого власного комп'ютера і до будь-якого комп'ютера мережі Інтернет. Визначте, як перетворено IP-адресу вашого комп'ютера для роботи в мережі Інтернет. Визначте, з яким доменним ім'ям представлений ваш комп'ютер в мережі Інтернет.

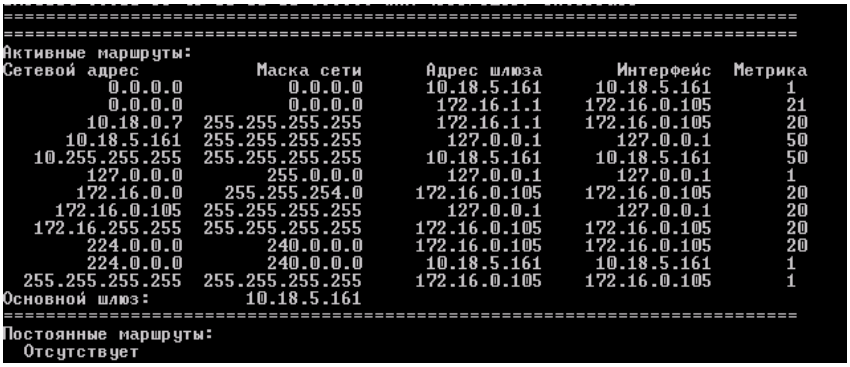
21. Набравши у вікні URL браузера адресу WWW.SIRENA.NET вийдіть на інший сервер, що виконує функції, аналогічні NOC.CARAVAN.RU

22. Виконайте операції трасування вашого комп'ютера з цього сайту.

23. Визначте вузли, пов'язані супутниковим каналом.

24. Виконайте команду route для визначення маршрутів, за якими пакети від вашого комп'ютера доставляються на наступні вузли мережі. Наприклад при виконанні команди route print ми можемо отримати такі результати.

>route print



```
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0     10.18.5.161     10.18.5.161       1
          0.0.0.0          0.0.0.0      172.16.1.1    172.16.0.105      21
       10.18.0.7  255.255.255.255      172.16.1.1    172.16.0.105      20
     10.18.5.161  255.255.255.255       127.0.0.1       127.0.0.1      50
  10.255.255.255  255.255.255.255     10.18.5.161     10.18.5.161      50
       127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1       1
      172.16.0.0    255.255.254.0     172.16.0.105    172.16.0.105      20
    172.16.0.105  255.255.255.255       127.0.0.1       127.0.0.1      20
  172.16.255.255  255.255.255.255     172.16.0.105    172.16.0.105      20
       224.0.0.0        240.0.0.0     172.16.0.105    172.16.0.105      20
       224.0.0.0        240.0.0.0     10.18.5.161     10.18.5.161       1
 255.255.255.255  255.255.255.255     172.16.0.105    172.16.0.105      1
Основной шлюз:        10.18.5.161
===========================================================================
Постоянные маршруты:
  Отсутствует
```

25. За допомогою утиліти netstat виведіть перелік мережевих з'єднань і статистичну інформацію для протоколів UDP, TCP, ICMP, IP.

ПИТАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

1. Прочитайте довідковий матеріал про протокол DHCP (Dynamic Host Configuration Protocol)
2. Прочитайте довідковий матеріал про сервери служби імен Microsoft WINS (Windows Internet Naming Service).
3. Вивчіть ключі утиліт ping та tracert вашої операційної системи.
4. Проаналізуйте інші можливості серверів NOC.CARAVAN.RU і WW.SIRENA.NET
5. Прочитайте матеріал про всесвітню службу доменних імен та можливості утиліти nslookup.
6. Визначте адресу та доменне ім'я маршрутизатора, через який здійснюється ваш вихід в Інтернет і протрасуйте маршрут до нього командою tracert <маршрутизатор>

Комп'ютерний практикум № 7

ТЕХНОЛОГІЇ БЕЗДРОТОВИХ МЕРЕЖ. ФІЗИЧНИЙ РІВЕНЬ ПРОТОКОЛІВ IEEE 802.11

Мета роботи: познайомиться з протоколами і технологіями передачі даних в бездротових мережах на фізичному рівні, отримати навички вибору обладнання для побудови бездротової локальної обчислювальної мережі.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Сімейство стандартів IEEE 802.11

Стандарт IEEE 802.11, розробка якого була завершена в 1997 р., є базовим стандартом і визначає протоколи, необхідні для організації бездротових локальних мереж (Wireless Local Area Network, WLAN). Основні з них – протокол управління доступом до середовища MAC (Medium Access Control – нижній підрівень канального рівня) і протокол PHY передачі сигналів у фізичному середовищі. В якості останньої допускається використання радіохвиль і інфрачервоного випромінювання.

Стандартом IEEE 802.11 визначений єдиний підрівень MAC, що взаємодіє з трьома типами протоколів фізичного рівня, які відповідають різним технологіям передачі сигналів – по радіоканалах в діапазоні 2,4 ГГц з широкосмугового модуляцією з прямим розширенням спектра (Direct Sequence Spread Spectrum, DSSS) і перескоком частоти (FHSS), а також за допомогою інфрачервоного випромінювання. Специфікаціями стандарту передбачені два значення швидкості передачі даних – 1 і 2 Мбіт/с.

У порівнянні з дротяними локальними мережами Ethernet можливості підрівня MAC розширені за рахунок включення в нього ряду функцій, зазвичай, що виконуються протоколами більш високого рівня, зокрема, процедур фрагментації та ретрансляції пакетів . Це викликано прагненням підвищити ефективну пропускну здатність системи завдяки зниженню накладних витрат на повторну передачу пакетів.

Управління живленням

Для економії енергоресурсів мобільних робочих станцій, які використовуються в бездротових локальних мережах, стандартом IEEE 802.11 передбачено механізм перемикання станцій в так званий пасивний режим з мінімальним споживанням потужності.

Архітектура та компоненти мережі

В основу стандарту IEEE 802.11 покладена стільникова архітектура, причому мережа може складатися як з однієї, так і декількох осередків. Кожна сота управляється базовою станцією, званою точкою доступу (Access Point, AP), яка разом з розташованими в межах радіусу її дії робочими станціями користувачів утворює базову зону обслуговування (Basic Service Set, BSS) Точки доступу багатостільникової мережі взаємодіють між собою через розподільну систему (Distribution System, DS), що є еквівалентом магістрального сегменту кабельних локальних мереж. Вся інфраструктура, що включає точки доступу і розподільну систему утворює розширену зону обслуговування (Extended Service Set).

Стандартом передбачений також односотовий варіант бездротової мережі, який може бути реалізований і без точки доступу, при цьому частина її функцій виконуються безпосередньо робочими станціями.

Роумінг

Для забезпечення переходу мобільних робочих станцій із зони дії однієї точки доступу до іншої в багатостільникових системах передбачені спеціальні процедури сканування (активного і пасивного прослуховування ефіру) і приєднання (Association), однак суворих специфікацій по реалізації роумінгу стандарт IEEE 802.11 не передбачає.

Забезпечення безпеки

Для захисту WLAN стандартом IEEE 802.11 передбачено цілий комплекс заходів безпеки передачі даних під загальною назвою Wired Equivalent Privacy, WEP. Він включає засоби протидії несанкціонованому доступу до мережі (механізми і процедури аутентифікації), а також запобігання перехоплення інформації (шифрування).

Стандарт IEEE 802.11a

Є найбільш "широкосмуговим" з сімейства стандартів IEEE 802.11, передбачаючи швидкість передачі даних до 54 Мбіт/с (редакцією стандарту, затвердженою в 1999 р., визначено три обов'язкові швидкості – 6, 12 і 24 Мбіт/с і п'ять необов'язкових – 9, 18, 36, 48 і 54 Мбіт/с).

На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікаціями IEEE 802.11a передбачена робота в діапазоні 5 ГГц. В якості методу модуляції сигналу вибрано ортогональне частотне мультиплексування (OFDM). Найбільш істотна відмінність між цим методом і радіотехнологіями DSSS і FHSS полягає в тому, що OFDM припускає паралельну передачу корисного сигналу одночасно по декількох частотах діапазону, в той час як технології розширення спектру передають сигнали послідовно. В результаті підвищується пропускна здатність каналу і якість сигналу.

До недоліків IEEE 802.11a відноситься більш висока споживана потужність радіопередавачів для частот 5 ГГц, а так само менший радіус дії

(устаткування для 2,4 ГГц може працювати на відстані до 300м, а для 5 ГГц – близько 100м).

Стандарт IEEE 802.11b

Завдяки високій швидкості передачі даних (до 11 Мбіт/с), практично еквівалентної пропускної здатності звичайних дротяних локальних мереж Ethernet, а також орієнтації на "освоєний" діапазон 2,4 ГГц, цей стандарт завоював найбільшу популярність у виробників устаткування для бездротових мереж.

В остаточній редакції стандарт IEEE 802.11b, відомий, також, як Wi-Fi (Wireless Fidelity), був прийнятий в 1999р. В якості базової радіотехнології в ньому використовується метод DSSS з 8-розрядними послідовностями Уолша.

Оскільки обладнання, що працює на максимальній швидкості 11 Мбіт/с має менший радіус дії, ніж на більш низьких швидкостях, то стандартом 802.11b передбачене автоматичне зниження швидкості при погіршенні якості сигналу .

Як і у випадку базового стандарту IEEE 802.11, чіткі механізми роумінгу специфікаціями IEEE 802.11b не визначені.

Специфікація IEEE 802.11g

Специфікації IEEE 802.11g є розвиток стандарту 802.11b і дозволяють підвищити швидкість передачі даних в бездротових локальних мережах до 22 Мбіт/с (і вище) завдяки використанню більш ефективної модуляції сигналу. Одним з переваг стандарту є зворотна сумісність з IEEE 802.11b.

Фізичний рівень протоколу 802.11

Огляд протоколів сімейства 802.11b/g доцільно розпочато саме з протоколу 802.11, який, хоча вже й не зустрічається в чистому вигляді, в той же час є прабатьком всіх інших протоколів. У стандарті 802.11, як і у всіх інших стандартах даного сімейства, передбачено використання частотного діапазону

від 2400 до 2483,5 МГц, тобто частотний діапазон шириною 83,5 МГц, який розбитий на кілька частотних підканалів.

Технологія розширення спектру

В основі всіх бездротових протоколів сімейства 802.11 лежить технологія розширення спектру (Spread Spectrum, SS). Принцип даної технології в тому, що первинно вузькополосний (в сенсі ширини спектра) корисний інформаційний сигнал при передачі перетвориться таким чином, що його спектр виявляється значно ширше спектра первинного сигналу. Тобто спектр сигналу наче «розмазується» по частотному діапазону. Одночасно з розширенням спектра сигналу відбувається і перерозподіл спектральної енергетичної щільності сигналу – енергія сигналу також «розмазується» по спектру. В результаті максимальна потужність перетвореного сигналу виявляється значно нижче потужності вихідного сигналу. При цьому рівень корисного інформаційного сигналу може в буквальному сенсі порівнюватися з рівнем природного шуму. В результаті сигнал стає в якомусь сенсі «невидимим» – він просто губиться на рівні природного шуму.

Власне, саме в зміні спектральної енергетичної щільності сигналу і полягає ідея розширення спектра. Якщо підходити до проблеми передачі даних традиційним способом, тобто так, як це робиться в радіоефірі, де кожній радіостанції відводиться свій діапазон мовлення, то неминуче виникне проблема: в обмеженому радіодіапазоні, призначеному для спільного використання, неможливо «умістити» всіх бажаючих. Тому необхідно знайти такий спосіб передачі інформації, при якому користувачі могли б співіснувати в одному частотному діапазоні і при цьому не заважати один одному. Саме це завдання і вирішує технологія розширення спектра.

Існує декілька різних технологій розширення спектру в протоколах IEEE 802.11. Наприклад, використовується технологія розширення спектру методом прямої послідовності (DSSS).

Технологія DSSS

При потенційному кодуванні інформаційні біти – логічні нулі і одиниці – передаються прямокутними імпульсами напруги. Прямокутний імпульс тривалості T має спектр, ширина якого обернено пропорційна тривалості імпульсу. Тому чим менше тривалість інформаційного біта, тим більший спектр займає такий сигнал.

Для навмисного розширення спектра спочатку вузькополосного сигналу в технології DSSS в кожен інформаційний біт, що передається (логічний 0 або 1) в буквальному сенсі вбудовується послідовність так званих чіпів. Якщо інформаційні біти – логічні нулі або одиниці – при потенційному кодуванні інформації можна уявити у вигляді послідовності прямокутних імпульсів, то кожен окремий чіп – це теж прямокутний імпульс, але його тривалість в кілька разів менше тривалості інформаційного біта. Послідовність чіпів являє собою послідовність прямокутних імпульсів, тобто нулів і одиниць, однак ці нулі і одиниці не є інформаційними. Оскільки тривалість одного чіпа в n разів менше тривалості інформаційного біта, то і ширина спектра перетвореного сигналу буде в n-разів більше ширини спектра первинного сигналу. При цьому і амплітуда сигналу зменшиться в n раз.

Чипові послідовності, що вбудовуються в інформаційні біти, називають шумоподібними кодами (PN-послідовності), що підкреслює ту обставину, що результуючий сигнал стає шумоподібним і його важко відрізнити від природного шуму.

Як розширити спектр сигналу і зробити його не відрізнятись від природного шуму, зрозуміло. Для цього, в принципі, можна скористатися довільною (випадковою) чіповою послідовністю. Однак, виникає питання: а як такий сигнал приймати? Адже якщо він стає шумоподібним, то виділити з нього корисний інформаційний сигнал не так то просто, якщо взагалі можливо. Виявляється, можливо, але для цього потрібно відповідним чином підібрати

чіпову послідовність. Використовувані для розширення спектру сигналу чіпові послідовності повинні відповідати певним вимогам автокореляції. Під терміном автокореляції в математиці мають на увазі ступінь подібності функції самій собі в різні моменти часу. Якщо підібрати таку чіпову послідовність, для якої функція автокореляції матиме різко виражений пік лише для одного моменту часу, то такий інформаційний сигнал можливо буде виділити на рівні шуму. Для цього в приймачі отриманий сигнал помножується на ту ж чіпову послідовність, тобто обчислюється автокореляційна функція сигналу. В результаті сигнал стає знову вузькополосним, тому його фільтрують у вузькій смузі частот і будь-яка перешкода, яка потрапляє в смугу вихідного широкосмугового сигналу, після множення на чіпову послідовність, навпаки, стає широкополосною і відсікається фільтрами, а в вузьку інформаційну смугу потрапляє лише частина перешкоди, по потужності значно менша, ніж перешкода, яка діє на вході приймача (рисунок 7.1).

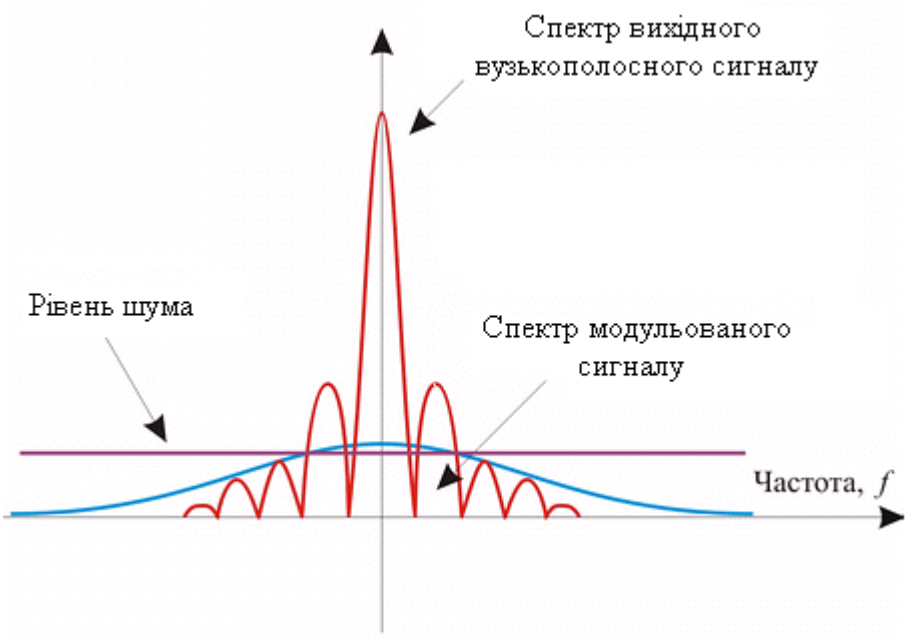


Рисунок 7.1. Використання технології розширення спектру дозволяє передавати дані на рівні природного шуму.

Коди Баркера

Чіпових послідовностей, що відповідають зазначеним вимогам автокореляції, існує досить багато, але для нас особливий інтерес представляють так звані коди Баркера, оскільки саме вони використовуються в протоколі IEEE 802.11.

Коди Баркера мають найкращі серед відомих псевдовипадкових послідовностей властивості шумоподібності, що й зумовило їх широке застосування. У протоколах сімейства IEEE 802.11 використовується код Баркера завдовжки в 11 чіпів (11100010010). Для того, щоб передати сигнал «логічна одиниця» передається пряма послідовність Баркера, а логічний нуль – інверсна послідовність.

Швидкість 1 Мбіт/с

У стандарті IEEE 802.11 передбачено два швидкісних режими: 1 і 2 Мбіт/с. Для кодування даних на фізичному рівні використовується метод DSSS з 11-чіповими кодами Баркера. При інформаційній швидкості 1 Мбіт/с швидкість проходження окремих чіпів послідовності Баркера становить 11×10^6 чіп/с, а ширина спектра такого сигналу складає 22 МГц. Враховуючи, що ширина частотного діапазону становить 83,5 МГц, отримуємо, що всього в даному частотному діапазоні можна вмістити 3 не накладених частотних каналів. Весь частотний діапазон, проте, прийнято ділити на 11 частотних каналів (що перекриваються) по 22 МГц, віддалених один від одного на 5 МГц. Приміром, перший канал займає частотний діапазон від 2400 до 2423 МГц і центрований щодо частоти 2412 МГц. Другий канал центрований щодо частоти 2417 МГц, а останній, 11 канал, центрований щодо частоти 2462 МГц. При такому розгляді 1, 6 і 11 канали не перекриваються один з одним і мають 3 мегагерцовий зазор один щодо одного. Саме ці три канали можуть використовуватися незалежно один від одного.

Для модуляції синусоїдального несучого сигналу (процес, необхідний для інформаційного наповнення несучого сигналу) використовується відносна двійкова фазова модуляція (Differential Binary Phase Shift Key, DBPSK). При цьому кодування інформації відбувається за рахунок зсуву фази синусоїдального сигналу по відношенню до попереднього стану сигналу. Двійкова фазова модуляції передбачає два можливих значення зсуву фази – 0 і π. Тоді логічний нуль може передаватися синфазним сигналом (зсув по фазі дорівнює 0), а одиниця – сигналом, який зсунуть по фазі на π.

Швидкість 2 Мбіт/с

Інформаційна швидкість 1 Мбіт/с є обов'язковою в стандарті IEEE 802.11 (Basic Access Rate), але в налаштуваннях можлива і швидкість в 2 Мбіт/с (Enhanced Access Rate). Для передачі даних на такій швидкості використовується та ж технологія DSSS з 11-чіповими кодами Баркера, але для модуляції несучого коливання застосовується відносна квадратурна фазова модуляція (Differential Quadrature Phase Shiftey). При відносній квадратурної фазової модуляції зрушення фаз може приймати чотири різних значення: 0, π / 2, π і 3π / 2. Використовуючи чотири різних стани сигналу, можна в одному дискретному стані закодувати послідовність двох інформаційних біт (дібіт) і тим самим в два рази підвищити інформаційну швидкість передачі. Приміром, дібіту 00 може відповідати зсув фази, що дорівнює 0; дібіту 01 – зсув фази, що дорівнює π / 2; дібіту 11 – зсув фази, що дорівнює π; дібіту 10 – зсув фази, рівний 3π / 2.

При інформаційній швидкості 2 Мбіт/с швидкість проходження окремих чіпів послідовності Баркера залишається колишньою, тобто 11×10^6 чіп/с, а отже, не змінюється і ширина спектра сигналу.

Фізичний рівень протоколу 802.11b/b +

Протокол IEEE 802.11b, прийнятий в липні 1999 року, є свого роду розширенням базового протоколу 802.11 і крім швидкостей 1 і 2 Мбіт/с передбачає швидкості 5,5 і 11 Мбіт/с. Для роботи на швидкостях 1 і 2 Мбіт/с використовуються технологія розширення спектра з використанням кодів Баркера, а для швидкостей 5,5 і 11 Мбіт/с використовуються так звані комплементарні коди (Complementary Code Keying, CCK).

CCK-послідовності

Комплементарні коди або CCK-послідовності мають таку властивість, що сума їх автокореляційних функцій для будь-якого циклічного зсуву, відмінного від нуля, завжди дорівнює нулю.

У стандарті IEEE 802.11b йдеться про комплексні комплементарні 8-чіпові послідовності, визначених на множині комплексних елементів.

Використовуючи безліч комплексних елементів {1, -1, j,-j} можна сформувати вісім однакових за модулем, але відмінних по фазі комплексних чисел. Тобто, елементи 8-чипової CCK-послідовності можуть приймати одне з наступних восьми значень: 1, -1, j, -j, 1 + j, 1-j, -1 + j,-1-j. Основна відмінність CCK-послідовностей від розглянутих раніше кодів Баркера полягає в тому, що існує не строго задана послідовність, за допомогою якої можна було кодувати або логічний нуль, або одиницю, а цілий набір послідовностей. Враховуючи, що кожен елемент 8-чиповой послідовності може приймати одне з восьми значень в залежності від значення фази, ясно, що можна скомбінувати $8^8 = 16777216$ варіантів послідовностей, однак, не всі вони будуть комплементарними. Але навіть з урахуванням вимоги комплементарності можна сформувати досить велике число різних CCK-послідовностей. Ця обставина дозволяє кодувати в одному переданому символі кілька інформаційних біт і тим самим підвищити інформаційну швидкість передачі.

Взагалі кажучи, використання CCK-кодів дозволяє кодувати 8 біт на один символ при швидкості 11 Мбіт/с і 4 біт на символ при швидкості 5,5 Мбіт/с. При

цьому в обох випадках символьна швидкість передачі становить 1,385 × 10^6 символів в секунду (11/8 = 5,5 / 4 = 1,385), а враховуючи, що кожен символ задається 8-чиповой послідовністю, отримуємо, що в обох випадках швидкість проходження окремих чіпів становить 11 × 10^6 чіпів в секунду. Таким чином, і ширина спектра сигнала как при скорости 11 Мбит/с и 5,5 Мбит/с составляет 22

МГц.

При розгляді можливих швидкостей передачі 5,5 і 11 Мбіт/с в протоколі IEEE 802.11b залишається без уваги питання: навіщо потрібна швидкість 5,5 Мбіт/с, якщо використання CCK-послідовностей дозволяє передавати дані на швидкості 11 Мбіт/с? Теоретично це дійсно так, але тільки якщо не враховувати при цьому перешкод. У реальних умовах зашумленість каналів передачі і відповідно співвідношення рівнів шуму і сигналу може виявитися таким, що передача на високій інформаційній швидкості, тобто коли в одному символі кодується безліч інформаційних біт, може виявитися неможливою з причини їх помилкового розпізнавання. Необхідно відзначити, що чим вище зашумленість каналів зв'язку, тим менше інформаційна швидкість передачі. При цьому важливо, що приймач і передавач правильно аналізували завадову обстановку і вибирали прийнятну швидкість передачі.

Двійкове пакетне згортальне кодування PBCC

Для подальшого розгляду протоколу 802.11b/b + необхідно познайомитися з ще одним типом кодування – так званим двійковим пакетним згортальним кодуванням (Packet Binary Convolutional Coding, PBCC).

Ідея згортального кодування полягає в наступному. Вхідна послідовність інформаційних біт перетворюється в спеціальному згортальному кодері таким чином, щоб кожному вхідному біту відповідало більше одного вихідного. Тобто загортальний кодер додає певну надлишкову інформацію до вихідної послідовності. Якщо, наприклад, кожному вхідному биту відповідає два вихідних, то говорять про згортальне кодування зі швидкістю r = 1/2. Якщо ж

кожним двом вхідним бітам відповідає три вихідних, то швидкість згортального кодування становитиме вже 2/3.

Будь-який загортальний кодер будується на основі декількох послідовно пов'язаних запам'ятовуючих комірок і логічних елементів, що пов'язують ці комірки між собою. Кількість запам'ятовуючих комірок визначає кількість можливих станів кодера. Якщо, приміром, в згортальному кодері використовується шість запам'ятовуючих комірок, то в кодері зберігається інформація про шість попередніх станів сигналу, а з урахуванням значення вхідного біта отримаємо, що в такому кодері використовується сім біт вхідної послідовності. Такий загортальний кодер називається кодером на сім станів (K = 7).

Вихідні біти, що формуються в згортальному кодері, визначаються значеннями вхідного біта і бітами, збереженими в запам'ятовуючих комірках, тобто значення кожного сформованого вихідного біта залежить не тільки від вхідного інформаційного біта, але і від кількох попередніх бітів.

У технології PBCC використовуються згортальні кодери на сім станів (K = 7) зі швидкістю r=1/2. Головною перевагою загортальних кодерів є завадостійкість сформованої ними послідовності. Справа в тому, що при надмірності кодування, навіть, в разі виникнення помилок прийому вихідна послідовність біт може бути безпомилково відновлена. Для відновлення початкової послідовності бітів на стороні приймача застосовується декодер Вітербо.

Дібіт, що формується в згортальному кодері, використовується надалі як символ що передається, але попередньо цей дібіт піддається фазової модуляції. Причому в залежності від швидкості передачі можлива двійкова, квадратурна або навіть восьмипозиційний фазова модуляція.

Метод пакетного згортального кодування опціонально передбачений як альтернативний метод кодування в протоколі IEEE 802.11b на швидкостях

передачі 5,5 і 11 Мбіт/с. Крім того, саме цей режим кодування ліг в основу протоколу IEEE 802.11b + – розширення протоколу IEEE 802.11b. Власне, протоколу IEEE 802.11b + як такого офіційно не існує, проте дане розширення підтримано багатьма виробниками бездротових пристроїв. У протоколі IEEE 802.11b + передбачається ще одна швидкість передачі даних – 22 Мбіт/с з використанням технології PBCC.

При швидкості передачі 5,5 Мбіт/с для модуляції дібіта, формованого згортальним кодером, використовується двійкова фазова модуляція, а при швидкості 11 Мбіт/с – квадратурна фазова модуляція. При цьому для швидкості 11 Мбіт/с в кожному символі кодується по одному вхідному біту і швидкість передачі біт відповідає швидкості передачі символів, а при швидкості 5,5 Мбіт/с швидкість передачі бітів дорівнює половині швидкості передачі символів (оскільки кожному вхідному біту в даному випадку відповідає два вихідних символи). Тому і для швидкості 5,5 Мбіт/с, і для швидкості 11 Мбіт/с символьна швидкість складає 11×10^6 символів в секунду.

Для швидкості 22 Мбіт/с в порівнянні зі вже розглянутої нами схемою PBCC передача даних має дві особливості. Перш за все, використовується 8-позиційна фазова модуляція (8-PSK), тобто фаза сигналу може приймати вісім різних значень, що дозволяє в одному символі кодувати вже 3 біта. Крім того, в схему крім згортального кодера доданий пунктурний кодер (Puncture). Сенс такого рішення досить простий: збитковість згортального кодера, що дорівнює 2 (на кожен вхідний біт припадає два вихідних), досить висока і при певних умовах завадової обстановки є зайвою, тому можна зменшити надмірність, щоб, наприклад, кожним двом вхідним бітам відповідало три вихідних .

Для цього можна, звичайно, розробити відповідний згортальний кодер, але краще додати в схему спеціальний пунктурний кодер, який буде просто знищувати зайві біти.

У згортальний кодер (K = 7, R = 1/2) дані надходять зі швидкістю 22 Мбіт/с . Після додавання збитковості в загортальному кодері біти зі швидкістю потоку 44 Мбіт/с надходять в пунктурний кодер 4:3, в якому надмірність зменшується так, щоб на кожні чотири вхідних біта доводилося три вихідних. Отже, після пунктурного кодера швидкість потоку складе вже 33 Мбіт/с (не інформаційна, а загальна швидкість з урахуванням доданих надлишкових бітів). Отримана в результаті послідовність направляється в фазовий модулятор 8-PSK, де кожні три біта упаковуються в один символ. При цьому швидкість передачі складе 11 × 10^6 символів в секунду, а інформаційна швидкість – 22 Мбіт/с (рисунок 7.2).

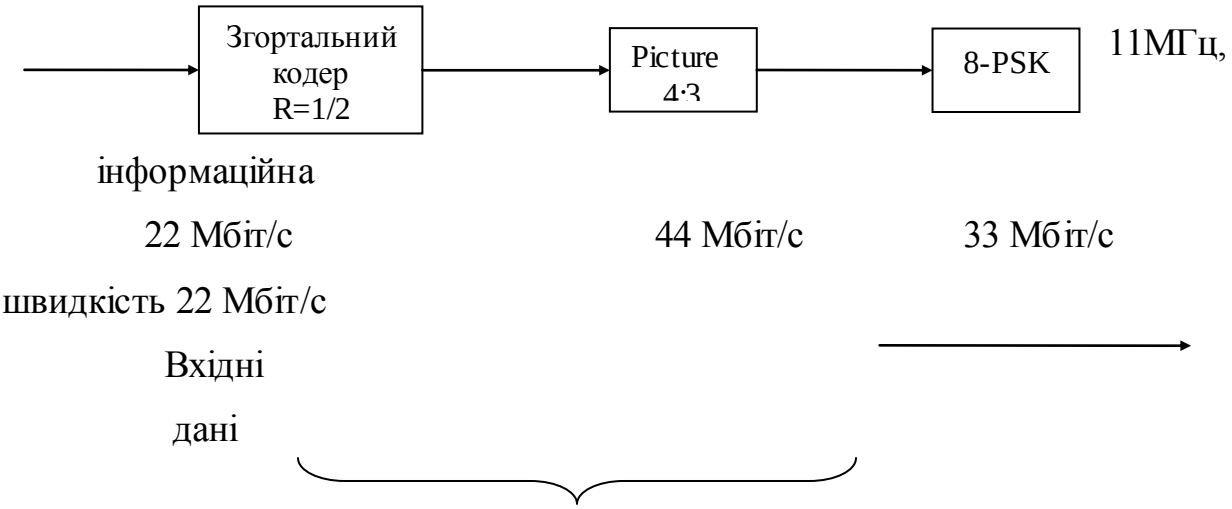


Рис. 7.2. Реалізація швидкості 22 Мбіт/с в протоколі 802.11g.

У таблиці 7.1 наводяться відповідності між швидкостями передачі і типом кодування.

Таблиця 7.1. - відповідності між швидкостями передачі

Швидкість передачі,Мбіт/с		Метод кодування	Модуляція	Швидкість загортального кодування	Символьна швидкість, 10^6 символ/с	Кількість біт в одному символі
1	(обов'язково)	Код Баркера	DBPSK	-	1	1

2	(обов'язково)	Код Баркера	DQPSK	-	1	2
5,5	(обов'язково)	CCK	DQPSK	-	1,375	2
	(опціонально)	PBCC	DBPSK	1/2	11	0,5
11	(обов'язково)	CCK	DQPSK	-	1,375	8
	(опціонально)	PBCC	DQPSK	1/2	11	1
22	(обов'язково)	PBCC	DQPSK	3/4	11	2

Фізичний рівень протоколу IEEE 802.11g

Стандарт IEEE 802.11g є логічним розвитком стандарту IEEE 802.11b/b+ і передбачає передачу даних в тому ж частотному діапазоні, але з більш високими швидкостями. Крім того, стандарт IEEE 802.11g повністю сумісний з IEEE 802.11b, тобто будь-який пристрій IEEE 802.11g має підтримувати роботу з пристроями IEEE 802.11b. Максимальна швидкість передачі в стандарті IEEE 802.11g становить 54 Мбіт/с.

При розробці стандарту IEEE 802.11g розглядалися кілька конкуруючих технологій: метод ортогонального частотного поділу OFDM, запропонований до розгляду компанією Intersil, і метод двійкового пакетного згортального кодування PBCC, опціонально реалізований в стандарті IEEE 802.11b і запропонований компанією Texas Instruments. В результаті стандарт IEEE 802.11g заснований на компромісному рішенні: в якості базових застосовуються технології OFDM і CCK, а опціонально передбачено використання технології PBCC.

Ортогональне частотне розділення каналів з мультиплексуванням

Поширення сигналів в відкритому середовищі, яким є радіоефір, супроводжується виникненням різних перешкод, джерелом яких служать самі сигнали що поширюються. Класичний приклад такого роду перешкод – ефект багатопроменевої інтерференції сигналів, що полягає в тому, що в результаті багаторазових відбиттів сигналу від природних перешкод один і той же сигнал може потрапляти в приймач різними шляхами. Але подібні шляхи поширення

мають і різні довжини, а тому для різних шляхів поширення ослаблення сигналу буде неоднаковим. Отже, в точці прийому результуючий сигнал являє собою суперпозицію (інтерференцію) багатьох сигналів, які мають різні амплітуди і зміщених один відносно одного по часу, що еквівалентно додаванню сигналів з різними фазами.

Наслідком багатопроменевої інтерференції є спотворення сигналу. Багатопроменева інтерференція властива будь-якого типу сигналів, але особливо негативно вона позначається на широкосмугових сигналах. Справа в тому, що при використанні широкосмугового сигналу в результаті інтерференції певні частоти складаються синфазно, що призводить до збільшення сигналу, а деякі, навпаки, – противофазно, викликаючи ослаблення сигналу на даній частоті.

Говорячи про багатопроменеву інтерференцію, що виникає при передачі сигналів, розрізняють два крайніх випадки. У першому випадку максимальна затримка між різними сигналами не перевищує часу тривалості одного символу і інтерференція виникає в межах одного переданого символу. У другому випадку максимальна затримка між різними сигналами більше тривалості одного символу, а в результаті інтерференції складаються сигнали, що представляють різні символи, і виникає так звана міжсимвольна інтерференція (Inter Symbol Interference, ISI).

Найбільш негативно на спотворення сигналу впливає міжсимвольна інтерференція. Оскільки символ – це дискретний стан сигналу, що характеризується значеннями несучої частоти, амплітуди і фази, то для різних символів змінюються амплітуда і фаза сигналу, тому відновити вихідний сигнал вкрай складно.

Щоб уникнути, а точніше, частково компенсувати ефект багатопроменевого розповсюдження, використовуються частотні еквалайзери, проте у міру зростання швидкості передачі даних або за рахунок збільшення

символьної швидкості, або через ускладнення схеми кодування, ефективність використання еквалайзерів падає.

У стандарті IEEE 802.11b з максимальною швидкістю передачі 11 Мбіт/с при використанні CCK-кодів схеми компенсації міжсимвольної інтерференції цілком успішно справляються з покладеним на них завданням, але при більш високих швидкостях такий підхід стає неприйнятним.

Тому при більш високих швидкостях передачі застосовується принципово інший метод кодування даних – ортогональне частотне розділення каналів з мультиплексуванням (Orthogonal Frequency Division Multiplexing, OFDM). Ідея даного методу полягає в тому, що потік переданих даних розподіляється по безлічі частотних підканалів і передача ведеться паралельно на всіх цих підканалах. При цьому висока швидкість передачі досягається саме за рахунок одночасної передачі даних по всіх каналах, а швидкість передачі в окремому підканалі може бути і невисокою. Оскільки в кожному з частотних підканалів швидкість передачі даних можна зробити не надто високою, це створює передумови для ефективного придушення міжсимвольної інтерференції.

При частотному поділі каналів необхідно, щоб ширина окремого каналу була, з одного боку, досить вузькою для мінімізації спотворення сигналу в межах окремого каналу , а з іншого – досить широкою для забезпечення необхідної швидкості передачі. Крім того, для економного використання всієї смуги каналу,який розділяється на підканали, бажано як можна більш щільно розташувати частотні підканали, але при цьому уникнути міжканальної інтерференції, щоб забезпечити повну незалежність каналів один від одного. Частотні канали, що задовольняють перерахованим вимогам, називаються ортогональними. Несучі сигнали всіх частотних підканалів (а точніше, функції, що описують ці сигнали) ортогональні один одному.

Важливо, що хоча самі частотні підканали можуть частково перекривати один одного, ортогональність несучих сигналів гарантує частотну незалежність

каналів один від одного, а, отже, і відсутність міжканальної інтерференції (рисунок 7.3).

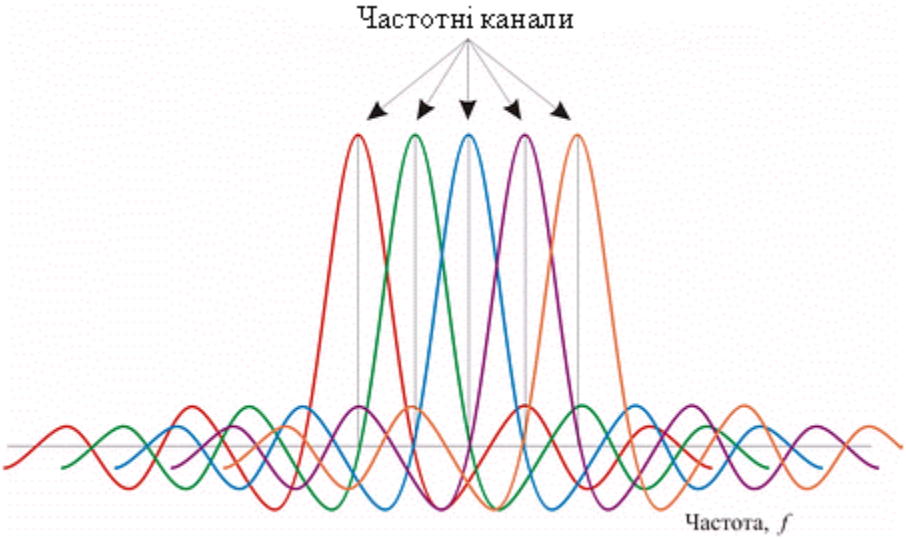


Рисунок 7.3. Приклад частотних каналів що перекриваються з ортогональними несучими.

Розглянутий спосіб розподілу широкосмугового каналу на ортогональні частотні підканали називається ортогональним частотним поділом з мультиплексуванням (OFDM). Одним з ключових переваг методу OFDM є поєднання високої швидкості передачі з ефективною протидією багатопроменевому поширенню. Якщо говорити точніше, то сама по собі технологія OFDM не усуває багатопроменевого розповсюдження, але створює передумови для усунення ефекту міжсимвольної інтерференції. Справа в тому, що невід'ємною частиною технології OFDM є охоронний інтервал (Guard Interval, GI) – циклічне повторення закінчення символу, що прибудовують на початку символу (рисунок 4).

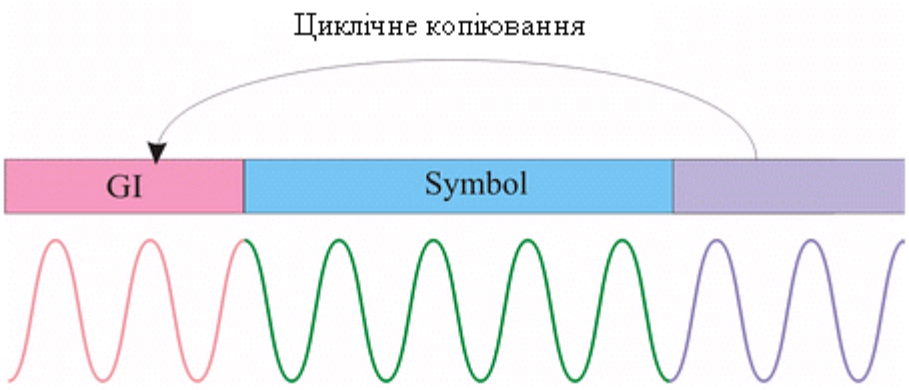


Рисунок 7.4. Охоронний інтервал GI.

Охоронний інтервал є надмірною інформацією і в цьому сенсі знижує корисну (інформаційну) швидкість передачі, але саме він служить захистом від виникнення міжсимвольної інтерференції. Ця надлишкова інформація додається до символу що передається в передавачі і відкидається при прийомі символу в приймачі.

Наявність охоронного інтервалу створює тимчасові паузи між окремими символами, і якщо тривалість охоронного інтервалу перевищує максимальний час затримки сигналу в результаті багатопроменевого розповсюдження, то міжсимвольної інтерференції не виникає (рисунок 7.5).

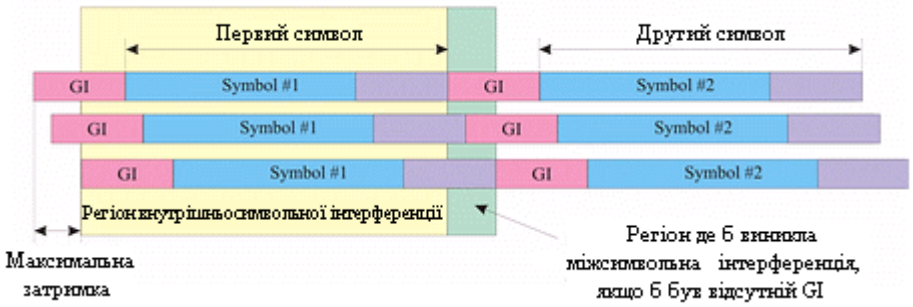


Рисунок 7.5. Уникнення міжсимвольної інтерференції за рахунок використання охоронних інтервалів.

При використанні технології OFDM тривалість охоронного інтервалу становить одну четверту тривалості самого символу. При цьому сам символ має тривалість 3,2 мкс, а охоронний інтервал – 0,8 мкс. Таким чином, тривалість символу разом з охоронним інтервалом становить 4 мкс.

Швидкісні режими і методи кодування в протоколі IEEE 802.11g

У протоколі IEEE 802.11g передбачена передача на швидкостях 1, 2, 5,5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48 і 54 Мбит/с. Деякі з даних швидкостей є обов'язковими, а деякі – опціональними. Крім того, одна і та ж швидкість може реалізовуватися при різній технології кодування. Протокол IEEE 802.11g включає в себе як підмножини протоколи IEEE 802.11b/b +.

Технологія кодування PBCC опціонально може використовуватися на швидкостях 5,5; 11; 22 і 33 Мбіт/с. Взагалі ж у самому стандарті обов'язковими є швидкості передачі 1, 2, 5,5, 6, 11, 12 і 24 Мбіт/с, а більш високі швидкості передачі (33, 36, 48 і 54 Мбіт/с) – опціональними.

Для обов'язкових швидкостей в стандарті IEEE 802.11g використовується тільки кодування CCK і OFDM, а гібридне кодування і кодування PBCC є опціональним. Співвідношення між різними швидкостями передачі і методами кодування що використовуються відображено в таблиці 2.

У протоколі IEEE 802.11b для модуляції використовувалася або двійкова (BDPSK), або квадратурна (QDPSK) відносна фазова модуляція. У протоколі IEEE 802.11g на низьких швидкостях передачі також використовується фазова модуляція (тільки не відносна), тобто двійкова і квадратурна фазові модуляції BPSK і QPSK. При використанні BPSK-модуляції в одному символі кодується тільки один інформаційний біт, а при використанні QPSK-модуляції – два інформаційних біта. Модуляція BPSK використовується для передачі даних на швидкостях 6 і 9 Мбіт/с, а модуляція QPSK – на швидкостях 12 і 18 Мбіт/с.

Для передачі на більш високих швидкостях використовується квадратурна амплітудна модуляція QAM (Quadrature Amplitude Modulation), при якій інформація кодується за рахунок зміни фази і амплітуди сигналу. У протоколі IEEE 802.11g використовується модуляція 16-QAM і 64-QAM. У першому випадку маємо 16 різних станів сигналу, що дозволяє закодувати 4 біта в одному символі. У другому випадку маємо вже 64 можливих станів сигналу, що

дозволяє закодувати послідовність 6 біт в одному символі. Модуляція 16-QAM застосовується на швидкостях 24 і 36 Мбіт/с, а модуляція 64-QAM - на швидкостях 48 і 54 Мбіт/с.

Виникає питання: чому при одному і тому ж типі модуляції можливі різні швидкості передачі? Справа в тому, що при використанні технології OFDM використовується згортальне кодування з різними пунктирними кодерами, що призводить до різної швидкості згортального кодування. В результаті при використанні одного і того ж типу модуляції можуть виходити різні значення інформаційної швидкості – все залежить від швидкості згортального кодування. Так, при використанні BPSK-модуляції зі швидкістю згортального кодування 1/2 отримуємо інформаційну швидкість 6 Мбіт/с, а при використанні згортального кодування зі швидкістю 3/4 – 9 Мбіт/с.

Таблиця 7.2.

Швидкість передачі, Мбіт/с		Метод кодування	Модуляція
1	(обов'язково)	Код Баркера	DBPSK
2	(обов'язково)	Код Баркера	DQPSK
5,5	(обов'язково)	CCK	DQPSK
	(опціонально)	PBCC	DBPSK
6	(обов'язково)	OFDM	BPSK
	(опціонально)	CCK-OFDM	BPSK
9	(опціонально)	OFDM, CCK-OFDM	BPSK
11	(обов'язково)	CCK	DQPSK
	(опціонально)	PBCC	DQPSK
12	(обов'язково)	OFDM	QPSK
	(опціонально)	CCK-OFDM	QPSK
18	(опціонально)	OFDM, CCK-OFDM	QPSK
22	(опціонально)	PBCC	DQPSK
24	(обов'язково)	OFDM	16-QAM
	(опціонально)	CCK-OFDM	
33	(опціонально)	PBCC	
36	(опціонально)	OFDM, CCK-OFDM	16-QAM
48	(опціонально)	OFDM, CCK-OFDM	64-QAM

54	(опціонально)	OFDM, CCK-OFDM	64-QAM

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

1. Використовуючи пакет NetCracker, вивчити склад і функціональні характеристики типового обладнання бездротових локальних мереж.

2. У відповідності з варіантом завдання побудувати бездротову мережу з використанням стандартів IEEE 802.11.

3. Для отриманої моделі мережі задати необхідні типи потоків даних між робочими станціями та серверами і провести імітаційне моделювання роботи мережі.

4. Проаналізувати середнє завантаження мережевого обладнання, а також кількість пакетів що втратили. Зробити висновки.

Таблиця 7.3.

№ Варіанта	Технологія магістралі	Кількість HTTP серверів	Кількість FTP серверів	Кількість Бездротових станцій
1	Ethernet	1	2	6
2	Token Ring	2	3	7
3	Ethernet	3	2	5
4	Token Ring	4	1	4
5	Ethernet	1	3	5
6	Token Ring	2	4	4
7	Ethernet	3	3	5
8	Token Ring	4	2	6
9	Ethernet	1	4	3
10	Token Ring	2	1	7
11	Ethernet	3	4	5
12	Token Ring	4	2	3
13	Ethernet	1	1	7
14	Token Ring	2	2	4
15	Ethernet	3	3	2

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

1. Характеристика сімейства стандартів IEEE 802.11.

2. З якою метою використовується технологія розширення спектра?
3. Поняття технології DSSS.
4. Двійкове пакетне згортальне кодування PBCC.
5. Ортогональне частотне розділення каналів з мультиплексуванням.
6. Які види модуляції використовуються в стандартах IEEE 802.11?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. http://standards.ieee.org/getieee802/download/802.11-1999.pdf
2. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
3. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
4. http://standards.ieee.org/getieee802/download/802.11g-2003.pdf
5. Леонов В. Обзор протоколов и технологий беспроводной передачи данных - http://www.ferra.ru/online/networks/25619
6. Семенов Ю.А. Telecommunication technologies – телекоммуникационные технологии - http://book.itep.ru

Комп'ютерний практикум № 8

ТЕХНОЛОГІЇ БЕЗДРОТОВИХ МЕРЕЖ. КАНАЛЬНИЙ РІВЕНЬ ПРОТОКОЛІВ IEEE 802.11

Мета роботи:познайомиться з протоколами і технологіями передачі даних в бездротових мережах на канальному рівні, отримати навички вибору обладнання для побудови бездротової локальної обчислювальної мережі.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Технологія колективного доступу в бездротових мережах сімейства IEEE 802.11 b/g

На фізичному рівні сімейства протоколів IEEE 802.11 визначаються механізми, які використовуються для перетворення даних, для забезпечення необхідної швидкості передачі залежно від середовища передачі даних. Таким чином, фізичний рівень визначає методи кодування/декодування і модуляції/демодуляції сигналу при його передачі та прийомі.

У той же час такі питання, як регулювання спільного використання середовища передачі даних, визначаються на більш високому рівні - рівні доступу до середовища передачі даних. Цей рівень називають MAC-рівнем (Media Access Control). Саме на MAC-рівні встановлюються правила спільного використання середовища передачі даних одночасно декількома вузлами бездротової мережі.

На MAC-рівні визначаються два основних типи архітектури бездротових мереж - Ad Hoc і Infrastructure Mode.

Режим Ad Hoc

У режимі Ad Hoc (Рисунок 8.1), який називають також Independent Basic Service Set (IBSS) або режимом Peer to Peer (точка-точка), станції безпосередньо взаємодіють одна з одною. Для цього режиму потрібно мінімум обладнання: кожна станція повинна бути оснащена бездротовим адаптером. При такій конфігурації не потрібно створення мережевої інфраструктури. Основним недоліком режиму Ad Hoc є обмежений діапазон дії можливої мережі.

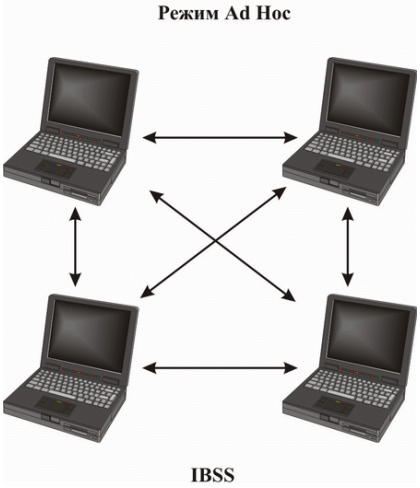


Рисунок 8.1. Режим функціонування Ad Hoc.

Режим Infrastructure Mode

У режимі Infrastructure Mode (рисунок 8.2) станції взаємодіють один з одним не прямо, а через точку доступу (Access Point), яка виконує в бездротової мережі роль своєрідного концентратора (аналогічно тому, як це відбувається в традиційних кабельних мережах). Розглядають два режими взаємодії з точками доступу - BSS (Basic Service Set) і ESS (Extended Service Set). В режимі BSS всі станції зв'язуються між собою тільки через точку доступу, яка може виконувати також роль моста до зовнішньої мережі. У розширеному режимі ESS існує інфраструктура декількох мереж BSS, причому самі точки доступу взаємодіють одна з одною, що дозволяє передавати трафік від однієї BSS до іншої. Між собою точки доступу з'єднуються за допомогою або сегментів кабельної мережі, або радіомостом.

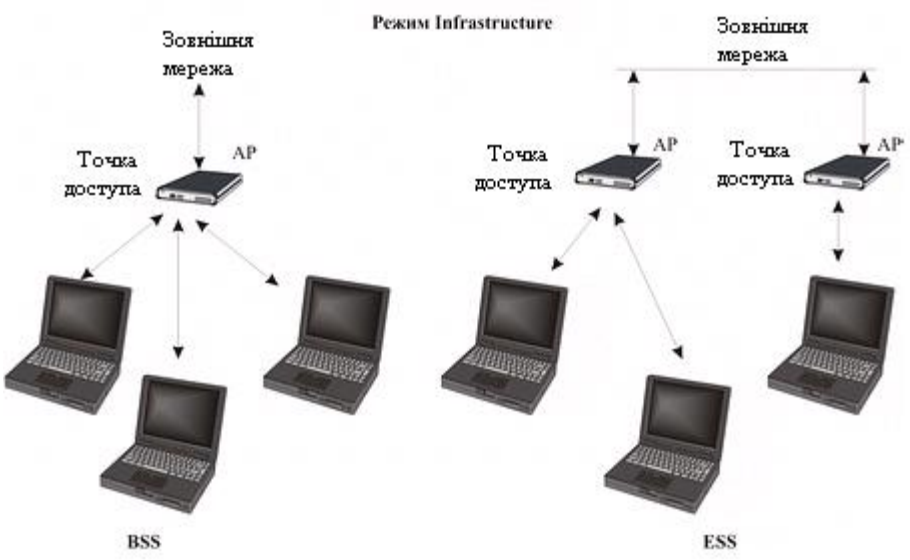


Рисунок 8.2. Режим функціонування Infrastructure Mode.

Крім двох різних режимів функціонування бездротових мереж на MAC-рівні визначаються правила колективного доступу до середовища передачі даних. Необхідність існування таких регламентують правил цілком очевидна. Якщо кожен вузол бездротової мережі, не дотримуючись жодних правил, став би передавати дані в ефір, то в результаті інтерференції декількох таких сигналів вузли, яким призначалася відправлена інформація, не змогли б не тільки її отримати, але і зрозуміти, що дана інформація адресована їм. Саме тому, необхідно існування жорстких регламентуючих правил, які визначали б колективний доступ до середовища передачі даних.

На MAC-рівні протоколу IEEE 802.11 визначаються два типи колективного доступу до середовища передачі даних: функція розподіленої координації (Distributed Coordination Function, DCF) і функція централізованої координації (Point Coordination function, PCF).

Функція розподіленої координації DCF

На перший погляд організувати спільний доступ до середовища передачі даних досить просто. Для цього необхідно лише забезпечити, щоб всі вузли передавали дані тільки тоді, коли середовище є вільним, тобто коли жоден з

вузлів не передає дані. Проте такий механізм неминуче призведе до колізій, оскільки велика ймовірність того, що два або більше вузлів одночасно, намагаючись отримати доступ до середовища передачі даних, вирішать, що середовище вільне і почнуть одночасну передачу. Саме тому необхідно розробити алгоритм, здатний знизити ймовірність виникнення колізій і в той же час гарантувати всім вузлам мережі рівноправний доступ до середовища передачі даних.

Одним з варіантів організації такого рівноправного доступу до середовища передачі даних є функція розподіленої координації (DCF). Ця функція заснована на методі колективного доступу з виявленням несучої і механізмом запобігання колізій (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA). При такій організації кожен вузол, перш ніж почати передачу, «прослуховує» середовище, намагаючись виявити несучий сигнал, і лише за умови, що середовище вільне, може почати передачу даних.

Проте, в цьому випадку велика ймовірність виникнення колізій: коли два або більше вузлів мережі одночасно (або майже одночасно) вирішать, що середовище вільне, і почнуть передавати дані. Для того щоб знизити ймовірність виникнення подібних ситуацій, використовується механізм уникнення колізій (Collision Avoidance, CA). Суть даного механізму полягає в наступному. Кожен вузол мережі, переконавшись, що середа вільна, перш ніж почати передачу, вичікує протягом певного проміжку часу. Цей проміжок є випадковим і складається з двох складових: обов'язкової проміжку DIFS (DCF Interframe Space) і проміжку зворотного відліку, що обирається випадковим чином (backoff time). В результаті кожен вузол мережі перед початком передачі вичікує протягом випадкового проміжку часу, що, природно, значно знижує ймовірність виникнення колізій, оскільки ймовірність того, що два вузли мережі будуть вичікувати протягом одного і того ж проміжку часу, надзвичайно мала.

Для того щоб гарантувати всім вузлам мережі рівноправний доступ до середовища передачі даних, необхідно відповідним чином визначити алгоритм вибору тривалості проміжку зворотного відліку (backoff time). Проміжок зворотного відліку хоча і є випадковим, але в той же час визначається на підставі безлічі деяких дискретних проміжків часу, тобто, дорівнює цілому числу елементарних часових проміжків, які називаються тайм-слотами (SlotTime). Для вибору проміжку зворотного відліку кожен вузол мережі формує так зване вікно конкурентного доступу (Contention Window, CW), що використовується для визначення кількості тайм-слотів, протягом яких станція вичікувала перед передачею. Фактично вікно CW - це діапазон для вибору кількості тайм-слотів, причому мінімальної розмір вікна визначається в 31 тайм-слот, а максимальний розмір - в 1023 тайм-слот. Проміжок зворотного відліку визначається як кількість тайм-слотів, яке визначається виходячи з розміру вікна CW:

$$Backoff\ \ time = Random[CW_{\min}, CW_{\max}] \times SlotTime$$

Коли вузол мережі намагається отримати доступ до середовища передачі даних, то після обов'язкового проміжку очікування DIFS запускається процедура зворотного відліку, тобто включається зворотний відлік лічильника тайм-слотів починаючи від обраного значення вікна CW. Якщо протягом усього проміжку очікування середовище залишалося вільним (лічильник зворотного відліку дорівнює нулю), то вузол починає передачу.

Після успішної передачі вікно CW формується знову. Якщо ж за час очікування передачу почав другий вузол мережі, то значення лічильника зворотного відлік зупиняється і передача даних відкладається. Після того як середу стане вільною, даний вузол знову починає процедуру зворотного відліку, але вже з меншим розміром вікна CW, який визначається попереднім значенням лічильника зворотного відліку і відповідно з меншим значенням часу очікування. При цьому очевидно, що чим більше число раз вузол відкладає

передачу через зайнятість середовища, тим вища ймовірність того, що наступного разу він отримає доступ до середовища передачі даних (Рисунок 8.3).

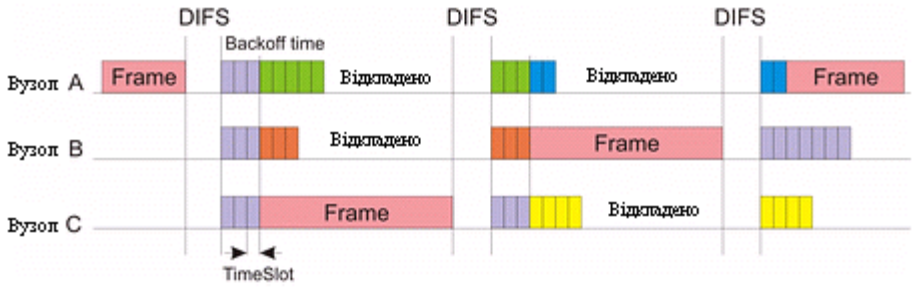


Рисунок 8.3. Реалізація рівноправного доступу до середовища передачі даних в методі DCF.

Розглянутий алгоритм реалізації колективного доступу до середовища передачі даних гарантує рівноправний доступ всіх вузлів мережі до середовища. Однак при такому підході вірогідність виникнення колізій хоч і мала, але все-таки існує. Зрозуміло, що знизити ймовірність виникнення колізій можна шляхом збільшення максимального розміру формованого вікна CW. У той же час це збільшить часи затримок при передачі і тим самим знизить продуктивність мережі. Тому в методі DCF для мінімізації колізій використовується наступний алгоритм. Після кожного успішного прийому кадру приймаюча сторона через короткий проміжок SIFS (Short Interframe Space) підтверджує успішний прийом, посилаючи відповідну квитанцію - кадр ACK (ACKnowledgement) (малюнок 4). Якщо в процесі передачі даних виникла колізія, то сторона що передає не отримує кадр ACK про успішний прийом. В цьому випадку розмір CW-вікна для вузла що предає збільшується майже вдвічі. Так, якщо для першої передачі розмір вікна дорівнює 31 слоту, то для другої спроби передачі він вже становить 63 слота, для третьої - 127 слотів, для четвертої - 255, для п'ятої - 511, а для всіх наступних - 1023 слота. Тобто для кожної і-й передачі (якщо всі попередні виявилися безуспішними) розмір CW-вікна збільшується за наступним правилом:

$$CW_i = 2CW_{i-1} + 1$$

Таким чином, збільшення розміру вікна відбувається динамічно по мірі зростання числа колізій, що дозволяє, з одного боку, зменшити тимчасові затримки і, з іншого боку, знизити ймовірність виникнення колізій.

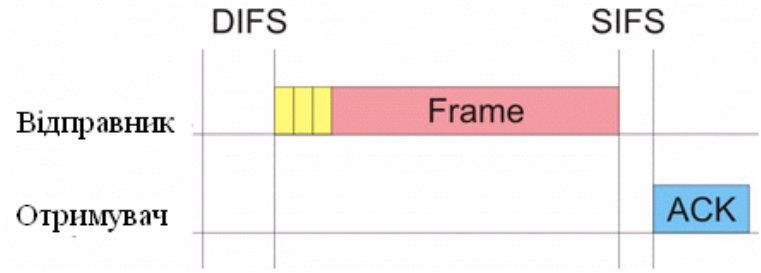


Рисунок 8.4. Кадри квитанції, відсилаються в разі успішної передачі даних.

Говорячи про алгоритм реалізації рівноправного доступу до середовища передачі даних, необхідно також враховувати і розмір кадру даних. Дійсно, якщо кадри даних будуть занадто великими, то при виникненні колізій доведеться повторно передавати великий обсяг інформації, що призведе до зниження продуктивності мережі. Крім того, при великому розмірі кадрів даних вузли мережі змушені простоювати протягом досить тривалого часу, перш ніж почати передачу.

У той же час використання кадрів даних невеликого розміру, хоча і дозволяє гарантувати рівноправний доступ усіх вузлів до середовища передачі даних і мінімізує витрати при виникненні колізій, не може не позначитися негативно на корисному мережевому трафіку. Справа в тому, що кожен кадр поряд з корисною інформацією містить інформацію службову (заголовок кадру). При зменшенні розміру кадру скорочується величина саме корисної інформації (даних користувача), що обумовлює передачу по мережі надлишкової кількості службової інформації. Тому розмір кадру - це свого роду золота середина, від правильного вибору якої залежить ефективність використання середовища передачі даних.

Розглянутий механізм регламентування колективного доступу до середовища передачі даних має одне вузьке місце - так звану проблему прихованих вузлів. Через наявність природних перешкод можлива ситуація, коли два вузли мережі не можуть «чути» один одного напряму. Такі вузли називають прихованими.

Для того щоб вирішити проблему прихованих вузлів, функція DCF опціонально передбачає можливість використання алгоритму RTS/CTS.

Алгоритм RTS/CTS

Відповідно с алгоритмом RTS/CTS кожен вузол мережі, перед тим як послати дані в «ефір», спочатку відправляє спеціальне коротке повідомлення, яке називається RTS (Ready To Send) і означає готовність даного вузла до відправки даних. Таке RTS-повідомлення містить інформацію про тривалість майбутньої передачі і про адресата і доступно всім вузлам в мережі (якщо тільки вони не приховані від відправника). Це дозволяє іншим вузлам затримати передачу на якийсь час, який дорівнює оголошеній тривалості повідомлення. Приймальня станція, отримавши сигнал RTS, відповідає посилкою сигналу CTS (Clear To Send), що свідчить про готовність станції до прийому інформації. Після цього передавальна станція надсилає пакет даних, а приймальня станція повинна передати кадр ACK, що підтверджує безпомилковий прийом. Послідовність відправки кадрів між двома вузлами мережі показана на рис.8.5.

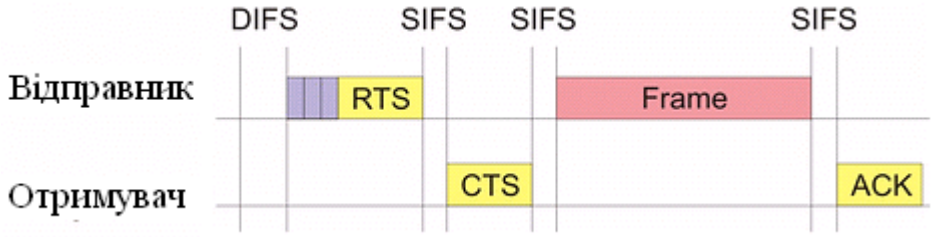


Рисунок 8.5. Взаємодія між двома вузлами мережі відповідно до алгоритму RTS/CTS.

Тепер розглянемо ситуацію, коли мережа складається з чотирьох вузлів: A, B, C і D (Малюнок 6). Припустимо, що вузол C знаходиться в зоні досяжності

тільки вузла A, вузол A знаходиться в зоні досяжності вузлів C і B, вузол B знаходиться в зоні досяжності вузлів A і D, а вузол D знаходиться в зоні досяжності тільки вузла B. Тобто в такій мережі є приховані вузли: вузол C прихований від вузлів B і D, вузол A прихований від вузла D.

У подібній мережі алгоритм RTS/CTS дозволяє впоратися з проблемою виникнення колізій, яка не вирішується за допомогою розглянутого базового способу організації колективного доступу в DCF. Дійсно, нехай вузол A намагається передати дані вузлу B. Для цього він посилає сигнал RTS, який, крім вузла B, отримує також вузол C, але не отримує вузол D. Вузол C, отримавши даний сигнал, блокується, тобто призупиняє спроби передавати сигнал до моменту закінчення передачі між вузлами A і B. Вузол B, у відповідь на отриманий сигнал RTS, посилає кадр CTS, який отримують вузли A і D. Вузол D, отримавши даний сигнал, також блокується на час передачі між вузлами A і B.

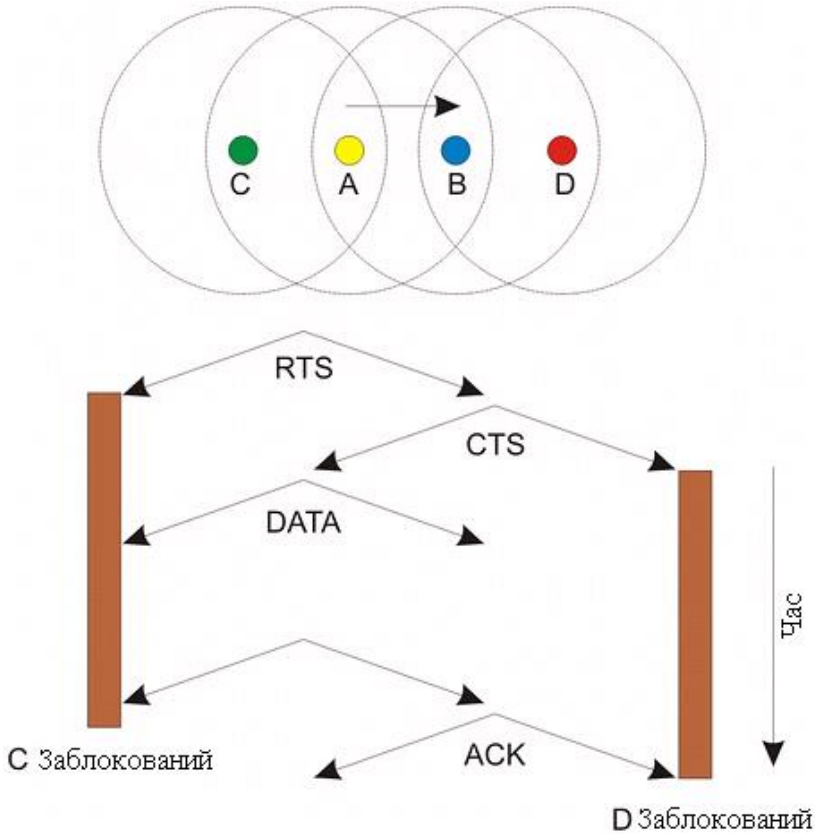


Рисунок 8.6. Рішення проблеми прихованих вузлів в алгоритмі RTS/CTS.

У алгоритму RTS/CTS є свої підводні камені, які в певних ситуаціях можуть призводити до зниження ефективності використання середовища передачі даних. Наприклад, в деяких ситуаціях можливе таке явище, як поширення ефекту помилкових блокувань вузлів, що в кінцевому рахунку може привести до ступору в мережі.

Розглянемо, наприклад, мережу, показану на рисунку 8.7. Нехай вузол B намагається передати дані вузлу A, посилаючи йому кадр RTS. Оскільки цей кадр отримує також і вузол C, то він блокується на час передачі між вузлами A і B. Вузол D, намагаючись передати дані вузлу C, посилає кадр RTS, але оскільки вузол C заблокований, то він не отримує відповіді і розпочинає процедуру зворотного відліку зі збільшеним розміром вікна. У той же час кадр RTS, посланий вузлом D, отримує і вузол E, який, помилково припускаючи, що за цим піде сеанс передачі даних від вузла D до вузла C, блокується. Проте це помилкова блокування, оскільки реально між вузлами D і C передачі немає. Більш того, якщо вузол F спробує передати дані помилково заблокованого вузлу E і пошле свій кадр RTS, то він помилково заблокує вузол G.

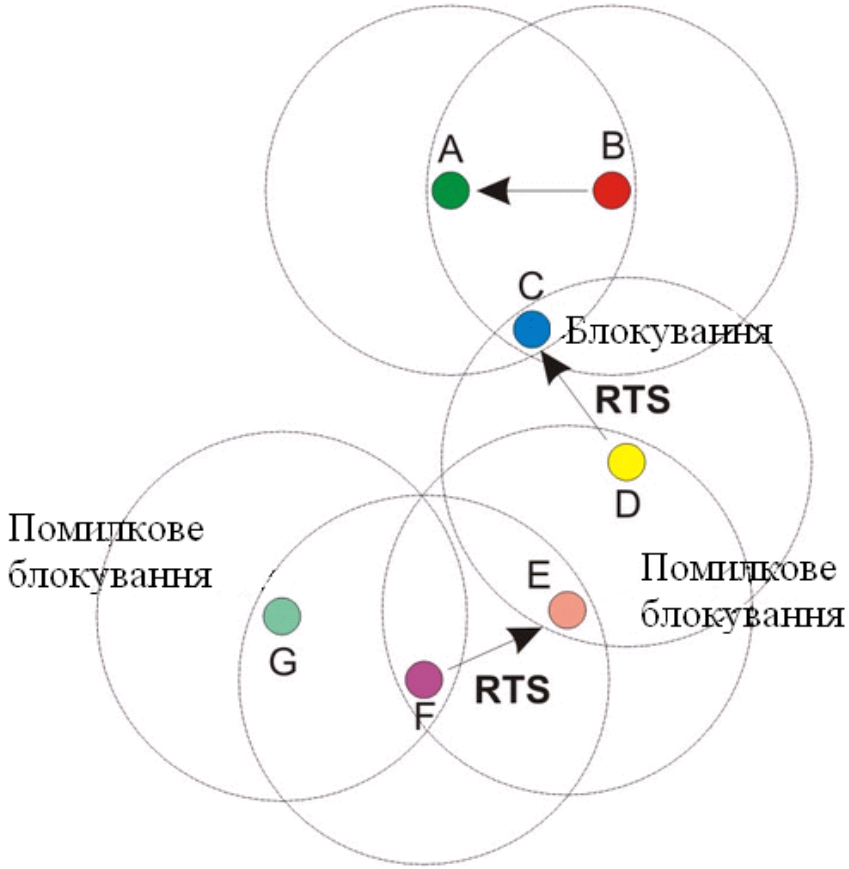


Рисунок 8.7. Виникнення помилкових блокувань вузлів мережі.

Описане явище помилкового блокування вузлів може призводити до короткочасного ступору всієї мережі.

Функція централізованої координації PCF

Розглянутий механізм розподіленої координації DCF є базовим для протоколів IEEE 802.11 і може використовуватися як в бездротових мережах, що функціонують в режимі Ad Hoc, так і в мережах, що функціонують в режимі Infrastructure, тобто в мережах, інфраструктура яких включає точку доступу.

Однак для мереж в режимі Infrastructure більш природним є дещо інший механізм регламентування колективного доступу, відомий як функція централізованої координації (Point Coordination Function, PCF). Механізм PCF є опціональним і застосовується тільки в мережах з точкою доступу.

У разі задіяння механізму PCF один з вузлів мережі (точка доступу) є центральним і називається центром координації (Point Coordinator, PC). На центр координації покладається завдання управління колективним доступом всіх інших вузлів мережі до середовища передачі даних на основі певного алгоритму опитування або виходячи з пріоритетів вузлів мережі. Тобто центр координації опитує всі вузли мережі, внесені в його список, і на підставі цього опитування організовує передачу даних між усіма вузлами мережі. Важливо, що такий підхід повністю виключає конкуруючий доступ до середовища, як у випадку механізму DCF, і робить неможливим виникнення колізій, а для залежних від часу додатків гарантує пріоритетний доступ до середовища. Таким чином, PCF може використовуватися для організації пріоритетного доступу до середовища передачі даних.

Функція централізованої координації не заперечує функцію розподіленої координації, а швидше, доповнює її, накладаючись поверх. Фактично в мережах з механізмом PCF реалізується як механізм PCF, так і традиційний механізм DCF. Протягом певного проміжку часу реалізується механізм PCF, потім - DCF, а потім все повторюється заново.

Для того щоб мати можливість чергувати режими PCF і DCF, необхідно, щоб точка доступу, що виконує функції центру координації та реалізує режим PCF, мала б пріоритетний доступ до середовища передачі даних. Це можна зробити, якщо використовувати конкурентний доступ до середовища передачі даних (як і в методі DCF), але для центру координації дозволити використовувати проміжок очікування, менший DIFS. В цьому випадку якщо центр координації намагається отримати доступ до середовища, то він очікує (як і всі інші вузли мережі) закінчення поточної передачі і, оскільки для нього визначається мінімальний режим очікування після виявлення «тиші» в ефірі, першим отримує доступ до середовища. Проміжок очікування, що визначається

для центру координації, називається PIFS (PCF Interframe Space), причому SIFS <PIFS <DIFS.

Режими DCF і PCF об'єднуються в так званому суперфреймі, який утворюється з проміжку без конкурентного доступу до середовища, який називається CFP (Contention-Free Period) , і наступного за ним проміжку конкурентного доступу до середовища CP (Contention Period) (малюнок 8).

Суперфрейм починається з кадру-маячка (beacon), отримавши який всі вузли мережі припиняють спроби передавати дані на час, обумовлений періодом CFP. Кадри маячки несуть службову інформацію про тривалість CFP-проміжку і дозволяють синхронізувати роботу всіх вузлів мережі.

Під час режиму PCF точка доступу опитує всі вузли мережі про кадри, які стоять в черзі на передачу, посилаючи їм службові кадри CF_POLL.

Опитувані вузли у відповідь на отримання кадрів CF_POLL посилають підтвердження CF_ACK. Якщо підтвердження не отримано, то точка доступу переходить до опитування наступного вузла.

Крім того, щоб мати можливість організувати передачу даних між усіма вузлами мережі, точка доступу може передавати кадр даних (DATA) і поєднувати кадр опитування з передачею даних (кадр DATA + CF_POLL) . Аналогічно вузли мережі можуть поєднувати кадри підтвердження з передачею даних DATA + CF_ACK (рисунок 9).

Допускаються наступні типи кадрів під час режиму PCF:

• DATA - кадр даних

• CF_ACK - кадр підтвердження

• CF_POLL - кадр опитування

• DATA + CF_ACK - комбінований кадр даних та підтвердження

• DATA + CF_POLL - комбінований кадр даних та опитування

• DATA + CF_ACK + CF_POLL - комбінований кадр даних, підтвердження та опитування

• CF_ACK + CF_POLL - комбінований кадр підтвердження та опитування

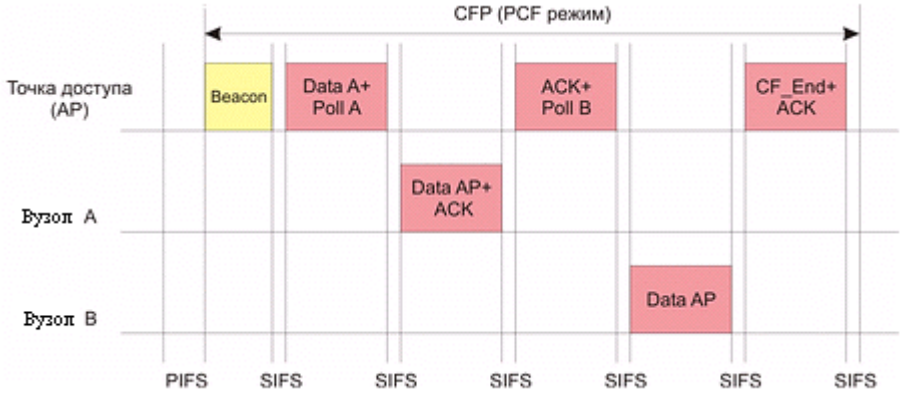


Рисунок 8.9. Організація передачі даних між вузлами мережі в режимі PCF.

Максимальна швидкість передачі даних у протоколах IEEE 802.11b / g

Максимальна швидкість, обумовлена протоколом IEEE 802.11b, становить 11 Мбіт/с, а для протоколу IEEE 802.11g - 54 Мбіт/с.

Проте слід чітко розрізняти повну швидкість передачі і корисну швидкість передачі. Справа в тому, що технологія доступу до середовища передачі даних, структура переданих кадрів, заголовки, які додаються до переданих кадрів на різних рівнях моделі OSI, - все це передбачає наявність досить великого обсягу службової інформації. В результаті корисна чи реальна швидкість передачі, тобто швидкість передачі даних користувача, завжди виявляється нижче повної швидкості передачі.

Більше того, реальна швидкість передачі залежить і від структури бездротової мережі. Так, якщо всі клієнти мережі використовують один і той же протокол, наприклад IEEE 802.11g, то мережа є гомогенною і швидкість передачі даних у такій мережі вище, ніж в змішаній мережі, де є клієнти як IEEE 802.11g, так і IEEE 802.11b. Справа в тому, що клієнти IEEE 802.11b «не чують» клієнтів IEEE 802.11g, які використовують OFDM-кодування. Тому з метою забезпечення спільного доступу до середовища передачі даних клієнтів, що використовують різні типи модуляції, в подібних змішаних мережах точки

доступу повинні відпрацьовувати певний механізм захисту. В результаті використання механізмів захисту в змішаних мережах реальна швидкість передачі стає ще менше.

Крім того, реальна швидкість передачі даних залежить і від використовуваного протоколу (TCP або UDP) і від розміру довжини пакета. Природно, що протокол UDP передбачає більш високі швидкості передачі. Теоретичні максимальні швидкості передачі даних для різних типів мереж і протоколів представлені в таблиці 1.

Тип мережі	Модуляція	Максимальна швидкість з'єднання, Мбіт/с	Теоритична максимальна швидкість передачі за протоколом TCP, Мбіт/с	Теоритична максимальна швидкість передачі за протоколом UDP, Мбіт/с
802.11b	CCK	11	5,9	7,1
802.11g (разом з 802.11b)	OFDM/CCK	54	14,4	19,5
802.11g (тільки)	OFDM/CCK	54	24?4	30,5

Розширення протоколу IEEE 802.11g

Не встиг ще остаточно утвердитися стандарт IEEE 802.11g, що передбачає максимальну швидкість з'єднання до 54 Мбіт/с, як стали з'являтися бездротові пристрої з написами «802.11g +», «108 Мбіт/с» «Turbo Mode», «Super -G »і т.д.

Фактично, мова йде про якесь не стандартизоване розширення протоколу IEEE 802.11g, що дозволяє домогтися більш високих швидкостей передачі. У рішеннях під маркою 802.11g + на фізичному рівні використовуються ті ж самі режими передачі, що й у протоколі IEEE 802.11g. Власне, мова йде не про зміну фізичного рівня, а про деякі зміни MAC-рівня, тобто рівня доступу до середовища передачі даних.

В основі всіх технологій розширення протоколу IEEE 802.11g лежать такі принципи, як пакетна передача (packet bursting), запозичена з протоколу IEEE

802.11e, а також стиснення даних, швидкі кадри і зв'язування каналів. В режимі блокової передачі всі пакети, передані в одному блоці, використовують скорочені заголовки, що дозволяє зменшити обсяг переданої службової інформації і тим самим збільшити корисний трафік.

Технологія Super-G використовує пакетну передачу, "швидкі кадри" і стиснення даних "на льоту", а також зв'язування двох каналів. Основна ідея, що лежить в основі технології Super-G полягає у зв'язуванні двох каналів (channel bonding) для збільшення загальної пропускної здатності. Оскільки теоретична пропускна здатність одного каналу в протоколі IEEE 802.11g становить 54 Мбіт/с, то при зв'язуванні двох каналів можна досягти пропускної здатності в 108 Мбіт/с. Саме тому, продукти, що підтримують технологію Super-G часто супроводжують написами типу 108 Мбіт/с.

Стандарт IEEE 802.11g використовують одинадцять каналів в частотній смузі 2,4 ГГц, які розділені проміжками по 5 МГц. Оскільки загальноприйнята ширина кожного каналу складає 22 МГц є три канали без часткового накладення (1, 6 і 11), центральні частоти яких відстоять один від одного на 25 МГц. Реалізація режиму Super-G можлива тільки на центральному каналі 6.

Технологія Super-G передбачає два режими функціонування: динамічний і статичний. Статичний режим передбачається використовувати в WLAN на базі тільки устаткування Super-G, при цьому включаються всі функції Super-G, включаючи об'єднання двох каналів.

Динамічний режим передбачається використовувати в змішаних мережах WLAN, тобто коли є як клієнти Super-G, так і клієнти IEEE 802.11b/g. Оскільки клієнти IEEE 802.11b/g не підтримують режиму Super-G, то при виявленні таких клієнтів в мережі при використанні динамічного режиму відбувається автоматичний перехід роботи всієї мережі на звичайний режим IEEE 802.11b/g.

Крім того, багато виробників реалізують також і гібридний режим роботи, коли технологія Super-G використовується без зв'язування каналів.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

1. Використовуючи пакет NetCracker, вивчити склад і функціональні характеристики типового обладнання бездротових локальних мереж.

2. У відповідності з варіантом завдання побудувати бездротову мережу з використанням стандартів IEEE 802.11.

3. Для отриманої моделі мережі задати необхідні типи потоків даних між робочими станціями та серверами і провести імітаційне моделювання роботи мережі.

4. Проаналізувати середню завантаження мережного обладнання, а також кількість пакетів що втрачаються. Зробити висновки.

Таблиця 8.2.

№ Варіанта	Тип архітектури	Кількість HTTP серверів	Кількість FTP серверів	Кількість бездротових станцій
1	Ad Hoc	2	1	4
2	Infrastructure Mode	3	2	5
3	Ad Hoc	2	3	3
4	Infrastructure Mode	1	4	4
5	Ad Hoc	3	1	4
6	Infrastructure Mode	4	2	4
7	Ad Hoc	3	3	5
8	Infrastructure Mode	2	4	4
9	Ad Hoc	4	1	2
10	Infrastructure Mode	1	2	5
11	Ad Hoc	4	3	5
12	Infrastructure Mode	2	4	3
13	Ad Hoc	1	1	6

14	Infrastructure Mode	2	2	4
15	Ad Hoc	2	3	3

СПИСОК КОНТРОЛЬНИХ ПИТАНЬ

Характеристика основних режимів роботи бездротових мереж.

Функції Mac-рівня в протоколах IEEE 802.11.

Способи доступу до середовища передачі DCF і PCF.

Яким чином забезпечується рівноправний доступ абонентів до середовища передачі в методі DCF?

У чому полягає проблема помилкового блокування вузлів мережі?

Як вирішується проблема прихованих вузлів?

Які способи підвищення швидкості передачі даних використовуються в бездротових мережах?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. http://standards.ieee.org/getieee802/download/802.11-1999.pdf
2. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
3. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
4. http://standards.ieee.org/getieee802/download/802.11g-2003.pdf
5. Леонов В. Обзор протоколов и технологий беспроводной передачи данных - http://www.ferra.ru/online/networks/25619
6. Семенов Ю.А. Telecommunication technologies - телекоммуникационные технологии - http://book.itep.ru