МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА**

М. Ю. КАРПЕНКО, Н. В. МАКОГОН

КОНСПЕКТ ЛЕКЦІЙ
з курсу

«КОМП'ЮТЕРНІ МЕРЕЖІ»

*(для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки,
151 – Автоматизація та комп'ютерно-інтегровані технології,
126 – Інформаційні системи та технології)*

**Харків
ХНУМГ ім. О. М. Бекетова
2019**

Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки, 151 – Автоматизація та комп'ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с.

Автори: М. Ю. Карпенко,
Н. В. Макогон

Рецензент: канд. фіз.-мат. наук, доц. О. Б. Костенко

Рекомендовано кафедрою прикладної математики і інформаційних технологій, протокол засідання № 1 від 31.08.2016.

ЗМІСТ

ЗМІСТОВИЙ МОДУЛЬ 1. ЛОКАЛЬНІ ТА ГЛОБАЛЬНІ КОМП'ЮТЕРНІ МЕРЕЖІ

1 ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

Механізм взаємодії комп'ютерів у мережі багато в чому є запозиченими із взаємодії комп'ютерів з периферійними пристроями, тому варто це детально розглянути.

1.1 Зв'язок комп'ютера з периферійними пристроями

Для організації зв'язку в обох цих пристроях передбачені зовнішні інтерфейси (рис. 1.1).

Інтерфейс – це певна логічна та фізична сутність між незалежними об'єктами, що взаємодіють між собою. Інтерфейс задає параметри та характеристики взаємодії об'єктів.

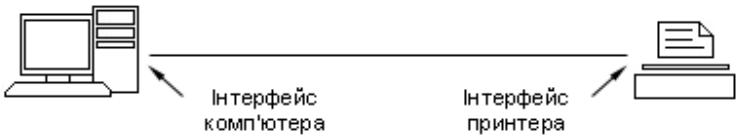


Рисунок 1.1 – Зовнішні інтерфейс

Фізичний інтерфейс (порт) – визначається набором електричних зв'язків та характеристиками сигналів. Зазвичай, це роз'єм з набором контактів, кожен з яких має певне призначення. Роз'єми різних пристроїв об'єднуються за допомогою кабелю, в якому кожен провідник під'єднується до певного контакту.

Логічний інтерфейс – набір інформаційних повідомлень певного формату, якими обмінюються два пристрої, а також набір правил обміну цими повідомленнями.

В комп'ютері стандартним інтерфейсом є USB та COM порти, що призначені для під'єднання до комп'ютера різноманітних периферійних пристроїв.

В периферійному пристрої інтерфейс зазвичай представлено контролером периферійного пристрою, який приймає команди та дані від комп'ютера і керує

роботою периферійного пристрою. Назворот контролер повідомляє комп’ютер про здійснені операції та свій стан (рис.1.2).

Програмну підтримку функціонування периферійного пристрою виконує програма-драйвер, що встановлюється на комп’ютер і керує контролером периферійного пристрою. Драйвер периферійного пристрою є посередником між процесором і периферійним пристроєм, він передає команди до контролера і здійснює високорівневі операції (наприклад, розділення документа на сторінки, друкування певного символу).

Для одного контролера можна розробити різні драйвери, які будуть різнитися якістю керування процесом.

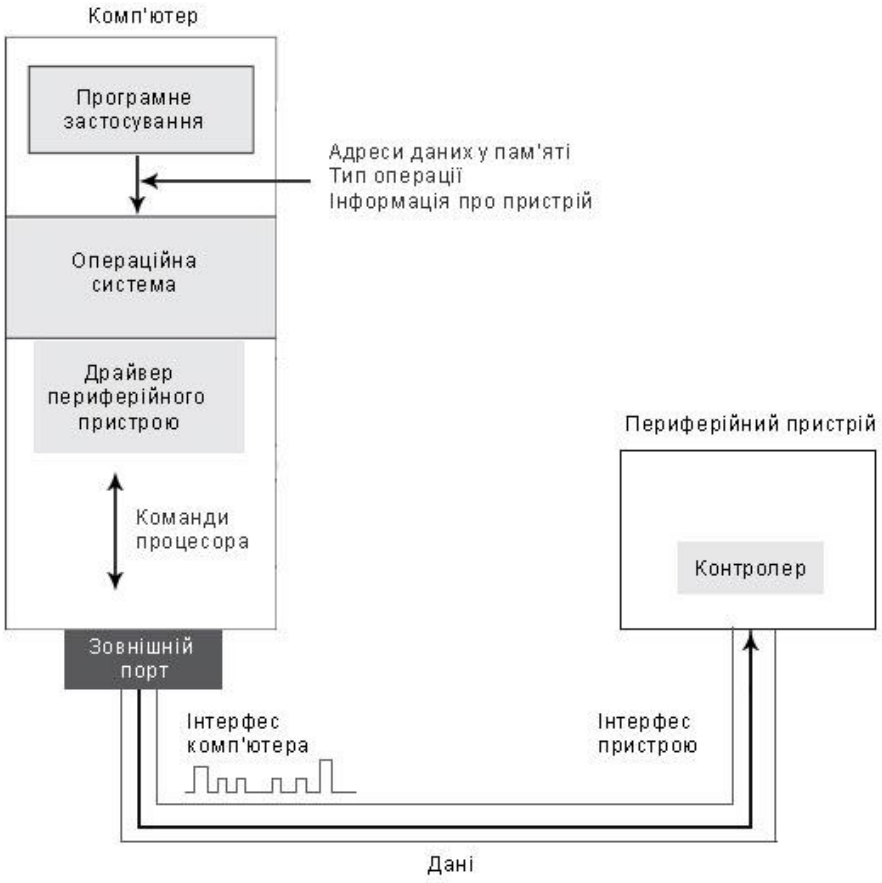


Рисунок 1.2 – Схема зв’язку комп’ютера з периферійним пристроєм

Програмне застосування, яке виконує обмін даними з периферійним пристроєм звертається до драйверу пристрою і повідомляє йому адреси байтів пам’яті, що треба передати.

Драйвер послідовно передає байти по лінії зв’язку. Для виокремлення початку байта, першим передається стартовий сигнал специфічної форми, потім інформативні біти (на один біт – відповідний електричний сигнал) і наприкінці стоповий сигнал специфічної форми та контрольний біт для перевірки достовірності переданої інформації.

Після отримання чергового байту інформації, контролер його інтерпретує і запускає задану операцію для периферійного пристрою. Після завершення роботи, драйвер периферійного пристрою повідомляє операційну систему про виконання завдання. Операційна система повідомляє про це програмне застосування.

1.2 Простий зв’язок між двома комп’ютерами

В найпростішому випадку взаємодія двох комп’ютерів може здійснюватися через COM чи USB порти, це так зване «нуль-модемне з’єднання» (рис. 1.3).

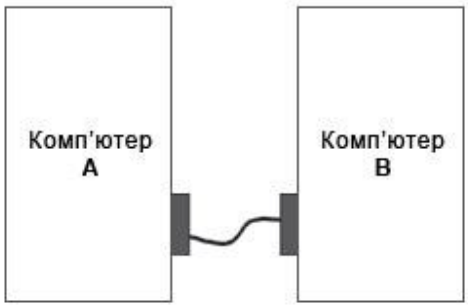


Рисунок 1.3 – Простий зв’язок між двома комп’ютерами

Програма що працює на комп’ютері А не може безпосередньо доступитися до ресурсів комп’ютера В. Вона має просити (за допомогою повідомлень) відповідну програму, що працює на комп’ютері В. Повідомлення можуть містити як інформаційні дані (вміст певного файлу), так і команди на виконання певних дій (рис. 1.4).

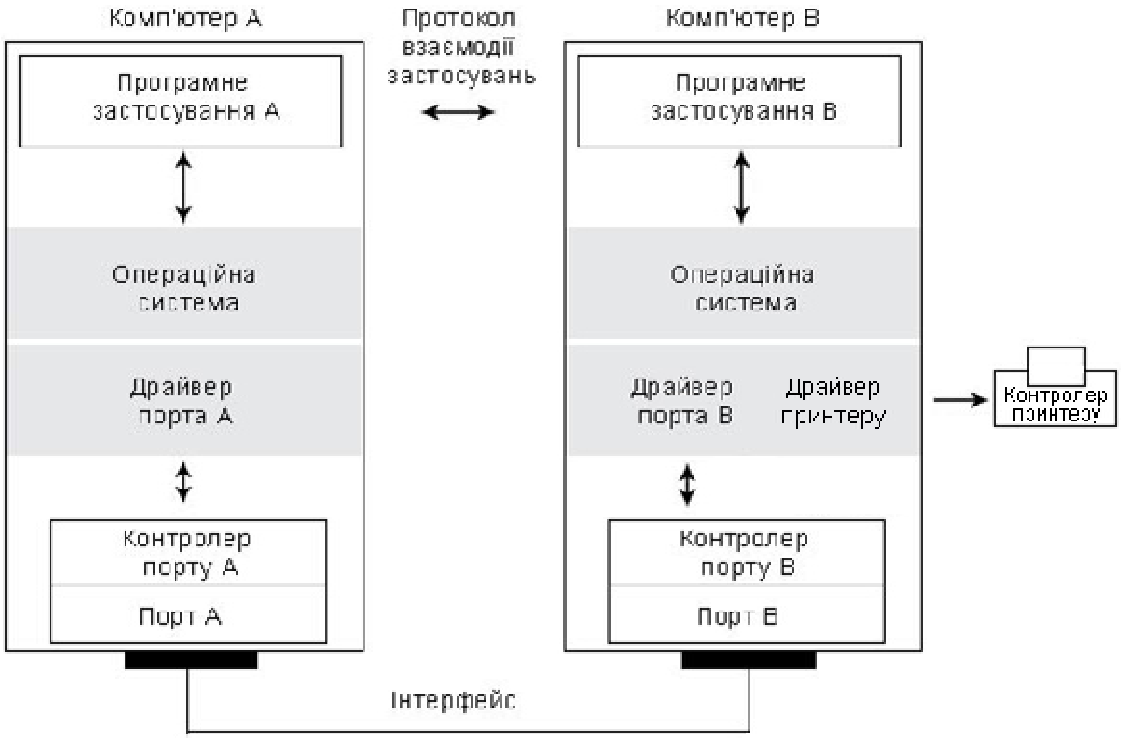


Рисунок 1.4 – Мережна взаємодія комп’ютерів та периферійних пристроїв

Драйвери і контролери портів працюють подібно до попереднього прикладу. Разом вони виконують передачу інформації по кабелю між двома комп’ютерами. В справжніх мережах подібні функції виконують мережні адаптери та їх драйвери.

1.3 Модулі «Клієнт» та «Сервер»

Потреба у доступі до віддалених файлів та ресурсів може виникати у користувачів багатьох різноманітних застосувань:

- текстових редакторів.
- графічних редакторів.
- СУБД (Системи управління базами даних).

Очевидно, що функції з організації обміну нераціонально втілювати у склад кожного програмного застосування. Ефективніше цю задачу вирішує пара спеціалізованих модулів:

Клієнт – модуль, що призначений для формування повідомлень-запитів до віддаленого комп’ютера від різних типів програмних застосувань. В зворотному

напрямку – прийом результатів та передача їх до відповідних програмних застосувань.

Сервер – модуль, який постійно очікує запити від клієнтів. Після отримання запиту, він виконується. Один сервер є спроможним виконувати запити відразу від кількох клієнтів (одночасно чи послідовно).

Важливою функцією клієнтської програми є здатність відрізняти запит до віддаленого ресурсу від запиту до локального ресурсу. Клієнтська програма сама розпізнає і перескеровує (Redirect) запит до віддаленого комп'ютера звільнюючи програмні застосування від таких завдань (рис. 1.5).

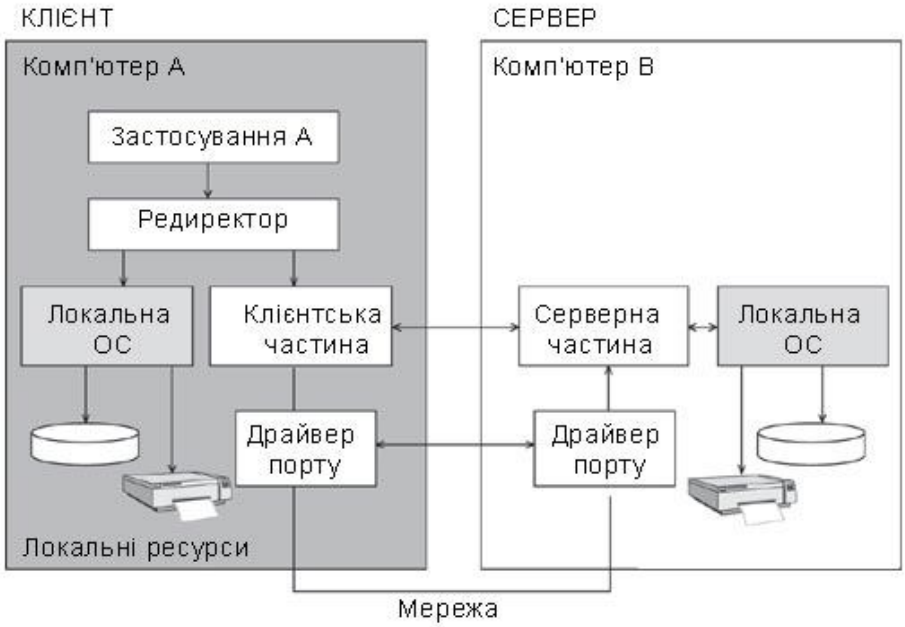


Рисунок 1.5 – Мережний зв'язок «клієнт-сервер»

Клієнт і сервер виконують системні функції по обслуговуванню запитів всіх програмних застосувань комп'ютера А на віддалений доступ до ресурсу комп'ютера В (принтеру, файлам, факсу). Для того, щоб програмні застосування комп'ютера В могли користуватися ресурсами комп'ютера А, схему доповнюють клієнтом для комп'ютера В і сервером для комп'ютера А.

Терміни «клієнт» і «сервер» використовують для позначення як програмних модулів так і комп'ютерів. Якщо комп'ютер переважно надає свої ресурси іншим

комп’ютерам, то він називається сервером, якщо їх споживає – то клієнтом. Іноді комп’ютер може бути як клієнтом так і сервером.

1.4 Мережні сервіси (служби) і застосування

Сервісом (*service*) називається надання користувачам спільного доступу до певного типу ресурсів (наприклад, доступ до файлів – файловий сервіс, сервіс друку, сервіс електронної пошти, сервіс віддаленого доступу).

Програми, що реалізують мережні сервіси відносяться до класу розподілених програм.

Розподілена програма – це програма, що складається з кількох взаємодіючих частин. Кожна частина може виконуватися на окремому комп’ютері мережі.

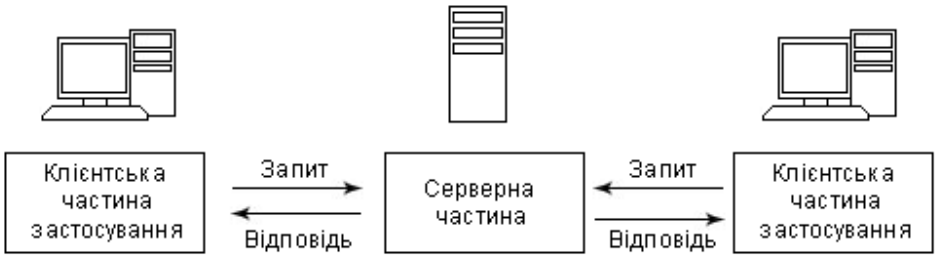


Рисунок 1.6 – Спільний доступ до відкритих ресурсів

Мережні служби – це системні розподілені програми, що реалізують мережні сервіси.

2 ЛОКАЛЬНІ МЕРЕЖІ

2.1 Призначення локальних обчислювальних мереж

На базі економічної та високопродуктивної електронної техніки у 80-х роках визначилась нова тенденція розвитку інформаційно-обчислювальної техніки – створення локальних обчислювальних мереж **LAN** (Local Area Network) різноманітного призначення. **Локальна обчислювальна мережа** – це комунікаційна мережа, яка забезпечує в межах деякої обмеженої території взаємозв’язок для широкого кола програмних продуктів. Вона підтримує зв’язок між ЕОМ, терміналами, обладнанням, забезпечує сумісне використання ресурсів.

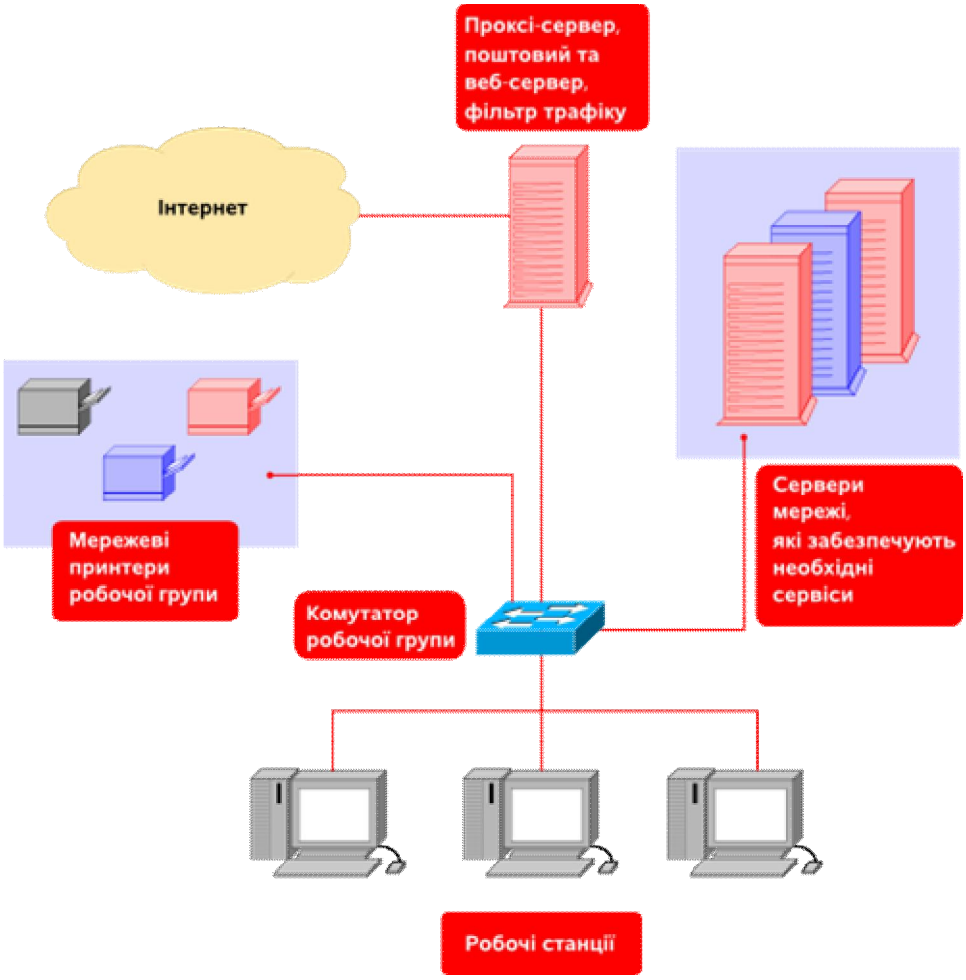


Рисунок 2.1 – Структура локальної комп’ютерної мережі

Спочатку локальні обчислювальні мережі створювалися для наукових цілей з метою сумісного використання загальних ресурсів. Це пояснювалось тим, що в багатьох випадках широко розповсюджені персональні комп’ютери не забезпечували створення та функціонування достатньо потужних автоматизованих інформаційних систем через недостатність власних ресурсів. Для таких автоматизованих інформаційних систем необхідно було застосовувати потужніші комп’ютери – **сервери** , які дозволяли б концентрувати мережні ресурси і були б розраховані на ефективну роботу в мережі для сумісного використання користувачами. Сьогодні найпоширенішими стають локальні обчислювальні мережі комерційного призначення.

Локальна комп'ютерна мережа являє собою об'єднання певного числа комп'ютерів (іноді досить великого) на відносно невеликій території.

2.2 Переваги використання локальної обчислювальної мережі

Наявність в офісі, конторі, установі (підприємстві, цеху) локальної обчислювальної мережі створює для користувачів принципово нові можливості завдяки об'єднанню прикладних систем персональних комп'ютерів та іншого обладнання мережі. Впровадження локальної обчислювальної мережі дозволяє персонально використовувати обчислювальні ресурси всієї мережі, а не тільки окремого комп'ютера, створювати різноманітні масиви управлінської, комерційної та іншої інформації загального призначення, автоматизувати документообіг в цілому. З'являються можливості колективного використання різних спеціалізованих засобів та інструментів для вирішення певного кола професійних задач (наприклад, засобів машинної графіки, підготовки звітів, відомостей, доповідей, публікацій та інших документів). Крім організації внутрішніх служб, локальна обчислювальна мережа дозволяє розгорнути зовнішні по відношенню до організації такі служби, як телексний (телетайпний) зв'язок, поштова кореспонденція, електроні дошки оголошень, електронні газети, тощо, а також підтримує вихід в глобальні (регіональні) мережі та користування їх послугами.

З розширенням бізнесу виростають витрати на офісні приміщення. При виконанні більшого обсягу робіт організації вимушені розширювати штати, що приводить до необхідності розширення площ. Це примусило деякі організації розпочати експерименти з виконанням певних робіт вдома (ввід даних, бухгалтерський облік тощо). Завдяки під'єднанню домашнього персонального комп'ютера до комп'ютерної мережі компанії для цього працівника зникає необхідність кожного дня відвідувати організацію.

Повністю увібрала в себе особливості сучасної інформатики техніка **телеконференцій**. Учасники телеконференцій можуть користуватися необхідними базами даних, а у випадку необхідності здійснювати автоматизоване опрацювання інформації. Поряд з цим мережі надають можливість проводити відеоконференції, які дозволяють влаштовувати сумісні зустрічі партнерів з різних кінців світу. Формування технологій відеоконференцій неможливе без широкосмугових ліній зв'язку, телебачення, комп'ютерних інформаційних мереж. Зображення і звук від відеокамер і мікрофонів, під'єднаних до комп'ютера, передаються кожному учаснику наради і виводяться на монітори і динаміки їх комп'ютерів. Такі конференції дозволяють зекономити значні кошти і час, що витрачаються на дорогу.

2.3 Визначення локальної обчислювальної мережі

Як випливає із назви, локальна комп'ютерна мережа є системою, яка охоплює відносно невеликі віддалі. **Міжнародний комітет IEEE802 (Інститут інженерів по електроніці і електротехніці, США)**, що спеціалізується на стандартизації в галузі локальних комп'ютерних мереж, дає наступне визначення цим системам: "Локальні комп'ютерні мережі відрізняються від інших видів мереж тим, що вони звичайно обмежені невеликим географічним районом, таким, як група поруч розташованих будівель, і, в залежності від каналів зв'язку здійснюють передачу даних в діапазонах швидкостей від помірних до високих з низьким рівнем помилок ." Значення параметрів району, загальна протяжність, кількість вузлів, швидкість передачі і топологія локальної обчислювальної мережі можуть бути різними, але комітет IEEE802 обмежує використання в локальних мережах кабелів довжиною до кількох кілометрів, підтримки декількох сотень станцій різноманітної топології при швидкості передачі інформації порядку 1-2 і більше Мбіт/с".

Локальні комп'ютерні мережі – це системи розподіленої обробки даних і, на відміну від глобальних та регіональних комп'ютерних мереж, охоплюють невеликі території (діаметром 5-10 км) всередині окремих контор, банків, бірж, вузів, установ, науково-дослідних організацій і т.д. При допомозі загального каналу зв'язку локальна мережа може об'єднувати від десятків до сотень абонентських вузлів, що включають персональні комп'ютери, зовнішні запам'ятовуючі пристрої, дисплеї, друкуючі і копіюючі пристрої, касові і банківські апарати, інтерфейсні схеми та інші. Локальні мережі можуть під'єднуватися до інших локальних і великих (регіональних або глобальних) мереж ЕОМ за допомогою спеціальних шлюзів, мостів і маршрутизаторів, які реалізуються на спеціалізованих пристроях або на персональних комп'ютерах з відповідним програмним забезпеченням.

Відносно невелика складність і вартість локальних обчислювальних мереж, основу яких складають персональні комп'ютери, забезпечують широке використання їх в сферах автоматизації комерційної, банківської та інших видів діяльності, діловодства, технологічних і виробничих процесів, для створення розподілених управлінських, інформаційно-довідкових, контрольно-вимірювальних систем, систем промислових роботів і гнучких промислових виробництв. У більшості випадків успіх використання локальних мереж

обумовлений їх доступністю масовому користувачу, з одного боку, і тими соціально-економічними наслідками, які вони вносять в різноманітні види людської діяльності з іншого. Якщо на початку своєї діяльності локальні мережі здійснювали обмін міжмашинною і міжпроцесорною інформацією, то на наступних стадіях свого розвитку вони дозволяють передавати, в доповненні до цього, текстову, цифрову, графічну і мовну інформацію. Завдяки цьому почали з'являтися центри машинної обробки ділової (документальної) інформації – наказів, звітів, відомостей, калькуляцій, рахунків, листів і т.д. Такі центри об'єднали певну кількість автоматизованих робочих місць і стали новим етапом на шляху створення в майбутньому безпаперових технологій для застосування в керівних, фінансових, облікових та інших підрозділах. Це дозволило відмовитись від громіздких, незручних і трудомістких карткових каталогів, конторських і бухгалтерських книг та іншого, замінивши їх компактними і зручними комп'ютерними носіями інформації – магнітними і оптичними дисками, магнітними стрічками і т.д. У разі необхідності можна легко отримати копію документа на паперовому носії.

2.4 Види класифікацій локальних обчислювальних мереж

Широка і постійно зростаюча номенклатура локальних обчислювальних мереж, мережні програмні продукти і технології покладають на потенційного користувача складну задачу вибору потрібної системи з великої кількості існуючих. Сьогодні в світі нараховується десятки тисяч різних локальних обчислювальних мереж і для їх розгляду корисно мати систему класифікації. Усталеної класифікації локальних мереж поки що не існує, але для них можна виявити певні класифікаційні ознаки за:

- призначенням;
- типом використовуваних ЕОМ (Електронна обчислювальна машина);
- організацією управління;
- організацією передачі інформації;
- топологією;
- методами теледоступу;
- фізичниими носіями сигналів;
- управлінням доступом до фізичного середовища передачі і т.і.

Розглянемо деякі з них.

Класифікація за призначенням. За призначенню локальні обчислювальні мережі можна розділити на: керуючі (організаційними, технологічними, адміністративними та іншими процесами), інформаційні (інформаційно-пошукові), розрахункові, інформаційно-розрахункові, обробки документальної інформації і так далі.

Класифікація за типом використовуваних в мережі ЕОМ. За типом використовуваних в мережі ЕОМ локальні мережі можна розділити на однорідні і неоднорідні. Прикладом однорідної локальної обчислювальної мережі може служити мережа DECNET, в яку входять ЕОМ тільки фірми DEC. Часто однорідні локальні обчислювальні мережі характеризуються і однотиповим складом абонентських засобів, наприклад, тільки комплексами машинної графіки або тільки дисплеями. Неоднорідні локальні обчислювальні мережі містять різні класи ЕОМ (мікро-, міні-, великі) і різні моделі всередині класів ЕОМ, а також різне абонентське обладнання.

Класифікація за організацією управління. За організацією управління однорідні локальні обчислювальні мережі в залежності від наявності (або відсутності) центральної абонентської системи діляться на дві групи. До першої групи відносяться мережі з централізованим управлінням. Для таких мереж характерні велика кількість службової інформації і пріоритетність під'єднаних до моноканалу станцій (по розміщенню або прийнятому пріоритету). В загальному випадку локальна обчислювальна мережа з централізованим управлінням (не обов'язково на основі моноканалу) має централізовану систему (ЕОМ), яка керує роботою мережі. Прикладний процес центральної системи організовує проведення сеансів, зв'язаних з передачею даних, здійснює діагностику мережі, веде статистику і облік роботи. В локальній обчислювальній мережі з моноканалом центральна система реалізовує, також, загальну ступінь захисту від конфліктів. При виході із ладу центральної системи вся локальна обчислювальна мережа зупиняє роботу. Мережі з централізованим управлінням відрізняється простотою забезпечення функцій взаємодії між ЕОМ в локальній мережі і, як правило, характеризуються тим, що більша частина інформаційно-обчислювальних ресурсів концентрується в центральній системі. Застосування локальної мережі з централізованим управлінням доцільне при невеликому числі абонентських систем. У тому випадку, коли інформаційно-обчислювальні ресурси локальної мережі рівномірно розподілені по великому числу абонентських систем, централізоване управління малопридатне, оскільки не забезпечує потрібну

надійність мережі і призводить до різкого збільшення службової (управлінської) інформації. В цьому випадку доцільно застосовувати локальні мережі з децентралізованим або розподіленим управлінням. В цих мережах всі функції управління розподілені між системами мережі. Однак, для проведення діагностики, збору статистики і проведення інших адміністративних функцій, в мережі використовується спеціально виділена абонентська система або прикладний процес в такій системі. В децентралізованих локальних обчислювальних мережах на основі моноканалу у порівнянні з централізованими ускладнюються проблеми захисту від конфліктів, для чого застосовуються багаточисленні тракти, що враховують суперечливі вимоги надійності і максимального завантаження моноканалу. Одна із найрозповсюдженіших децентралізованих форм управління передбачає два рівні захисту від конфліктів. На першому рівні сконцентровані функції, що визначають активність моноканалу і блокування передачі у випадку виявлення будь-якої активності. На другому рівні виконуються складніші функції аналізу системних затримок, які управляють моментами початку передачі інформації якійсь із підсистем локальної мережі.

Класифікація за формуванням передачі інформації. По формуванню передачі інформації локальні мережі поділяються на мережі з маршрутизацією інформації і селекцією інформації. Взаємодія абонентських систем з маршрутизацією інформації забезпечується визначенням шляхів передачі блоків даних по адресах їх призначення. Цей процес виконується всіма комунікаційними системами, що знаходяться в мережі. При цьому абонентські системи можуть взаємодіяти по різних шляхах (маршрутах) передачі блоків даних, а для скорочення часу передачі здійснюється пошук найкоротшого по часу маршруту.

В мережах з селекцією інформації взаємодія абонентських систем проводиться вибором (селекцією) адресованих їм блоків даних. При цьому всім абонентським системам доступні всі блоки даних, що передаються в мережі. Як правило, це пов’язано з тим, що локальна мережа з селекцією інформації, будується на основі моноканалу.

Класифікація за топологією мережі (порівняльна таблиця можливостей). Топологія, тобто конфігурація з’єднання елементів в локальних мережах, притягує до себе увагу більше, ніж інші характеристики мережі. Це пов’язано з тим, що саме топологія багато в чому визначає основні властивості мережі, наприклад, такі, як надійність (живучість), продуктивність та інші. Механізм передачі даних,

допустимий в тій чи іншій локальній мережі, багато в чому визначається топологією мережі. По топологічних ознаках локальні мережі поділяються на мережі з довільною, кільцевою, деревовидною конфігурацією, мережі типу «загальна шина» (моноканал), «зірка» та ін. (рис. 2.2 – 2.4).

Таблиця 2.1 – Порівняльні характеристики топології обчислювальних мереж

Характеристики	Топологія		
	Зірка	Кільце	Шина
Вартість розширення	Незначна	Середня	Середня
Необхідність виключення при розширенні	Ні	Так	Ні
Під'єднання абонентів	Пасивне	Активне	Пасивне
Захист при відмовах	Незначний	Незначний	Висока
Розміри системи	Будь-які	Будь-які	Обмежені
Контроль помилок	Простий	Простий	Ускладнений
Захищеність від прослуховування	Добра	Добра	Незначна
Вартість під'єднання	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороша	Задовільна	Погана
Можливість роботи в реальному	Дуже хороша	Хороша	Погана
режимі часу			
Розводка кабелю	Добра	Задовільна	Добра
Планові витрати	Незначні	Середні	Незначні
Обслуговування	Дуже хороше	Середнє	Середнє
Характер відмови	Повна	Повна	Часткова

Зіркоподібна топологія передбачає з'єднання каналів приєднаних до різних абонентів в одній точці, яка називається центральним вузлом.

Кільцева топологія передбачає послідовне з'єднання абонентів з каналами передачі даних, внаслідок чого утворюється замкнуте кільце. Кожен абонент відіграє роль ретранслятора повідомлення з невеликою часовою затримкою.

Магістральна (шинна) топологія реалізується у вигляді пасивного моноканалу (магістралі). Ця топологія найпоширеніша. Вона використовується у випадку, коли інформація передається рідко (в порівнянні з можливостями комп'ютерів), дані комплектуються в пакет, дістають адресу і після того, як магістраль стане доступною, відбувається передача повідомлення.

Існують інші підходи до класифікації топології локальних мереж. Згідно одного з них конфігурації локальних мереж ділять на два основні класи – широкотрансляційні і послідовні. В широкотрансляційних конфігураціях кожний персональний комп'ютер передає сигнали, які можуть бути сприйняті всіма іншими персональними комп'ютерами. До таких конфігурацій відносяться загальна шина, дерево, зірка з пасивним центром. В послідовних конфігураціях кожен фізичний підрівень передає інформацію тільки одному персональному комп'ютеру. **Широкотрансляційні конфігурації** – це, як правило, локальна мережа з селекцією інформації, а послідовні – локальні мережі з маршрутизацією інформації.

Класифікація мереж по методах теледоступу. Крім топології локальної мережі процес передачі даних багато в чому визначається програмним забезпеченням ЕОМ абонентських систем, в основному їх операційними системами, оскільки кожна з них підтримує відповідний метод теледоступу зі сторони терміналів. Моноканал розглядається також, як один із терміналів, тому дуже важливо знати, наскільки розрізняються операційні системи і методи теледоступу всіх абонентських комплексів, під'єднаних до мережі. Розрізняють локальні мережі з єдиною операційною підтримкою і єдиними методами теледоступу, орієнтованими на локальні мережі, і локальні мережі з різними фізичними носіями сигналів. Тип носія визначає основні властивості пристрою обміну сигналами, який під'єднується до фізичного середовища передачі. Єдина операційна підтримка, що включає метод теледоступу, передбачена в однорідних локальних мережах. Складніше з локальними мережами, що використовують ЕОМ різних класів і моделей, наприклад міні-ЕОМ і великі обчислювальні машини. Методи теледоступу підтримують багаторівневі системи інтерфейсів. Розрізняють багаторівневі (модель відкритих систем) і двохрівневі локальні обчислювальні мережі. До двохрівневих відносяться закриті термінальні комплекси із стандартними методами теледоступу (базисний телекомунікаційний метод доступу).

Класифікація мереж за методом управління середовищем передачі даних. Важливою класифікаційною ознакою локальної обчислювальної мережі є метод управління середовищем передачі даних. У локальній обчислювальній мережі з моноканалом можна виділити два методи доступу до моноканалу: детермінований і імовірнісний. До першої групи відносяться: метод вставки реєстру, метод циклічного опиту, централізований і децентралізований маркерний метод і інші.

До другої групи (імовірнісні методи доступу) – методи прослуховування моноканалу на початок передачі, з прогнозуванням, зіткненням та деякі інші.

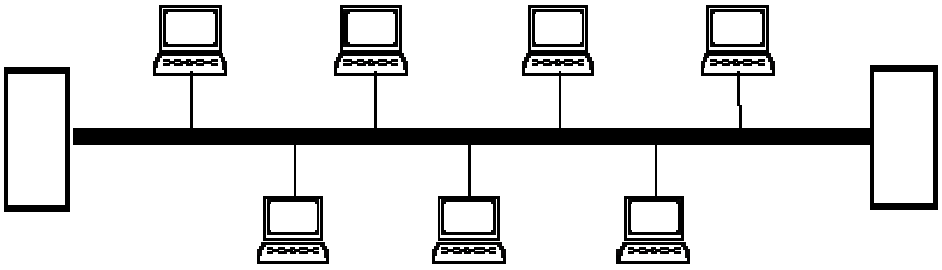


Рисунок 2.2 – Магістральне з’єднання (шинна топологія)

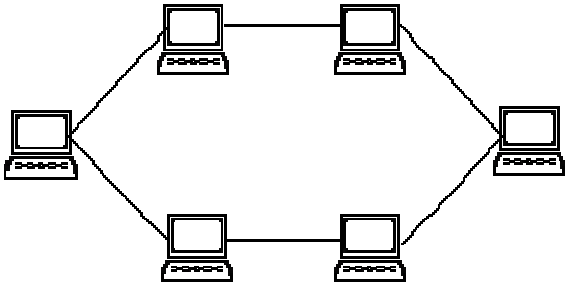


Рисунок 2.3 – Кільцеве з’єднання

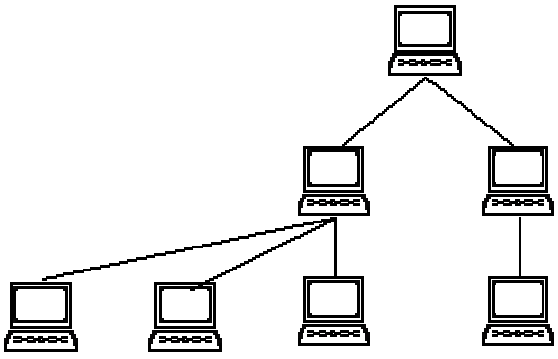


Рисунок 2.4 – Ієрархічне з’єднання

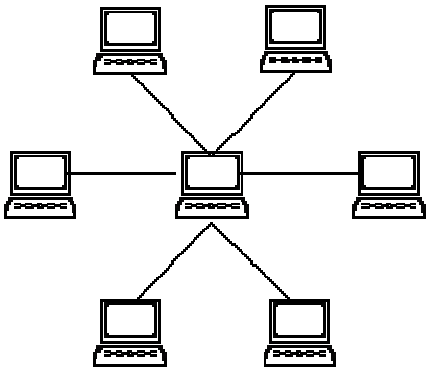


Рисунок 2.5 – З’єднання типу зірка.

3 МЕРЕЖНІ АРХІТЕКТУРНІ РІШЕННЯ

3.1 Функції, узагальнена структура і класифікація мереж

3.1.1 Визначення і функції

Під архітектурою будемо розуміти сукупність принципів і правил у відповідності з якими будуються обчислювальні системи різних видів. Розглядаючи питання архітектури комп'ютерних мереж (КМ), насамперед, необхідно визначити їх призначення та область застосування. Так *основним призначенням* комп'ютерної мережі є надання великому числу користувачів одночасного доступу до її обчислювальних ресурсів. Виходячи з цього, *комп'ютерна мережа може бути визначена як система розподіленої обробки інформації, що складається з комп'ютерів, територіально-розосереджених і взаємодіючих між собою за допомогою засобів зв'язку*. Комп'ютери, що входять до складу мережі, виконують досить широке коло функцій, основними серед яких є:

- організація доступу до мережі;
- управління передачею інформації;
- надання обчислювальних ресурсів і послуг абонентам мережі.

Відповідно до цього по функціональній ознаці всю безліч систем КМ можна розділити на абонентські, комутаційні і головні (Host) підсистеми.

Абонентська підсистема являє собою комп'ютер, орієнтований на роботу в складі КМ і забезпечує користувачам доступ до її обчислювальних ресурсів.

Комутаційні підсистеми є вузлами комутації мережі передачі даних і забезпечують організацію складових каналів передачі даних між абонентським підсистемами. Як керуючі елементи вузлів комутації використовуються процесори телеобробки або спеціальні комутаційні (мережеві) процесори.

Великою різноманітністю характеризуються Host підсистеми або мережеві сервери. **Сервером** прийнято називати спеціальний комп'ютер, що виконує основні сервісні функції, такі як: управління мережею, збір, обробку, зберігання і надання інформації абонентам КМ. У зв'язку з великим числом сервісних функцій доцільне розділення серверів за їх функціональним призначенням. Наприклад, **файл-сервер** визначається як мережевий комп'ютер, що здійснює операції по зберіганню, обробці і наданню файлів даних абонентам КМ. У свою чергу, комп'ютер, що забезпечує абонентським системам ефективний доступ до КМ, отримав назву **сервер доступу** і т.д.

3.1.2 Узагальнена структура

На основі вищесказаного структуру КМ можна показати у вигляді, представленому на рисунку 3.1.

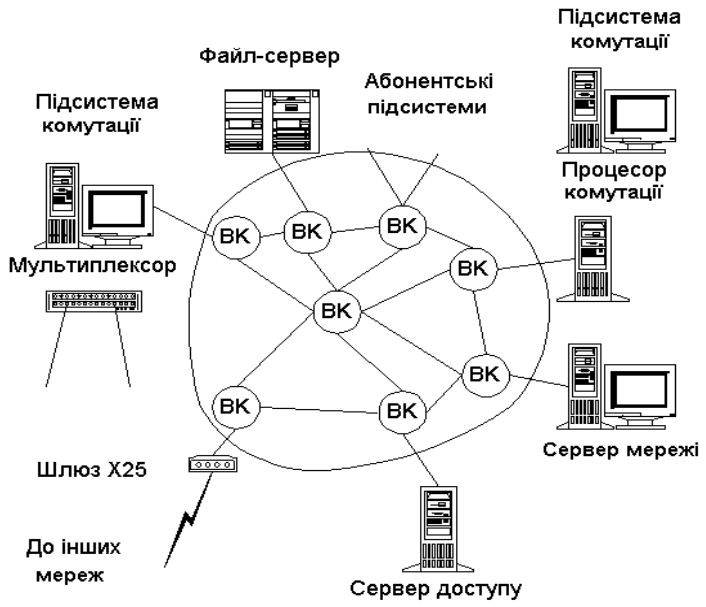


Рисунок 3.1 – Узагальнена структура КМ

3.2 Класифікація комп’ютерних мереж

В залежності від основної класифікаційної ознаки покриття території всі КМ поділяють на групи:

- локальні (Local Area Network);
- глобальні (Wide Area Network);
- регіональні (Metropolitain Area Network);
- корпоративні КМ.

Локальні КМ за покриттям території є найменшими з перелічених. Найчастіше вони займають простір протяжністю в кілька кілометрів і поєднують *абонентські підсистеми* розташовані в кількох приміщенням чи корпусах. Прикладом такої мережі може бути локальна мережа ІКІТ, інших структурних підрозділів Академії народного господарства.

Глобальні КМ за покриттям є найбільшими і розташовуються на одного чи навіть кількох континентів. Такі мережі об’єднують між собою як окремі *абонентські підсистеми*, так локальні мережі. Приклад – всесвітня мережа Internet.

Регіональні КМ покривають територію міста, регіону, країни. Приклад – українська глобальна мережа URAN.

Останнім часом швидкими темпами розвиваються корпоративні КМ. Вони поєднують розрізнені локальні мережі підрозділів підприємств та корпорацій, навчальних закладів. Приклад – проект корпоративної КМ ТАНГ.

3.3 Еталонна модель взаємодії відкритих систем

Еталонна модель взаємодії відкритих систем, або модель зв'язку відкритих систем, або Open System Interconnection (OSI) — семирівнева логічна модель роботи КМ. Модель OSI являє собою групу протоколів чи правил зв'язку, організованих у сім рівнів (рис. 3.2). Ці рівні пов'язують прикладні процеси, розміщені на верхньому рівні, з фізичним середовищем передавання, що розташоване на нижчому рівні. Кожен рівень OSI виконує визначену функцію по передачі даних і базується на основі нижчого рівня. Хоча вони повинні працювати в строгій черговості, але кожний з рівнів допускає кілька варіантів. Перші три рівні OSI — фізичний, канальний, мережний відносяться до передачі і

маршрутизації даних. Четвертий, транспортний рівень забезпечує зв'язок між першими трьома і вищими рівнями. Останні три рівні — сеансовий, представницький і прикладний, обслуговують користувацькі додатки.

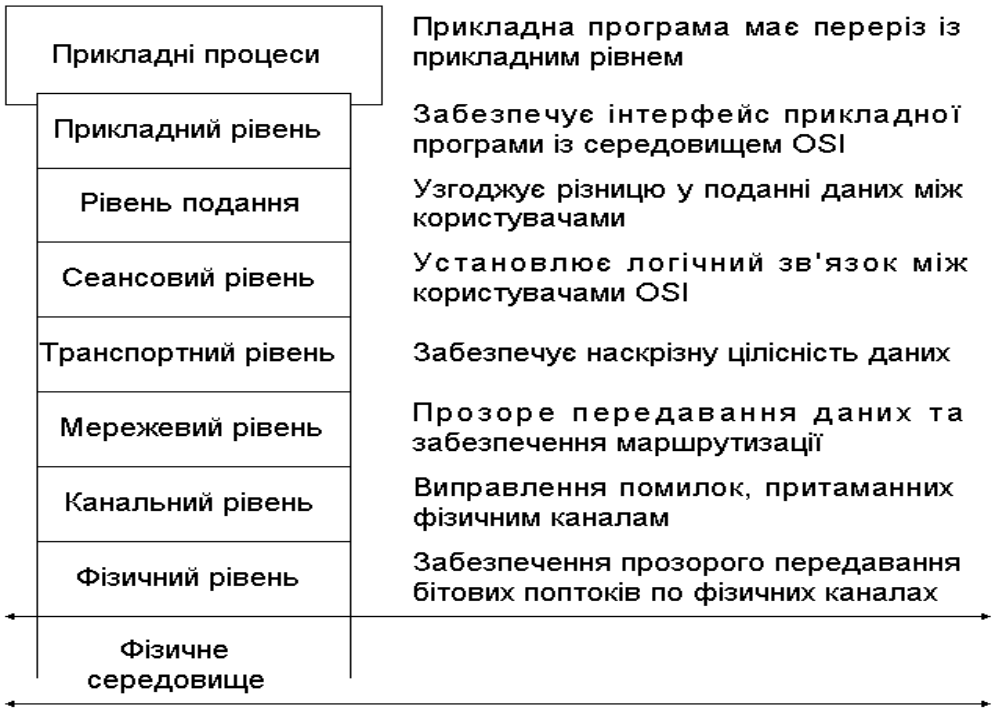


Рисунок 3.2 – Основні функції рівнів КМ

Нульовий рівень – фізичне середовище передавання КМ. Під фізичним середовищем передавання інформації у КМ розуміють усі існуючі засоби (носії сигналу):

- багатожильні кабелі;
- звійні пари проводів;
- бі- та триаксіальні і силові кабелі;
- волоконно-оптичний кабель;
- телефонні кабелі;
- коаксіальні кабелі;
- радіоканали;
- супутникові, телеметричні канали.

Перший рівень – фізичний рівень КМ визначає межу між фізичним середовищем (лінією зв'язку) та канальним рівнем. Еталонна модель КМ фізичний рівень визначає так: “Фізичний рівень забезпечує механічні, електричні, функціональні та процедурні способи активації, підтримки та деактивації фізичних з'єднань при побітовому передаванні між канальними об'єктами”. Для КМ фізичний рівень забезпечує інтерфейс між ПК, що бере (беруть) участь у взаємодії, та середовищем передавання дискретних сигналів. Фізичний рівень через інтерфейс керує потоком даних.

Другий рівень – канальний рівень відкритих КМ формує з даних, що передаються на фізичному рівні, так звані кадри або послідовності кадрів. На цьому рівні здійснюється також керування доступом до середовища передачі даних, яке використовується кількома ПК.

Канальний рівень КМ долає обмеження, властиві фізичним ланцюгам, а також визначає та по змозі усуває помилки, що їх допущено у процесі передавання даних за рахунок замаскованих недоліків якості передавання. Канальний рівень дає змогу мережному рівню регулювати взаємозв'язки комунікацій у фізичних середовищах (у середині фізичного рівня).

Третій рівень – мережний рівень відкритих КМ реалізує додаткові функції маршрутизації для того, щоб “кадри” канального рівня були прозорі (доступні) для різноманітного мережного обладнання, засобів передавання та доступу.

Четвертий рівень – транспортний рівень відкритих КМ відповідає за прозоре передавання інформації надійним та економічно вигідним способом між об'єктами (ПК) сеансового рівня. Транспортний рівень звільняє об'єкти сеансового рівня від проблем реального транспортування даних. Він також оптимізує послуги мережі з метою досягнення мінімального рівня вартості експлуатаційних характеристик та відповідає за цілісність даних, що передаються в мережі. Функції транспортного рівня містять наскрізне послідовне керування, наскрізне керування потоком, знаходження та виправлення помилок, поточний контроль якості послуг.

П'ятий рівень – сеансовий рівень відкритих КМ відповідає за взаємодію та підтримку діалогу між процесами певного типу. Логічна асоціація (взаємодія та підтримка діалогу між процесами певного типу) називається сеансом. Для КМ може бути передбачено кілька різних сеансових рівнів і відповідно кілька протоколів для процесів різних типів, наприклад передавання усної мови у

цифровому коді та інтерактивні обчислення. Для того щоб взаємодіяли два та більше процесів, має бути встановлена логічна асоціація між цими процесами. Отже, сеансовий рівень є відповідальним за встановлення та припинення сеансу, а також за керування діалогом під час цього сеансу.

Шостий рівень – рівень подання (представлення) даних у відкритих КМ відповідає за сумісність подання даних між прикладними процесами, що взаємодіють, такими як формати даних (екрани дисплеїв або виводи принтера), коди та символи перетворень. Рівень здійснює також перетворення представлення інформації, що передається між відкритими системами.

Сьомий рівень – прикладний рівень забезпечує прикладним програмам (або за термінологією OSI — прикладним процесам) доступ до середовища OSI. Цей рівень – єдиний, що забезпечує послуги безпосередньо прикладній програмі.

Діапазон функцій, які потенційно забезпечуються прикладним рівнем, є різноманітним. Як найвищий рівень у моделі КМ, прикладний рівень не має інтерфейсу з рівнем, розміщеним вище.

3.4 Базові мережні топології

Геометрична форма плоскої проекції середовища передавання називається топологією (конфігурацією) КМ. Залежно від способу поєднання фізичних компонентів у КМ можуть використовуватися такі топології:

- топологія зірки (Star topology);
- кільцева топологія (Ring network);
- шинна топологія (Bus topology);
- ієрархічна топологія (Clusters topology).

Архітектуру КМ, в якій усі вузли мережі сполучені з одним центральним вузлом, називають топологією зірки. Мережа з топологією зірки одна з найпоширеніших КМ. У мережах такого типу (рис 3.3) вузол А, як правило, відповідає за маршрутизацію трафіка через себе до інших компонентів, а також відповідає за локалізацію несправностей. До позитивних властивостей мережі з топологією зірки можна віднести такі:

- можливість керування;
- достатньо просте програмне забезпечення;

- легкість простий потік трафіка;
- швидкого пошуку помилок;
- відносну простоту та незначні витрати при потребі нарощування мереж.

Ця топологія має і ряд недоліків: виникнення «вузьких місць» у разі, коли трафіком керує пристрій, що розміщений на найвищому рівні.

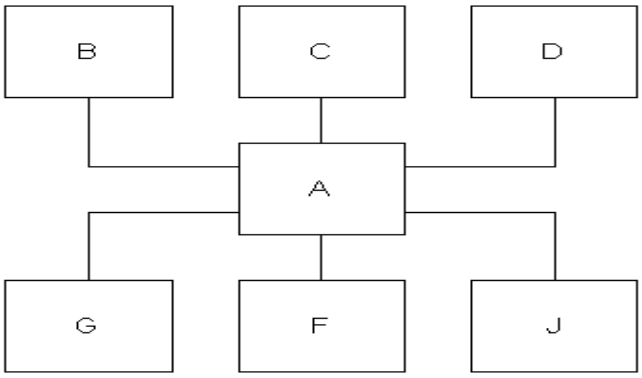


Рисунок 3.3 – КМ з топологією зірки

У мережі з кільцевою топологією (рис. 3.4) вузол дістає повідомлення від одного зі своїх сусідів і далі або обробляє його сам, або ретранслює іншому сусідові, причому дані поширюються колом і здебільшого лише в одному напрямі.

До позитивних властивостей мережі з кільцевою топологією можна віднести такі: нечасті перевантаження, притаманні ієрархічній або зіркоподібній топології; логічна організація кільцевої мережі є відносно простою. Ця топологія має недолік, що полягає в наявності одного каналу, який поєднує всі компоненти в кільце. Якщо відмовляє канал між двома вузлами, настає відказ усієї мережі.

Для усунення зазначеної ситуації необхідно зарезервувати канал або застосувати перемикачі для обходу вузлів, що відмовили.

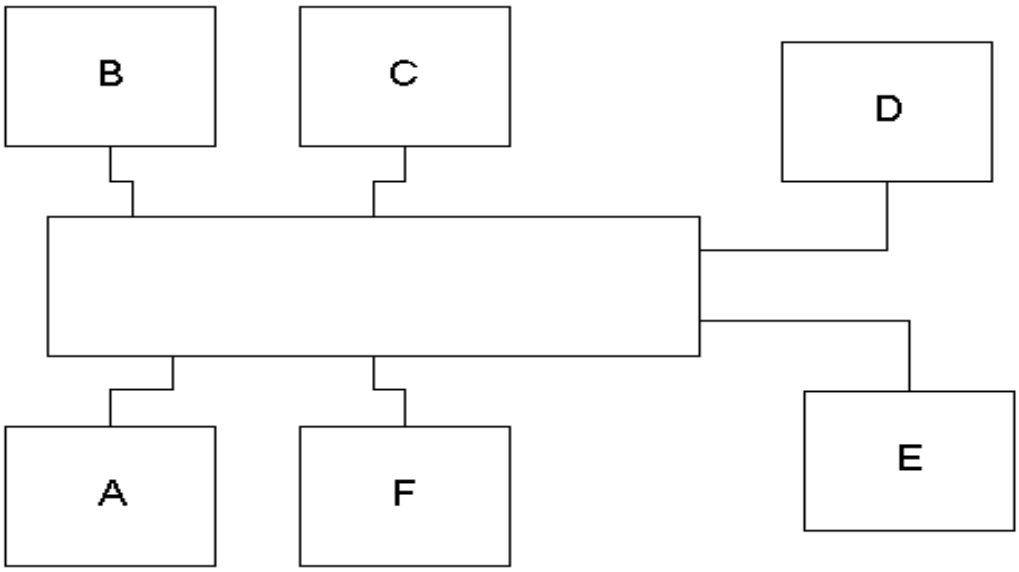


Рисунок 3.4 – КМ з кільцевою топологією

Архітектуру КМ, при якій усі вузли підімкнені до спільного лінійного інформаційного каналу, називають шинною топологією(рис. 3.5), мережі із шинною топологією є досить популярними. Шина дозволяє, щоб кожне повідомлення приймалось усіма станціями. Відповідно в момент передавання працює одна-єдина станція у широкомовному режимі на кілька станцій.

Серед позитивних характеристик мережі із шинною топологією можна назвати такі:

- відносно просте керування трафіком між підімкненими пристроями;
- легше додати абонента до “шини”, ніж до зірки та кільця, яке має бути розірваним;
- більша надійність, оскільки на функціонування справних вузлів зможуть впливати несправні вузли або тракти, що поєднують їх через шину.

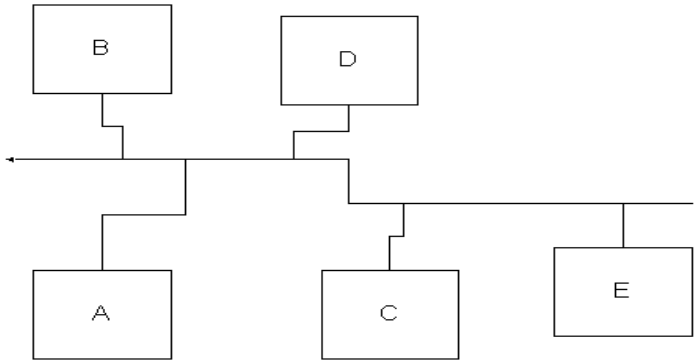


Рисунок 3.5 – КМ з шинною топологією

Шинна топологія має й окремі недоліки, а саме:

- наявність одного каналу, що поєднує всі компоненти. Якщо відмовив канал між двома вузлами, настає відказ усієї мережі. Для усунення такої ситуації необхідно зарезервувати канал або застосувати перемикачі для об ду вузлів, що відмовили;
- трудність локалізації відказів із точністю до окремої компоненти, яку підімкнено до шини. Це зумовлюється відсутністю точок концентрації, через що проблема розрізнення несправностей стає важко розв'язуваною.

Ієрархічною називають топологію КМ, при якій вузли об'єднують в групи (кластери) зі спільним контролером (рис. 3.6), причому правила взаємодії між вузлами всередині одного кластера та між вузлами різних кластерів різні. Мережі із ієрархічною топологією мають відносно просте програмне забезпечення. Здебільшого мережею керує пристрій який має найвищий пріоритет, і він же ініціює поширення трафіка в мережі. Такий підхід забезпечує своєрідну точку концентрації для керування діагностування помилок.

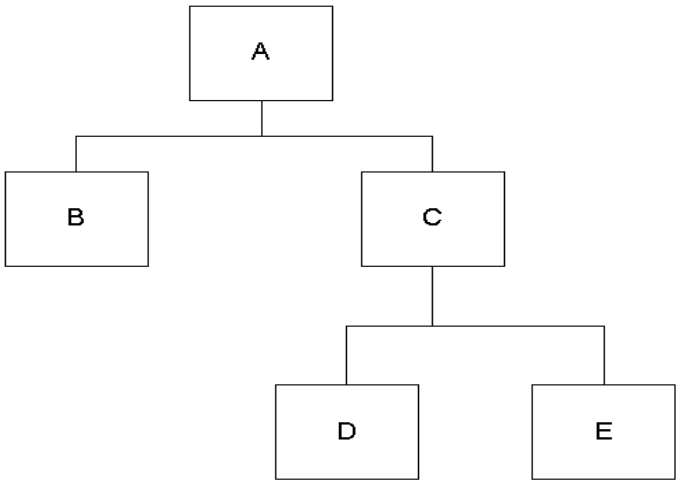


Рисунок 3.6 – КМ з ієрархічною топологією

Часто в КМ з ієрархічною топологією застосовується метод побудови супідрядних ієрархічних структур. У супідрядних ієрархічних структурах пристрій, розміщений вище за ієрархів забезпечує безпосереднє керування пристроями, що в ієрархії містяться нижче. Це зменшує навантаження на центральний пристрій, наприклад вузол А. У мережах з ієрархічною топологією є можливість поступової еволюції (нарощування) пристроїв мережі в напрямку складнішої структури КМ.

Позитивними властивостями мережі з ієрархічною топологією є такі:

- відносна простота програмного забезпечення; можливість швидкого пошуку помилок;
- відносна простота і незначні витрати у разі потреби нарощування мережі.

Ця топологія має й деякі недоліки:

- виникнення “вузьких місць” в разі, коли трафіком керує пристрій, розташований найвище;
- мала надійність за відсутності технічного резервування; часте виникнення конфліктних ситуацій, пов'язаних із втратою інформації за напрямами «згори — донизу» та «знизу — угору».

На практиці деколи застосовують гібридні технології. До них можна віднести, наприклад, коміркову топологію, топологію сніжинка і т. ін. Коміркова топологія (рис. 3.7) знайшла застосування лише останніми роками, і тому недостатньо досліджена у практиці, її привабливість полягає у відносній стійкості до перевантажень та відказів. Завдяки множинності шляхів, створюваних з компонентів мережі, трафік може бути напрямлений в обхід вузлів, які відмовили або зайняті. Незважаючи на те, що такий підхід характеризується складністю та високою вартістю (протоколи є порівняно складними з погляду логіки роботи), численні користувачі надають перевагу комірковим мережам як надійнішим за мережі інших типів.

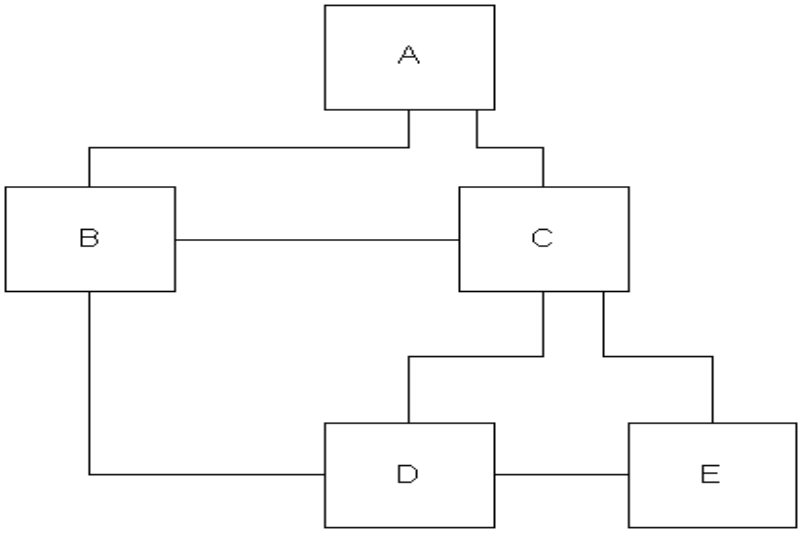


Рисунок 3.7 – КМ з комірковою топологією

ЗМІСТОВИЙ МОДУЛЬ 2. РОЗРОБКА ТА АНАЛІЗ ЕФЕКТИВНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

4 ПРОТОКОЛИ НИЖНЬОГО РІВНЯ ВЕЛИКИХ МЕРЕЖ

На сучасному етапі канальний рівень протоколу розділяють на два підрівні:

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

Перший забезпечує керування логічним каналом і не залежить від фізичного середовища, а другий – доступ до фізичних з`єднань і залежить від них.

4.1 Стандартні реалізації багатопротокольних мереж на канальному рівні

На початку розвитку локальних мереж у кожній окремій мережі можна було передавати кадри тільки одного формату. З часом, коли комп`ютерні мережі стали достатньо складними і об`єднують значну кількість локальних мереж з різними форматами кадрів, виникла потреба реалізувати можливості одночасного передавання мережею кадрів різних форматів.
Для цього на кожному комп`ютері до адаптера додають спеціальну програму керування – драйвер, яка завантажується резидентно в пам`ять. Сьогодні є три підходи до організації взаємодії драйверів адаптерів з ПЗ, яке реалізує протокольні функції.

- У 1989 році Microsoft та 3COM розробили специфікацію NDIS(Network Device Interface Specification), яка регламентує спосіб роботи мережевого адаптера з декількома протоколами. Використовується у таких системах як LAN manager, Windows for Workgroups,Windows 9x, Windows NT, Lantastic,Pathworks. Існують реалізації NDIS як для 16-бітових систем(NDIS 2.0) так і для 32-бітових(NDIS 3.0).
- Фірма Nowell розробила та використовує ODI(Open Datalink Interface), що організований подібно до NDIS, але з іншим програмним інтерфейсом.
- Для мереж TCP/IP є компактні драйвери, розроблені фірмою FTP Software відповідно до специфікації PDS(Packet Driver Specification).

4.2 Протоколи керування доступом

Розглянемо найнижчий підрівень канального рівня протоколу – підрівень керування доступом до фізичного середовища. Головною функцією цього підрівня є забезпечення доступу окремих станцій до передавального середовища так, щоб перепускна здатність каналу зв`язку використовувалася ефективно.

Спосіб організації доступу станції мережі до передавального середовища називається методом доступу. Є велика кількість методів доступу. Вони різняться:

характером фізичного середовища – методи доступу для моноканалу та мереж з ретрансляцією;

характером керування – з централізованим та децентралізованим керуванням;

характером доступу – конкурентні або з передаванням повноважень.

Розглянемо деякі методи доступу.

4.2.1 Тактові системи

Основним принципом організації тактових систем(slotted systems) є циклічний розподіл усього часу передавання на однакові часові проміжки - такти.За кожною станцією закріплено відповідний слот. Тактові системи мають наступні недоліки:

- неефективність використання каналу. Внаслідок нерівномірності навантаження з`являється багато порожніх слотів. Вислідна швидкість передавання невисока;
- зі збільшенням кількості станцій ефективність мережі зменшується.Тому тактові системи не використовуються у великих мережах.

4.2.2 Метод опитування. Централізоване керування

Метод опитування використовують у шинних або ефірних мережах (polled networks). У цьому випадку один з приєднаних до мережі пристроїв вважається головним і називається контроллером мережі. Він керує передаванням. Найпростіший варіант централізованого керування реалізується на базі циклічного опитування. Контроллер по черзі опитує (надсилає кадри) приєднані пристрої. Вони відповідають, надсилаючи в мережу або інформацію, або спеціальний кадр, якщо інформації нема. Контролер після одержання кадру опитує наступний пристрій і т.д. У такій шині об`єднано два потоки: інформаційний і керування.

Мережі з опитуванням, зазвичай, невеликі. Їх використовують у лабораторному, аеро-космічному,побутовому і військовому обладнанні. Недоліки цих мереж такі:

- наявність великого потоку керування, навіть якщо в абонента нема інформації для передавання. Однак водночас постійно контролюється працездатність пристроїв;
- надійність мережі визначається надійністю контролера. Якщо він вийде з ладу, то вийде з ладу вся мережа;
- мережа обмежена щодо кількості абонентів. Чим більше абонентів, тим більше потрібно часу для опитування, отже тим менша перепускна здатність.

Прикладом мережі з опитуванням є мережа стандарту MIL 1553B.

4.3 Особливості функціонування мережі стандарту MIL 1553B

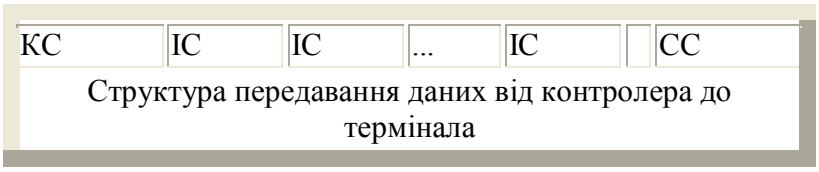
Стандарт мережі MIL 1553B розроблено для ВПС США як основу передавання даних у військових літальних апаратах. Пізніше його скопіювали у стандарт ГОСТВ 24.394-80 для радянських військових літаків. Мережа, згідно з цим стандартом, характеризується високою пропускною здатністю, надійністю, незначною чутливістю до завад. Бортова система забезпечує обмін даними між різними автономними підсистемами, що розміщені в різних частинах літака. Такі підсистеми призначені для розв`язування задач обчислювального типу, збирання та первинного опрацювання інформації від давачів.

З`єднання:двопроводова інформаційна магістраль у вигляді екранованої скрученої пари. Станцію мережі приєднують за допомогою адаптера. Адаптер складається з розв`язувального трансформатора, приймача-передавача, генератора тактових імпульсів, шифратора-дешифратора. Шифратор-дешифратор виконує основні функції перетворення даних, а саме: кодування-декодування даних у коді Манчестер II, перетворення з паралельного коду в послідовний і навпаки, контроль достовірності прийнятого слова, декодування адреси термінала та ін.Слова формує термінал.

Передаванням даних керує одна з підсистем – контролер. Обмін даними відбувається асинхронно в напівдуплексному режимі. На початку слова є спеціальний синхронізаційний символ. У кінці слова є один розряд для перевірки слова на парність. Дані передаються в послідовному коді зі швидкіст 1 Мбіт/с і до

47 тисяч інформаційних слів за секунду. Довхина магістралі не перевищує 100 м. Ймовірність появи помилки під час передавання слова не більше 10^-7.

У випадку передавання даних від контролера до термінала контролер передає командне слово, в якому зазначено адресу термінала, вимогу виконати операцію приймання даних і кількість інформаційних слів. Далі відбувається передавання інформаційних слів. Потім контролер чекає від терміналу слово стану, яке підтверджує , що збоїв нема.



Структура передавання даних від контролера до термінала

Передавання даних від термінала до контролера відбувається так. Контролер ініціює обмін передаванням командного слова, у якому є вимога виконати операцію передавання даних, адреса термінала, кількість інформаційних слів. Термінал, який бере участь в обміні, відповідає контролеру словом стану, після чого починає передавати задану кількість інформаційних слів.

Структура передавання даних від термінала до контролера

У випадку передавання даних між двома терміналами контролер передає магістраллю два командні слова. У першому з них зазначено адресу термінала, який повинен прийняти дані, вимогу виконати операцію приймання, кількість інформаційних слів, у другому – адресу термінала, який передає дані, вимогу виконати операцію передавання, кількість інформаційних слів. Закінчується обмін тим, що термінал-приймач пересилає слово стану для контролера.

Структура передавання даних від термінала до термінала

Можна також організувати передачу даних усім терміналам відразу. У цьому випадку контролер передає в магістраль слово з фіксованою адресою, яку розпізнають усі термінали.

Стандарт допускає передавання в одному повідомленні до 32 інформаційних слів, а також команд без інформаційних слів. Є три типи слів: командне, інформаційне, стану. У слові будь-якого типу є 20 розрядів : 16 інформаційних, 1 контрольний, 3 для синхронізації .

4.4 Методи конкурентного доступу

У мережах з централізованим керуванням та маркерних мережах станція повинна чекати, щоб одержати дозвіл на передавання. Крім того, багато часу витрачається на передавання службової інформації. Розробники методів конкурентного доступу вирішили дати змогу будя-якійстанції передавати інформацію тоді, коли їй буде потрібно, а також спробували мінімізувати наслідки неминучих у такому випадку колізій. Вони ставили собі за мету забезпечити мінімум службової інформації та максимальну швидкість доступу до каналу зв`язку.

Методи конкурентного доступу (їх ще називають методами доступу з суперництвом) діють, як звичайно у моноканалі. Вперше такий підхід застосовано під час розробки мережі для університету штату Гаваї (система ALOHA). У цій системі середовищем передавання був радіоканал. Кожна станція , яка мала кадр для передавання, передавала його. Однак у випадку, коли передавачів, що працювали одночасно, було багато, то деякі станції передавали кадри також одночасно, отже передавання накладалися. Виникали колізії. Тому мережа Aloha була ефективною тільки тоді, коли інтенсивність надходження кадрів для передавання була малою. Реальна перепускна здатність мережі досягала 19% від максимальної.

Найбільшого поширення методи конкурентного доступу набули у шинних мережах. Власне в них було вперше використано принцип "слухай перш ніж говорити" – контроль сигналу носія, тобто прослуховування каналу. У таких мережах станція постійно прослуховує канал. Якщо канал вільний, станція починвє передавання, якщо ж зайнятий – чекає. Цей метод називається методом доступу з контролем сигналу носія (МДКН) (Carrier Sense Multiple Access (CSMA)). Однак виявилось що тут також можливі колізії. Максимальна ефективність цього методу становить 53%.

Найбільшої ефективності (93%) вдалося досягти за допомогою методу доступу МДКН/ВК (Carrier Sense Multiple Access with Collision Detection

(CSMA/CD)). У цьому випадку час очікування на передавання після вивільнення каналу вибирається випадково з використанням давача випадкових чисел. Таким чином зменшується ймовірність взаємного блокування повторних передавань станцій.

Станція постійно прослуховує середовище передаванняй аналізує адреси всіх кадрів, що передаються. Якщо кадр адресовано цій станції, то вона його приймає, а потім знову прослуховує середовище. У випадку, коли від протоколу верхнього рівня надійшов запит на передавання кадру, то станція його передає відразу, якщо середовище передавання вільне, або чекає поки воно вивільниться. Якщо передавання закінчилось нормально, то станція прослуховує середовище. Якщо ж виявлена колізія, то станція визначає випадковий інтервал затримки і знову очікує вивільнення середовища.

Перевагою МДКН/ВК є висока ефективність, а також те, що тут немає службової інформації. Недоліки методу: мережа з МДКН/ВК ефективна, якщо навантаження мале; зі збільшенням навантаження вплив колізій збільшується. У мережі МДКН/ВК не можна гарантувати тривалості передавання кадру.

Прикладом мережі з МДКН/ВК є ЛМ Ethernet.

4.5 Маркерні методи доступу

Маркерний метод доступу (token passing) полягає в тому, що мережу вводять спеціальний кадр – маркер, який переходить від станції до станції почергово. Як звичайно, це залежить від адреси станції (за зростанням або спаданням її номера). Остання станція передає маркер першій і так виникає логічне кільце. Станція, яка в конкретний момент часу має маркер, одержує право на передавання.

Маркерний метод доступу означено для мереж шинної, кільцевої, зірко- та деревоподібної конфігурацій, моноканалу і мереж з ретрансляцією. Його використовують у мережах Arcnet, Domain, Token Ring, Ringnet та ін.

4.5.1 Маркерний доступ у шинній мережі

Станція, що є в логічному кільці, постійно прослуховує шину і приймає адресований їй кадр. Якщо цей кадр маркерний, то станція у випадку наявності

інформації спочатку передає інформаційний кадр, а потім – маркерний, якщо ж інформації на передавання немає то тільки маркерний.

00000000	Адреса одержувача	Адреса відправника	Контрольна сума

Структура маркерного кадру

Використання логічного, а не фізичного кільця передбачає реалізацію таких функцій:

- відєднання станції від логічного кільця;
- приєднання станції до логічного кільця;
- зміна параметрів алгоритму (наприклад, максимальний час, протягом якого станція може утримувати маркер);
- втрата та дублювання маркерів;

Будь-яка станція може від`єднатися від логічного кільця в той момент, коли має маркер. Для цього вона надсилає попередній у логічному кільці станції кадр **Налагодження наступного вузла**, а опісля від`єднується.

00001000	Адреса одержувача	Адреса відправника	Нова адреса наступної станції	Контрольна сума

Структура кадру Налагодження наступного вузла

Зворотна операція, тобто приєднання, може відбуватися кількома способами. Перший спосіб такий. Кожна станція через n тактів запускає процедуру суперництва. На початку процедури вона передає кадр Шукання наступного вузла, в якому є вікно.Станції які бажають приєднатися до кільця, надсилають у вікні кадр Налагодження наступного вузла.

00000001	Адреса одержувача	Адреса відправника	Контрольна сума	Вікно

Структура маркерного кадру

Другий спосіб – це процедура реконфігурації. Станція, якій потрібно приєднатися до кільця, починає передавати збійну послідовність, що призведе до втрати маркера і реконфігурації мережі. Після збою всі станції перебувають у стані бездіяльності. Станція збуджується, коли закінчився тайм-аут або одержано маркер. Тривалість тайм-ауту пропорційна до номера станції, тому станція з

найменшим номером збудиться першою. Така станція є у стані опитування, тобто вона передає маркерні пакети станції з наступною за порядком адресою. Якщо через деякий час відповіді нема, маркер знову передається станції з наступною адресою і т.д. Попередня станція сприймає початок передавання маркерів як відповідь і переходить у режим нормальної роботи. Так триває доти, доки станція з найбільшим номером не перешле маркер першій станції, яка вже перебуває у стані нормальної роботи. Після цього маркер у першої станції і розпочинається нормальна робота мережі.

4.5.2 Мережа з ретрансляцією і передаванням маркера

Головна відмінність кільцевої мережі від шини-моноканалу полягає в тому, що у станціях кільцевої мережі інформацію приймають, аналізують і далі передають на сусідню станцію. Завдяки проміжному прийманню та передаванню кадрів у мережі з ретрансляцією сигнал у проміжній станції можна підсилити. Тому у кільцевих мережах довжина з`єднань не обмежена, на відміну від моноканальних мереж.

У кільцевій мережі маркер не має поля адреси. Натомість він може бути у двох станах – вільному та зайнятому. Якщо станції мережі не мають інформаційних кадрів то по мережі проходить вільний маркер. Станція, яка має інформацію для передавання чекає вільного маркера. Коли цей маркер надходить до неї, станція змінює його стан на зайнятий і додає ще інформаційний кадр. Зайнятий маркер переміщується кільцем. Змінити його стан на вільний може тільки та станція, яка його зайняла. Інформаційний кадр, доданий до маркера має у заголовку адресу призначення, яку станції, приймаючи та передаючи цей кадр, аналізують. Станція, якій цей кадр адресовано, передає його на вищий рівень, а крім того, повторює далі по мережі. Таким чином маркер з інформаційним кадром через деякий час знову потрапляє на станцію, яка його зайняла. У цьому випадку станція забирає кадр з мережі і вивільняє маркер. Якщо в шинній мережі якась станція від’єднується, то шина продовжує працювати. У кільцевій мережі від`єднання однієї станції виводить з ладу цілу мережу, тому потрібно вжити спеціальних закладів щодо збільшення її надійності. Зокрема, одним із способів зробити кільцеві мережі надійнішими є зірково-кільцева топологія або встановлення спеціальних реле, цо від`єднують станцію. Іншим способом може бути шунтування або введення другого, рівнобіжного кільця.

4.6 Метод доступу з запитом пріоритету

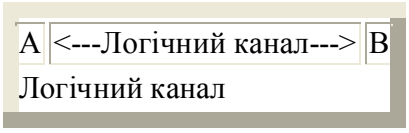
Метод доступу з запитом пріоритету (Demand Priority Protocol(DPP)) розроблено фірмами HP та AT&T і стандартизовано IEEE в 1995 році (стандарт IEEE-802.12). Його реалізовано у мережі 100VG Anylan.

Ця мережа має топологію розгалуженого дерева. Центром кожної зірки є комутатор, який має вхідні та вихідні порти. До вхідних портів приєднані пристрої нижніх рівнів дерева, які називаються вузлами. Вхідний порт приєднано до комутатора верхнього рівня. Комутатор періодично опитує свої вихідні порти про наявність інформації для передавання. Запит на передавання, який надходить від вузла, має рівень пріоритету. Нормальний пріоритет використовують для передавання файлів, а високий – відеоінформації, мовлення тощо. Якщо приєднаний до комутатора пристрій має кадр найвищого пріоритету, він передає його комутатору. Той аналізує адресну інформацію і передає кадр іншому вузлу або комутатору верхнього рівня.

Перевагою доступу з запитом пріоритету є відсутність колізій, можливість передавання різних типів даних (файлів, аудіо, відео), висока ефективність використання смуги пропускання при високих навантаженнях (95%).

4.7 Протоколи керування логічним каналом

Вишим підрівнем канального рівня протоколу взаємодії відкритих систем є LLC – підрівень керування логічною ланкою передавання (логічним каналом). Його функція – забезпечити правильне передавання даних між двома станціями (відправником інформації та її одержувачем) для довільного фізичного середовища передавання. У цьому випадку між об`єктами канального рівня налагоджується логічний канал.Увесь сервіс передавання забезпечує MAC-підрівень.



Розглянемо приклади протоколів керування логічним каналом та функцій, які вони виконують, а саме протоколи BSC(Byte Sequence Control), модемні протоколи та протокол HDLC (High-level Data Link Control).

4.8 Керування логічним каналом протоколу BSC

Протокол BSC розроблено фірмою IBM. Для керування та передавання цей протокол використовує символи стандартного коду ASCII. Передавання даних синхронне, напівдуплексне. Кадри бувають інформаційними та керування. Кадри керування повідомляють про початок та кінець сеансу, помилки під час передавання; інформаційні кадри переносять повідомлення. Символи керування коду ASCII, що використовуються у кадрах, такі:

Символи керування BSC					
SOH	1		ACK	6	^F
STX	2	^B	DLE	16	^P
ETX	3	^C	NAK	21	^U
EOT	4	^D	SYN	22	^V
ENQ	5	^E	ETB	23	^W

Структура кадрів протоколу BSC наступна:

SYN
SYN
Символи керування
Загальна структура
SYN
SYN
SOH
Заголовок
ETB
STX
Інформація
ETB
ETX
BCC1
BCC2
Розширена структура

Сеанс зв`язку складається з таких фаз:

- приєднання каналу (наприклад, набирання телефонного номеру);
- запит на передавання;
- передавання кадрів;

- закінчення передавання;
- від`єднання каналу.

Види інформаційних кодів,які надходять у канал, не обмежені (вимога прозорості), і серед них можуть бути службові символи протоколу BSC, що утруднить роботу програм керування. Щоб вирішити цю проблему, ввели спеціальний символ DLE (Data Link Escape). Його ставлять перед кожним символом керування в заголовку, кінці і основній частині. Цей процесс називається процедурою вставляння байтів. Післяцього в головній частині перед символами керування ставлять ще по одному DLE.

SOH	Передує заголовку кадру
STX	Передує основі кадру
ETX	Є після закінчення заголовка або основи кадру
EOT	Кінець сеансу зв`язку
ENQ	Запит на сеанс зв`язку
ACK	Символ підтвердження приймання
DLE	Використовується для вставляння байтів
NAK	Кадр має помилку, запит на повторення
SYN	Передається на початку кадру
ETB	Є після закінчення заголовку або основи кадру
RVI	Переданий кадр був правильний але запит на припинення.
TTD	немає інформації для передавання.Підтримуйте зв`язок
Символи керування кадрів	

4.9 Протоколи модемів

Подібною до протоколу BSC є група протоколів передавання файлів за допомогою модема. Як і BSC, ці протоколи використовують символи керування коду ASCII. Головна мета цих протоколів – забезпечити передавання даних ненадійною ланкою передавання. Кожен кадр у них має фіксовану довжину та захищений контрольною сумою. Різні протоколи надають різний сервіс передавання. Складніші з них забезпечують захист сполучення від помилок, засвідчення сполучення, перевірку пароля.

До протоколів без захисту від помилок належать:

Xmodem

Один із перших модемних протоколів. Рожроблений у 1977 р. В. Христенсоном. Принцип роботи:приймач постійно передає в канал символ NAK. Передавач, прийнявши цей символз каналу, починає передавання: надсилає в канал символ SOH, два номери інформаційного блоку (номер та його двійкове доповнення), блок інформації, що має фіксовану довжину 128 байт, та байт контрольної суми. Останній формується як залишок від ділення суми всіх байтів блоку на 255. Контрольну суму повторно обчислює приймач. Якщо передане та обчислене значення не збігаються, то приймач передає в канал символ NAK, у протилежному випадку – ACK. Завершується передавання подвійним надсиланням символу EOT.

Відсоток виявлення помилок протоколом Xmodem досить значний (99,6%). Однак цей протокол має і суттєві недоліки: малу швидкість передавання, великий обсяг службової інформації.

Xmodem-CRC

Модифікація протоколу Xmodem. Кожен кадр має два контрольні байти. Протокол виявляє всі поодинокі, подвійні та непарні помилки, а також усі пакети помилок довжиною до 16 знаків. На початку передавання замість NAC приймач передає символ C. Якщо після трьох C відповіді не одержано, приймач починає роботу за Xmodem.

Xmodem-1k

Модифікація протоколу Xmodem-CRC. Довжина інформаційного блоку збільшена до 1024 байтів. Кількість службової інформації зменшена. У системах з розподілом часу зменшується вплив затримок.

Ymodem

Модифікація Xmodem-CRC. Реалізоване групове передавання файлів. Ім`яфайлу та шлях до нього передаються в нульовому інформаційному блоці.В кінці кожного файлу передається до десяти разів символ EOT. Кінець сеансу позначається нульовим (порожнім) іменем шляху. Протокол використовують в операційних системах CP/M, RZ/SZ (Unix),пакеті MTEZ.

Ymodem-g

Застосовують у високошвидкісних модемах та для захищених від помилок каналів. Передавання цим протоколом ініціює символ G. Передавач, який одержав G, відразу розпочинає передавання на найбільшій можливій швидкості. Швидкістю передавання керує протокол XON/XOFF.

Протокол XON/XOFF використовують так: якщо приймач не готовий до роботи, то він надає символ XOFF; тоді передавач тимчасово припиняє передавання, доки не отримає символ XON.

Виявивши помилку приймач передає багато символів CAN. Підтверджує прийманняфайлу символ ACK. Протокол не захищає від помилок у каналі, у випадку їх виявлення передавання файлу припиняється.

Zmodem

Продовження протоколів Xmodem та Ymodem. У ньому реалізовано таке: віконний механізм захисту від спотворення кадрів; динамічна адаптація до якості каналу зв`язку шляхом зміни розміру блоку та швидкості передавання; захист інформації керування та доступу до передавання від імітації сигналів керування. Достовірність передавання підвищується завдяки 32 розрядній контрольній комбінації. Якщо передавання файлу було припинене, то воно відновлюється з місця преривання. Протокол Zmodem використовують у каналах з високою ймовірністю помилки та у високоякісних каналах як самостійно так і з протоколами канального рівня X.25, V.42, MNP, Fastlink.

4.10 Протокол HDLC

Держстандарт 26113-83 (HDLC) відповідає міжнародним стандартам 4335, 6256, 3309 ISO. Він описує роботу двопунктової ланки передавання даних. Повний цикл функціонування двопунктової ланки передавання даних складається з таких фаз: Логічне роз`єднання, Ініціалізація, Налагодження сполучення, Передавання інформації, Завершення сполучення, Логічне роз`єднання.

Логічне роз`єднання** є першою і водночас останньою фазою процедур керування ланкою передавання даних, вона автоматично розпочинається після вмикання та перед вимиканням станції. Фаза **Ініціалізація** призначена для обміну інформацією про параметри програми, потрібні в інших фазах, вона є необов`язковою. Фаза **Налагодження сполучення має на меті налагодити логічне

сполучення. Фаза **Передавання інформації** – основна. У ній відбувається обмін інформацією. Після її закінчення станція переходить у фазу **Завершення сполучення**. Якщо характеристики каналу різко погіршаться, тоді можливий перехід до фази **Логічне роз`єднання** або **Налагодження сполучення**. Фаза **Завершення сполучення** є перехідною між фазами **Передавання інформації** і **Логічне роз`єднання**. Для передавання інформації використовують три типи кадрів: інформаційний(I-кадр), службовий нумеровагий (S-кадр), службовий не нумерований (U-кадр) . I-кадр має службову та інформаційну частину, останні - лише службову. Усі кадри функціонально можна розділити на команди та відповіді. Команди наказують, що зробити, відповіді відсилаються після одержання команди. Деякі кадри можуть бути тільки командами, інші – тільки відповідями, ще інші – командами та відповідями одночасно.

I-кадри: єдиною командою/відповіддю є команда I(Information transfer), що переносить інформацію і підтверджує приймання.

S-кадри:

- RR(Recieve Ready) – к/в -Повідомляє про готовність до приймання;
- RNR(recieve Not Ready) - к/в – Повідомляє про неготовність до приймання.

U-кадри:

- SABM (Set Asynchronous Balanced Mode), – вимагає налаштувати зв`язок у нерозширеному форматі;
- SABME (Set Asynchronous Balanced Mode Enlarged), – вимагає налаштувати зв`язок у розширеному форматі;
- FRMR (FrameReject), – повідомляє про приймання некоректного кадру
- DISC (Disconnect), – вимагає припинити сполучення

UA (Unnumbered Acknowledgment), – дає згоду на виконання команди;

- DM (Disconnect Mode), – повідомляє про незгоду виконати команду або про наявність режиму роз`єднання;
- SIM (Set Initialization Mode), – вимагає провести ініціалізацію передаванням параметрів на віддалену станцію;
- RIM (Reset Initialization Mode) –вимагає провести ініціалізацію прийманням параметрів з віддаленої станції;
- UI (Unnumbered information), – ненумерований інформаційний кадр.

ЗМІСТОВИЙ МОДУЛЬ 3. ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

5 ЗАГАЛЬНІ ПИТАННЯ ПРОЕКТУВАННЯ МЕРЕЖ

5.1 Принципи ієрархічного проектуваня мерж

Проектування будь-якої мережі потрібно починати з самого нижчого рівня – фізичного середовища передачі інформації. За великим рахунком, проектування фізичного рівня стосується бітів і байтів, оптимального вибору пропускної спроможності ліній зв'язку, середовища передачі інформації і сигнального методу передачі, а також отримання даних з каналу. Всі перераховані питання дуже важливі, так як стабільність каналів зв'язку багато в чому визначає стабільність передачі і трафік по мережі. Часто виникаючі проблеми фізичного рівня приводять до мережевих змін, викликаючи необхідність оновлення таблиць маршрутизації. Однак токологія (структура) мережі має незрівнянно більший вплив на її стабільність, ніж вибір між технологіями ATM або Frame Relay для прокладання віддалених мережевих з'єднань. Правильно вибрана топологія є базою всіх стабільно працюючих мереж. Для того, щоб зрозуміти це твердження, спробуйте відповісти на питання: чому мережі зависають? Найбільш проста відповідь звучить так: мережі зависають через не збіжність (невідповідність) протоколу маршрутизації. Оскільки всі протоколи маршрутизації в процесі збіжності породжують петлі (жоден протокол маршрутизації не може надати точну інформацію щодо маршрутів у процесі оновлення таблиці маршрутизації), дуже важливо якомога швидше завершити процес збіжності після виникнення непередбачених змін у мережі. Час, необхідний протоколу маршрутизації для завершення процесу конверсії, залежить від двох факторів:

- кількості маршрутизаторів, що приймають участь у процесі конверсії;
- обсягу оброблюваної маршрутизаторами інформації.

Кількість маршрутизаторів, що бере участь у процесі конверсії, залежить від розмірів ділянки мережі, на яку впливає зміна топології. Додавання («суммирование», агрегація) дозволяє приховати частину інформації про маршрути від маршрутизаторів. Як наслідок маємо зменшення оброблюваної маршрутизаторами інформації, оскільки маршрутизатори, що не мають інформації про заданий пункт призначення, не повинні вносити зміни до маршрутизації

таблиці при зміні маршруту до даної пункту призначення або при пошкодженні каналу, що призвело до його недоступності.

Обсяг оброблюваної маршрутизаторами інформації при визначенні кращого маршруту до пункту призначення залежить від загальної кількості таких маршрутів. В зв'язку з цим агрегація також дозволяє зменшити обсяг оброблюваних маршрутизаторами інформації при зміні мережі топології. Таким чином, сумирование є ключевым поняттям, що дозволяє зменшити кількість учасників у процесі конверсії маршрутизаторів та обсягу оброблюваної ними інформації. Крім того, сумація залежить від успішного вибору схем адресації, в яку із самого початку закладаються передумови для його проведення. Вдала схема адресації завжди базвється наретельно спланованій топології, що лежить в основі мережі. Недолуге проектування мережі практично не лишає шансів для вибору оптимальних схем адресації «з метою» на подальше проведення суммирования. Незважаючи на те, що багато хто намагається вирішити мережеві проблеми, викликані невдалою вибором топології та схем адресації, за допомогою більш продуктивних маршрутизаторів, усіляких доработок адресної схеми або удосконалених протоколів маршрутизації, практика свідчить: ніщо не може замінити вдало вибрану топологію мережі.

5.2 Топологія ієрархічних мереж

З будь-якою проблемою легше впоратися, якщо вона розбита на кілька дрібніших підзадач, і в цьому сенсі великі мережі не є винятком. Велика мережа може бути розділена на кілька порівняно невеликих ділянок, кожен з яких можна розглядати окремо від інших. Більшість вдало спроектованих великих мереж є ієрархічними, тобто розбитими на кілька рівнів. Кожен рівень являє собою окрему проблемну область, в рамках якої структура рівня розробляється з урахуванням однієї чи кількох чітко визначених цілей. Концепція ієрархічних мереж дуже нагадує концепцію еталонної моделі OSI, відповідно до якої процес взаємодії між комп'ютерами розбивається на кілька функціональних рівнів, що виконують певне коло завдань. Рівні ієрархічної моделі повинні якомога точніше відповідати поставленим перед ними цілей. Спроба делегування якомусь певному рівню занадто великого числа функціональних завдань призводить, як правило, до плутанини, що ускладнює документування і підтримку. У більшості випадків ієрархічна модель мережі мають на увазі визначення трьох рівнів. Як показано на рис. 5.1, кожен рівень ієрархічної мережі виконує власні функціональні завдання.

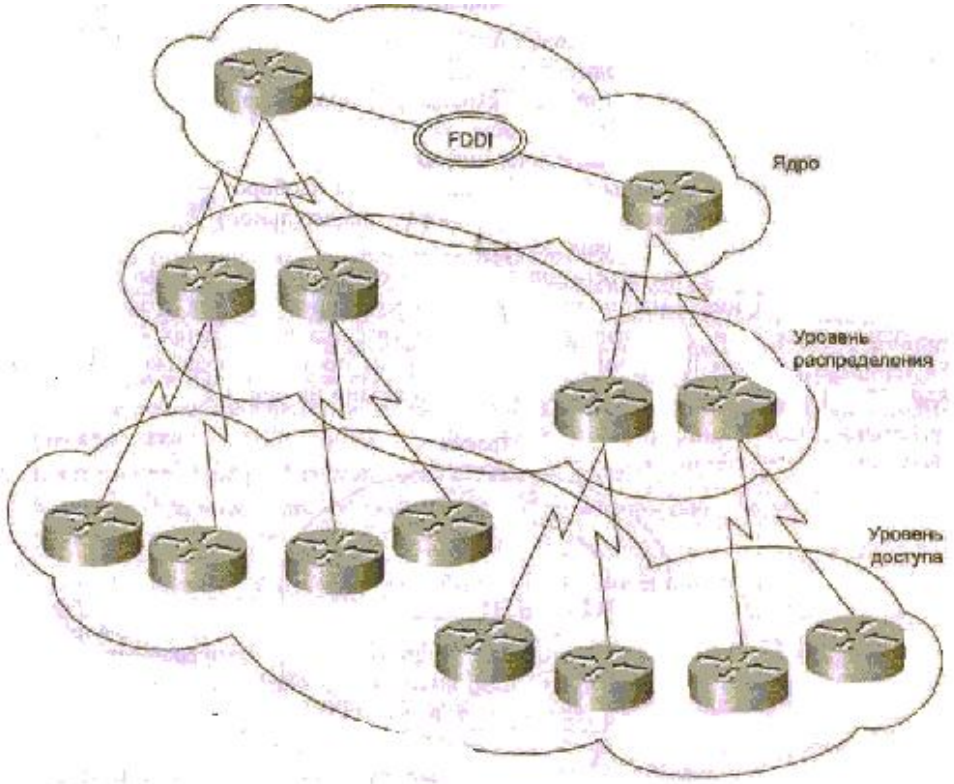


Рис. 5.1 – Функціональні завдання на різних ієрархічних рівнях мережі

1. Ядро (core) мережі відповідає за високошвидкісну передачу мережевого трафіку; пер первинних призначення пристрою, що входить в ядро мережі, полягає в комутації пакетів.

2. На рівні розподілу (distribution layer) відбувається підсумовування маршрутів і агрегація трафіку.

3.Рівень доступу (access layer) відповідає за формирование мережевий трафіку, Виконує го контроль точок входу в ятір и надає інші служби Прикордонний прістроїв.Теперь, коли ви вже знаєте назви рівнів ієрархічної моделі мережі, повернемося назад і спробуємо поглянути на взаємовідношення цих рівнів з згадуваними раніше фундаментальними принципами проектування мереж. Зверніть увагу на наведену нижче нове формулювання двох основних принципів розробки структури мережі. В даному випадку нам необхідно з'ясувати, чи вписуються ці принципи в ієрархічну модель.Размеры участка сети, на который влияет изменение топологии, должны быть строго ограничены; при этом желательно, чтобы данный участок сети был как можно меньшим.

Маршрутизатор (а також інші мережеві пристрої) повинні обробляти мінімально можливий обсяг інформації.

Кожен з цих принципів може бути реалізований за допомогою підсумовування, яке здійснюється на рівні розподілу ієрархічної моделі мережі. Таким чином, це означає, що область збіжності протоколу маршрутизації повинна бути обмежена рівнем розподілу. Так, пошкодження каналу передачі інформації рівня доступу не повинно стати причиною зміни таблиці маршрутизації ядра і навпаки – пошкодження лінії зв'язку ядра не повинно надати скільки-небудь значного впливу на таблиці маршрутизації пристроїв рівня доступу. В ієрархічних мережах агрегація трафіку і його напрямок в високошвидкісні канали передачі інформації відбувається в міру просування трафіку від рівня доступу до ядра мережі. Аналогічно, поділ трафіку і його напрямок по менш швидкісних каналів передачі даних відбувається в міру просування трафіку від ядра мережі до пристроїв рівня доступу.

Слід зазначити, що агрегація трафіку на кордонах рівнів ієрархічної мережі мають на увазі не тільки можливість вибору в якості маршрутизаторів рівня доступу менш продуктивних пристроїв, але і вказує на той факт, що ці пристрої не будуть надто обтяжені комутацією пакетів. Отже, що звільнилися обчислювальні ресурси маршрутизаторів рівня доступу можуть бути використані для реалізації мережевих правил. Одним з найбільш серйозних недоліків ієрархічної структури мережі є потенційна можливість появи одиночних точок відмови на фізичному рівні. При цьому слід зазначити: чим суворіше ієрархія мережі, тим вище ймовірність того, що пошкодження одного пристрою або каналу передачі інформації викличе великі неполадки в її роботі. Зрозуміло, якщо такий серйозний збій в роботі мережі абсолютно неприйнятний, слід подбати про заходи забезпечення надмірності, яка могла б значно зменшити наслідки цього недоліку ієрархічної моделі мережі.

5.3 Принципи логічної структуризації й проектування мереж

5.3.1 Основні поняття та визначення

Під логічної **структуризацією** і проектуванням мережі розуміється розбиття загальної розділяється середовища на логічні сегменти, які представляють самостійні колективні середовища з меншою кількістю вузлів. Мережа, розділена на логічні сегменти, має більш високу **продуктивність** і надійність.

Основні недоліки мережі, побудованої на одному поділюваному середовищі, починають виявлятися при перевищенні деякого порогу кількості вузлів, підключених до середи. Найбільш важкі умови для вузлів мережі створює метод доступу CSMA / CD-технології Ethernet. Але і в інших технологіях, таких як Token Ring чи FDDI, де метод доступу носить менш випадковий характер і навіть часто називається детермінованим, випадковий фактор доступу до середовища все одно присутній і проявляє свій негативний вплив на пропускну здатність, дістається окремому вузлу.

Всім технологіям властивий експонентний зростання величини затримок доступу при збільшенні коефіцієнта використання мережі, відрізняється тільки поріг, при якому настає різкий перелом у поведінці мережі, коли майже прямолінійна залежність переходить в круту експонента. Для всього сімейства технологій Ethernet – це 30-50%, для технології Token Ring – 60%, а для технології FDDI – 70%. Кількість вузлів, при яких коефіцієнт використання мережі починає наближатися до небезпечної межі, залежить від типу функціонують у вузлах додатків. Якщо раніше для мереж Ethernet вважалося, що 30 вузлів – це цілком прийнятне число для одного поділюваного сегмента, то сьогодні для **мультимедійних** додатків, що перекачують великі файли даних, цю цифру потрібно уточнювати за допомогою натурних або імітаційних експериментів.

При завантаженні мережі до 30% технологія Ethernet на поділюваному сегменті добре справляється з передачею трафіку, що генерується кінцевими вузлами. Однак при підвищенні інтенсивності генерованого вузлами трафіку мережа все більше часу починає працювати неефективно, повторно передаючи кадри, які викликали колізію. При зростанні інтенсивності генерованого графіка до такої величини, коли коефіцієнт використання наближається до одиниці, вірогідність зіткнення кадрів настільки збільшується, що практично будь-який кадр, який будь-яких станція намагається передати, стикається з іншими кадрами, викликаючи колізію. Мережа перестає передавати корисну інформацію користувача і **працює** "на себе", обробляючи колізії.

Сегменти Ethernet не рекомендується завантажувати так, щоб середнє значення коефіцієнта використання перевищувало 30%. Саме тому в багатьох системах **управління мережами** порогова межа для індикатора коефіцієнта завантаження мережі Ethernet за умовчанням встановлюється на величину 30. В

результаті, навіть мережу середніх розмірів важко побудувати на одному поділюваному сегменті так, щоб вона працювала ефективно при зміні інтенсивності генерованого станціями трафіку.

Крім того, при використанні розділяється середовища проектувальник мережі стикається з жорсткими обмеженнями максимальної довжини мережі, які для всіх технологій лежать в межах декількох кілометрів, і тільки **технологія FDDI** дозволяє будувати **локальні мережі**, довжина яких вимірюється десятками кілометрів.

Обмеження, що виникають із-за використання загальної розділяється середовища, можна подолати. Для цього необхідно розділити мережу на кілька поділюваних середовищ і з'єднати окремі сегменти мережі такими пристроями, як **мости**, комутатори або маршрутизатори.

Перераховані пристрої передають кадри з одного свого порту на інший, аналізуючи адресу призначення, поміщений в цих кадрах (на відміну від **концентраторів**, які повторюють кадри на всіх своїх портах, передаючи їх в усі приєднані до них сегменти, – незалежно від того, в якому з них знаходиться станція призначення). Мости й комутатори виконують операцію передачі кадрів на основі плоских адрес го рівня, тобто MAC – адрес, а маршрутизатори на основі номери мережі (мережевих адрес). При цьому єдина колективна середовище, створене **концентраторами** (або в граничному випадку одним сегментом кабелю), ділиться на кілька частин, кожна з яких приєднана до порту мосту, **комунікатора** або маршрутизатора.

Логічний сегмент являє собою єдине середовище. Розподіл мережі на логічні сегменти призводить до того, що навантаження, що припадає на кожний з новостворених сегментів, майже завжди виявляється менше, ніж навантаження, яку відчувала вихідна мережу. Отже, зменшуються шкідливі ефекти від поділу середовища: знижується час очікування доступу, а в мережах Ethernet – і інтенсивність колізій. Більшість великих мереж розробляється на основі структури із загальною магістраллю, до якої через мости і маршрутизатори приєднуються підмережі. Ці підмережі обслуговують різні відділи. Підмережі можуть ділитися і далі на сегменти, призначені для обслуговування робочих груп.

Сегментація збільшує гнучкість мереж. При побудові мережі як сукупності підмереж кожна підмережа може бути адаптована до специфічних потреб робочої

групи чи відділу. Наприклад, в одній підмережі може використовуватися технологія Ethernet і ОС NetWare, а в іншій – Token Ring і OS -400, у відповідності з традиціями того чи іншого відділу чи потребами наявних додатків. Разом з тим, у користувачів обох підмереж є можливість обмінюватися даними через міжмережеві пристрої – мости, комутатори, маршрутизатори. Процес розбиття мережі на логічні сегменти можна розглядати і в зворотному напрямку – як **процес** створення великої мережі з модулів вже наявних підмереж.

Підмережі підвищують безпеку даних. При підключенні користувачів до різних фізичних сегментах мережі можна заборонити доступ певних користувачів до **ресурсів** інших сегментів. Встановлюючи різні логічні фільтри на мостах, комунікаторах і маршрутизаторах, можна контролювати доступ до ресурсів, чого не дозволяють зробити повторювачі (пристрій для відновлення і посилення сигналів в мережі для збільшення її довжини).

Підмережі спрощують управління мережею. Побічним ефектом зменшення графіка, балансування навантаження та підвищення безпеки даних є спрощення управління мережею. Проблеми дуже часто локалізується усередині сегмента. Як і у випадку структурованої кабельної системи, проблеми однієї підмережі не впливають на інші підмережі. Підмережі утворюють логічні домени управління мережею.

5.3.2 Структуризація за допомогою повторювачів і мостів

Всі сучасні реалізації Ethernet (за винятком коаксіальних версій) вимагають для зв'язку кінцевих вузлів застосування тих чи інших активних проміжних пристроїв Ці пристрої є пунктами концентрації індивідуальних кабелів (проводів) підходять до крайовим і іншим проміжним вузлам мережі, і називаються "концентраторами". На жаль, немає усталеної термінології, що погоджує в струнку систему такі поняття як "концентратор", "повторювач", "хаб", "міст" і "комутатор". Під "концентратором" часто мають на увазі і повторювач простий пристрій, і комутатор, що дозволяє поєднувати пристрої з різними технологіями (Ethernet, Token Ring, FDDI). Концентратори розрізняються по виконуваних функцій (повторювачі, мости, комутатори 2-го рівня, комутатори 3-го рівня), типами і кількістю портів, конструктивного виконання. Повторювач (repeater) у мережах Ethernet на коаксіальному кабелі використовується як засіб подолання обмежень на довжину кабелю і кількості підключених вузлів (по електричних характеристиках). У мережах на кручений парі і оптоволокні повторювач є

найдешевшим варіантом сполучного пристрою і частіше називається "хабом" (hub).

У найпростішому випадку повторювач має два порти. Завданням повторювача є: передача сигналу з одного порту в інші з відновленням форми і обробкою колізій, а також ізоляція порту, на якому він виявляє безперервні помилки. Кожен порт має власний трансивер-приймач, передавач і детектор колізій. Повторювач прослуховує сигнали на всіх портах. При виявленні несе на одному з портів він синхронізується з преамбулі і прийняту послідовність сигналів транслює в усі інші порти з номінальною амплітудою імпульсів. Після зникнення несучої всі порти знову переходять у стан очікування сигналу на будь-якому з портів. Якщо під час трансляції сигналу в будь-якому з портів виявляється колізія, повторювач в усі порти посилає jam-послідовність. Це робиться для того, щоб вузли, підключені до всіх портів, могли б розпізнати колізію. Якщо транслювати одного з портів виявляє колізію поспіль 32 рази, то порт ізолюється (partitioned) - сигнали з цього порту перестають транслюватиметься в інші. Пакети в сегментований порт транслюватися. Якщо трансивер вдається передати пакет в сегмент трансльовані порт без колізії, сегментація знімається і порт переходить в нормальний режим роботи. Ця автоізоляція (auto partition) призначена для підвищення живучості мережі. Для повторювачів Fast Ethernet правила ізоляції та "реабілітації" дещо складніше. Приводом для ізоляції є і довга "балакуча" (jabber) посилка (більше 1 518 байтів). Повторювач працює на рівні фізичних сигналів - закованих бітових ланцюжків. Для збільшення числа підключаються вузлів і відстані між ними в мережі може бути присутнім безліч з'єднаних між собою повторювачів. Мережа на повторювачах повинна задовольняти наступним обмеженням.

1. Петльові з'єднання повторювачів неприпустимі - мережа не повинна мати замкнутих контурів.
2. Між будь-якою парою станцій мережі на 10 Мбіт / с може бути не більше чотирьох повторювачів.
3. Затримка поширення сигналів між будь-якою парою вузлів не повинна перевищувати 25 мкс для 10 Мбіт / с і 2,5 мкс для 100 Мбіт / с.
4. Повторювач Fast Ethernet 100 Мбіт / с класу I в сегменті може бути тільки один.
5. Повторювачів класу II може бути не більше двох.

Міст (bridge) є засобом передачі кадрів між двома або більше сегментами-доменами колізій. Міст аналізує заголовок кадру його цікавлять MAC - адреси джерела і одержувача. Міст прослуховує кадри, що приходять кожен на свій порт, і становив, таблиці MAC - адрес вузлів, підключених до цих портів (за адресами джерела) Якщо приходить кадр має адресу призначення, що належить тому ж сегменту то цей кадр мостом фільтрується – нікуди не транслюється. Якщо адреса призначення відомий мосту і відноситься до іншого сегменту, міст транслює цей кадр у відповідний порт. Якщо положення адресата призначення ще не відомо мосту кадр транслюється в усі порти (крім того, звідки він прийшов). Широкомовні і багатоадресні кадри також транслюються в усі порти. Трансляція передбачає доступ до сегмента за звичайною схемою: очікування відсутності несучої, передача кадру і, в разі колізій, повторні спроби передачі. Для виконання цих процедур міст повинен мати буферну пам'ять для проміжного зберігання кадрів, а також пам'ять для зберігання таблиць MAC-адрес вузлів сегментів усіх портів. Описаний алгоритм поведінки відноситься до "прозорим" мостам.

Кадри з широкомовними MAC-адресами передаються мостом на всі його порти, як і кадри з невідомим адресою призначення. Такий режим розповсюдження кадрів називається "затопленням мережі * (flood). Наявність мостів в мережі не перешкоджає поширенню широкомовних кадрів по всіх сегментах мережі, зберігаючи її прозорість. Однак це є перевагою лише в тому випадку, коли широкомовна адресу вироблений коректно працюють вузлом. Однак часто трапляється так, що в результаті яких-небудь програмних або апаратних збоїв протокол верхнього рівня або сам мережевий адаптер починають працювати некоректно і постійно з високою інтенсивністю генерувати кадри з широкомовною адресою протягом тривалого проміжку часу.

5.3.3 Обмеження топології мережі, побудованої на мостах

Слабкий захист від широкомовного шторму – одне з головних обмежень моста, але не єдине. Іншим серйозним обмеженням функціональних можливостей мостів є неможливість підтримки петлеподібні конфігурацій мережі. Якщо в мережі побудованої з використанням мостів, з'являться замкнуті маршрути, то це призведе до наступних наслідків:

1) "розмноження" кадру, тобто появи декількох його копій;
2) нескінченної циркуляції копій кадру по зашморгу в протилежних напрямках, тобто засмічення мережі непотрібним трафіком;

3) постійної перебудови мостами своїх адресних таблиць, так як кадр з адресою джерела буде з'являтися то на одному порту, то на іншому;
4) великий затримці передачі кадрів за рахунок їх буферірованія і послідовного обслуговування портів.

Щоб виключити всі ці небажані ефекти, мости потрібно застосовувати так, щоб між логічними сегментами не було петель, тобто будувати за допомогою мостів тільки деревоподібні структури, що гарантують наявність тільки одного шляху між будь-якими двома сегментами. Міст доцільно встановлювати в точці мережі, що забезпечує не більше 20% передач через міст.

5.4 Обгрунтування розміру (діаметра) мережі Ethernet

При виборі конфігурації мережі Ethernet, що складається з сегментів різних типів, виникає багато питань, пов'язаних, перш за все, з максимально допустимим розміром (діаметром) мережі і максимально можливим числом різних елементів. Мережа буде працездатною тільки в тому випадку, якщо максимальна затримка поширення сигналу в ній не перевищить граничної величини. Ця величина визначається обраним методом управління обміном CSMA / CD (Carrier - Sense Multiple Access with Collision Detection - множинний доступ з контролем несучої і виявленням колізій), заснованим на виявленні та вирішенні колізій.

Перш за все нагадаємо, що для одержання складних конфігурацій Ethernet з окремих сегментів застосовуються концентратори двох основних типів:

- репітерние концентратори, які представляють собою набір репітерів і ніяк логічно не розділяють сегменти, підключені до них;
- комутуючі {awitching) концентратори або комутатори, які передають інформацію між сегментами, але не передають конфлікти із сегмента на сегмент.

Застосування репітерного концентратора не розділяє зону конфлікту, в той час як кожен комутуючих концентратор ділить зону конфлікту на частини. У разі комутатора оцінювати працездатність треба для кожної частини мережі окремо, а в разі репітерних концентраторів треба оцінювати працездатність всієї мережі в цілому.

Допустимі розміри мережі Ethernet визначаються низкою чинників.

- Обмеження на довжину кабельного сегмента, пов'язані з загасанням і спотворенням форми сигналу: 10 Base -5 – 500 м і правило "5-4-3", 10 Bas -2 – 185 (300) м і правило "5-4-3", 10 Base-T / 100 Base - TX / 100 Base - T 4 – 100 м.
- Обмеження на кількість вузлів в домені колізій: не більше 1 024.
- Обмеження на кількість повторювачів між будь-якою парою вузлів: Ethernet – 4, Fast Ethernet – 1 або 2, Gigabit Ethernet – 1.
- Обмеження на розмір домену колізій, пов'язані з часом поширення сигналу між кінцевими вузлами мережі: час подвійного обороту для Ethernet і Fast Ethernet не повинно перевищувати 512 bt, для Gigabit Ethernet – 2 048 bt.

Для мереж на мідних кабелях, як правило, досить виконати перші три умови. Оптоволокно, особливо одномодове, дозволяє значно збільшувати довжину кабельного сегмента, але при цьому обмежуючим фактором буде виступати затримка поширення сигналу. Затримки 25,6 мкс (для 10 Мбіт / с) і 2,6 мкс (для 100 Мбіт / с) відповідають довжині скляного волокна близько 5000 і 500 м.

При описі тимчасових діаграм мереж типу Ethernet й Fast Ethernet, а також при визначенні граничних розмірів мережі широко використовуються такі терміни.

- IPG (interpacket gap, межпакетная щілину) - мінімальний проміжок часу між переданими пакетами (9,6 мкс для Ethernet; 0,96 мкс для Fast Ethernet). Інша назва – міжкадровий інтервал.
- BT (Bit Time, час біта) - інтервал часу для передачі одного біта (100 не для Ethernet; 10 не для Fast Ethernet).
- PDV (Path Delay Value, значення затримки в дорозі) - час проходження сигналу між двома вузлами мережі (кругове, то це подвоєне). Враховує сумарну затримку в кабельній системі, мережевих адаптерах, повторювачах та інших мережевих пристроях.
- Collision window (вікно колізій) - максимальне значення PDV для даного сегмента.
- Collision domain (область колізій, зона конфлікту) - частина мережі, на яку поширюється ситуація колізії, конфлікту.
- Slot time (час каналу) - максимально допустимий вікно колізій для сегмента (512 bt).
- Minimum frame size - мінімальний розмір кадру (512 біт або 64 байта).

Maximum frame size - максимальний розмір кадру (1518 байт).
- Maximum network diameter (максимальний діаметр мережі) – максимальна допустима довжина сегмента, при якій його вікно колізій не перевищує часу каналу slot time.
- Truncated binary exponential back off (усічена двійкова експонентна відстрочка) – затримка перед дотримуюся щей спробою передачі пакета після колізії (допускається максимум 16 спроб).

Друга модель, яка застосовується для оцінки конфігурації Ethernet, заснована на точному розрахунку часових характеристик обраної конфігурації мережі. Вона іноді дозволяє вийти за межі жорстких обмежень моделі 1. Застосування моделі 2 зовсім необхідно в тому випадку, коли розмір проектованої мережі близький до максимально допустимого.

У моделі 2 використовуються дві системи розрахунків:

- перша система припускає обчислення подвійного (кругового) часу проходження сигналу по мережі і порівняння його з максимально припустимою величиною (512 bt);

- друга система перевіряє допустимість скорочення (на 49 bt) величини одержуваного міжкадрового тимчасового інтервалу, межпакетной щілини (IPG - Inter Packet **Gap)** у мережі.

При цьому обчислення в обох системах розрахунків ведуться для найгіршого випадку, для шляху максимальної довжини, тобто для такого шляху переданого по мережі пакету, який вимагає для свого проходження максимального часу. При першій системі розрахунків виділяються три типи сегментів:

- початковий сегмент - це сегмент, відповідний початку шляху максимальної довжини;
- кінцевий сегмент - це сегмент, розташований в кінці шляху максимальної довжини;
- проміжний сегмент - це сегмент, що входить в шлях максимальної довжини, але не є ні початковою, ні кінцевим.

Проміжних сегментів у вибраному шляху може бути кілька, а початковий і кінцевий сегменти при різних розрахунках можуть мінятися місцями один з одним. Виділення трьох типів сегментів дозволяє автоматично враховувати

затримки сигналу на всіх концентраторах, що входять в шлях максимальної довжини, а також у приемопередающих вузлах адаптерів.

6 ПРОТОКОЛИ СЕРЕДНЬОГО ТА ВИСОКОГО РІВНІВ МЕРЕЖ

6.1 Стандартні мережеві протоколи

Протоколи - це набір правил і процедур, що регулюють порядок здійснення зв'язку. Комп'ютери, що беруть участь в обміні, повинні працювати за одними і тими ж протоколами, щоб в результаті передачі вся інформація відновлювалася в первісному вигляді.

Про протоколи нижніх рівнів (фізичного і канального), що відносяться до апаратури, йщла мова у розділах. Зокрема, до них відносяться методи кодування і декодування, а також керування обміном в мережі. Докладніше деякі з них будуть викладені в лекціях, присвячених стандартним мережам. Зараз ми зупинимося на особливостях протоколів більш високих рівнів, реалізованих програмно.

Зв'язок мережевого адаптера з мережевим програмним забезпеченням здійснюють драйвери мережевих адаптерів. Саме завдяки драйверу комп'ютер може не знати ніяких апаратних особливостей адаптера (його адрес, правил обміну, характеристик). Драйвер уніфікує, робить однаковим взаємодію програмних засобів високого рівня з будь-яким адаптером даного класу. Драйвери, що поставляються разом з мережевими адаптерами, дозволяють програмам однаково працювати з платами різних постачальників і навіть з платами різних локальних мереж (Ethernet, Arcnet, Token-Ring і т.д.). Якщо говорити про стандартну модель OSI, то драйвери, як правило, виконують функції канального рівня, хоча іноді вони реалізують і частину функцій мережного рівня: формують пакет у буферній пам'яті адаптера, дають команду на передачу, інформують комп'ютер щодо прийому пакета тощо (рис. 6.1).

Рисунок 6.1 – Функції драйвера мережевого адаптера в моделі OSI

Якість написання програми драйвера багато в чому визначає ефективність роботи мережі в цілому. Навіть при найкращих характеристиках мережного адаптера неякісний драйвер може різко погіршити обмін по мережі.

Перш ніж придбати плату адаптера, необхідно ознайомитися зі списком сумісного обладнання (Hardware Compatibility List, HCL), який публікують всі виробники мережевих операційних систем. Вибір там досить великий (наприклад, для Microsoft Windows Server список включає більше сотні драйверів мережевих адаптерів). Якщо в перелік HCL не входить адаптер якогось типу, краще його не купувати.

6.2 Протоколи високих рівнів

Існує кілька стандартних наборів (або, як їх ще називають, стеків) протоколів, які отримали зараз широке поширення:

- набір протоколів ISO / OSI;
- IBM System Network Architecture (SNA);
- Digital DECnet;
- Novell NetWare;
- Apple AppleTalk;
- набір протоколів глобальної мережі Інтернет, TCP / IP.

Включення в цей список протоколів глобальної мережі цілком зрозуміло, адже, як уже зазначалося, модель OSI використовується для будь-якої відкритої системи: на базі як локальної, так і глобальної мережі або комбінації локальної та глобальної мереж.

Протоколи перерахованих наборів діляться на три основні типи:

- прикладні протоколи (виконують функції трьох верхніх рівнів моделі OSI, – прикладного, представницького і сеансового);
- транспортні протоколи (реалізують функції середніх рівнів моделі OSI - транспортного та мережевого);
- мережеві протоколи (здійснюють функції трьох нижніх рівнів моделі OSI).

Прикладні протоколи забезпечують взаємодію додатків і обмін даними між ними. Найбільш популярні:

- FTAM (File Transfer Access and Management), – протокол OSI доступу до файлів;
- X.400, – протокол CCITT для міжнародного обміну електронною поштою;
- X.500, – протокол CCITT служб файлів та каталогів на декількох системах;
- SMTP (Simple Mail Transfer Protocol), – протокол глобальної мережі Інтернет для обміну електронною поштою;
- FTP (File Transfer Protocol), – протокол глобальної мережі Інтернет для передачі файлів;
- SNMP (Simple Network Management Protocol), – протокол для моніторингу мережі, контролю за роботою мережевих компонентів і управління ними;
- Telnet, – протокол глобальної мережі Інтернет для реєстрації на віддалених серверах і обробки даних на них;
- Microsoft SMBs (Server Message Blocks, блоки повідомлень сервера) і клієнтські оболонки або редиректори фірми Microsoft;
- NCP (Novell NetWare Core Protocol) і клієнтські оболонки або редиректори фірми Novell.

Транспортні протоколи підтримують сеанси зв'язку між комп'ютерами і гарантують надійний обмін даними між ними. Найбільш популярні з них наступні:

- TCP (Transmission Control Protocol), – частина набору протоколів TCP / IP для гарантованої доставки даних, розбитих на послідовність фрагментів;
- SPX, – частина набору протоколів IPX / SPX (Internetwork Packet Exchange / Sequential Packet Exchange) для гарантованої доставки даних, розбитих на послідовність фрагментів, запропонованих компанією Novell;
- NWLink, – реалізація протоколу IPX / SPX компанії Microsoft;
- NetBEUI (NetBIOS Extended User Interface, розширений інтерфейс - NetBIOS), – встановлює сеанси зв'язку між комп'ютерами (NetBIOS) і надає верхнім рівням транспортні послуги (NetBEUI).

Мережеві протоколи управляють адресацією, маршрутизацією, перевіркою помилок і запитами на повторну передачу. Широко поширені такі з них:

- IP (Internet Protocol), – TCP / IP-протокол для негарантованої передачі пакетів без встановлення з'єднань;
- IPX (Internetwork Packet Exchange), – протокол компанії NetWare для негарантованої передачі пакетів і маршрутизації пакетів;
- NWLink, – реалізація протоколу IPX / SPX компанії Microsoft;

- NetBEUI, – транспортний протокол, що забезпечує послуги транспортування даних для сеансів та додатків NetBIOS.

Всі перераховані протоколи можуть бути поставлені у відповідність тим або іншим рівням еталонної моделі OSI. Але при цьому треба враховувати, що розробники протоколів не занадто строго дотримуються цих рівнів. Наприклад, деякі протоколи виконують функції, що відносяться відразу до декількох рівнів моделі OSI, а інші - тільки частина функцій одного з рівнів. Це призводить до того, що протоколи різних компаній часто виявляються несумісні між собою. Крім того, протоколи можуть бути успішно використані виключно в складі свого набору протоколів (стека протоколів), який виконує більш-менш закінчену групу функцій. Саме це і робить мережеву операційну систему "фірмовою", тобто по суті, – несумісною зі стандартною моделлю відкритої системи OSI.

6.3 Методи взаємодії абонентів у мережі

Модель OSI допускає два основні методи взаємодії абонентів у мережі:

- метод взаємодії без логічного з'єднання (або метод дейтаграм).
- метод взаємодії з логічним з'єднанням.

Метод дейтаграм – це найпростіший метод, в якому кожен пакет розглядається як самостійний об'єкт (рис. 5). Пакет при цьому методі передається без встановлення логічного каналу, тобто без попереднього обміну службовими пакетами для з'ясування готовності приймача, а також без ліквідації логічного каналу, тобто без пакета підтвердження закінчення передачі. Дійде пакет до приймача чи ні – невідомо (перевірка факту отримання переноситься на більш високі рівні).

Метод дейтаграм (рис. 6.2) висуває підвищені вимоги до апаратури (так як приймач завжди повинен бути готовий до прийому пакета). Переваги методу в тому, що передавач і приймач працюють незалежно один від одного, до того ж пакети можуть накопичуватися в буфері і потім передаватися разом, можна також використовувати трансляцію передачу, тобто адресувати пакет всім абонентам одночасно. Недоліки методу - це можливість втрати пакетів, а також марною завантаження мережі пакетами в разі відсутності або неготовності приймача.

Метод з логічним з'єднанням (рис. 6.3) розроблений пізніше, ніж метод дейтаграм, і відрізняється ускладненим порядком взаємодії.

При цьому методі пакет передається тільки після того, як буде встановлено логічне з'єднання (канал) між приймачем і передавачем. Кожному інформаційному пакету супроводжує один або кілька службових пакетів (установка з'єднання, підтвердження отримання, запит повторної передачі, розрив з'єднання). Логічний канал може встановлюватися на час передачі одного або декількох пакетів.

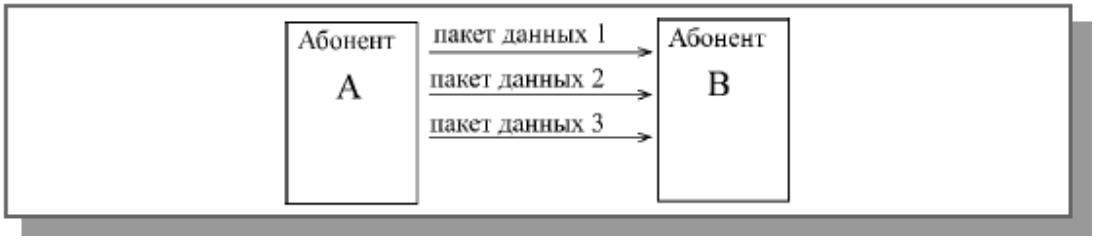


Рисунок 6.2 – Метод дейтаграм

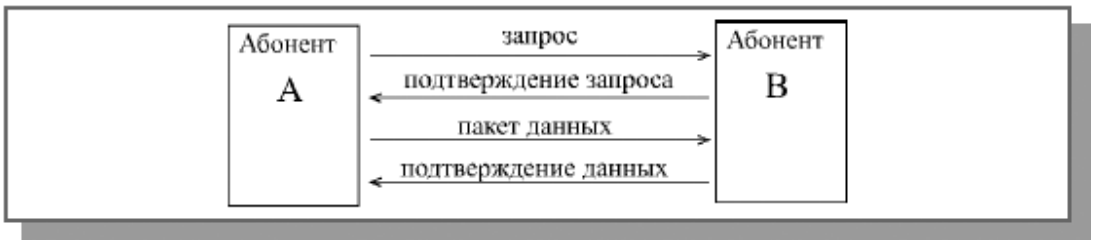


Рисунок 6.3 – Метод з логічним з'єднанням

Метод з логічним з'єднанням, як уже говорилося, більш складний, ніж метод дейтаграм, але набагато надійніше, оскільки до моменту ліквідації логічного каналу передавач впевнений, що всі його пакети дійшли до місця призначення, причому дійшли успішно. Не буває при даному методі і перевантаження мережі через марних пакетів. Недолік методу з логічним з'єднанням полягає в тому, що досить складно вирішити ситуацію, коли приймає абонент з тих чи інших причин не готовий до обміну, наприклад, через обрив кабелю, відключення живлення, несправності мережного обладнання, збою в комп'ютері. При цьому потрібно алгоритм обміну з повторенням непідтвердженого пакету задану кількість разів, причому важливий і тип непідтвердженого пакету. Не може цей метод передавати широкомовні пакети (тобто адресовані всім абонентам), так як не можна організувати логічні канали відразу з усіма абонентами.

Приклади протоколів, що працюють за методом дейтаграмм: протоколи IP і IPX.

Приклади протоколів, що працюють за методом з логічним з'єднанням: TCP і SPX.

Саме для того, щоб об'єднати переваги обох методів, ці протоколи використовуються у вигляді зв'язаних наборів: TCP / IP і IPX / SPX, в яких протокол більш високого рівня (TCP, SPX), що працює на базі протоколу нижчого рівня (IP, IPX) , гарантує правильну доставку пакетів в потрібному порядку.

Протоколи IPX / SPX, розроблені компанією Novell, утворюють набір (стек), використовуваний в мережевих програмних засобах досить широко поширених локальних мереж Novell (NetWare). Це порівняно невеликий і швидкий протокол, що підтримує маршрутизацію. Прикладні програми можуть звертатися безпосередньо до рівня IPX, наприклад, для посилки широкомовних повідомлень, але значно частіше працюють з рівнем SPX, що гарантує швидку і надійну доставку пакетів. Якщо швидкість не надто важлива, то прикладні програми застосовують ще більш високий рівень, наприклад, протокол NetBIOS, що надає зручний сервіс. Компанією Microsoft запропонована своя реалізація протоколу IPX / SPX, звана NWLink. Протоколи IPX / SPX і NWLink підтримуються операційними системами NetWare і Windows. Вибір цих протоколів забезпечує сумісність по мережі будь-яких абонентів з даними операційними системами.

Набір (стек) протоколів TCP / IP був спеціально розроблений для глобальних мереж і для міжмережевого взаємодії. Він спочатку орієнтований на низьку якість каналів зв'язку, на велику ймовірність помилок і розривів зв'язків. Цей протокол прийнятий у всесвітній комп'ютерній мережі Інтернет, значна частина абонентів якої підключається по комутованих лініях (тобто звичайними телефонними лініями). Як і протокол IPX / SPX, TCP / IP також підтримує маршрутизацію. На його основі працюють протоколи вищих рівнів, такі як SMTP, FTP, SNMP. Недолік протоколу TCP / IP-більш низька швидкість роботи, ніж у IPX / SPX. Однак зараз протокол TCP / IP використовується і в локальних мережах, щоб спростити узгодження протоколів локальних і глобальних мереж. В даний час він вважається основним в найпоширеніших операційних системах.

В стек протоколів TCP / IP часто включають і протоколи всіх верхніх рівнів (рис. 6.4). І тоді вже можна говорити про функціональної повноті стека TCP / IP.

Як протокол IPX, так і протокол IP є самими низькорівневими протоколами, тому вони безпосередньо інкапсулюють свою інформацію, звану дейтаграмою, до

поля даних переданого по мережі пакету (рис. 6.5). При цьому в заголовок дейтаграми входять адреси абонентів (відправника та одержувача) більш високого рівня, ніж MAC-адреси, – це IPX-адреси для протоколу IPX або IP-адреси для протоколу IP. Ці адреси включають номера мережі й вузла, хоста (індивідуальний ідентифікатор абонента). При цьому IPX-адреси (Рис. 8) більш прості, мають всього один формат, а в IP-адресу (Рис. 9) можуть входити три формату (класу A, B і C), що розрізняються значеннями трьох початкових бітів.

Рисунок 6.4 – Співвідношення рівнів моделі OSI і стека протоколів TCP / IP5

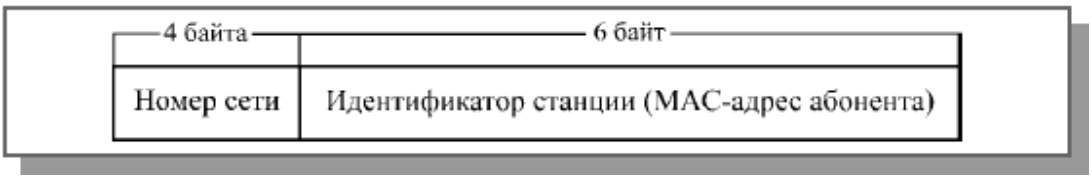


Рисунок 6.5 – Формат IPX-адреси

Цікаво, що IP-адреса не має ніякого зв'язку з MAC-адресами абонентів. Номер вузла в ньому присвоюється абоненту незалежно від його MAC-адреси. В якості ідентифікатора станції IPX-адреса включає в себе повний MAC-адресу одержувача.

Номер мережі – це код, присвоєний кожної конкретної мережі, тобто кожній широкомовної області загальної, єдиної мережі. Під широкомовної областю розуміється частина мережі, яка прозора для широкомовних пакетів, пропускає їх безперешкодно.

Протокол NetBIOS (мережева базова система вводу / виводу) був розроблений компанією IBM для мереж IBM PC Network і IBM Token-Ring за зразком системи BIOS персонального комп'ютера. З тих пір цей протокол став фактичним стандартом (офіційно він не стандартизований), і багато мережеві операційні системи містять у собі емулятор NetBIOS для забезпечення сумісності. Спочатку NetBIOS реалізовував сеансовий, транспортний і мережевий рівні, проте в подальших мережах на більш низьких рівнях використовуються стандартні протоколи (наприклад, IPX / SPX), а на частку емулятора NetBIOS залишається тільки сеансовий рівень. NetBIOS забезпечує більш високий рівень сервісу, ніж IPX / SPX, але працює повільніше.

На основі протоколу NetBIOS був розроблений протокол NetBEUI, який являє собою розвиток протоколу NetBIOS до транспортного рівня. Однак недолік NetBEUI полягає в тому, що він не підтримує межсетевое взаємодію і не забезпечує маршрутизацію. Тому даний протокол використовується тільки в простих мережах, не розрахованих на підключення до Інтернет. Складні мережі орієнтуються на більш універсальні протоколи TCP / IP і IPX / SPX. Протокол NetBEUI в даний час вважається застарілим, хоча навіть в операційній системі Windows XP передбачена його підтримка, правда, тільки як додаткова опція.

Нарешті, згадуваний уже набір протоколів OSI – це повний набір (стек) протоколів, де кожен протокол точно відповідає певному рівню стандартної моделі OSI. Набір містить Маршрутизовані і транспортні протоколи, серії протоколів IEEE 802, протокол сеансового рівня, представницького рівня і кілька протоколів прикладного рівня. Поки широкого поширення цей набір протоколів не отримав, хоча він і повністю відповідає еталонної моделі OSI.

6.4 Стандартні мережеві програмні засоби

Функції верхніх рівнів еталонної моделі OSI виконують мережеві програмні засоби. Для установки мережі досить мати набір мережевого обладнання, його драйвери, а також мережеве програмне забезпечення. Від вибору програмного забезпечення залежить дуже багато: припустимий розмір мережі, зручність використання і контролю мережі, режими доступу до ресурсів, продуктивність мережі в різних режимах і т.д. Правда, замінити одну програмну систему на іншу значно простіше, ніж змінити обладнання.

З точки зору розподілу функцій між комп'ютерами мережі, всі мережі можна розділити на дві групи:

Однорангові мережі, що складаються з рівноправних (з погляду доступу до мережі) комп'ютерів. Мережі на основі серверів, в яких існують тільки виділені (dedicated) сервери, які займаються виключно мережевими функціями. Виділений сервер може бути єдиним чи їх може бути кілька. Згідно з цим, виділяють і типи програмних засобів, що реалізують дані види мереж.

6.5 Однорангові мережі

Однорангові мережі (Peer-to-Peer Network) і відповідні програмні засоби, як правило, використовуються для об'єднання невеликої кількості комп'ютерів (Рис. 6.10). Кожен комп'ютер такої мережі може одночасно бути і сервером і клієнтом мережі, хоча цілком припустиме призначення одного комп'ютера тільки сервером, а іншого тільки клієнтом. Принципова можливість суміщення функцій клієнта і сервера. Важливо також і те, що в однорангової мережі будь-який сервер може бути невиділений (non-dedicated), може не тільки обслуговувати мережу, але й працювати як автономний комп'ютер (щоправда, запити до нього по мережі сильно знижують швидкість його роботи). У тимчасової мережі можуть бути і виділені сервери, тільки обслуговуючі мережу.

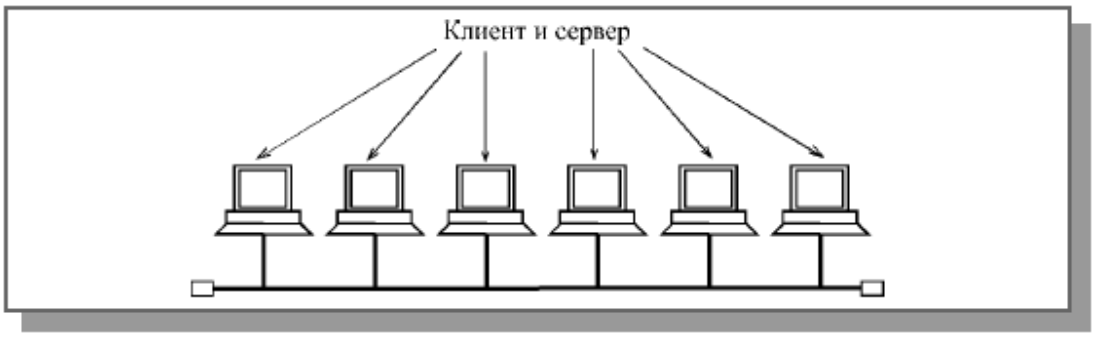


Рисунок 6.6 – Однорангова мережа

Саме в даному випадку найбільш правильно говорити про розподілених дискових ресурсах, про віртуальному комп'ютері, а також про підсумовуванні обсягів дисків всіх комп'ютерів мережі. Якщо всі комп'ютери є серверами, то будь-який файл, створений на одному з них відразу ж стає доступним всім іншим комп'ютерам, його не треба передавати на централізований сервер.

Перевагою однорангових мереж є їх висока гнучкість: в залежності від конкретної задачі мережа може використовуватися дуже активно або зовсім не використовуватися. Через великий самостійності комп'ютерів у таких мережах рідко буває ситуація перевантаження (до того ж кількість комп'ютерів зазвичай невелика). Установка однорангових мереж досить проста, до того ж не потрібні додаткові дорогі сервери. Крім того, немає необхідності в системному адмініструванні, користувачі можуть самі управляти своїми ресурсами.

В однорангових мережах допускається визначення різних прав користувачів щодо доступу до мережевих ресурсів, але система розмежування прав не надто розвинена. Якщо кожен ресурс захищений своїм паролем, то користувачеві доводиться запам'ятовувати велику кількість паролів.

До недоліків однорангових мереж відносяться також слабка система контролю і протоколювання роботи мережі, труднощі з резервним копіюванням розподіленої інформації. До того ж вихід з ладу будь-якого комп'ютера-сервера призводить до втрати частини загальної інформації, тобто всі такі комп'ютери повинні бути по можливості високонадійними. Ефективна швидкість передачі інформації по тимчасовій мережі часто виявляється недостатньою, оскільки важко забезпечити швидкодія процесорів, великий об'єм оперативної пам'яті і високі швидкості обміну з жорстким диском для всіх комп'ютерів мережі. До того ж комп'ютери мережі працюють не тільки на мережу, але й вирішують інші завдання.

Кілька прикладів однорангових мережевих програмних засобів:

- NetWare Lite компанії Novell (зараз вже не виробляється);
- LANtastic компанії Artisoft (випуск практично припинений);
- Windows for Workgroups компанії Microsoft (перша версія ОС Windows з вбудованою підтримкою мережі, випущена в 1992 році);
- Windows NT Workstation компанії Microsoft;
- Windows 95 ... Windows XP компанії Microsoft.

Перші однорангові мережні програмні засоби представляли собою мережеві оболонки, що працюють під управлінням DOS (наприклад, NetWare Lite). Вони перехоплювали всі запити DOS, ті запити, які викликані зверненнями до мережевих пристроїв, оброблялися і виконувалися мережевий оболонкою, а ті, які

викликані звертаннями до "місцевим", немережевим ресурсів, поверталися назад в DOS і оброблялися стандартним чином.

Пізніші однорангові мережні програмні засоби вже були вбудовані в операційну систему Windows. Це набагато зручніше, так як виключається етап установки мережевих програм. Тому мережеві оболонки зараз вже практично не використовуються, хоча багато їх характеристики були помітно краще, ніж у мережевих засобів Windows.

Зараз вважається, що однорангова мережа найбільш ефективна в невеликих мережах (близько 10 комп'ютерів). При значній кількості комп'ютерів мережеві операції сильно сповільнять роботу комп'ютерів і створять безліч інших проблем. Тим не менш, для невеликого офісу однорангова мережа – оптимальне рішення.

Найпоширеніша в даний момент однорангова мережа – це мережа на основі Windows XP (або більш ранніх версій ОС Windows).

При цьому користувач, купуючи комп'ютер з встановленою операційною системою, автоматично отримує і можливість виходу в мережу. Природно, це в багатьох випадках набагато зручніше, ніж купувати і встановлювати нехай навіть і більш досконалі продукти інших фірм.

Якщо набуття комп'ютер ще й має встановлений мережевий адаптер, то побудувати мережу користувачеві зовсім просто. Треба тільки з'єднати комп'ютери кабелем і налаштувати мережеві програми.

У Windows передбачена підтримка спільного використання дисків (в тому числі гнучких дисків і CD), а також принтерів. Є можливість об'єднання всіх користувачів у робочі групи для більш зручного пошуку необхідних ресурсів і організації доступу до них. Користувачі мають доступ до вбудованої системи електронної пошти. Це означає, що всі користувачі мережі отримують можливість спільно застосовувати багато ресурсів ОС свого комп'ютера.

При налаштуванні мережі користувач повинен вибрати тип мережного протоколу. За замовчуванням використовується протокол TCP / IP, але можливе застосування IPX / SPX (NWLink), а також NetBEUI. При виборі TCP / IP можна задавати адреси IP вручну або за допомогою автоматичної настройки адресації (в цьому випадку комп'ютер сам привласнить собі адресу з діапазону, не використовуваного в Інтернет).

Крім того, треба задати індивідуальне ім'я комп'ютера і визначити робочу групу, до якої він відноситься.

Після цього можна дозволити доступ по мережі до ресурсів кожного комп'ютера мережі, до його файлів, папок, принтерів, сканерів, доступу в Інтернет.

6.6 Мережі на основі сервера

Мережі на основі сервера (Server-based Network) застосовуються в тих випадках, коли в мережу повинне бути об'єднано багато користувачів. У цьому випадку можливостей одноранговой мережі може не вистачити. Тому в мережу включається спеціалізований комп'ютер – сервер, який обслуговує тільки мережу і не вирішує жодних інших завдань (рис. 6.7). Такий сервер називається виділеним. Сервер може бути і спеціалізований на вирішенні однієї задачі, наприклад, сервер друку, але найчастіше серверами виступають саме комп'ютери. У мережі може бути і кілька серверів, кожен з яких вирішує свою задачу.

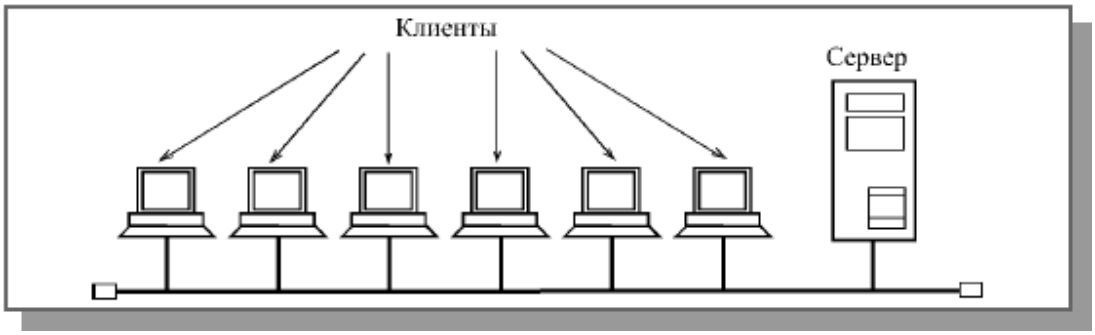


Рисунок 6.7 – Мережа на основі сервера

Сервери спеціально оптимізовані для швидкої обробки мережевих запитів на колективні ресурси і для керування захистом файлів і каталогів. При великих розмірах мережі потужності одного сервера може виявитися недостатньо, і тоді в мережу включають декілька серверів. Сервери можуть виконувати і деякі інші завдання: мережевий друк, вихід у глобальну мережу, зв'язок з іншою локальною мережею, обслуговування електронної пошти і т.д. Кількість користувачів мережі на основі сервера може досягати декількох тисяч. Одноранговой мережею такого розміру просто неможливо було б керувати. Крім того, в мережі на основі серверів можна легко міняти кількість підключаються комп'ютерів, такі мережі називаються масштабованими.

У будь-якому випадку в мережі на основі сервера існує чіткий поділ комп'ютерів на клієнтів (або робочі станції) і сервери. Клієнти не можуть працювати як сервери, а сервери – як клієнти і як автономні комп'ютери. Очевидно, що всі мережеві дискові ресурси можуть розташовуватися тільки на сервері, а клієнти можуть звертатися тільки до сервера, але не один до одного. Однак це не означає, що вони не можуть спілкуватися між собою, просто пересилка інформації від одного клієнта до іншого можлива тільки через сервер, наприклад, через каталог, доступний всім клієнтам. В даному випадку реалізується деяка "логічна зірка" з сервером в центрі, хоча фізична топологія мережі може бути будь-хто.

Гідністю мережі на основі сервера часто називають надійність. Це вірно, але тільки з однією обмовкою: якщо сервер дійсно дуже надійний. В іншому випадку будь-яка відмова сервера призводить до повного паралічу мережі на відміну від ситуації з однорангової мережею, де відмова одного з комп'ютерів не призводить до відмови всієї мережі. Безперечне достоїнство мережі на основі сервера – висока швидкість обміну, так як сервер завжди оснащується швидким процесором (або навіть декількома процесорами), оперативною пам'яттю великого об'єму і швидкими жорсткими дисками. Так як всі ресурси мережі зібрані в одному місці, можливе застосування набагато потужніших засобів управління доступом, захисту даних, протоколювання обміну, ніж в однорангових мережах.

До недоліків мережі на основі сервера відносяться її громіздкість у разі невеликої кількості комп'ютерів, залежність всіх комп'ютерів-клієнтів від сервера, більш висока вартість мережі внаслідок використання дорогого сервера. Але, говорячи про вартість, треба також враховувати, що при одному і тому ж обсязі мережевих дисків великої диск сервера виходить дешевше, ніж багато дисків меншого обсягу, що входять до складу всіх комп'ютерів однорангової мережі.

Приклади деяких мережевих програмних засобів на основі сервера:

- NetWare компанії Novell (найпоширеніша мережна ОС);
- LAN Server компанії IBM (майже не використовується);
- LAN Manager компанії Microsoft;
- Windows NT Server компанії Microsoft;
- Windows Server 2003 компанії Microsoft.

На файл-сервері в даному випадку встановлюється спеціальна мережева операційна система, розрахована на роботу сервера. Ця мережна ОС оптимізована для ефективного виконання специфічних операцій по організації мережевого обміну. На робочих станціях (клієнтах) може встановлюватися будь-яка сумісна операційна система, що підтримує мережу.

Для забезпечення надійної роботи мережі при аваріях електроживлення застосовується безперебійне електроживлення сервера. В даному випадку це набагато простіше, ніж при тимчасовій мережі, де бажано оснащувати джерелами безперебійного живлення всі комп'ютери мережі. Для адміністрування мережі (тобто управління розподілом ресурсів, контролю прав доступу, захисту даних, файлової системи, резервування файлів і т.д.) у випадку мережі на основі сервера необхідно виділяти спеціального людини, що має відповідну кваліфікацію. Централізоване адміністрування полегшує обслуговування мережі та дозволяє оперативно вирішувати всі питання. Особливо це важливо для надійного захисту даних від несанкціонованого доступу. У разі ж однорангової мережі можна обійтися і без фахівця-адміністратора, правда, при цьому всі користувачі мережі повинні мати хоч якесь уявлення про адміністрування.

Процес установки серверної мережевий операційної системи набагато складніше, ніж у випадку тимчасової мережі. Так, він включає в себе такі обов'язкові процедури:

- форматування та розбиття на розділи жорсткого диска комп'ютера-сервера;
- привласнення індивідуального імені сервера;
- присвоєння імені мережі;
- встановлення та налаштування мережевого протоколу;
- вибір мережевих служб;
- введення пароля адміністратора.

Мережева операційна система на базі сервера Windows Server 2003 надає користувачам набагато більше можливостей, ніж у випадку тимчасової мережі.

Вона дозволяє будувати складні ієрархічні структури мережі на основі логічних груп комп'ютерів (доменів, domain), наборів доменів (дерев, tree) і наборів дерев (лісу, forest).

Домен являє собою групу комп'ютерів, керованих контролером домену, спеціальним сервером. Домен використовує власну базу даних, що містить облікові записи користувачів, і управляє власними ресурсами, такими як принтери та загальні файли. Кожному домену присвоюється своє ім'я (зазвичай домен розглядається як окрема мережа зі своїм номером). У кожен домен може входити кілька робочих груп, які формуються з користувачів, які вирішують загальну або подібні завдання. В принципі домен може включати тисячі користувачів, проте зазвичай домени не надто великі, і кілька доменів об'єднуються в дерево доменів. Це спрощує управління мережею. Точно так само кілька дерев може об'єднуватися в ліс, найбільшу адміністративну структуру, підтримувану даної ОС.

У процесі установки Windows Server 2003 необхідно задати тип протоколу мережі. За замовчуванням використовується TCP / IP, але можливе застосування NWLink (IPX / SPX).

Кожному серверу необхідно призначити роль, яку він буде виконувати в мережі:

- контролер домену (управляє роботою домену);
- файловий сервер (зберігає спільно використовувані файли);
- сервер друку (управляє мережевим принтером);
- Web-сервер (містить сайт, доступний по мережі Інтернет або по локальній мережі);
- комунікаційний сервер (забезпечує роботу електронної пошти і конференцій);
- сервер віддаленого доступу (забезпечує віддалений доступ).

Кожному користувачеві мережі необхідно привласнити своє облікове ім'я та пароль, а також права доступу до ресурсів (повноваження). Права доступу можуть задаватися як індивідуально, так і цілої робочій групі користувачів. Windows Server 2003 забезпечує наступні види повноважень для папок:

- повний контроль (перегляд, читання, запис, видалення папки, підпапок, файлів, запуск на виконання, установка прав доступу до папки);
- зміна (перегляд, читання, запис, видалення підпапок і файлів, запуск на виконання);
- читання і виконання (перегляд, читання, запуск на виконання);
- перегляд вмісту папки;

- запис нового вмісту в папку;
- читання інформації з папки.

Ті ж самі рівні повноважень (крім перегляду вмісту) передбачені і для файлів, доступних по мережі.

Мережні операційні системи NetWare компанії Novell сьогодні дуже популярні, що пояснюється їх високою продуктивністю, сумісністю з різними апаратними засобами і розвиненою системою засобів захисту даних. Компанія Novell випускає мережеві програмні засоби з 1979 року: кілька версій мережевих ОС на базі файлових серверів (одна з останніх версій – NetWare 6 і 6.5), клієнтське програмне забезпечення, а також засоби діагностики роботи мереж. Популярні донедавна мережеві оболонки однорангових мереж, такі як NetWare Lite і Personal NetWare зараз вже не виробляються.

Відмінною особливістю мережевих програмних засобів Novell завжди була їхня відкритість, тобто сумісність з операційними системами різних фірм: Windows, UNIX, Macintosh, OS / 2. Крім того, вони завжди забезпечували можливість роботи з апаратними засобами практично всіх відомих виробників. Це дозволяє будувати на їх основі мережі з різноманітних абонентів – від найпростіших до найскладніших.

Всі мережеві продукти NetWare допускають підключення бездискових робочих станцій (клієнтів), що дозволяє при необхідності значно знизити вартість мережі. У всіх продуктах передбачена підтримка мережевих мостів.

Продуктам Novell NetWare властиві і недоліки, наприклад, їх вартість для невеликих мереж виявляється досить високою в порівнянні з ціною продуктів інших виробників. Крім того, їх установка порівняно складна, але вони вже стали фактичним стандартом, тому їх позиції на ринку досить міцні.

Розглянемо коротко особливості мережевої ОС Novell NetWare 6.5.

Як і у випадку Microsoft Windows Server 2003, Novell NetWare 6.5 вимагає створення деревовидної ієрархічної структури, що включає в себе мережеві дерева, сервери, користувачів, групи та інші об'єкти.

Novell NetWare 6.5 передбачає обов'язкове розбиття жорстких дисків з використанням власної системи зберігання файлів NSS (Novell Storage Services),

яке вимагає створення логічних розділів (Volumes) на диску. Це дозволяє серверу більш ефективно вирішувати мережеві задачі.

Для кожного сервера мережі треба вибрати один з трьох типів, а саме.

- Настроюваний сервер (зокрема, Web-сервер, FTP-сервер).
- Основний файловий сервер.
- Спеціальний сервер (наприклад, DNS / DHCP-сервер, контролюючий мережеві адреси та імена, чи сервер резервного копіювання).
- Крім того, треба задати тип використовуваного протоколу – TCP / IP або IPX / SPX.

На комп'ютери-клієнти слід встановити клієнтське програмне забезпечення. Це порівняно проста процедура.

Кожному клієнту надається обліковий запис, надаються свої права доступу до ресурсів. Клієнти можуть бути об'єднані в робочі групи, кожній з яких присвоюються імена і права доступу.

Передбачені наступні види доступу до файлів і каталогів (папок):

- зміна прав доступу до каталогу чи файлу;
- перегляд каталогу;
- створення каталогів і файлів в даному каталозі;
- видалення каталогів і файлів в даному каталозі;
- зміна вмісту файлів;
- будь-які операції над файлами каталогу;
- запис до файлу.

7 ЗАСОБИ КЕРУВАННЯ МЕРЕЖАМИ

7.1 Класифікація засобів моніторингу та аналізу

Всі засоби моніторингу та аналізу мереж, можна розділити на кілька великих класів:

Системи управління мережею (Network Management Systems) – централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці

системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею – включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п. Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView.

Засоби управління системою (System Management). Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому – комунікаційне устаткування. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку.До найбільш відомих систем управління системами відносяться LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks і CA Unicenter.

Вбудовані системи діагностики і управління (Embedded Systems). Ці системи виконуються у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління концентратором Distrebuted 5000, реалізує функції автосигментаціеї портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора і деякі інші. Як правило, вбудовані модулі управління також виконують роль SNMP-агентів, які поставляють дані про стан пристрою системам управління.

Аналізатори протоколів (Protocolanalyzers). Представляють собою програмні або апаратно-програмні системи, які обмежуються на відміну від систем управління лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах – зазвичай кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують повне декодування захоплених пакетів, тобто показувати в зручній для

користувача формі вкладеність пакетів протоколів різних рівнів один в одного з розшифруванням змісту окремих полів кожного пакета.

Обладнання для діагностики і сертифікації кабельних систем. Умовно це устаткування можна поділити на чотири основні групи: мережні монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультиметри). Мережеві монітори (називають також мережевими аналізаторами) призначені для тестування кабелів різних категорій. Слід розрізняти мережеві монітори і аналізатори протоколів. Мережеві монітори збирають дані лише про статистичні показники трафіку – середньої інтенсивності загального трафіку мережі, середньої інтенсивності потоку пакетів з певним типом помилки і т.п. Призначення пристроїв для сертифікації кабельних систем, безпосередньо випливає з їх назви. Сертифікація виконується відповідно до вимог одного з міжнародних стандартів на кабельні системи. Кабельні сканери використовуються для діагностики мідних кабельних систем. Тестери призначені для перевірки кабелів на відсутність фізичного розриву.

Експертні системи. Цей вид систем акумулює людські знання про виявлення причин аномальної роботи мереж і можливі способи приведення мережі у працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу та аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів. Найпростішим варіантом експертної системи є контекстно-залежна help-система. Більш складні експертні системи являють собою так звані бази знань, що володіють елементами штучного інтелекту. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron.

Багатофункціональні пристрої аналізу та діагностики. У зв'язку з розповсюдженням локальних мереж виникла необхідність розробки недорогих портативних приладів, які суміщають функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів і, навіть, деяких можливостей ПЗ мережного управління. Як приклад такого роду пристроїв можна привести Compas компанії MicrotestInc. або 675 LANMeterкомпанії FlukeCorp.

7.2 Системи управління

Відповідно до рекомендацій ISO можна виділити такі функцій **засобів управління мережею**:

Управління конфігурацією мережі,– полягає в конфігурації компонентів мережі, включаючи їх місце розташування, мережні адреси і ідентифікатори, управління параметрами мережевих операційних систем, підтримку схеми мережі: також ці функції використовуються для іменування об'єктів.

Обробка помилок, – це виявлення і усунення наслідків збоїв у роботі мережі.

Аналіз продуктивності, – допомагає на основі накопиченої статистичної інформації оцінювати час відповіді системи і величину трафіка, а також планувати розвиток мережі.

Управління безпекою, – включає в себе контроль доступу та збереження цілісності даних. У функції входить процедура аутентифікації, перевірки привілеїв, підтримка ключів шифрування, управління правами. До цієї ж групи можна віднести важливі механізми управління паролями, зовнішнім доступом, з'єднання з іншими мережами.

Облік роботи мережі, – включає реєстрацію і управління використовуваними ресурсами і пристроями. Ця функція оперує такими поняттями як час використання і плата за ресурси.

З наведеного списку видно, що системи управління виконують не тільки функції моніторингу та аналізу роботи мережі, необхідні для отримання вихідних даних для налаштування мережі, але і включають функції активного впливу на мережу – управління конфігурацією і безпекою, які потрібні для відпрацювання виробленого плану настройки та оптимізації мережі. Сам етап створення плану налаштування мережі зазвичай залишається за межами функцій системи управління, хоча деякі системи управління мають у своєму складі експертні підсистеми, що допомагають адміністратору або интегратору визначити необхідні заходи з настроювання мережі.

Засоби управління мережею (NetworkManagement), не слід плутати із засобами управління комп'ютерами та їх операційними системами (SystemManagement). Типовими представниками засобів управління мережами є системи HPOpenView, SunNetManager і IBMNetView.

Засоби управління системою зазвичай виконують такі функції:

- облік використовуваних апаратних і програмних засобів. Система автоматично збирає інформацію про комп'ютери і створює записи в базі даних про апаратні і програмні ресурси. Після цього адміністратор може швидко з'ясувати, що він має і де це знаходиться. Наприклад, дізнатися про те, на яких комп'ютерах потрібно оновити драйвери принтерів, які ПК мають достатню кількість пам'яті і дискового простору і т. п;
- розподіл й встановлення програмного забезпечення. Після завершення обстеження адміністратор може створити пакети розсилки програмного забезпечення, що являється дуже ефективним способом для зменшення вартості такої процедури. Система може також дозволяти централізовано встановлювати і адмініструвати програми, які запускаються з файлових серверів, а також дати можливість кінцевим користувачам запускати такі програми з будь-якої робочої станції мережі;
- віддалений аналіз продуктивності і виникаючих проблем. Адміністратор може віддалено управляти ресурсами будь-якого ПК, що працює в мережі. База даних системи управління зберігає детальну інформацію про конфігурацію всіх комп'ютерів в мережі для того, щоб можна було виконувати віддалений аналіз виникаючих проблем.

Прикладами засобів управління системою є такі продукти, як SystemManagementServer компанії Microsoft або LANDeskManager фірми Intel.

Останнім часом в області систем управління спостерігаються дві досить чітко виражені тенденції:

інтеграція в одному продукті функцій управління мережами і системами;
розподіленість системи управління, при якій в системі існує кілька консолей, які збирають інформацію про стан пристроїв і систем та видають керуючі дії.

7.3 Стандарти управління мережою

Зведені дані щодо стандартів управління та їх розробників наведено у таблицы 7.1.

Таблиця 7.1 осовністандарти та розробники систем управління мережею

Організація	Стандарти	Особливості
IETF	SNMP	Управління має бути простим, орієнтоване на змінні
ISO	CMIP, CMIS	Управління має бути потужним, об'єктно-орієнтованим
ITU-T	TMN	Визначена тільки архітектура
DMTF	WBEM, CIM	Управління мережами і системами, об'єктно-орієнтоване
OMG	CORBA	Архітектура віддалених об'єктів

Нині найуспішнішим сімейством стандартів є SNMP. Він лідирує за кількістю керованих систем (агентів). Керуючі системи (менеджери) зазвичай підтримують безліч стандартів, тому тут складно говорити про лідерство SNMP. За кількістю вкладених грошей, можливо, лідирує Telecommunications Management Network (TMN).

Показово простежити залежність популярності стандартів від середовища їх застосування. У локальних і глобальних мережах передачі даних, що використовують Протокол інтернету (Internet Protocol, IP) найбільш широко розповсюджений стандарт SNMP. У системах відомчих автоматичних телефонних станцій (ВАТС) та в публічних телефонних мережах найбільш часто використовуються пропрієтарні рішення. У мобільних мережах в основному використовуються рішення на основі стандартів ISO.

Майже всі успіхи SNMP пов'язані з особливостями процесу стандартизації в IETF:

стандарти безкоштовні і вільно розповсюджувані;
стандарти легко доступні в електронній формі;
швидкий розвиток стандартів, продумані етапи стандартизації;
на всіх етапах ведеться технічна експертиза;
робочі групи очолюють технічні, а не політичні лідери;
прототипи систем на основі стандартів демонструють їх придатність.

7.3.1 Протокол SNMP

Створення систем управління мережами неможливе без орієнтації на певні стандарти, тому що управляюче програмне забезпечення та мережеве обладнання розробляють сотні компаній. Оскільки корпоративна мережа напевно неоднорідна,

керуючі інструменти не можуть відображати специфіки однієї системи або мережі. Найбільш поширеним протоколом управління мережами є протокол SNMP (SimpleNetworkManagementProtocol), його підтримують сотні виробників. Головні переваги протоколу SNMP – простота, доступність, незалежність від виробників. Значною мірою саме популярність SNMP затримала прийняття CMIP, варіанта керуючого протоколу за версією OSI. Протокол SNMP розроблений для управління маршрутизаторами в мережі Internet і є частиною стека TCP/IP.

У системах управління, побудованих на основі протоколу SNMP, стандартизуються наступні елементи:

- протокол взаємодії агента і менеджера;
- мова опису моделей MIB та повідомлень SNMP – мова абстрактної синтаксичної нотації ASN.1 (стандарт ISO 8824:1987, рекомендації ITU-T X.208);
- кілька конкретних моделей MIB (MIB-I, MIB-II, RMON, RMON 2), імена об'єктів яких реєструються в дереві стандартів ISO. Все інше віддається на розсуд розробника системи управління.

Протокол SNMP і тісно пов'язана з ним концепція SNMP MIB були розроблені для управління маршрутизаторами Internet як тимчасове рішення. Але, як це часто буває з усім тимчасовим, простота і ефективність вирішення забезпечили успіх цього протоколу, і сьогодні він використовується при управлінні практично будь-якими видами обладнання і програмного забезпечення обчислювальних мереж. І хоча в області управління телекомунікаційними мережами спостерігається стійка тенденція застосування стандартів ITU-T, в які входить протокол CMIP, і тут є досить багато прикладів успішного використання SNMP-управління. Агенти SNMP вбудовуються в аналогові модеми, модеми ADSL, комутатори ATM і т. д.

SNMP – це протокол, що використовується для отримання від мережевих пристроїв інформації про їх статус, продуктивність та характеристики, які зберігаються в спеціальній базі даних мережевих пристроїв, що називається MIB (ManagementInformationBase). Існують стандарти, що визначають структуру MIB, в тому числі набір типів її змінних (об'єктів в термінології ISO), їх імена і допустимі операції цими змінними (наприклад, читати). У MIB, поряд з іншою інформацією, можуть зберігатися мережеві та / або MAC-адреси пристроїв, значення лічильників оброблених пакетів і помилок, номери, пріоритети та

інформація про стан портів. Деревоподібна структура MIB містить обов'язкові (стандартні) піддерева, а також в ній можуть знаходитися приватні (private) піддерева, що дозволяють виробнику інтелектуальних пристроїв реалізувати будь-які специфічні функції на основі його специфічних змінних. Агент в протоколі SNMP – це елемент, який надає менеджерам на керуючих станціях мережі доступ до значень змінних MIB, і тим самим дає їм можливість реалізовувати функції з управління та спостереження за пристроєм. Типова структура системи управління зображена на рисунку 7.1.

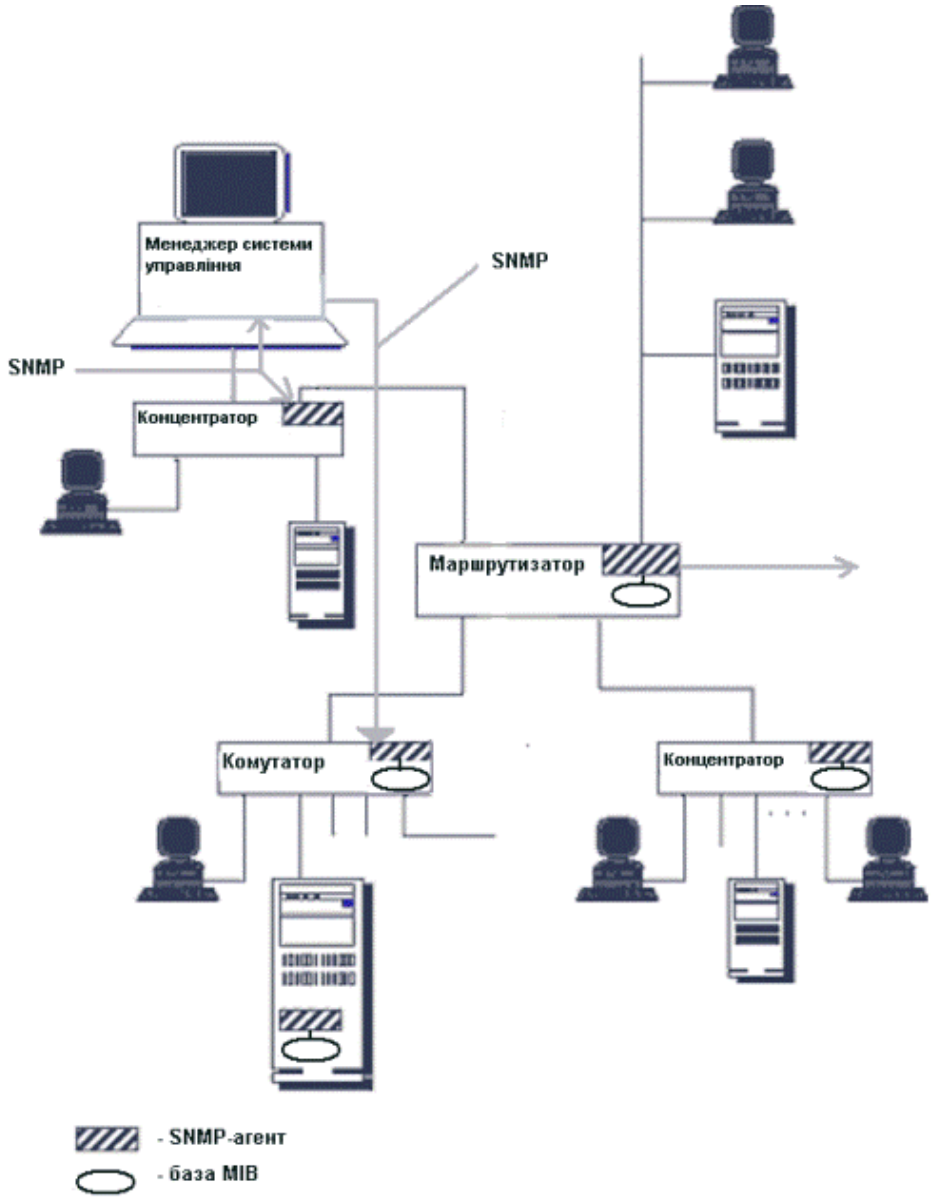


Рисунок 7.1 – Типова структура управління мережею (SNMP)

7.3.2 Стандарти управління OSI

7.3.2.1 Загальні відомості. Концепція SMAE

Модель мережевого управління OSI - OSI Management Framework - визначена в документі ISO / IEC 7498-4: Basic Reference Model, Part 4, Management Framework.

Документ ISO / IEC 7498-4 складається з наступних основних розділів:

Терміни та загальні концепції.
Модель управління системами.
Інформаційна модель.
Функціональні області управління системами.
Структура стандартів управління системами.

Функціональні області управління системами вже були розглянуті вище.

Стандарти ISO в галузі управління використовує термінологію, яка частково збігається з термінологією систем управління SNMP.

Як показано на малюнку, обмін керуючою інформацією з використанням протоколу управління (Management Protocol) відбувається між суб'єктами програм управління системами (Systems Management Application Entities, SMAE):

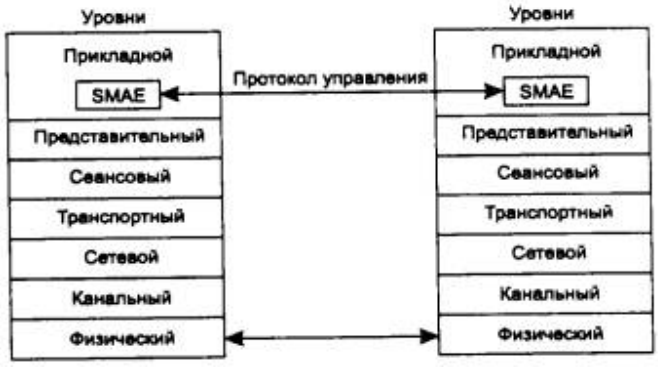


Рисунок 7.2 – Обмін управлінькою інформацією з використанням Management Protocol

Суб'єкти SMAE розташовані на прикладному рівні семирівневої моделі OSI і є елементами служби управління. Під суб'єктом в моделі OSI розуміється активний в даний момент елемент протоколу будь-якого рівня, який бере участь у взаємодії. Прикладами SMAE є агенти та менеджери систем управління.

7.3.2.2 Агенти та менеджери

Визначення функцій агентів і менеджерів в стандартах OSI досить добре узгоджуються з визначеннями систем SNMP, за деякими винятками в термінології. Повідомлення, які агент посилає менеджеру за своєю ініціативою, називаються повідомленнями - notifications.

Наприклад, якщо деякий елемент мережі X відмовив, то менеджеру необхідно оновити свою базу даних конфігурації мережі. Елемент X, який є для системи управління керованим об'єктом (managed object), може послати повідомлення агенту. Елемент X може знаходитися в тій же керованої системі, що і агент, або може перебувати в іншій системі. У свою чергу агент надсилає повідомлення менеджеру про те, що елемент X відмовив. Відповідно до цього повідомленням менеджер оновлює базу даних конфігурації.

ПРИМІТКА. У стандартах Internet під об'єктом розуміється окремий атрибут бази MIB, що є моделлю керованого ресурсу, а в стандартах ISO об'єкт позначає всю модель керованого ресурсу.

Менеджер не тільки збирає і порівнює дані, одержувані від агентів, на основі цих даних він може також виконувати адміністративні функції, керуючи операціями віддалених агентів.

У стандартах OSI різниця між менеджерами та агентами не дуже чітка. Суб'єкт SMAE, що виконує в одній взаємодії роль менеджера, може в іншій взаємодії виконувати роль агента, і навпаки.Стандарти OSI не визначають способів взаємодії агента з керованими об'єктами. Стандарти OSI також не говорять про те, як агент взаємодіє з керованими об'єктами, які перебувають за межами керованої системи, тобто об'єктами, з якими потрібно взаємодіяти через мережу. У таких випадках може знадобитися, наприклад, щоб один агент запросив дані про деякий об'єкт від іншого агента. Порядок такого роду взаємодії також не визначається стандартами OSI.

Щоб менеджер і агент змогли взаємодіяти, кожен повинен мати певні відомості про один одного. Ці відомості модель OSI називає контекстом додатку (Application Context, AC). AC описує елементи прикладного рівня стека OSI, які використовуються агентами і менеджерами.

ПРИМІТКА. Необхідно зазначити, що стандарти управління OSI значною мірою орієнтовані на стек протоколів OSI (саме стек, а не модель OSI), так само як системи управління SNMP орієнтовані на роботу зі стеком TCP / IP.

Прикладний рівень стека OSI включає кілька допоміжних служб загального призначення, які використовуються прикладними протоколами і клієнтськими програмами (в тому числі і додатками управління) для автоматизації найбільш часто виконуваних дій. Це не закінчені протоколи прикладного рівня, подібні протоколах ftp, telnet або NCP, за допомогою яких користувач мережі може виконати якусь корисну дію, а допоміжні системні функції, які допомагають розробнику прикладного протоколу або програми написати її компактно і ефективно. На прикладному рівні стека OSI існують наступні допоміжних служби:

- ACSE (Association Control Service Element). Відповідає за встановлення з'єднань між додатками різних систем. З'єднання (сесія, сеанс) на прикладному рівні OSI носить назву асоціації. Асоціації бувають індивідуальними та груповими (shared);
- RTSE (Reliable Transfer Service Element). Займається підтримкою відновлення діалогу, викликаного розривом нижележащих комунікаційних служб, в рамках асоціації;
- ROSE (Remote Operations Service Element). Організовує виконання програмних функцій на віддалених машинах (аналог служби виклику віддалених процедур RPC).

7.3.2.3 Управління системами, управління рівнем та операції рівня

Основна модель управління OSI включає: управління системами, управління N-рівнем і операції N-рівня. Це розбиття на три області зроблено для того, щоб врахувати всі можливі ситуації, що виникають при управлінні.

Управління системами має справу з керованими об'єктами на всіх семи рівнях OSI, включаючи прикладний рівень. Воно засноване на надійній передачі з встановленням з'єднання керуючої інформації між кінцевими системами.

Необхідно підкреслити, що модель управління OSI не дозволяє використання служб без встановлення з'єднання.

Управління N-рівнем обмежено керованими об'єктами якогось певного рівня семирівневої моделі. Протокол управління використовує при цьому комунікаційні протоколи нижчих рівнів. Управління N-рівнем корисно, коли немає можливості використовувати всі семи рівнів OSI. У цьому випадку допускається користуватися протоколом управління N-рівня, який строго призначений для даного рівня. Прикладами рівневого протоколу управління є протоколи управління для локальних мереж, розроблені інститутом IEEE (SMT технології FDDI), які обмежені рівнями 1 і 2.

Нарешті, операції N-рівня зводяться до моніторингу та управління на основі керуючої інформації, що міститься в комунікаційних протоколах тільки даного рівня. Наприклад, дані моніторингу мережі, що містяться в кадрах STM-n технології SDH, відносяться до операцій N-рівня, а саме фізичного рівня. Стандарти на управління N-рівнем і операції N-рівня не входять в набір стандартів управління OSI. Стандарти OSI розглядають лише управління системами за допомогою повного семирівневого стека.

Основна модель управління системами передбачає виконання керуючих операцій і передачу повідомлень між одноранговими системами, що означає необов'язковість жорсткого розподілу ролей на керуючі та керовані системи. Ця модель полегшує реалізацію розподілених аспектів управління. З іншого боку, допускається реалізація однорангових систем як керуючих і керованих.

7.3.2.4 Інформаційна модель управління

Керований об'єкт – це представлення OSI про ресурс з метою управління. Ресурс може бути описаний як керований об'єкт. Конкретний керований об'єкт - це екземпляр (instance) деякого класу керованих об'єктів. Модель управління OSI широко використовує об'єктно-орієнтований підхід. Клас керованих об'єктів - це набір властивостей, які можуть бути обов'язковими або умовними. За допомогою опису одного класу керованих об'єктів, наприклад комутаторів, можна створити інший клас керованих об'єктів, наприклад комутаторів, що підтримують техніку VLAN, успадкувавши всі властивості класу комутаторів, але додавши нові атрибути.

Для управління ресурсами менеджер і агент повинні бути обізнані про деталі цих ресурсів. Деталізація представлення керованих об'єктів, які потрібні для виконання функцій управління, зберігається в репозиторії, відомому як Management Information Base (MIB). Бази MIB OSI зберігають не тільки описи класів керованих об'єктів, але й характеристики мережі та її елементів. Бази MIB містять характеристики кожної частини керованого обладнання і ресурсів. MIB також включає опис дій, які можуть виконуватися на основі зібраних даних або ж викликані зовнішніми командами. Бази MIB дозволяють зовнішнім системам опитувати, змінювати, створювати і видаляти керовані об'єкти (реальні ресурси мережі при цьому, природно, продовжують працювати). Протокол CMIP і локальні інтерфейси управління забезпечують доступ до цих можливостей.

MIB - це концептуальна модель, і вона не має ніякого зв'язку зі способом фізичного або логічного зберігання даних в ресурсі. Стандарти не визначають аспекти власне зберігання даних. Протоколи OSI визначають синтаксис інформації, що зберігається в MIB, і семантику обміну даними.

7.3.3 Протокол CMIP та послуги CMIS

Доступ до керуючої інформації, що зберігається в керованих об'єктах, забезпечується за допомогою елемента системи управління, званого службою CMSIE (Common Management Information Service Element). Служба CMSIE побудована в архітектурі розподіленого додатку, де частину функцій виконує менеджер, а частина - агент. Взаємодія між менеджером і агентом здійснюється по протоколу CMIP. Послуги, що надаються службою CMSIE, називаються послугами CMIS (Common Management Information Services).

Протокол CMIP та послуги CMIS визначені в стандартах X.710 і X.711 ITU-T. Послуги CMIS поділяються на дві групи: послуги, що ініціюються менеджером (запити), та послуги, що ініціюються агентом (повідомлення).

Послуги, що ініціюються менеджером, включають наступні операції:

M-CREATE, – інструктує агента про необхідність створити новий екземпляр об'єкту певного класу або новий атрибут усередині екземпляра об'єкта;
M-DELETE, – інструктує агента про необхідність видалення деякого екземпляра об'єкту певного класу або атрибуту усередині екземпляра об'єкта;

M-GET, – інструктує агента про повернення значення деякого атрибуту певного екземпляра об'єкту;
M-SET, – інструктує агента про зміну значення деякого атрибуту певного екземпляра об'єкту;
M-ACTION, – інструктує агента про необхідність виконання певної дії над одним або кількома примірниками об'єктів.

Агент ініціює тільки одну операцію: M-EVENT_REPORT - відправка повідомлення менеджеру.

Для реалізації своїх послуг служба CMISE повинна використовувати служби прикладного рівня стека OSI - ACSE, ROSE.

Відмінність послуг CMIS від аналогічних послуг SNMP полягає в більшій гнучкості. Якщо запити GET і SET протоколу SNMP застосовні тільки до одного атрибуту одного об'єкта, то запити M-GET, M-SET, M-ACTION і M-DELETE можуть застосовуватися до більш ніж одного об'єкту. Для цього стандарти CMIP / CMIS вводять такі поняття, як огляд (scoping), фільтрація (filtering) і синхронізація (synchronization).

7.3.4 Порівняння протоколів SNMP та CMIP

Застосування протоколу SNMP дозволяє будувати як прості, так і складні системи управління, а застосування протоколу CMIP визначає деякий, досить високий початковий рівень складності системи управління, так як для його роботи необхідно реалізувати ряд допоміжних служб, об'єктів і баз даних об'єктів.

Агенти CMIP виконують, як правило, більш складні функції, ніж агенти SNMP. Через це операції, які менеджеру можна виконати над агентом SNMP, носять атомарний характер, що призводить до численних обмінів між менеджером і агентом.

Повідомлення (traps) агента SNMP надсилаються менеджеру без очікування підтвердження, що може привести до того, що важливі мережеві проблеми залишаться непоміченими, оскільки відповідне повідомлення виявиться втраченим, у той час як повідомлення агента CMIP завжди передаються за допомогою надійного транспортного протоколу і в разі втрати будуть передані повторно.

Вирішення частини проблем SNMP може бути досягнуто за рахунок застосування більш інтелектуальних MIB (до яких відноситься RMON MIB), але для багатьох пристроїв і ситуацій таких MIB немає (або немає стандарту, або немає відповідної MIB в керованому обладнанні).

Протокол CMIP розрахований на інтелектуальних агентів, які можуть по одній простій команді від менеджера виконати складну послідовність дій.

Протокол CMIP істотно краще масштабується, тому що може впливати відразу на декілька об'єктів, а відповіді від агентів проходять через фільтри, які обмежують передачу керуючої інформації тільки певним агентам і менеджерам.

7.4 Вбудовані засоби моніторингу і аналізу мереж

7.4.1 Агенти SNMP

На сьогоднішній день існує кілька стандартів на бази даних управляючої інформації. Основними є стандарти MIB-I і MIB-II, а також версія бази даних для віддаленого управління RMON MIB. Крім цього, існують стандарти для спеціальних MIB пристроїв конкретного типу, а також приватні MIB конкретних фірм-виробників обладнання.

Початкова специфікація MIB-I визначала лише операції читання значень змінні величини. Операції зміни чи установки значень об'єкта є частиною специфікацій MIB-II.

Версія MIB-I (RFC 1156) визначає до 114 об'єктів, які поділяються на 8 груп:

System, – загальні дані про пристрій (наприклад, ідентифікатор постачальника, час останньої ініціалізації системи).
Interfaces, – описуються параметри мережевих інтерфейсів пристрою (наприклад, їх кількість, типи, швидкості обміну, максимальний розмір пакету).
AddressTranslationTable, – описується відповідність між мережевими і фізичними адресами (наприклад, за протоколом ARP).
InternetProtocol, – дані, що відносяться до протоколу IP (адреси IP-шлюзів, хостів, статистика про IP-пакети).
ICMP, – дані, що пов'язані з протоколом обміну керуючими повідомленнями ICMP.

TCP, – дані, що належать до протоколу TCP.
UDP, – дані, що належать до протоколу UDP (кількість переданих, прийнятих та помилкових UPD-дейтаграмм).
EGP, – дані, що пов'язані з протоколом обміну маршрутною інформацією ExteriorGatewayProtocol, який використовується в мережі Internet (число прийнятих з помилками і без помилок повідомлень).

З цього переліку груп змінних видно, що стандарт MIB-I розроблявся з жорсткою орієнтацією на управління маршрутизаторами, які підтримують протоколи стека TCP/IP.

У версії MIB-II (RFC 1213), прийнятої в 1992 році, був істотно (до 185) розширено набір стандартних об'єктів, а кількість груп збільшилася до 10.

У число об'єктів, що описують кожен конкретний інтерфейс пристрою, включені наступні:

IfType, – тип протоколу, який підтримує інтерфейс. Цей об'єкт приймає значення всіх стандартних протоколів канального рівня, наприклад, rfc877-x25, ethernet-csmacd, iso88023-csmacd, iso88024-tokenBus, iso88025-tokenRing і т. д.
IfMtu, – максимальний розмір пакета мережного рівня, який можна послати через цей інтерфейс.
IfSpeed, – пропускна здатність інтерфейсу в бітах в секунду (100 для Fast Ethernet).
IfPhysAddress, – фізичну адресу порту, для Fast Ethernet ним буде MAC-адреса.
IfAdminStatus, – бажаний статус порту:
up, – готовий передавати пакети;
down, – не готовий передавати пакети;
testing, – знаходиться в тестовому режимі.
IfOperStatus, – фактичний поточний статус порту, має ті ж значення, що і ifAdminStatus.
IfInOctets, – загальна кількість байт, прийняте даним портом, включаючи службові, з моменту останньої ініціалізації SNMP-агента.
IfInUcastPkts, – кількість пакетів з індивідуальним адресою інтерфейсу, доставлених протоколу верхнього рівня.

IfInNUcastPkts, – кількість пакетів з широкомовним або мультівещательнимі адресою інтерфейсу, доставлених протоколу верхнього рівня.
IfInDiscards, – кількість пакетів, які були прийняті інтерфейсом, виявилися коректними, але не були доставлені протоколу верхнього рівня, швидше за все через переповнення буфера пакетів або ж з іншої причини.
IfInErrors, – кількість пакетів, що прийшли, які не були передані протоколу верхнього рівня через виявлення в них помилок.

Окрім об'єктів, що описують статистику за вхідними пакетів, є аналогічні об'єкти, пов'язані з вихідними пакетами. Як видно з опису об'єктів MIB-II, ця база даних не дає детальної статистики по характерних помилок кадрів Ethernet, крім цього, вона не відображає зміну характеристик у часі, що часто цікавить мережевого адміністратора. Ці обмеження були згодом зняті новим стандартом на MIB - RMON MIB, який спеціально орієнтований на збір детальної статистики по протоколу Ethernet, до того ж з підтримкою такої важливої функції, як побудова агентом залежностей статистичних характеристик від часу.

7.4.2 Агенти RMON

Нововведенням до функціональних можливостей SNMP є специфікація RMON, яка забезпечує віддалену взаємодію з базою MIB. До появи RMON протокол SNMP не міг використовуватися віддалено, він допускав лише локальне управління пристроями. База RMONMIB має поліпшений набір властивостей для віддаленого управління, оскільки містить агреговану інформацію про пристрій, що не вимагає передачі по мережі великих обсягів інформації. Об'єкти RMONMIB включають додаткові лічильники помилок в пакетах, гнучкіші засоби аналізу графічних трендів і статистики, більш потужні засоби фільтрації для захоплення і аналізу окремих пакетів, а також більш складні умови встановлення сигналів попередження. Агенти RMONMIB більш інтелектуальні порівняно з агентами MIB-I або MIB-II і виконують значну частину роботи по обробці інформації про пристрій, яку раніше виконували менеджери. Ці агенти можуть розташовуватися усередині різних комунікаційних пристроїв, а також бути виконані у вигляді окремих програмних модулів, що працюють на універсальних ПК і ноутбуках (прикладом може служити LANalyzerNovell).

Об'єкту RMON присвоєно номер 16 в наборі об'єктів MIB, а сам об'єкт RMON об'єднує 10 груп наступних об'єктів:

Statistics, – поточні накопичені статистичні дані про характеристики пакетів, кількості колізій тощо.
History, – статистичні дані, збережені через певні проміжки часу для подальшого аналізу тенденцій їх змін.
Alarms, – порогові значення статистичних показників, при перевищенні яких агент RMON посилає повідомлення менеджеру.
Host, – дані про хости мережі, у тому числі про їх MAC-адресах.
HostTopN, – таблиця найбільш завантажених хостів мережі.
TrafficMatrix, – статистика про інтенсивність трафіка між кожною парою хостів мережі.
Filter, – умови фільтрації пакетів.
PacketCapture, – умови захоплення пакетів.
Event, – умови реєстрації і генерації подій.

Дані групи пронумеровані у вказаному порядку, тому, наприклад, група Hosts має числове ім'я 1.3.6.1.2.1.16.4.

Десяту групу складають спеціальні об'єкти протоколу TokenRing.

Всього стандарт RMONMIB визначає близько 200 об'єктів в 10 групах, зафіксованих в двох документах - RFC 1271 для мереж Ethernet і RFC 1513 для мереж TokenRing.

Відмінною рисою стандарту RMONMIB є його незалежність від протоколу мережевого рівня (на відміну від стандартів MIB-I і MIB-II, орієнтованих на протоколи TCP / IP). Тому, його зручно використовувати в гетерогенних середовищах, що використовують різні протоколи мережевого рівня.

Розглянемо більш докладно групу Statistics, яка визначає, яку інформацію про кадри Ethernet може надати агент RMON.

До групи Statistics входять наступні об'єкти:

etherStatsDropEvents, – загальне число подій, при яких пакети були проігноровані агентом через нестачу його ресурсів. Самі пакети при цьому не обов'язково були втрачені.
etherStatsOrtets, – загальне число байт (включаючи помилкові пакети), прийнятих з мережі (крім заголовка але з байтами контрольної суми).
etherStatsPkts, – загальне число отриманих пакетів (включаючи помилкові).

etherStatsBroadcastPkts, – загальне число хороших пакетів, які були надіслані широкомовною адресою.

etherStatsMulticastPkts, – загальне число хороших пакетів, отриманих за мультівещательнимі адресою.

etherStatsCRCAlign Errors, – загальне число отриманих пакетів, які мали довжину (виключаючи заголовок) між 64 і 1518 байт, не містили ціле число байт (alignment error) або мали невірну контрольну суму (FCS error).

etherStatsUndersizePkts, – загальне число пакетів, які мали довжину менше, ніж 64 байт, але були правильно сформовані.

etherStatsOversizePkts, – загальне число отриманих пакетів, які мали довжину більше, ніж 1518 байт, але були тим не менш правильно сформовані.

etherStatsFragments, – загальне число отриманих пакетів, які не складалися з цілого числа байт або мали невірну контрольну суму і мали до того ж довжину, меншу 64 байт.

etherStatsJabbers, – загальне число отриманих пакетів, які не складалися з цілого числа байт або мали невірну контрольну суму і мали до того ж довжину, більшу 1518 байт.

etherStatsCollisions, – найкраща оцінка числа колізій на даному сегменті Ethernet.

etherStatsPkts640ctets, – загальна кількість отриманих пакетів (включаючи погані) розміром 64 байт.

etherStatsPkts65to1270ctets, – загальна кількість отриманих пакетів (включаючи погані) розміром від 65 до 127 байт.

etherStatsPktsl28to2550ctets, – загальна кількість отриманих пакетів (включаючи погані) розміром від 128 до 255 байт.

etherStatsPkts256to5110ctets, – загальна кількість отриманих пакетів (включаючи погані) розміром від 256 до 511 байт.

etherStatsPkts512tol0230ctets, – загальна кількість отриманих пакетів (включаючи погані) розміром від 512 до 1023 байт.

etherStatsPktsl024tol5180ctets, – загальна кількість отриманих пакетів (включаючи погані) розміром від 1024 до 1518 байт.

Як видно з опису об'єктів, за допомогою агента RMON, вбудованого в повторювач або інше комунікаційне обладнання, можна провести дуже детальний аналіз роботи сегмента Ethernet або Fast Ethernet. Спочатку можна отримати дані про типи помилок в кадрах, що зустрічаються в сегменті, а потім доцільно зібрати

за допомогою группи History залежності інтенсивності цих помилок від часу (в тому числі і прив'язавши їх до часу). Після аналізу тимчасових залежностей часто вже можна зробити деякі попередні висновки про джерело помилкових кадрів і на цій підставі сформулювати більш тонкі умови захоплення кадрів зі специфічними ознаками (задавши умови в групі Filter). Після цього можна провести ще більш детальний аналіз за рахунок вивчення захоплених кадрів, витягуючи їх з об'єктів группи Packet Capture.

Пізніше був прийнятий стандарт RMON 2, який поширює ідеї інтелектуальної RMON MIB на протоколи верхніх рівнів, виконуючи частину роботи аналізаторів протоколів.

7.4.3 Аналізатори протоколів

У ході проектування нової або модернізації старої мережі часто виникає необхідність в кількісному вимірі деяких характеристик мережі таких, наприклад, як інтенсивності потоків даних по лініях зв'язку, затримки, що виникають на різних етапах обробки пакетів, часи реакції на запити того чи іншого виду, частота виникнення певних подій та інших характеристик.

Для цих цілей можуть бути використані різні засоби і насамперед - засоби моніторингу в системах управління мережею, які вже обговорювалися в попередніх розділах. Деякі вимірювання мережі можуть бути виконані і вбудованими в операційну систему програмами.

Але найбільш досконалим засобом дослідження мережі є аналізатор протоколів. Процес аналізу протоколів включає захоплення циркулюючих в мережі пакетів, що реалізують той чи інший мережевий протокол, і вивчення вмісту цих пакетів. Ґрунтуючись на результатах аналізу, можна здійснювати обґрунтовану і зважену зміну будь-якого компонента мережі, оптимізацію її продуктивності, пошук і усунення неполадок. Очевидно, що для того, щоб можна було зробити якісь висновки про вплив деякої зміни на мережу, необхідно виконати аналіз протоколів і до, і після внесення змін.

Аналізатор протоколів є самостійним спеціалізованим пристроєм, або персональним комп'ютером, зазвичай переносним, класу Notebook, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням. Мережева карта і програмне забезпечення, що використовуються повинні відповідати топології мережі (кільце, шина, зірка). Аналізатор підключається до

мережі точно так, як і звичайний вузол. Відмінність полягає в тому, що аналізатор може приймати всі пакети даних, що передаються по мережі, в той час як звичайна станція - лише адресовані їй. Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережевого адаптера і декодує одержувані дані, та додаткового програмного коду, що залежить від типу топології досліджуваної мережі. Крім того, поставляється ряд процедур декодування, орієнтованих на певний протокол, наприклад, IPX. До складу деяких аналізаторів може входити також експертна система, яка може видавати користувачеві рекомендації про те, які експерименти слід проводити в даній ситуації, що можуть означати ті чи інші результати вимірювань, як усунути деякі види несправності мережі.

Незважаючи на відносне різноманіття аналізаторів протоколів, представлених на ринку, можна назвати деякі риси, в тій чи іншій мірі притаманні всім їм:

Інтерфейс користувача. Більшість аналізаторів мають розвинений дружній інтерфейс, який базується, як правило, на Windows чи Motif. Цей інтерфейс дозволяє користувачеві: виводити результати аналізу інтенсивності трафіку; отримувати миттєву і середню статистичну оцінку продуктивності мережі; задавати певні події і критичні ситуації для відстежування їх виникнення; робити декодування протоколів різного рівня і представляти в зрозумілій формі вміст пакетів.

Буфер захоплення. Буфери різних аналізаторів відрізняються за обсягом. Буфер може розташовуватися на мережевій карті, або для нього може бути відведено місце в оперативній пам'яті одного з комп'ютерів мережі. Якщо буфер розташований на мережевій карті, то управління ним здійснюється апаратно, і за рахунок цього швидкість введення підвищується. Однак це призводить до подорожчання аналізатора. У разі недостатньої продуктивності процедури захоплення, частина інформації буде губитися, і аналіз буде неможливий. Розмір буфера визначає можливості аналізу по більш або менш представницьким вибіркам даних, що захоплюються. Але яким би великим не був буфер захоплення, рано чи пізно він заповниться. У цьому випадку або припиняється захоплення, або заповнення починається з початку буфера.

Можливість *вимірювання середньостатистичних показників трафіку в сегменті локальної мережі*, в якому встановлений мережевий адаптер аналізатора.

Вимірюється коефіцієнт використання сегменту, матриці перехресного трафіку вузлів, кількість хороших і поганих кадрів, що пройшли через сегмент.

Можливість роботи з декількома агентами, котрі поставляють захоплені пакети з різних сегментів локальної мережі. Ці агенти найчастіше взаємодіють з аналізатором протоколів за власним протоколом прикладного рівня.

Фільтри. Фільтри дозволяють керувати процесом захоплення даних, і, тим самим, дозволяють економити простір буфера. Залежно від значення певних полів пакета, заданих у вигляді умови фільтрації, пакет або ігнорується, або записується в буфер захоплення. Використання фільтрів значно прискорює і спрощує аналіз, оскільки виключає перегляд непотрібних в даний момент пакетів.

Перемикачі - це деякі умови початку і припинення процесу захоплення даних з мережі, що задаються користувачем. Такими умовами можуть бути виконання ручних команд запуску і зупинки процесу захоплення, тривалість процесу захоплення, поява певних значень в кадрах даних. Перемикачі можуть використовуватися спільно з фільтрами, дозволяючи більш детально й тонко проводити аналіз, а також продуктивніше використовувати обмежений обсяг буфера захоплення.

Пошук. Деякі аналізатори протоколів дозволяють автоматизувати перегляд інформації, що знаходиться в буфері, і знаходити в ній дані по заданим критеріям. У той час, як фільтри перевіряють вхідний потік на предмет відповідності умовам фільтрації, функції пошуку застосовуються до вже накопичених в буфері даних.

Багатоканальність. Деякі аналізатори протоколів дозволяють проводити одночасний запис пакетів від декількох мережевих адаптерів, що зручно для зіставлення процесів, що відбуваються в різних сегментах мережі. Можливості аналізу проблем мережі на фізичному рівні у аналізаторів протоколів мінімальні, оскільки всю інформацію вони отримують від стандартних мережевих адаптерів. Тому вони передають і узагальнюють інформацію фізичного рівня, яку повідомляє їм мережевий адаптер, а вона багато в чому залежить від типу мережного адаптера. Деякі мережні

адаптери повідомляють більш детальні дані про помилки кадрів та інтенсивності колізій в сегменті, а деякі взагалі не передають таку інформацію верхнім рівням протоколів, на яких працює аналізатор протоколів.

Методологія проведення аналізу може бути представлена у вигляді наступних шести етапів:

Захоплення даних.
Перегляд захоплених даних.
Аналіз даних.
Пошук помилок (більшість аналізаторів полегшують цю роботу, визначаючи типи помилок і ідентифікуючи станцію, від якої прийшов пакет з помилкою).
Дослідження продуктивності. Розраховується коефіцієнт використання пропускної здатності мережі або середній час реакції на запит.
Докладне дослідження окремих ділянок мережі. Зміст цього етапу конкретизується в міру того, як проводиться аналіз.

Зазвичай процес аналізу протоколів займає відносно небагато часу - 1-2 робочих дні.

7.5 Обладнання для діагностики та сертифікації кабельних систем

До обладнання даного класу відносяться мережеві аналізатори, прилади для сертифікації кабелів, кабельні сканери і тестери. Перш, ніж перейти до більш докладного огляду цих пристроїв, наведемо деякі необхідні відомості про основні електромагнітні характеристики кабельних систем.

7.5.1 Основні електромагнітні характеристики кабельних систем

Основними електричними характеристиками, що впливають на роботу кабелю, є: затухання, імпеданс (хвильовий опір), перехресні наводки двох кручених пар і рівень зовнішнього електромагнітного випромінювання.

Перехресні наводки між витими парами або NearEndCrosstalk (NEXT) - являють собою результат інтерференції електромагнітних сигналів, що виникають у двох кручених парах. Один з кабелів крученої пари передає сигнал, а другий - приймає. При проходженні сигналу по одному з кабелів, наприклад, по тому, що

передає, у кабелі, що приймає сигнал виникають перехресні наводки. Величина NEXT залежить від частоти переданого сигналу - чим вище величина NEXT, тим краще (для категорії 5 NEXT повинен бути не менше 27 Дб при частоті 100 Мгц, для кабелю категорії 3 на частоті 10 МГц NEXT повинен бути не менше 26 Дб).

Затухання (Attenuation), – являє собою втрату амплітуди електричного сигналу при його поширенні по кабелю. Затухання має два основних джерела: електричні характеристики кабелю і поверхневий ефект. Останній пояснює залежність затухання від частоти. Затухання вимірюється в децибелах на метр. Для кабелю категорії 5 при частоті 100 Мгц загасання не повинно перевищувати 23.6 Дб на 100 м, а для кабелю категорії 3, за стандартом IEEE 802.3 10BASE-T, допустима величина затухання на сегменті довжиною 100 м не повинна перевищувати 11,5 Дб при частоті змінного струму 10 МГц.

Імпеданс (хвильовий опір), – це повний (активне і реактивне) опір в електричному ланцюзі. Імпеданс вимірюється в омах і є відносно постійною величиною для кабельних систем. Для неекранованої крученої пари найбільш часті значення імпедансу, – 100 і 120 Ом. Характерні значення імпедансу для мереж стандарту Ethernet на коаксіальному кабелі становлять 50 Ом, а для мереж стандарту Arcnet, – 93 Ом. Різкі зміни імпедансу по довжині кабелю можуть викликати процеси внутрішнього відображення, що призводять до виникнення стоячих хвиль. Стояча хвиля — тип коливань у неперервному середовищі, при яких кожна точка середовища здійснює періодичний рух зі сталою амплітудою, залежною від її положення. Стоячі хвилі не переносять енергію. Робоча станція, підключена до кабелю у районі вузла стоячої хвилі, не зможе отримувати адресовані їй повідомлення.

Активний опір, – це опір постійному струму в електричному ланцюзі. На відміну від імпедансу активний опір не залежить від частоти і зростає зі збільшенням довжини кабелю. Для неекранованої крученої пари категорії 5 активний опір не повинен перевищувати 9.4 Ом на 100 м.

Ємність, – це властивість металевих провідників накопичувати енергію. Два електричних провідника в кабелі, розділені діелектриком, являють собою конденсатор, здатний накопичувати заряд. Ємність є небажаною величиною, тому її слід робити якомога менше. Високе значення ємності в кабелі приводить до спотворення сигналу і обмежує смугу пропускання лінії. Для кабельних систем категорії 5 значення ємності не повинен перевищувати 5.6нФ на 100 м.

Рівень зовнішнього електромагнітного випромінювання, або електричний шум - це небажана зміна напруги в провіднику. Електричний шум буває двох типів: фоновий і імпульсний. Електричний шум можна також розділити на низько-, середньо- і високочастотний. Джерелами фонового електричного шуму є в діапазоні до 150 КГц лінії електропередачі, телефони і лампи денного світла; в діапазоні від 150 КГц до 20 Мгц комп'ютери, принтери, ксерокси; в діапазоні від 20 МГц до 1 ГГц – теле- і радіопередавачі, мікрохвильові печі. Основними джерелами імпульсного електричного шуму є мотори, перемикачі і зварювальні агрегати. Електричний шум вимірюється в мВ. Кабельні системи на крученій парі не сильно схильні до впливу електричного шуму (на відміну від впливу NEXT).

7.5.2 Мережеві аналізатори

Мережеві аналізатори (не слід плутати їх з аналізаторами протоколів) являють собою еталонні вимірювальні інструменти для діагностики та сертифікації кабелів і кабельних систем. Як приклад можна привести мережеві аналізатори компанії HewlettPackard - HP 4195A і HP 8510C. Мережеві аналізатори містять високоточний частотний генератор і вузькосмуговий приймач. Передаючи сигнали різних частот в передавальну пару і вимірюючи сигнал у приймальній парі, можна виміряти затухання і NEXT. Мережеві аналізатори - це великогабаритні і дорогі прилади, призначені для використання в лабораторних умовах спеціально навченим технічним персоналом.

7.5.3 Кабельні сканери

Дані прилади дозволяють визначити довжину кабелю, NEXT, затухання, імпеданс, схему розводки, рівень електричних шумів і провести оцінку отриманих результатів. Існує досить багато пристроїв даного класу, наприклад, сканери компаній MicrotestInc., FlukeCorp., DatacomTechnologiesInc., ScopeCommunicationInc. На відміну від мережевих аналізаторів сканери можуть бути використані не тільки спеціально навченим технічним персоналом, але навіть адміністраторами-новачками.

Для визначення місця розташування несправності кабельної системи (обриву, короткого замикання, неправильно встановленого роз'єму і т.д.) використовується метод "кабельного радара", або TimeDomainReflectometry (TDR). Суть цього методу полягає в тому, що сканер випромінює в кабель короткий електричний імпульс і вимірює час затримки до приходу відбитого

сигналу. За полярності відображеного імпульсу визначається характер пошкодження кабелю (коротке замикання або обрив). У правильно встановленому і підключеному кабелі відбитий імпульс зовсім відсутній.

Точність вимірювання відстані залежить від того, наскільки точно відома швидкість розповсюдження електромагнітних хвиль у кабелі. У різних кабелях вона буде різною. Швидкість розповсюдження електромагнітних хвиль у кабелі (NVP) зазвичай задається у відсотках до швидкості світла у вакуумі. Сучасні сканери містять в собі електронну таблицю даних про NVP для всіх основних типів кабелів і дозволяють користувачеві встановлювати ці параметри самостійно після попереднього калібрування.

Найбільш відомими виробниками компактних кабельних сканерів є компанії MicrotestInc., WaveTekCorp., ScopeCommunicationInc.

7.5.4 Тестери

Тестери кабельних систем - найбільш прості і дешеві прилади для діагностики кабелю. Вони дозволяють визначити пошкодження кабеля, проте, на відміну від кабельних сканерів, не дають відповіді на питання про те, в якому місці стався збій.

СПИСОК ЛІТЕРАТУРИ

1. Кулаков Ю.О. Комп’ютерні мережі : підручник / Ю. О. Кулаков, Г. М. Луцький. –Київ : Юніор, 2003. – 400с., іл.

2. Кулаков Ю.О. Комп’ютерні мережі : навч. посібник з грифом МОН України / Ю. О. Кулаков, І. А. Жуков. – Вид-во Нац. Авіа. Ун-ту «НАУ-друк», 2009.– 329с.

3. Комп’ютерні мережі. Книга 1 : навч. посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник .– Львів : «Магнолія 2006», 2013. – 256 с.

4. Комп’ютерні мережі. Книга 2 : навч. посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник .– Львів : «Магнолія 2006», 2013. – 328 с.

5. Кулаков Ю.О. Комп’ютерні мережі : навч. посібник / Ю. О. Кулаков, І. А. Жуков. – Київ : Лира, 2009. – 392 с.

6. Буров Є.В. Комп’ютерні мережі : підручник / Є. В. Буров. – Київ : Лира, 2013. – 262 с.

7. Зайченко Ю.П. Комп'ютерні мережі. // Навчальний посібник. Рекомендовано МОНУ. – . Київ, Слово, 2003. – 284 с.

8. Таненбаум Э. С. Компьютерные сети / Э. С. Таненбаум – 5-е изд. – Київ : Лира, 2012. – 960 с.

9. Лунтовський А. О. Проектування та дослідження комп'ютерних мереж : навч. посіб. (гриф МОН) / А. О. Лунтовський, І. В. Мельник – Київ : Лира, 2010. – 361 с.

10. В. Олифер, Н. Олифер. Компьютерные сети. Принципы, технологии, протоколы : Учебник для вузов. – 4-е изд. – Київ : Лира, 2012. – 944 с.

11. Кривуцы В. Г. Телекоммуникационные сети и технологии. – Київ : Лира, 2007. – 324 с.

Навчальне видання

КАРПЕНКО Микола Юрійович
МАКОГОН Наталія Вікторівна

КОНСПЕКТ ЛЕКЦІЙ
з курсу

КОМП'ЮТЕРНІ МЕРЕЖІ

(для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки, 151 – Автоматизація та комп'ютерно-інтегровані технології, 126 – Інформаційні системи та технології)

Відповідальний за випуск *О. Б. Костенко*

За авторською редакцією
Комп'ютерне верстання *М. Ю. Карпенко*

План 2017, поз. 249 Л

Підп. до друку 03.07.2017. Формат 60×84/16
Друк на ризографі Ум. друк. арк. 4,2
Тираж 50 пр. Зам. №

Видавець і виготовлювач:
Харківський національний університет
міського господарства імені О. М. Бекетова,
вул. Маршала Бажанова, 17, Харків, 61002
Електронна адреса: rectorat@kname.edu.ua
Свідоцтво суб'єкта видавничої справи:
ДК № 5328 від 11.04.2017.