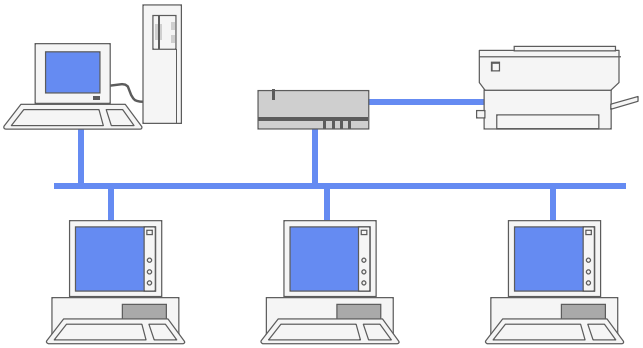
Міністерство освіти України
Львівський державний університет імені Івана Франка

В.М.Горлач, В.М.Макар

Побудова та адміністрування INTRANET-мереж

Частина 1 Основи мережних технологій

Тексти лекцій



Рекомендовано до друку
науково-методичною радою
факультету прикладної математики та інформатики
Протокол № 3 від 13.05.99
Методичні матеріали ТЛ № 3/99

Львів ЛДУ 1999

Горлач В.М., Макар В.М. Побудова та адміністрування INTRANET-мереж. Ч. 1. Основи мережних технологій: Тексти лекцій.– Львів: Видавничий центр Львів. ун-ту, 1999.– 45 с.

У текстах лекцій особлива увага приділена принципам організації та функціонування комп'ютерних мереж. Висвітлені питання використання мережних сервісів, класифікації мереж, характеристик середовища передавання даних, еталонної моделі взаємодії відкритих систем, мережних топологій, методів передавання даних та доступу до середовища передавання. Описані основні архітектури сучасних комп'ютерних мереж, розглянуто окремі питання адресації та маршрутизації в мережі Internet, дано порівняльні характеристики найбільш поширених мережних операційних систем.

Для студентів факультету прикладної математики та інформатики, а також широкого кола користувачів комп'ютерних мереж.

Рецензенти: канд. фіз.-мат. наук Р.Є. Рикалюк
(Львівський державний університет імені Івана Франка);

канд. фіз.-мат. наук Ю.В. Нікольський
(Державний університет "Львівська політехніка").

Редактор М.В. Ріпей

Зміст

Лекція 1. Комп'ютерні мережі та їх класифікація

Виникнення комп'ютерних мереж

Інтенсивний розвиток мережних технологій пов'язаний з появою в 1960-х роках великих обчислювальних машин, або мейнфреймів (mainframe) серії IBM 360. Складний комплекс електронних та електромеханічних пристроїв, зокрема периферійних (зовнішніх) пристроїв-накопичувачів на магнітних стрічках, барабанах та дисках, потребував спеціальних умов експлуатації та великого штату обслуговуючого персоналу. Для більш ефективного використання цієї техніки створювались обчислювальні центри, до складу яких, звичайно, входили комп'ютери різної потужності та комплекс периферійних пристроїв. Концентрація обчислювальних потужностей вимагала їх колективного використання. Так з'явились перші системи телеобробки (обробки на відстані) завдань, що грунтувались на використанні різних типів термінальних (також і інтелектуальних) пристроїв, які могли знаходитись і за межами обчислювальних центрів. Поява персональних комп'ютерів та необхідність обміну інформацією між їх користувачами суттєво прискорили розвиток мережних технологій. Невдовзі з'явилась потреба об'єднання комп'ютерних систем не лише у межах однієї установи чи фірми, але й у масштабах регіону, країни та всього світу. Потребу в спільному інформаційному просторі сьогодні відчувають не лише науковці та бізнесмени, а й велика кількість користувачів домашніх комп'ютерів. Обмін повідомленнями електронної пошти, розклад руху транспортних засобів, прогноз погоди, доступ до наукової, довідкової, художньої інформації та багато інших послуг має змогу отримувати користувач персонального комп'ютера, що під'єднався до ресурсів глобальних комп'ютерних мереж.

+ Визначення 1: Комп'ютерною мережею називається сукупність вузлів (персональних комп'ютерів, робочих станцій, мейнфреймів, окремих пристроїв), які взаємодіють між собою за допомогою апаратних засобів та спеціального програмного забезпечення.

+ Визначення 2 (Міжнародної організації стандартів - ISO): Комп'ютерною мережею називається послідовне біторієнтоване передавання інформації між пов'язаними один з одним незалежними пристроями.

Мережний сервіс

Набір послуг, що надаються клієнтам мережею, залежить від призначення та реалізації мережі.

Файл-сервер дає змогу клієнтам користуватись файлами, що розміщені на носіях інформації серверу. В повному обсязі сервісу частина логічного дискового простору робочої станції є відображенням частини дискового простору файл-серверу, що дає змогу працювати з цією областю диска файл-серверу так, як з локальним диском робочої

станції. Завданням серверу є забезпечення заданого рівня множинного доступу робочих станцій до файлів, розв'язання колізій у випадку одночасного звернення кількох станцій до одного набору даних, розмежування прав доступу тощо. Спрощений варіант – файловий обмін, у процесі якого вузли мережі можуть тільки пересилати один одному файли (наприклад, використовуючи протокол FTP (File Transfer Protocol)).

Принт-сервер забезпечує обслуговування клієнтів мережі, в загальному випадку, декількома друкуючими пристроями (принтерами). При цьому сервер забезпечує прийом та постановку завдань на друк у чергу, виведення їх на принтери з урахуванням замовлених послуг друку та встановлених пріоритетів. Звичайно, до принт-серверу підключаються принтери, що здатні забезпечити широкий спектр послуг друку (швидкісні алфавітно-цифрові; лазерні для якісного чорно-білого, струменеві для кольорового друку тощо). Є спеціальні пристрої (деякі моделі принтерів обладнуються власним мережним адаптером), які дозволяють підключати принтер до мережі як окремий вузол, при цьому адміністратор здійснює віддалене управління таким принтером, використовуючи спеціальні програмні засоби.

Факс-сервер забезпечує колективне використання клієнтами мережі факс-модема та телефонної лінії, як пристрою виведення (типу принтера). Факс-сервером також може бути спеціалізований пристрій, що має інтерфейс доступу до мережі. Колективне використання вхідних повідомлень можливе при наявності засобів файлового обміну клієнтів з сервером, оскільки стандартне факсимільне повідомлення не містить адреси отримувача (тільки номер телефону).

Віддалений термінал (алфавітно-цифровий або графічний) забезпечує доступ робочої станції до обчислювальних ресурсів віддаленого комп'ютера (наприклад, мейнфрейму або Unix-машини) в режимі терміналу.

Сервер застосувань є одним з варіантів технології "клієнт-сервер", в якому основна обробка та пошук інформації для групи користувачів одного застосування здійснюється на сервері. Функції клієнтської частини застосування, встановленої на машині користувача, можуть бути зведені до введення та відображення результатів. Такий підхід, у порівнянні зі звичним колективним доступом до даних, дає змогу суттєво зменшити мережний трафік (завантаження), що особливо важливо в мережах з "повільними" каналами передавання даних.

Електронна пошта (E-mail) забезпечує обмін повідомленнями (файлами даних) між клієнтами, незалежно від ступеня їх віддаленості один від одного. Електронна пошта не вимагає присутності адресата за комп'ютером у момент надсилання йому повідомлення. Аналогічно до звичайної пошти, електронний лист, що має адреси відправника та от-

римувача, через систему поштових серверів доставляється в особисту "скриньку" (спеціально виділену дискову область) поштового серверу, на якому зареєстрована E-mail-адреса отримувача. До електронного листа можна приєднувати файли даних (тексти, малюнки, звукові повідомлення тощо).

Діалог (Chat) дає змогу двом клієнтам (або групі клієнтів) мережі обмінюватись повідомленнями в реальному часі. При наявності відповідних мультимедійних технічних засобів можна здійснювати аудіо- або відеодіалог. Мультимедійне спілкування групи клієнтів у реальному часі забезпечує можливість проведення аудіо- або відеоконференцій між віддаленими клієнтами. (Корпорація Microsoft використовує комп'ютерні відеоконференції для проведення виробничих нарад за участю працівників представництв корпорації в різних країнах світу).

Розподілена обробка інформації може грунтуватись на взаємодії процесів у різних вузлах мережі на рівні обміну блоками даних (наприклад, механізм DDE – Dynamic Data Exchange).

Перелічені базові мережні послуги можуть спільно (чи в певних комбінаціях) використовуватись у складних системах розподіленої обробки інформації. Наприклад, Web-сервер та Web-клієнт (браузер) забезпечують за текстовими та графічними вказівниками віддалений доступ до текстової, графічної, аудіо- та відеоінформації, що розсіяна по "сайтах" світової мережі Internet.

Класифікація мереж

Мережі класифікують за різними критеріями, серед яких найбільш вживані такі:

1)за пропускною здатністю
- низька, до сотень Кбіт/с – мережі, що містять "повільні" канали на зразок телефонних ліній, зокрема глобальна мережа Internet;
- середня, 0.5-20 Мбіт/с – локальні мережі, звичайно, в межах будівлі;
- висока, більше ніж 20 Мбіт/с – базові (або "хребтові", backbone) мережі, що з'єднують сервери або локальні мережі "швидкими" каналами, наприклад оптоволоконними лініями;

2)за смугою каналу
- вузькосмугові (Baseband) - безпосередня (немодульована) передача тільки одного повідомлення в довільний момент часу;
- широкосмугові (Broadband) - одночасна передача кількох повідомлень частотно-розділеними каналами;

3)за розмірами *

* Іноді обмежуються спрощеною класифікацією LAN/WAN. Зокрема Internet часто відносять до WAN.

- LAN (Local-Area Network) – локальна мережа в межах офісу, будівлі;
- CAN (Campus-Area Network) - кампусна мережа, що об'єднує віддалені вузли та локальні мережі, звичайно, без використання телефонних ліній та модемів;
- MAN (Metropolitan-Area Network) - територіальна (міська) мережа з радіусом, що дорівнює десяткам кілометрів, та високою швидкістю передавання даних (100 Мбіт/с);
- WAN (Wide-Area Network) - широкомасштабна мережа (регіон, країна), що використовує віддалені мости та маршрутизатори з наявністю ліній низької пропускної здатності;
- GAN (Global-Area Network) - глобальна (міжнародна) мережа;

4)<u>за співвідношенням вузлів</u>

- одноранговi (Peer-To-Peer) - невеликі локальні мережі, де кожен вузол може виступати як у ролі клієнта, так і сервера (наприклад, на базі операційних систем Windows for Workgroups, Windows'95);
- розподілені (Distributed) - мережа без лідера, в якій сервером називається машина, програма або пристрій, що забезпечують мережний сервіс, але не управління мережею (наприклад Unix Usenet);
- мережі з централізованим управлінням (Server Based), в яких сервер надає решта вузлам право використовувати спільні ресурси (наприклад, Novell NetWare, Microsoft LAN Manager, IBM LAN Server, Banyan VINES, Windows NT);

5)<u>за доступом</u>

- мережі з розподіленим середовищем передавання (Shared-Media Networks), в яких у будь-який момент часу можуть взаємодіяти тільки два вузли (Ethernet, ARCnet...);
- мережі з комутацією (Switching Networks), в яких шляхом мультиплексування одночасно можуть взаємодіяти декілька пар вузлів;

6)<u>за спільністю операційних систем</u>

- гомогенні мережі, що грунтуються на однакових або споріднених ОС усіх вузлів (наприклад, Windows for Workgroups-Windows'95-Windows NT);
- гетерогенні мережі, в яких вузли використовують різнорідні ОС (наприклад, NetWare-Windows'95-Unix).

Будь-яка класифікація мереж є доволі умовною, оскільки реальні конфігурації здебільшого охоплюють одразу декілька класифікаційних груп.

Лекція 2. Середовище та методи передавання даних

У будь-якій комп'ютерній мережі передавання даних здійснюється за допомогою електричних (електромагнітних) сигналів. Середовище передавання може бути обмеженим (фізичний провідник сигналу - кабель) або ж необмеженим (передавання мікрохвильових та подібних їм сигналів через відкритий ефір). Кожне середовище має свої переваги та вади. Одним з основних показників є швидкість затухання сигналу, яка визначається фізичними характеристиками середовища та природою сигналу. Вибираючи середовище передавання, буруть до уваги також інші показники: вартість (придбання, монтажу та обслуговування), пропускну здатність, безпеку передавання інформації тощо.

Необмежене середовище

Необмежене середовище забезпечує передавання та прийом електромагнітних сигналів без пристрою (каналу), який би містив цей сигнал у собі. Прикладами комунікаційних систем, що використовують необмежене середовище, є мікрохвильовий, лазерний, інфрачервоний та радіозв'язок.

Мікрохвильові комунікації реалізуються в двох варіантах - наземному та супутниковому. Звичайно, такі комунікації використовують для передавання на великі відстані багатьох телефонних каналів, даних, каналів телебачення для віддалених районів тощо. Супутникові комунікації використовують мікрохвильові промені від та до супутника, що знаходиться на геостаціонарній орбіті Землі. Такий зв'язок дає змогу об'єднувати спільним комунікаційним середовищем країни та континенти.

Наземна мікрохвильова передача використовується для налагодження зв'язку між окремими будівлями в межах локальної або кампусної мережі, якщо прокладання витої пари або коаксіального кабелю пов'язане з труднощами та високою вартістю робіт. Мікрохвильовий спосіб зв'язку підтримує високі швидкості передавання, однак більш залежний від зовнішніх впливів (дощ, туман, сильна хмарність), що особливо характерно для великих відстаней.

Лазерні комунікації використовують промінь світла (звичайно, інфрачервоного), що модулюється імпульсами для передавання даних. Прийнятий промінь, в свою чергу, перетворюється в послідовність біт. Найчастіше використовують два паралельні промені, що дає змогу виконувати передавання сигналів в обох напрямках. Лазерні комунікації

дають змогу досягнути найвищих швидкостей передавання даних, однак обмежені відстанями та необхідністю прямої видимості.

На початку 1980-х років фахівці фізичного факультету Львівського університету налагодили експериментальний лазерний зв'язок між будівлями головного корпусу університету та фізичного факультету. Оскільки між будівлями не було прямої видимості, на міській ратуші було встановлено спеціальне дзеркало, на яке лазерні приймачі-передавачі на обох будівлях скеровували свої промені.

Інфрачервоні комунікації найчастіше використовуються у приміщеннях. Прикладом інфрачервоних комунікацій є різноманітні пульти дистанційного управління. Інфрачервоні системи зв'язку дешеві, однак малий радіус дії є перешкодою їх широкого використання.

Радіозв'язком звично називають електромагнітні хвилі в частотному діапазоні від 3 до 300 МГц. Цей діапазон поділяють на короткі та ультракороткі хвилі. Радіохвилі поширюються у всіх напрямках від передавальної антени. Прикладом радіозв'язку є поширення радіопередач, телебачення, службові системи зв'язку з мобільними абонентами. Недоліком такого виду зв'язку є малі швидкості передавання, вплив перешкод (рельєф місцевості, будівлі тощо), вузька смуга передавання.

Обмежене середовище

Обмежене середовище - це провід (кабель), який проводить електричний або світловий сигнал. Найбільш поширеними є багатожильні, коаксіальні та волоконно-оптичні кабелі, виті пари.

Багатожильні кабелі часто застосовуються для з'єднання як вузлів мережі, так і периферійних пристроїв (клавіатура, монітор, маніпулятор "мишка", принтер) із системним блоком комп'ютера. Різні проводи кабелю можуть використовуватись з різною метою. Наприклад, вісім проводів - для передавання даних, дев'ятий - для індикації активності всієї шини, ще два - для підтримки протоколів взаємодії вузла-відправника та вузла-приймача. Передавання даних паралельними лініями збільшує пропускну здатність каналу, вивільняє його від передавання службової інформації тощо. Багатожильні кабелі використовуються в конфігураціях мереж з двоточковими з'єднаннями (топології зірки та кільця). Недоліками такого середовища передавання є висока вартість та складність підімкнення нових вузлів.

Вита пара (Twisted Pair) є парою взаємно ізольованих

провідників, що скручені між собою на зразок спіралі. Скручування провідників дає змогу збільшити провідність та зменшити зовнішні електромагнітні впливи. Одна або декілька пар провідників поміщені в спільну ізолюючу (іноді екрановану) оболонку. Вита пара застосовується лише у двоточкових з'єднаннях, однак такий носій є дешевшим за багатожильні кабелі. Нові технологічні рішення дають змогу використовувати виту пару в мережах високої пропускної здатності.

Коаксіальний кабель (Coaxial Cable) містить два провідники. Назва відображає той факт, що обидва провідники мають спільну вісь. В центрі кабелю знаходиться провід, поміщений у пластиковий кожух-ізолятор. Цей кожух покритий іншим провідником, який одночасно є захисним екраном. Зверху цього провідника можуть бути ще кілька ізолюючих та екрануючих покриттів. Розрізняють "тонкий" та "товстий" ("жовтий") коаксіальний кабель. Сьогодні тонкий коаксіальний кабель найбільш часто вживають, проектуючи локальні мережі з використанням шинної архітектури Ethernet.

Волоконно-оптичний кабель виготовляється зі скла або світлопровідних пластикових волокон, розміщених у центрі товстої захисної трубки, покритої зовнішньою оболонкою. Світлові імпульси генеруються лазером або світлодіодом та передаються світловодом до приймача, що виконаний на основі фотодетектора. Волоконно-оптичний кабель та обладнання для прийняття-передавання світлових сигналів складні в монтажі та значно дорожчі від інших типів обмежених середовищ передавання. Однак світлові сигнали у порівнянні з електричними майже не підлягають затуханню, їм не шкодять зовнішні електромагнітні впливи, а швидкість передавання даних - найвища. Сьогодні такі лінії передавання даних з'єднують віддалені потужні сервери в мережі Internet.

Методи передавання даних

Розрізняють три основні методи передавання даних: комутація каналів, повідомлень та пакетів.

Комутація каналів. У мережі попередньо встановлюється фізичне з'єднання від відправника до адресата. Таке з'єднання є каналом, що об'єднує послідовно з'єднані ділянки. Комутацію каналів забезпечує службове повідомлення, яке прокладає зв'язок від одного пункту комутації до іншого. Після налагодження фізичного з'єднання з пункту призначення до відправника надходить сигнал зворотнього зв'язку, і лише тоді розпочинається передавання даних. При цьому задіяні для передавання ділянки каналів недоступні для інших передач. Комутація каналів

пов'язана з часовими затримками на налагодження з'єднань та очікування звільнення необхідних канальних ділянок. Перевагою методу є збереження часової послідовності інформації, що передається. Якщо ця вимога є основною - то доводиться використовувати доволі дорогі виділені (скомутовані на тривалий час) канали зв'язку. Прикладом мережі з комутацією каналів є телефонні мережі (АТС - пункти комутації канальних ділянок).

Комутація повідомлень. Інформація між пунктами відправлення та прийняття проходить шляхом запам'ятовування у проміжкових вузлах комутації. Для цього створюється віртуальний канал (віртуальний канал може складатись з фізичних каналів різної пропускної здатності), а фізичні з'єднання відбуваються лише між двома сусідніми пунктами комутації на час передавання повідомлення. Кожне повідомлення містить заголовок з адресою пункту призначення. Оскільки у будь-який момент часу зайнятою є лише одна канальна ділянка, то решта можуть бути використані для передавання інших повідомлень. Метод комутації повідомлень дає змогу збільшити пропускну здатність мережі та зменшити затримки передавання інформації.

Комутація пакетів. Цей метод є різновидом методу комутації повідомлень, в якому повідомлення поділяється на пакети фіксованого розміру. Кожен пакет отримує заголовок, в якому, окрім адрес відправника та отримувача, міститься порядковий номер пакета у повідомленні. Пакети передаються мережею незалежно один від одного і, можливо, надходять до адресата різними маршрутами. У пункті призначення з пакетів, з використанням їх нумерації, формується вихідне повідомлення. Метод комутації пакетів є одним з найпоширеніших, оскільки дає змогу досягнути найвищої пропускної здатності мережі.

Лекція 3. Принципи взаємодії відкритих систем

Модель OSI

Під *відкритою системою* розуміють таку систему, яка у випадку дотримання певних вимог (правил відкритості), може бути без будь-яких доповнень та змін під'єднана до іншої відкритої системи. Вимоги до відкритих систем визначені стандартом Open System Interconnection (OSI), що був введений у 1977 році Міжнародною організацією стандартів (ISO) та отримав код ISO7498.

Розглянемо дві системи A та B, які обмінюються даними через деяке середовище передавання. Цей процес можна розділити на фізичний (яким чином дані передаються в середовище передавання системою, що їх надсилає, та передаються із середовища до системи, що їх приймає) та логічний обмін (яким чином система, що передає дані, формує їх та забезпечує, щоб система, яка їх приймає, розуміла ці дані). Отже, фізично кожна система взаємодіє із середовищем передавання; логічно кожна система взаємодіє з іншою системою.

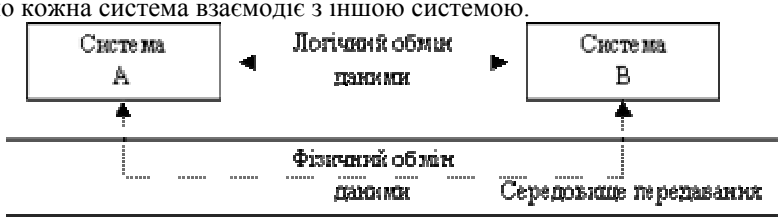


Рис. 4.1. Логічна та фізична взаємодія систем.

При спрощеному розгляді вважають, що мережа містить три основні компоненти:

1) з'єднання - складаються з фізичних елементів апаратури, необхідних для під'єднання комп'ютера до мережі, а також із середовища передавання інформації між вузлами;
2) зв'язок - визначає правила, за якими вузли з'єднуються один з одним для обміну інформацією;
3) послуги - визначають функції, які вузли можуть виконувати в мережі.

Для того, щоб мережа працювала, з'єднання, зв'язок та послуги мають бути об'єднані з дотриманням таких вимог:

- з'єднання забезпечують магістраль, по якій сигнали переміщаються між вузлами;
- зв'язок працює так, щоб один вузол міг надсилати

повідомлення, а інший - приймати та розуміти його;

- вузли уміють працювати спільно так, щоб користувач одного комп'ютера міг використовувати послуги, що їх надають інші комп'ютери чи периферійні пристрої.

Отже, ми розділили процес комунікації двох користувачів комп'ютерів у мережі на три рівні. Модель OSI визначає сім рівнів та завдання кожного з них. Усередині кожної системи взаємодія відбувається між рівнями по вертикалі. Міжсистемна взаємодія логічно відбувається по горизонталі - між відповідними рівнями. Реально ж, за відсутності безпосередніх горизонтальних зв'язків, відбувається спуск до нижнього рівня в системі, що відправляє повідомлення, зв'язок через середовище передавання та підйом до відповідного рівня в системі, що приймає повідомлення.

Перелічимо основні принципи архітектури відкритих систем, при побудові технології яких за основу взято поділ комунікаційного програмного забезпечення на певну кількість рівнів:

- потрібно створити стільки рівнів, щоб процес передавання та обробки інформації можна було розбити на частини, достатні для легкого розуміння;
- рівнів має бути не надто багато, аби уникнути труднощів їх інтеграції та опису;
- межу між рівнями слід провести в таких точках, де опис сервісу може бути коротким, а кількість взаємодій через цю межу мінімальною;
- аналогічні функції мають зосереджуватись в одному рівні;
- поділ слід зробити так, щоб кожний рівень був незалежним і давав змогу модернізувати та замінити його, не змінюючи інших рівнів.

Перш ніж розглянути основні рівні моделі взаємодії відкритих систем OSI, зауважимо, що еталонна модель має на меті визначити абстрактні рівні, всередині яких можуть розроблятись свої стандарти. Модель OSI визначає сім рівнів, кожний з яких є достатньо автономним і виконує чіткий набір своїх завдань. Сукупність правил та форматів, які визначають взаємодію об'єктів на n-рівні, називають n-протоколом. Важливо також усвідомлювати різницю між абстрактною моделлю та

конкретною реалізацією, в якій декілька еталонних рівнів нерідко об'єднуються спільною реалізацією - протоколом (набором (стеком) протоколів).

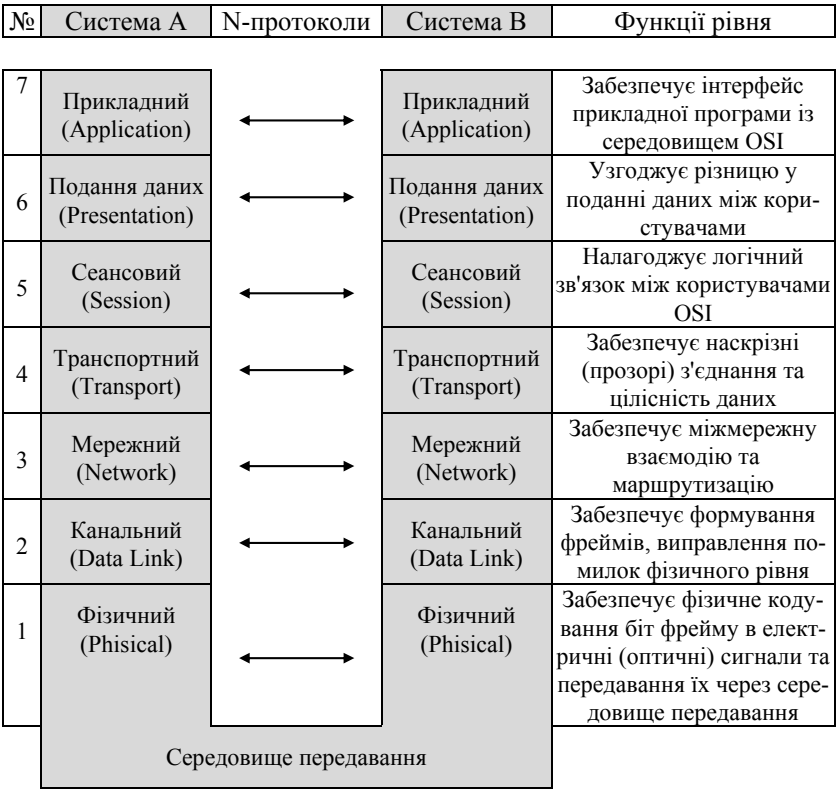


Рис. 4.2. Модель взаємодії відкритих систем OSI.

7. Прикладний рівень

Найвищий рівень моделі, який (єдиний з рівнів) забезпечує прикладним програмам (процесом) доступ до середовища OSI. Приклади завдань цього рівня - передавання файлів, електронна пошта, управління мережею. До протоколів прикладного рівня відносять такі:

- NICE (Network Information and Control Exchange) - спостереження та управління мережею;
- FTAM (File Transfer, Access and Management) - передавання, доступ та управління файлами;

- FTP (File Transfer Protocol) - пересилання файлів;
- X.400 - передавання повідомлень та сервіс електронної пошти;
- CMIP (Common Management Information Protocol) - протокол OSI управління мережею (сьогодні більш поширеним є протокол SNMP (Simple Network Management Protocol));
- TelNet - емуляція терміналу та віддалена реєстрація.

6. Рівень подання даних

Цей рівень відповідає за сумісність подання даних між прикладними процесами, що взаємодіють (перетворення форматів даних, кодових таблиць, стискання та розпаковування даних).

5. Сеансовий рівень

Сеансовий рівень забезпечує взаємодію та підтримку діалогу між процесами певного типу (такий логічний діалог називають сеансом). Можуть передбачатись кілька різних сеансових рівнів (і, відповідно, кілька протоколів) для процесів різних типів. Для взаємодії двох або більше процесів різних типів мають бути визначені сеанси взаємодії цих процесів. Отже, до переліку завдань сеансового рівня належить синхронізація та коректне передавання файлів під час діалогу, а також надійність з'єднання до закінчення сеансу.

До протоколів сеансового рівня належать такі:

- NetBIOS (Network Basic Input/Output System) - іменування вузлів, негарантована доставка коротких повідомлень без налагодження з'єднання, налагодження віртуальних з'єднань та гарантована доставка повідомлень, загальне управління. Протокол реалізує завдання 5, 6 та 7 рівнів. Є багато реалізацій, які не завжди сумісні з оригінальною розробкою фірми IBM;
- NetBEUI (Network Basic Extended User Interface) - реалізація та розширення NetBIOS від фірми Microsoft.

4. Транспортний рівень

Цей рівень відповідає за прозоре передавання інформації між об'єктами сеансового рівня з визначеним рівнем якості (швидкість, економічна доцільність, рівень вірогідності). На цьому рівні дані розділяються на частини, що поміщаються в нумеровані пакети та передаються на нижні рівні. У процесі прийому даних аналізуються номери прийнятих пакетів, а їх вміст у потрібному порядку збирається та

передається на вищі рівні. Транспортний рівень є проміжним та зв'язуючим між верхніми рівнями (End Systems), що залежні від прикладних процесів, та нижніми (Intermediate Systems), що прив'язані до конкретної мережі.

Нижні рівні можуть забезпечувати або не забезпечувати надійне передавання, у процесі якого отримувачу надходить безпомилковий пакет або повідомлення про неможливість передавання. Сервіс нижніх рівнів може бути зорієнтованим на налагодження з'єднання (Connection oriented) - при цьому передавання здійснюється без нумерації пакетів, оскільки кожен з них слідує за попередником тим самим шляхом. Після закінчення сеансу передавання з'єднання розривається. Зв'язок без налагодження з'єднань (Connectionless) вимагає нумерації пакетів, оскільки вони можуть губитися, повторюватися, надходити не за порядком.

Приклади протоколів транспортного рівня:

- TCP (Transmission Control Protocol) - протокол UNIX та Internet-мереж з налагодженням з'єднань;
- UDP (User Datagramm Protocol) - протокол UNIX-мереж без налагодження з'єднань;
- SPX (Sequenced Packet Exchange) - протокол Novell NetWare з налагодженням з'єднань.

3. Мережний рівень

Мережний (його ще називають пакетним) рівень реалізує додаткові функції маршрутизації для того, щоб кадри (фрейми) канального рівня були доступні (прозорі) для різноманітного мережного обладнання, засобів передавання та виду доступу. Завданнями рівня є визначення адрес, трансляція фізичних та мережних адрес, забезпечення міжмережної взаємодії, пошук шляху від відправника до отримувача (або між двома проміжковими вузлами), налагодження та обслуговування логічного зв'язку між вузлами.

Приклади протоколів мережного рівня:

- ARP (Address Resolution Protocol) - перетворює апаратні адреси в мережні;
- IP (Internet Protocol) - протокол UNIX та Internet-мереж доставки дейтаграм ;
- IPX (Internetwork Packet Exchange) - базовий протокол Novell NetWare, що відповідає за адресацію та маршрутизацію пакетів та

забезпечує сервіс для SPX.

2. Канальний рівень

Канальний рівень забезпечує формування кадрів (фреймів), що передаються через фізичний рівень отримувачу. На цьому рівні здійснюється також управління доступом до середовища передавання, яке використовується кількома вузлами мережі. Інститут електротехніки та електроніки IEEE (Institute of Electrical and Electronics Engineering) запропонував поділ канального рівня на два підрівні:

1) LLC (Logical Link Control) - управління логічним зв'язком, забезпечення інтерфейсу з мережним рівнем;
2) MAC (Media Access Control) - управління доступом до середовища передавання, доступ до рівня фізичного кодування та передавання сигналів.

Більшість мережних архітектур охоплюють канальний та фізичний рівні.

1. Фізичний рівень

Найнижчий рівень моделі OSI забезпечує фізичне кодування біт фрейма в електричні (оптичні) сигнали та передавання їх через середовище передавання. Фізичний рівень визначає типи кабелів, розняття, призначення контактів та формат фізичних сигналів.

Приклади специфікацій фізичного рівня:

- IEEE 802.1 - протокол управління мережею;
- IEEE 802.2 - протокол управління логічними з'єднаннями;
- IEEE 802.3 - базовий протокол архітектури Ethernet;
- IEEE 802.4 - базовий протокол архітектури Token Bus;
- IEEE 802.5 - базовий протокол архітектури Token Ring.

Лекція 4. Мережні топології та методи доступу до середовища передавання

Фізична топологія

Геометричну форму проекції середовища передавання даних на площину називають фізичною топологією (конфігурацією) мережі. Залежно від способу з'єднання вузлів мережі можуть використовуватись такі фізичні топології:

- шина (Bus);
- кільце (Ring);
- зірка (Star);
- сітка (Mesh).

Шинна топологія

відповідає конфігурації мережі, в якій усі вузли підімкнені до спільного лінійного каналу з допомогою відносно коротких з'єднань:

Рис. 5.1. Шинна топологія.

Переваги:

- вимагає мінімальної кількості кабелю, оскільки канал підводиться до кожного вузла найкоротшим шляхом;
- нескладне додавання в мережу нового вузла;
- просте управління трафіком між під'єднаними вузлами.

Недоліки:

- пошкодження одного з'єднання між двома вузлами виводить з ладу всю мережу;
- трудність локалізації дефектів середовища передавання.

Кільцева топологія

відповідає конфігурації мережі, в якій кожен вузол пов'язаний з двома іншими, а спільний канал утворює кільце:

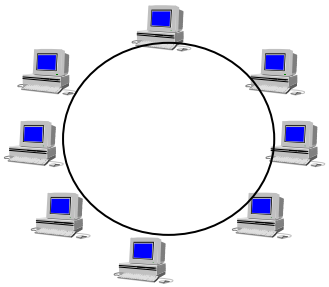


Рис. 5.2. Кільцева топологія.

Переваги:

- проста логічна організація;
- відсутність перевантажень середовища передавання.

Недолік, як і в шинній топології, пов'язаний з наявністю одного спільного каналу - пошкодження з'єднання між двома вузлами виводить з ладу всю мережу.

Топологія зірки

відповідає конфігурації мережі, в якій усі вузли з'єднані з центральним вузлом (концентратором).

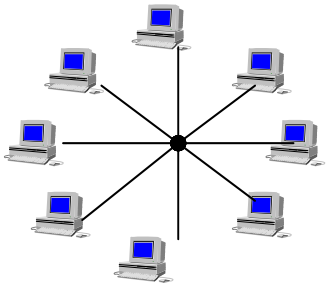


Рис. 5.3. Топологія зірки.

У мережах зіркоподібного типу, звичайно, центральний вузол відповідає за маршрутизацію пакетів та локалізацію несправностей (приклад такої мережі - телефонна мережа).

Переваги:

- легкість управління;
- надійність роботи та можливість швидкого виявлення дефектів;
- нескладне додавання в мережу нового вузла.

Недоліки:

- вимагає надлишкової кількості кабелю;
- пошкодження концентратора спричиняє вихід з ладу всієї мережі.

Сіткова топологія

відповідає конфігурації мережі, в якій усі вузли з'єднані між собою безпосередніми з'єднаннями.

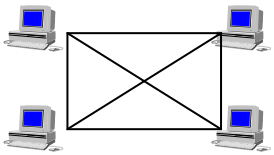


Рис. 5.4. Сіткова топологія.

Ідеальна сіткова топологія з N вузлами вимагає наявності у кожного вузла (N-1)-го мережного адаптера.

Переваги:

- висока надійність роботи;
- мінімальний час передавання даних.

Однак висока вартість обладнання, надлишкова кількість кабелю та інші недоліки, звичайно, перешкоджають широкому поширенню такої топології.

Гібридна топологія

використовує різні типи мережних топологій, звичайно, для об'єднання декількох локальних мереж (кампусні, глобальні мережі).

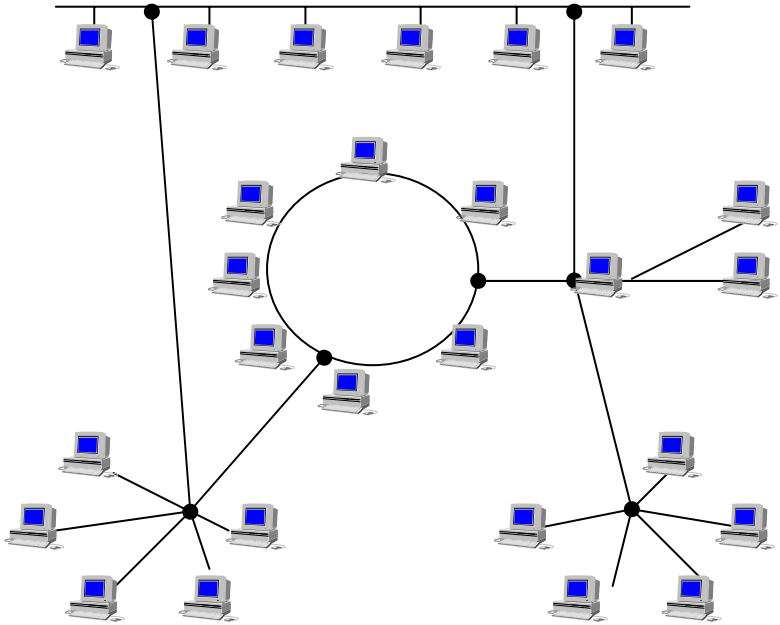


Рис. 5.5. Приклад мережі гібридної топології.

Логічна топологія

Логічна топологія мережі визначає потоки даних та порядок одержання права на їх передавання. Розрізняють логічну шину (реалізується на фізичних топологіях шини, зірки або сітки) та логічне кільце (реалізується на фізичних топологіях кільця та зірки). Логічна топологія та, тісно пов'язаний з нею, метод доступу до середовища передавання (Media Access Method) відповідають двом нижнім рівням моделі OSI.

У логічній шині інформація одночасно доступна всім вузлам. Реально ж зчитування здійснює тільки той вузол, якому адресовано повідомлення. Метод доступу до середовища - конкурентний (Contension), базований на прослуховуванні каналу.

У логічному кільці інформація передається послідовно від одного до іншого вузла. Кожен вузол приймає повідомлення тільки від попереднього, а відправляє - тільки наступному. Вузол ретранслює всі пакети й обробляє лише той, який адресовано йому. Метод доступу до середовища - детермінований, базований на мережній адресі вузла.

Конкурентні методи доступу

Використовуючи конкурентний метод доступу (метод випадкового доступу), кожен вузол може зробити спробу передавання повідомлення в будь-який момент. Якщо лінія зайнята або виявлено колізію (зіткнення повідомлень від кількох передавачів), спроба передавання відкладається на випадковий проміжок часу. Є цілий ряд алгоритмів, що дають змогу уникати або ж, принаймні, мінімізувати наслідки колізій. Системи, побудовані на конкурентному методі доступу до середовища, досить просто реалізуються, забезпечують швидкий доступ до шини, дають змогу легко підмикати та відмикати вузли, не потребують центрального керуючого пристрою, характеризуються високою живучістю. Головним недоліком таких систем є різке збільшення часу очікування доступу при збільшенні навантаження в мережі. Основні два різновиди - CSMA/CA і CSMA/CD.

Метод CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - реалізує вільний (множинний) доступ з прослуховуванням несучої та запобіганням колізіям. Станція, яка готова відправити повідомлення, прослуховує лінію. При відсутності несучої станція відправляє короткий сигнал запиту на передавання (RTS) і певний час очікує відповіді від адресата (CTS). При відсутності відповіді (що, звичайно, є наслідком колізії) спроба передавання відкладається, при одержанні відповіді - повідомлення відправляється адресату. Короткі повідомлення RTS-CTS виконують роль детекторів колізій. Ліпше, щоб колізія відбулась під час передавання короткого керуючого сигналу, ніж довгого повідомлення з інформацією користувача. Метод CSMA/CA не дає змогу повністю уникати колізій та, однак, достатньо ефективний для мереж з невеликою кількістю вузлів. Цей метод використовується в мережних архітектурах LocalTalk фірми Apple, відзначається простотою та дешевизною апаратного забезпечення.

Метод CSMA/CD (Carrier Sense Multiple Access/Collision Detect) - реалізує вільний (множинний) доступ з прослуховуванням несучої та виявленням колізій. Станція, яка готова відправити повідомлення, прослуховує лінію. При відсутності несучої станція починає передавання повідомлення, здійснюючи при цьому контроль за станом лінії. При виявленні колізії (зростанні активності лінії) передача припиняється, а

повторна спроба відкладається на випадковий проміжок часу. Максимальний час, протягом якого може виникнути колізія, відповідає подвоєному часу проходження сигналом максимальної відстані між двома вузлами мережі. Тривалість передавання пакету має бути більшою за максимальний час виявлення колізії. Метод CSMA/CD на практиці дуже ефективний і дає змогу використовувати до 90% доступної пропускної здатності каналу, однак, у порівнянні з CSMA/CA, вимагає більш дорогих апаратних засобів. Цей метод використовується у багатьох мережних архітектурах, зокрема, в найбільш поширеній архітектурі Ethernet.

Детерміновані методи доступу

Використовуючи детерміновані методи доступу, вузли мережі одержують доступ до середовища передавання у визначеному порядку. Розрізняють два основні методи детермінованого доступу - опитування (Polling) та передавання маркера (Token Passing).

Метод опитування визначає один з вузлів адміністратором доступу до каналу (інші назви - первинний вузол, контролер). Цей вузол у визначеному порядку опитує інші (вторинні) вузли стосовно наявності у них інформації, готової до передавання. Системні правила обмежують максимальний час передавання інформації одним з вторинних вузлів в одному циклі опитування. Метод опитування може використовуватись для різних мережних топологій. Однак найбільш природною для нього є топологія зірки, в якій центральний вузол відіграє роль адміністратора доступу. В великих ЕОМ (Mainframes), зокрема фірми IBM, цей метод використовується для опитування периферійних пристроїв введення даних (терміналів).

Метод передавання маркера подібний на метод опитування, який працює без центрального контролера. Первинним за чергою стає кожен з вузлів, що отримує спеціальний об'єкт - маркер. Передавання маркера розподіляє управління доступом між усіма вузлами мережі. Кожен вузол знає від кого отримано і кому слід передати маркер. Правила визначають кожному вузлу максимальний час управління маркером. Метод реалізується для обох логічних топологій - кільця та шини. Використовується в мережних архітектурах ARCnet, Token Ring, FDDI.

Метод передавання маркера подібний до методу опитування. Обидва методи викликають певну надлишковість у використанні каналу, вимагають додаткового часу та зменшують можливості передавання для кожного з вторинних вузлів. Перевагами обох методів є повна відсутність колізій, визначений час проходження сигналу, що мало залежить від навантаження в мережі, та можливість забезпечення найбільш активним вузлам пріоритетного використання каналу.

Лекція 5. З'єднувальні елементи

Складовими будь-яких мереж є апаратні (технічні) та програмні засоби (мережні операційні системи, утиліти та інструментальні засоби, прикладні програми тощо). Апаратні засоби у свою чергу можна розділити на вузли (комп'ютери, термінали, мейнфрейми, мережні принтери, касові термінали тощо) та з'єднувальні елементи.

Основними з'єднувальними елементами є :

- кабелі: коаксіальні, витi пари, оптичні;
- внутрімережні з'єднувальні елементи: роз'єми, повторювачі (Repeater), трансивери MAU (Media Attachement Unit) тощо;
- кабельні центри (Wiring center): хаби (Hub), концентратори, багатостанційні пристрої доступу MAU (Multistation Access Unit);
- міжмережні з'єднувальні елементи: мости (Bridge), маршрутизатори (Router), шлюзи (Gateway) тощо;
- компоненти безпровідного (Wireless) зв'язку: трансивери (радіо та інфрачервоні), антени тощо.

Мережа (логічна локальна мережа) являє собою, звичайно, сукупність кабельних сегментів (*кабельний сегмент* - це ланцюжок відрізків кабелів, що з'єднані між собою електрично), зв'язаних між собою повторювачами. *Повторювач* забезпечує проміжне підсилення та формування сигналів, дає змогу збільшувати протяжність мережі та кількість під'єднаних вузлів. Повторювач оперує на фізичному рівні моделі OSI.

Кабельні центри

З'єднання кабельних сегментів може бути здійснене через *кабельний центр - хаб*, що є пристроєм фізичного підімкнення декількох сегментів або променів. Інтелектуальний хаб (Intelligent Hub) має спеціальні засоби для діагностики та управління, які дають змогу оперативно одержувати відомості щодо активності та справності вузлів, відключати несправні вузли тощо. Розрізняють такі реалізації хабів:

- активний хаб: підсилює сигнали, потребує джерела живлення;
- пасивний хаб: лише узгоджує імпеданси ліній (архітектура ARCnet);
- Peer Hub: плата розширення для комп'ютера (архітектура ARCnet);
- звичайний хаб (Standalone Hub): самостійний пристрій з власним джерелом живлення;
- нарощуваний хаб (Stackable Hub): обладнаний засобами з'єднання кількох хабів у стек; інтелектуальність одного з хабів стеку, звичайно, перетворює весь стек в інтелектуальний; розрізняють

локальний та розподілений (де сегмент між хабами може досягати сотень метрів) стеки;

- концентратор: більш складний хаб, що дає змогу об'єднувати мережі різних архітектур.

Чіткої межі між хабами та концентраторами немає - і ті й інші можуть бути повторювачами, мостами або маршрутизаторами.

Мости

Серед міжмережних з'єднувальних елементів найбільш поширеним є міст. *Міст* є засобом передавання пакетів між локальними мережами, що оперує на двох нижніх рівнях моделі OSI та є прозорим для протоколів мережного рівня. Міст здійснює фільтрацію пакетів, не випускаючи з мережі пакети для внутрімережних адресатів, а також переадресацію - передавання пакетів в іншу мережу згідно з таблицею маршрутизації (або ж, за відсутності адресата в таблиці, в усі інші мережі). Таблиця маршрутизації, звичайно, укладається шляхом самонавчання за адресами відправників пакетів, що надходять до мережі. Мости класифікуються за кількома ознаками:

За рівнем протоколу:

- MAC-мости - працюють на MAC-підрівні канального рівня управління доступом до середовища передавання, дають змогу зв'язувати мережі однієї архітектури (з однаковими форматами пакетів);
- LLC-мости - працюють на LLC-підрівні канального рівня управління логічним зв'язком, дають змогу зв'язувати мережі різних архітектур;

За алгоритмом маршрутизації:

- Transparent Routing (прозорий) - міст сам визначає шлях для кожного пакета, запам'ятовуючи розташування всіх вузлів (характерно для архітектури Ethernet);
- Source Routing - шлях пакета вводиться в адресну частину відправником (використовується в архітектурі Token Ring);

За відношенням до серверу:

- внутрішній (Internal) міст - частина програмного забезпечення серверу, що відповідає за пересилання пакетів між сегментами (сервер при цьому обладнаний кількома мережними адаптерами);
- зовнішній (External, Standalone) міст - окремий пристрій.

За відстанню між мережами:

- локальний (Local) міст - з'єднує локальні мережі, що розташовані на невеликій відстані одна від іншої;
- віддалений (Remote) міст - з'єднує географічно віддалені локальні мережі через засоби телекомунікації (звичайно - виділені

або комутовані телефонні лінії, для підвищення продуктивності використовують декілька "паралельних" каналів зв'язку).

Маршрутизатори

Комутацію мереж третього (мережного) рівня забезпечують *маршрутизатори* - засоби з'єднування вузлів різних мереж, що використовують мережні (логічні) адреси вузлів. Мережі можуть бути віддалені, а шлях передавання пакетів пролягати через інші маршрутизатори. Мережна адреса при цьому трактується як ієрархічний опис розташування вузла. Маршрутизатори підтримують протоколи мережного рівня - IP, IPX, X.25 та деякі інші. Більш складні (відповідно, більш дорогі) мультипротокольні маршрутизатори підтримують одночасно декілька протоколів для гетерогенних мереж. Іноді розрізняють так звані Brouter (Bridging Router) - комбінацію моста та маршрутизатора, що одночасно оперує на мережному та канальному рівнях. Основними характеристиками маршрутизатора є:

- тип (одно- або мультипротокольний, LAN або WAN, Brouter);
- підтримувані протоколи;
- пропускна здатність;
- типи мереж, що можуть під'єднуватись;
- інтерфейси (LAN або WAN);
- кількість портів;
- можливість управління та моніторингу мережі.

Шлюзи

З'єднувальним елементом, що оперує на верхніх (5-7) рівнях моделі OSI, є *шлюз* - засіб з'єднання суттєво різнорідних мереж. На відміну від повторювачів, мостів та маршрутизаторів, що є прозорими для користувача, наявність шлюзу є відчутною. Шлюз виконує перетворення форматів та розмірів пакетів, протоколів, даних та деякі інші функції. Звичайно, шлюз реалізується на базі комп'ютера з великим об'ємом пам'яті. Прикладами шлюзів можуть бути:

- факс: забезпечує доступ до віддаленого факсу, перетворює дані в факс-формат;
- електронна пошта: забезпечує поштовий зв'язок між локальними мережами;
- Internet: забезпечує доступ до глобальної мережі Internet.
- мейнфрейм: з'єднує локальну мережу з великою машиною (виділення одного комп'ютера під шлюз дає змогу будь-якій станції

емулювати термінал без встановлення додаткових інтерфейсних адаптерів).

Лекція 6. Архітектура Ethernet

Мережна архітектура відповідає реалізації фізичного та канального рівнів моделі OSI. Архітектура визначає кабельну систему, кодування сигналів, швидкість передавання, структуру фреймів, топологію мережі та метод доступу до середовища передавання. Кожній з архітектур відповідає свій набір компонент - кабелі, розняття, мережні адаптери, кабельні центри тощо.

Перше покоління мережних архітектур забезпечувало низькі та середні швидкості передавання: LocalTalk -230 Кбіт/с, ARCnet - 2,5 Мбіт/с, Ethernet - 10 Мбіт/с, TokenRing - 16 Мбіт/с. Ці архітектури зорієнтовані на використання електричних кабелів.

Друге покоління мережних архітектур забезпечує високі швидкості передавання: FDDI -100 Мбіт/с, ATM - 155 Мбіт/с, Fast Ethernet - 100 Мбіт/с та, звичайно, зорієнтовані на використання оптоволоконних кабелів.

Різновиди Ethernet

Ethernet - архітектура мереж, що грунтується на логічній топології шини, з розподіленим середовищем передавання, методом доступу до середовища передавання CSMA/CD, описана стандартом IEEE802.3. За фізичною реалізацією розрізняють:

- 10Base5 - Thick ("товстий") Ethernet;
- 10Base2 - Thin ("тонкий") Ethernet;
- 10BaseT - Twisted-pair Ethernet (Ethernet на витій парі);
- 10Broad36 - мережа на широкосмуговому 75-Омному коаксіальному кабелі;
- 10BaseF - кілька варіантів мережі на оптоволоконному кабелі;
- 100BaseT - стандарти Fast Ethernet на витій парі (100 BaseT4, 100 BaseTX).

Перший елемент в умовному позначенні архітектури - швидкість передавання в Мбіт/с; другий елемент позначає спосіб передавання: Base - пряме немодульоване передавання, Broad - використання широкосмугового кабелю з частотним ущільненням каналів; третій елемент - середовище передавання (T - вита пара, F - оптоволокно) або довжина сегмента кабелю в сотнях метрів (сучасні мережні адаптери дають змогу збільшувати довжину сегмента, наприклад для 10Base2, до 300 метрів).

"Товстий" Ethernet

Вживаються також синоніми - ThickNet, Yellow (жовтий), 10Base5. "Товстий" Ethernet введено в 60-х роках. Класичний варіант використовує товстий коаксіальний кабель RG-11 жовтого кольору з посрібненим центральним проводом та подвійним екрануванням. Кабель має хвильовий опір 50 Ом, мале затухання та високий ступінь захисту від зовнішніх впливів. На кінцях кабелю встановлюються 50-Омні опори (термінатори), один з яких заземлюється. Кабель має через кожних 2,5 м розмітку у вигляді рисок, що позначають місця можливого підключення або розрізу. Відрізки кабелю можуть з'єднуватись рознятями. Для включення вузла на кабель встановлюється трансивер MAU (активний пристрій з живленням 12В), який може підключатись через Т-конектор або шляхом проколювання кабелю ("вампір"). Трансивер з'єднується з мережним адаптером за допомогою спеціального кабельного спуску (AUI Cable) довжиною до 50 м. Кабельний спуск містить лінії живлення трансивера та екрановані виті пари для сигналів прийому, передавання та виявлення колізій. Як "жовтий" кабель, так і кабельний спуск мають товщину до 1 см. Жорсткість кабелів створює додаткові експлуатаційні труднощі. Вартість устаткування та складність монтажу не сприяють широкому використанню цієї архітектури. Іноді "товстий" Ethernet використовують для прокладання базових (хребтових, Backbone) сегментів у процесі побудови кампусних мереж.

Основні характеристики:

- максимальна довжина сегмента - 500 м;
- максимальна кількість сегментів, з'єднаних з використанням повторювачів - 5 (загальна довжина - 2500 м);
- три з п'яти сегментів можуть використовуватись для включення вузлів (Trunk Segments), два інші - як подовжувачі (Link Segments);
- на одному сегменті (Trunk) може бути до 100 вузлів разом з повторювачами.

"Тонкий" Ethernet

Вживаються також синоніми - ThinNet, 10Base2. Один з найпопулярніших варіантів архітектур для локальних мереж, використовує тонкий коаксіальний кабель RG-58. Кабель має хвильовий опір 50 Ом, середні затухання та ступінь захисту від зовнішніх впливів.

На кінцях кабелю встановлюються 50-Омні опори, один з яких заземлюється. Відрізки кабелю можуть з'єднуватись I та Т-конекторами, відстань між якими не може бути меншою за 50 см. Включення вузла, що завжди супроводжується розрізанням кабелю, може здійснюватись через Т-конектор або Т-подібне відгалуження від Т-конектора, яке не може перевищувати 10 см. Таке обмеження створює експлуатаційні труднощі. Відсутність контакту в будь-якому місці сегмента (дуже поширена несправність) виводить з ладу роботу всієї мережі. Перешкоди в роботі можливі також унаслідок дотикання Т-конекторів до металевих корпусів інших розняттів комп'ютера. Оптимальний спосіб використання - для прокладання базової мережі між кабельними центрами.

Основні характеристики:

- максимальна довжина сегмента - 300 м;
- максимальна кількість сегментів, з'єднаних з використанням повторювачів - 5 (загальна довжина - 1500 м);
- три з п'яти сегментів можуть використовуватись для включення вузлів (Trunk Segments), два інші використовуються як подовжувачі (Link Segments);
- на одному сегменті (Trunk) може бути до 30 вузлів разом з повторювачами.

Можливі варіанти спільного використання "товстого" та "тонкого" кабелю в одному сегменті через спеціальні перехідні розняття.

Ethernet на витій парі

Вдосконалення мережних засобів, зокрема адаптерів, дало змогу широко застосовувати виту пару як середовище передавання. В рамках стандарту Ethernet створені специфікації 10BaseT, що використовує дві неекрановані виті пари UTP (Unshielded Twisted Pare) 3,4 або 5 категорій, та 100BaseT4, що грунтується на чотирьох витих парах UTP 5 категорії або екранованій витій парі STP (Shielded Twisted Pare). Для зв'язку між вузлами мережі необхідними є дві виті пари провідників: одна - для передавання, інша - для приймання інформації. Звичайно, замість двох кабелів по одній парі витих провідників у кожній використовують один кабель з чотирма парами провідників. Окрім економії та технічних переваг, це створює можливість переходу на більш швидкісні мережні архітектури без заміни самого кабелю.

Фізична топологія - зірка: кожен вузол мережі з'єднується зі своїм портом кабельного центру кабельним променем, що не повинен пере-

вищувати довжини 100 м. На кінцях кабелю за допомогою спеціального обтискаючого інструмента встановлюються 8-контактні розняття RJ-45. Найбільш поширеними є 8-ми та 16-ти портові кабельні центри, що комплектуються зовнішніми адаптерами електромережі. Звичайно, один з портів призначається для з'єднання з наступним кабельним центром (перехрещеними парами провідників). Більшість кабельних центрів мають також розняття для під'єднання тонкого коаксіального кабелю, що дає змогу гнучко комбінувати фізичну топологію мережі Ethernet та обидва найбільш поширених типи кабелю. Найбільш вразливе місце Ethernet на витій парі - кабельний центр, вихід з ладу якого паралізує всі вузли мережі, з'єднані з ним витими парами.

Слід відмітити основні характеристики та переваги витої пари:

- фізична топологія - зірка;
- максимальна довжина променя - 100 м;
- до кожного вузла під'єднується лише один кабель;
- пошкодження кабелю виводить з ладу лише один мережний вузол;
- несанкціоноване прослуховування пакетів у мережі ускладнюється.

Формати фреймів Ethernet

Весь обмін інформацією в мережі відбувається за допомогою фреймів (Frame - кадр, бітова послідовність) - пакетів MAC-підрівня канального рівня, що визначаються стандартом IEEE802.3 та мають незначні відмінності в реалізації для протоколів TCP/IP та IPX/SPX.

Таблиця. Структура фрейма Ethernet

Преамбула	**Заголовок**	**Дані**	**Контрольна сума**
8 байтів	14 байтів	46-1500 байтів	4 байти
Послідовність для синхронізації приймача, що закінчується маркером початку пакета	Містить MAC-адреси пунктів призначення та передавання (по 6 байтів) та поле довжини (IPX/SPX) або типу протоколу (TCP/IP)	Вмістиме цього блока залежить від типу фрейма	CRC-код для контролю вірогідності передавання

Фрейм розпочинається преамбулою, що відповідає за побітову синхронізацію передавання та приймання даних мережними адаптерами. З цією метою в преамбулі сім разів повторюється байт 10101010. Початок надходження інформації визначає маркер 10101011. У полі адреси пункту призначення пакета, що має довжину 2 або 6 байтів,

міститься MAC-адреса мережного адаптера вузла, якому адресується інформація. Перший біт адреси визначає тип відправлення: 0 - для конкретного вузла, 1 - для групи вузлів. Поле адреси відправника пакета містить MAC-адресу мережного адаптера вузла, що здійснив передавання інформації. Це поле має таку ж довжину, як і поле адреси пункту призначення пакета, а його перший біт завжди дорівнює 0. Заголовок закінчується полем довжини блока даних, розмір якого становить 2 байти. Фрейм Ethernet_II замість поля довжини містить тип мережного протоколу, що здійснив відправлення цього пакета. Такий тип фреймів використовується протоколом TCP/IP. Конкретний тип фрейма вказується під час завантаження мережного драйвера.

Структура поля блока даних визначається стандартом IEEE802.2 LLC-підрівня канального рівня.

Окрім цього, стандарт IEEE802.3 визначає максимальну (1518 бітів) та мінімальну (512 бітів) довжину фрейма.

Обмеження на мінімальну довжину фрейма пов'язане з механізмом виявлення конфліктів. У процесі передавання надто коротких повідомлень вузол може закінчити передавання кадру до моменту виявлення колізії. У цьому випадку вузол вважатиме передавання успішним і не робитиме спроб повторного передавання. Час, протягом якого вузол може виявити наявність у каналі фрейма, відправленого іншим вузлом, називається *вікном конфліктів*. Довжина вікна конфліктів визначається сумарним часом поширення сигналів між двома крайніми вузлами. Вважається, що за час, який дорівнює вікну конфліктів, вузол захоплює середовище передавання, оскільки за цей час всі інші вузли зобов'язані виявити наявність пакета в каналі. Стандарт визначає максимальну тривалість вікна конфліктів, яка використовується для обчислення максимальної довжини мережі та мінімального розміру фрейма.

Максимальна довжина фрейма пов'язана з ймовірністю появи в ньому помилки під час передавання.

У кінці фрейма знаходиться поле контрольної послідовності (CRC-коду) кадру, що має довжину 4 байти та обчислюється за допомогою стандартного полінома 32-ого степеня.

Лекція 7. Інші мережні архітектури

Мережні архітектури першого покоління

ARCnet (Attached Resource Computer network) - архітектура мереж, що грунтується на логічній топології шини, з розподіленим середовищем передавання, маркерним (Token passing) методом доступу до середовища передавання, описана стандартом IEEE802.4-85.

Одна з перших комерційних архітектур для локальних мереж, що використовує тонкий коаксіальний кабель та виту пару. Фізична топологія - комбінація шини та зірки. Відрізки кабелю (звичайно, застосовується тонкий коаксіальний кабель RG-62 з хвильовим опором 93 Ом) з'єднуються Т-конекторами, відстань між якими не може бути меншою за 1 м. Допускається не більше 8 вузлів у сегменті. Сегмент має закінчуватись термінатором або активним хабом (адаптером). Використовуються активні (від 4 до 64 портів) та пасивні хаби (4 порти). Активний хаб може бути з'єднаний з адаптером або іншим активним хабом сегментом кабелю до 610 м, з пасивним хабом - кабелем довжиною до 30 м.

Кожен адаптер мережі має свою унікальну восьмибітову адресу, яка задається під час інсталяції перемикачами в діапазоні від 1 до 254. Право на відправлення даних мережею передається за допомогою спеціального пакета-маркера, що формується контролером-вузлом з найменшою адресою. Вузол, що отримав маркер, здійснює запит щодо готовності отримувача і, одержавши підтвердження, відправляє пакет даних. Після цього маркер передається наступному вузлу. Вузол, що не отримав маркер за визначений час (840 мс), передає спеціальну довгу бітову послідовність, яка руйнує старий маркер та призводить до процесу визначення нового контролера.

Основні характеристики та переваги:

- швидкість передавання: 2,5 Мбіт/с у базовому варіанті, від 20 до 100 Мбіт/с у малопоширених модифікаціях на витій парі та оптоволоконному кабелі;
- низька (порівняно з Ethernet) вартість з'єднувальних схем;
- гнучка топологія.

Недоліки:

- низька ефективність використання каналу передавання;
- використання однобайтових адрес ускладнює об'єднання ме-

реж;

- малий розмір фрейма (508 байтів) ускладнює узгодження з вищими рівнями моделі OSI.

AppleTalk - мережна архітектура фірми Apple (штатна підсистема комп'ютерів Macintosh) використовує шинну топологію, виту пару як середовище передавання та метод доступу CSMA/CA. Швидкість передавання - 230 Кбіт/с, максимальна довжина мережі - 300 м.

Token Ring (маркерне кільце) - архітектура мереж, що грунтується на логічній топології кільця, з маркерним методом доступу до середовища передавання, описана стандартом IEEE802.5.

Основним провідником цієї архітектури є фірма IBM. Логічне кільце реалізується на фізичній топології зірки, в центрі якої міститься MAU (Multistation Access Unit) - хаб з портами для під'єднання кожного вузла. Для під'єднання кабелів використовуються спеціальні розняття, що забезпечують замикання кільця у випадку від'єднання вузла від мережі. Мережа може бути розширена завдяки додатковим MAU, що об'єднуються у спільне кільце. Використання витої пари STP забезпечує підключення не більше 260 вузлів до 33 MAU з максимальною відстанню 100 м між вузлом та хабом. Довжина кабелів, що з'єднує MAU, не повинна перевищувати 100 м при їх сумарній довжині до 200 м. Використання оптоволоконного кабелю збільшує довжину сегмента до 1 км.

Інформація передається кільцем в одному напрямку від одного вузла до іншого. Мережний адаптер копіює у свій буфер тільки ті пакети, що адресовані йому. Право на передавання інформації передається вузлу за допомогою трибайтового маркера, який складається з байта початкового роздільника, байта контролю доступу та байта кінцевого роздільника. У структуру байта контролю доступу входять поле пріоритету, що задає рівень пріоритету вузла, який має право захопити маркер, та біт маркера, який вказує вільним чи зайнятим є маркер. Маркер у кільце запускає активний "монітор" - вузол (звично, це сервер), що відповідає за його наявність та єдиність. Решта вузлів є резервними моніторами і, у випадку зникнення активного монітора, ініціюють процес визначення нового активного монітора. Кожен вузол отримує та регенерує всі пакети. Вузол, що бажає здійснити передавання інформації, повинен дочекатись вільного маркера, додати адресну інформацію, дані та помітити маркер зайнятим. Пакет, що не знайшов свого адресата за один оберт кільцем, вилучається монітором кільця або

вузлом, що здійснив його передавання.

Основні характеристики та переваги:

- швидкість передавання - 4 або 16 Мбіт/с;
- визначений час очікування (що не збільшується у випадку збільшення трафіка) та управління пріоритетами дає змогу використовувати Token Ring в мережах реального часу;
- великий розмір фрейма - 18000 байтів;
- легке об'єднання з мережами великих машин (mainframe);

Недоліки:

- висока вартість обладнання;
- складність побудови великих мереж WAN/GAN.

Token Bus - мережна архітектура, що визначена стандартом IEEE802.4 та використовує логічну топологію кільця, а фізичну - шини. Середовище передавання - коаксіальний кабель з хвильовим опором 75 Ом або оптоволокно, метод доступу - передача маркера. Підтримується система пріоритетів, що забезпечує заданий час відгуку для різних рівнів. Часто використовується у промисловій автоматиці, наприклад, на цій архітектурі грунтується протокол MAP (Manufacturing Automation Protocol).

Мережні архітектури другого покоління

Fast Ethernet являє собою розвиток архітектури Ethernet на витій парі завдяки підвищенню у 10 разів тактової частоти. Основні принципи архітектури (метод доступу, формат фрейма та інші) залишаються незмінними. Стандартом IEEE802.3u визначено три типи Fast Ethernet: 100 BaseT4 та 100 BaseTX - для витої пари, та 100 BaseFX - для оптоволоконного кабелю.

Архітектура 100 BaseTX має певні переваги - вона грунтується на використанні кабелю (неекранованої витої пари 5 категорії) та розняттів, аналогічних до вимог 10BaseT. Це дає змогу проводити заміну мережних адаптерів 10BaseT на 100 BaseTX без заміни кабелю та розняттів.

Усі типи Fast Ethernet мають обмеження 100 м на довжину променя та 200 м (400 м для FX) - на діаметр мережі (максимальну відстань між двома вузлами мережі).

100BaseVG - 100Мбіт/с, мережа на витій парі категорії 3 для звукової телефонії (VG - Voice-Grade). Архітектура розроблена фірмами Hewlett-Packard та AT&T Microelectronics у розвиток Ethernet (IEEE802.12), що грунтується на фізичній топології зірки та методі доступу Demand Priority (пріоритет запитів), який забезпечує визначений

час відгуку для критичних до часу задач.

100BaseVG-AnyLAN - 100Мбіт/с, мережа на витій парі категорії 3, 4 або 5, розширення архітектури 100BaseVG, введене фірмами Hewlett-Packard та IBM. 100BaseVG-AnyLAN являє собою певний гібрид архітектур Ethernet та Token Ring та підтримує їх формати фреймів (802.3 та 802.5). Окрім пріоритетів доступу, підтримує 2 рівні пріоритетів передавання, що дає змогу використовувати мережу для відеоконференцій, мультимедійних та інших критичних до часу застосувань.

FDDI (Fiber Distributed Data Interface) - 100Мбіт/с, стандартизована Американським національним інститутом стандартів (ANSI) специфікація X3T9.5 для високошвидкісного передавання даних у мережах на базі оптоволоконного кабелю. Топологія - подвійне кільце (можливе включення зірко- та деревоподібних підмереж через концентратор), метод доступу - маркерний з можливістю одночасного циркулювання у кільці багатьох пакетів. Максимальна кількість вузлів у мережі - 1000, відстань між вузлами - від 2 до 45 км, залежно від кабелю (багатомодовий або одномодовий), довжина кільця - до 100 км.

CDDI (Copper Distributed Data Interface) або TPDDI (Twisted Pair Distributed Data Interface) - суто "електрична" реалізація архітектури FDDI на витій парі. Суттєво дешевший варіант FDDI, в якому, однак, довжина сегмента не більша як 100 м.

ATM (Asynchronous Transfer Mode) - технологія комутації пакетів, що забезпечує передавання цифрових, голосових та мультимедійних даних одними й тими ж лініями. Швидкість передавання 662 Мбіт/с (в експериментальних реалізаціях - 2,5 Гбіт/с) ATM використовується як в локальних, так і в глобальних мережах. Грунтується на виділених та комутованих оптоволоконних лініях. Кожен вузол може мати виділений зв'язок (канал) з будь-яким іншим. Використання пакетів фіксованої довжини (по 53 байти) дає змогу здійснювати корекцію помилок та маршрутизацію на апаратному рівні, забезпечує рівномірність голосового потоку в аудіо- та відеоконференціях. Комутація пакетів дає змогу, якщо є потреба, налагоджувати велику кількість віртуальних каналів між відправником та адресатом.

Лекція 8. Мережні операційні системи, адміністрування та управління мережею

Мережні операційні системи

Мережна операційна система (ОС) - це пакет програм, що забезпечує реалізацію та управління мережею, дає змогу клієнтам користуватись мережним сервісом. Основними завданнями мережної ОС є забезпечення сумісного використання та розподілу ресурсів мережі; надання клієнтам мережного сервісу; адміністрування мережі; обміну повідомленнями між вузлами мережі; взаємодії процесів у мережі; надійного зберігання даних та інших завдань, пов'язаних з функціонуванням мережі. Важливою функцією мережної ОС є забезпечення системи захисту - конфіденційності зберігання даних, розмежування прав доступу до ресурсів, парольний захист, виявлення спроб несанкціонованого доступу, трасування дій користувачів, ведення журналів системних подій тощо.

Мережна ОС забезпечує підтримку різноманітних периферійних пристроїв, мережних адаптерів, протоколів та можливість їх конфігурування.

Програмне забезпечення клієнтської частини перетворює запити прикладної програми на використання мережних ресурсів у відповідні мережні формати, забезпечує їх пересилання через середовище передавання та здійснює зворотні перетворення. Клієнтська частина залежить від ОС, що встановлена на робочій станції (DOS, Windows'95'98, Unix, Macintosh, OS/2), та типів мереж.

У мережах з централізованим управлінням (виділеним сервером) мережна ОС є головною (або єдиною) системою, що управляє ресурсами серверу. Такі системи, звичайно, мають високу продуктивність та функціональні можливості, використовують власні дискові та файлові системи, що оптимізовані для роботи в мережі (NetWare, Windows NT).

Однорангові мережі дають змогу кожному вузлу мережі одночасно виступати в ролі сервера та клієнта. Тут мережна ОС може бути процесом, що виконується під управлінням ОС вузла (NetWare Lite, LANtastic, Windows for Workgroups), або складовою частиною ОС (Personal NetWare, Windows'95'98, Windows NT).

Клієнтська частина реалізується у вигляді оболонки (редиректора), що обслуговує мережні запити та працює під управлінням вихідної ОС вузла (DOS, Unix, OS/2), або є органічною частиною ОС (Windows'95'98'NT). Звичайно, клієнт може мати одночасний доступ до ресурсів різних мереж, що використовують спільне середовище передавання.

NetWare

Сім'я мережних ОС NetWare фірми Novell розпочала бурхливий розвиток із середини 1980-х років. Основні версії NetWare розраховані на мережі з виділеним сервером, який працює під управлінням ОС NetWare (фірма Novell поставляє також прості однорангові мережні ОС - Personal NetWare та NetWare Light) : NetWare 2.2 на базі процесора i286 - для простих мереж на 5, 10, 50, 100 користувачів, NetWare 3.12 на базі процесорів i386, i486 та 32-розрядних шин - для мереж на 20, 100, 250 користувачів, NetWare 4.x - найбільш потужна багатосерверна ОС для мереж масштабу підприємства допускає одночасне обслуговування кожним з серверів до 1000 користувачів.

Виділений файл-сервер використовує власну файлову систему, що оптимізована для роботи з мережними запитами. На кожному вузлі мережі інсталюється мережна оболонка (*shell*), яка виконує роль редиректора команд - локальні команди адресуються локальній ОС вузла, мережні команди підлягають обробці та адресуються в мережу.

Потужна система захисту від несанкціонованого доступу визначає чотири рівні відповідальності: звичайний користувач, оператор серверу, менеджер, супервізор. Передбачено вісім типів доступу до файлів: R - відкриття та читання відкритого файла (запуск програми); W - відкриття та запис у відкритий файл; C - створення нового файла та відновлення знищеного; E - знищення файла; M - перейменування та зміна атрибутів файла, F - пошук файла в директорії; A - управління доступом до файла (надання всіх прав (окрім супервізора) всім користувачам); S - право супервізора поєднує всі інші права доступу. Висока продуктивність системи управління файлами забезпечується тотальним кешуванням дискових директорій, а захист файлів від апаратних збоїв - дублюванням дисків та дзеркальним відображенням даних.

Служба директорій Novell-NDS (NetWare Directory Services) є однією з найліпших серед аналогічних служб інших мережних ОС. Вона забезпечує централізоване управління серверами та мережними пристроями. Зареєстрований у дереві директорій NDS користувач отримує доступ до ресурсів мережі незалежно від їх розташування, як до єдиної інформаційної системи. Така ієрархічна структура дає змогу адміністраторові керувати деревами NDS з будь-якої точки входу в мережу.

NetWare забезпечує стандартний набір основних мережних служб - потужну службу друку; засоби управління мережею Manage Wise; платформу віддаленого доступу NetWare Connect; електронну пошту, персональне календарне планування, складання розкладів, управління завданнями засобами підтримки групової роботи Group Wise та інші.

ОС NetWare використовує: на фізичному рівні OSI - підтримку форматів фреймів найбільш поширених архітектур (Ethernet, Token Ring, ARCnet, FDDI); на канальному рівні - відкритий інтерфейс пере-

дачі даних ODI; на мережному рівні - протокол обміну пакетами IPX та протокол обміну інформацією про маршрутизацію RIP; на транспортному рівні - протокол послідовного обміну пакетами SPX, на верхніх (5-7) рівнях моделі OSI працюють служба емуляції NetBIOS, протокол оголошень про послуги SAP та протокол ядра NCP.

Незважаючи на свою популярність та цілий ряд переваг, ОС NetWare не цілком задовольняє вимоги застосувань клієнт-сервер та поступається за вартістю свого основного конкурента - Windows NT.

Windows NT

ОС Microsoft Windows NT - це 32-розрядна пріоритетна багатозадачна операційна система з влаштованими мережними засобами та засобами безпеки є потужною платформою для серверних застосувань. Система може працювати на комп'ютерах різних архітектур: CISC (повний набір команд), RISC (скорочений набір команд) та з симетричною мультипроцесорною архітектурою. Забезпечується підтримка підсистем OS/2, POSIX та віртуальні DOS-машини для запуску DOS-застосувань. Пріоритетна багатозадачність та стійке ядро ОС забезпечують достатню для відповідальних застосувань надійність функціонування системи. Клієнтами мереж NT можуть бути комп'ютери з ОС DOS, WfW, Windows'95'98, Macintosh. Сервер Windows NT може також виступати як сервер застосувань NetWare.

Залежно від розміру та призначення мережа NT може складатись з робочих груп та доменів (domain). NT-комп'ютери в складі робочої групи мають окремі бази даних зареєстрованих користувачів SAM (Security Account Manager) та локальні політики безпеки. В моделі робочих груп відсутня можливість централізованого управління мережею. ОС Windows NT існує у двох версіях - Workstation та Server, які є оптимізованими для використання як робочої станції та серверу відповідно. У доменній моделі використовується спільна база SAM, що може бути розподілена між кількома контролерами (комп'ютерами, що працюють під управлінням Windows NT Server), та єдина політика безпеки. Для мереж масштабу підприємста передбачені багатодоменні моделі з налагодженням між доменами довірчих відносин щодо прав користувачів та доступу до спільних ресурсів.

Власна файлова система NTFS (що може використовуватись сумісно з FAT-розділами дисків) та влаштовані в ОС засоби безпеки дають змогу надійно захистити дані та гнучко управляти доступом користувачів до каталогів та файлів.

Архітектура мережної частини має багаторівневу структуру. На нижньому рівні драйвери NDIS забезпечують підтримку будь-яким мережним адаптером будь-якого транспортного протоколу. Підтримуються протоколи NetBEUI, TCP/IP, IPX/SPX та DLC для зв'язку з мейнфреймами. Інтерфейс TDI (Transport Driver Interface) забезпечує доступ-

ність будь-якого стеку транспортних протоколів для вищих (сеансового і вище) рівнів OSI.

ОС Windows NT разом з набором затосувань Microsoft BackOffice найбільш близька для вирішення більшості завдань, що покладаються на мережну ОС. Наявність утиліти Migration Tool for NetWare, що дає змогу переносити ресурси та бюджети користувачів серверів NetWare на Windows NT Server, підвищує конкурентноздатність Windows NT.

Однорангові мережі Windows for Workgroups та Windows'95'98

Windows for Workgroups. ОС Microsoft Windows 3.11 for Workgroups (WfW) є розширенням ОС Windows 3.1, яке забезпечує користувачам Windows спільний доступ до дисків, принтерів, факс-модемів, електронну пошту, діалог (Chat), динамічний обмін даними (мережний DDE) між застосуваннями робочих станцій, віддалений доступ та ін. Мережа WfW однорангова - кожен комп'ютер може виступати як клієнтом, так і сервером. Для зручності пошуку комп'ютерів у мережі їх об'єднують в робочі групи (Workgroup), при цьому кожен комп'ютер може входити тільки в одну групу.

Захист від несанкціонованого доступу до спільних ресурсів забезпечується пароленням входу в мережу в поєднанні з паролями доступу до спільних ресурсів. На кожному комп'ютері з ім'ям користувача пов'язується список паролів для доступу до спільних ресурсів. Якщо є спроба доступу до ресурсу, який не вказаний у списку паролів, система вимагає введення паролю з клавіатури.

Мережний протокол за замовчанням - NetBEUI. Оскільки цей протокол не підтримує маршрутизацію для міжмережного зв'язку, передбачені драйвер IPX Support Driver with NetBIOS Transport та підримка стеку протоколів TCP/IP.

Windows'95'98. 32-розрядні ОС Microsoft Windows'95'98 з пріоритетною багатозадачністю та влаштованими мережними засобами займають проміжне становище між WfW та Windows NT. У порівнянні з NetWare та Windows NT система безпеки Windows'95'98 є суттєво слабшою. Як доповнення до засобів безпеки WfW у Windows'95'98 є можливість захищати ресурси серверу на рівні імен користувачів (груп), подібно до NetWare, але з меншим різноманіттям прав.

Зручний інтерфейс користувача, однотипне відображення мережних ресурсів, підтримка найбільш поширених мережних протоколів забезпечують ОС Windows'95'98 найбільшу популярність як ОС робочої станції в мережах NetWare і Windows NT.

Адміністрування та управління мережею

Адмініструванням мереж є діяльність із забезпечення готовності програмних та апаратних засобів до обслуговування користувачів: створення та обслуговування бюджетів користувачів; визначення привілеїв та прав доступу; інсталяція та тестування програмних та апаратних за-

собів; резервне копіювання та відновлення файлів; підтримка життєздатності файлової системи; розв'язання програмних та апаратних проблем; управління та оптимізація мережного трафіка; захист мережних ресурсів від втручання ззовні тощо.

Складність задач адміністрування залежить від типу та розмірів мережі. В однорангових мережах адміністраторські роботи проводяться на кожній робочій станції. У мережах з централізованим управлінням скорочується кількість фізичних місць зберігання даних, на робочих станціях зберігається лише мінімальна клієнтська частина, а основне мережне програмне забезпечення розміщається на сервері, що полегшує його модифікацію чи модернізацію. Однак і в цьому випадку у великих (за розмірами, кількістю вузлів та користувачів) мережах завдання адміністратора є достатньо складними.

Терміном "мережне адміністрування (управління)" (Network Management) позначають автоматизовані дії, що скеровані на підтримку рівня продуктивності мережі та вирішення інших адміністраторських завдань. Застосовуються дві основні моделі адміністрування - модель IP та еталонна моделі OSI. Завдяки своїй простоті та універсальності найбільше поширена модель управління IP, до складу якої входять: структура управління інформацією SMI (Structure of Management Information), інформаційна база управління MIB (Management Information Base) та простий протокол мережного управління SNMP (Simple Network Management Protocol). SMI визначає спосіб подання інформації про об'єкт. Інформація організована як набір властивостей та їх значень у вигляді деревовидної структури. Всі об'єкти (мережі, вузли, застосування, функції та ін.) мають унікальне розташування в дереві. MIB містить визначення властивостей та їх значення. З MIB взаємодіє Management Agent - програма-агент, що виконується на керованій робочій станції, завданням якої є збір та передача інформації про об'єкти на запити менеджера - програми управління мережею. SNMP використовує управляючу станцію (на якій виконується менеджер) та агентів, що мають з цією станцією зв'язок. Агенти збирають та відправляють інформацію зі своїх вузлів менеджеру за його запитами. З ініціативи агента додатково передаються спеціальні повідомлення (traps) щодо заздалегідь визначених особливих ситуацій.

Лекція 9. Адресація та маршрутизація в IP-мережах

Адресація в IP-мережах

На відміну від фізичних MAC-адрес, формат яких залежить від конкретної мережної архітектури, IP-адреса будь-якого вузла мережі є чотирибайтовим числом. Записуються IP-адреси чотирма числами в діапазоні від 0 до 255, які представляються в двійковій, вісімковій, десятковій або шістнадцятковій системах числення та розділяються крапками (наприклад 192.168.40.250). Для більш ефективного використання єдиного адресного простору Internet введено класи мереж:

- Мережі класу **A (1-126)** мають 0 в старшому біті адрес. На мережну адресу відводиться 7 молодших бітів першого байта, на гост-частину - 3 байти. Таких мереж може бути 126 з 16 мільйонами вузлів у кожній.
- Мережі класу **B (128-191)** мають 10 у двох старших бітах адрес. На мережну адресу відводиться 6 молодших бітів першого байта та другий байт, на гост-частину - 2 байти. Таких мереж може бути близько 16 тисяч з 65 тисячами вузлів в кожній.
- Мережі класу **C (192-223)** мають 110 у трьох старших бітах адрес. На мережну адресу відводиться 5 молодших бітів першого байта та другий і третій байт, на гост-частину - 1 байт. Таких мереж може бути близько 2 мільйонів з 254 вузлами в кожній.
- Мережі класу **D (224-239)** мають 1110 у чотирьох старших бітах адрес. Решта біт є спеціальною груповою адресою. Адреси класу D використовуються у процесі звернення до груп комп'ютерів.
- Мережі класу **E (240-255)** зарезервовані на майбутнє.

Для зменшення трафіка в мережах з великою кількістю вузлів застосовується розділення вузлів за підмережами потрібного розміру. Адреса підмережі використовує кілька старших бітів гост-частини IP-адреси, решта молодших бітів - нульові. В цілому IP-адреса складається з адреси мережі, підмережі та локальної гост-адреси, яка є унікальною для кожного вузла. Для виділення номерів мережі, підмережі та госта (вузла) використовується маска підмережі - бітовий шаблон, в якому бітам, що використовуються для адреси підмережі, присвоюються значення 1, а бітам адреси вузла - значення 0. Розглянемо адресу 192.168.40.252 та значення маски 255.255.255.0. У цьому випадку маємо адресу підмережі 192.168.40 та адресу госта - 252. При цьому всі гости підмережі 192.168.40 мають встановити ту ж саму маску підмережі. Отже, мережа 192.168 може мати 256 підмереж з 254 вузлами в кожній. Використання ж маски 255.255.255.192 дасть змогу мати 1024 підмережі з 60 вузлами в кожній.

Комбінації всіх нулів або всіх одиниць у мережній, підмережній або гост-частині зарезервовані для загальних (broadcast) повідомлень та службових цілей. Наприклад, адреса 192.168.40.255 використовується для загального повідомлення всім вузлам підмережі 192.168.40.

Кожен гост може мати не тільки IP-адресу, але й ім'я (Host name). Як і цифрові IP-адреси, імена вузлів діляться на частини, що розділяються крапками. Починають запис від імені комп'ютера, далі йдуть імена локальних доменів (груп комп'ютерів) і закінчується ім'я вказанням імен вищих доменів (організаційних та територіальних). Список цих імен зберігається в спеціальній базі даних доменів служби імен DNS (Domain Name System). Наприклад, ім'я blues.franko.lviv.ua відповідає серверу з іменем Blues у домені franko.lviv.ua комп'ютерів кампусної мережі Львівського державного університету ім. І.Франка. Звертаючись до вузла, з однаковим успіхом можна використати як IP-адресу, так і його ім'я.

Стек протоколів TCP/IP

Архітектура протоколів TCP/IP призначена для об'єднаної мережі, що складається зі з'єднаних між собою за допомогою шлюзів окремих різнорідних комп'ютерних підмереж.

Протоколи цієї сім'ї розроблялись для мережі ARPAnet Міністерства оборони США, а пізніше отримали широке використання у мережах UNIX-машин та всесвітній мережі Internet. Стек протоколів TCP/IP розроблено та протестовано ще до прийняття стандартів ISO, а тому ієрархію управління в IP-мережах визначають п'ятьма рівнями: 1 - Hardware level, 2 - Network interfase, 3 - Internet level, 4 - Transport level, 5 - Application level.

1 - нижній рівень Hardware level описує середовище передавання.

2 - рівень Network interfase (мережний інтерфейс) містить апаратнозалежне програмне забезпечення, яке забезпечує поширення інформації на певному відрізку середовища передавання.

3 - рівень Internet (міжмережний) level представлений протоколами IP, ARP, RARP та ICMP. Головне його завдання - маршрутизація (вибір шляху передавання даних через множину проміжкових вузлів) під час передавання інформації від вузла-відправника до вузла-адресата. Інше важливе завдання протоколу IP - надання вищим рівням єдиного, уніфікованого та апаратно-незалежного інтерфейсу передавання інформації. Відповідність IP-адреси вузла його фізичній адресі в підмережі динамічно визначається за допомогою запитів протоколу ARP (Address Resolution Protocol) та запам'ятовування отриманих адрес. Протокол RARP (Reverse Address Resolution Protocol) виконує протилежні ARP

функції - перетворює фізичні MAC-адреси у відповідні їм IP-адреси. Для обміну керуючими повідомленнями, повідомленнями про помилки, які можуть виникати у процесі передавання даних між вузлами, для визначення доступності вузлів, адрес маршрутизаторів тощо використовується протокол ICMP (Internet Control Message Protocol). Якщо маршрутизатор отримує пакет, який не може бути переданим адресатові (найчастіше така ситуація виникає, якщо маршрутизатору не відомий маршрут до адресата), він повертає відправнику ICMP-повідомлення "Гост недоступний" (Host Unreachable). Адміністратори для з'ясування доступності госта часто користуються утилітою ping (у режимі командної стрічки її синтаксис такий: ping [IP_адреса | ім'я_госта]), яка грунтується на повідомленнях ICMP.

4 - протокол IP не забезпечує гарантовану доставку пакетів, збереження порядку та цілісності їх потоку. Ці завдання вирішують протоколи TCP (Transmission Control Protocol) та UDP (User Datagram Protocol), які відносяться до Transport (транспортного) level. Однак TCP та UDP реалізують різні режими передавання даних. UDP (як і IP) є дейтаграмним (datagram) протоколом без налагодження з'єднання. На відміну від UDP TCP є протоколом з налагодженням з'єднань - два вузли "домовляються" про обмін даними та управління цим потоком. Протокол TCP забезпечує організацію зв'язку між вузлами мережі з гарантованою доставкою повідомлень. Він контролює налагодження віртуального з'єднання з вузлом-адресатом, послідовність пакетів під час їх одержання в пункті призначення, опрацьовує помилки. TCP не підтверджує одержання пошкоджених або втрачених даних, що одразу є для відправника сигналом для виконання повторного передавання. Завдяки цьому стек протоколів TCP/IP задовольняє потреби поетапного передавання даних, клієнт-серверних застосувань тощо. Надійність TCP забезпечується певною втратою продуктивності передавання даних. Протокол UDP працює швидше ніж TCP, однак не гарантує доставку повідомлень. Особливістю UDP є також підтримка загальних повідомлень, завдяки яким один вузол має змогу одночасно звертатись до кількох інших.

5 - рівню Application (прикладному) level відповідають прикладні задачі, серед яких найбільш відомими є гіпертекстові засоби віддаленого доступу WWW, обмін файлами FTP (File Transfer Protocol), протокол служби логічних імен DNS (Domain Name Service), електронна пошта SMTP (Simple Mail Transfer Protocol) та емуляція термінала віддаленого UNIX-серверу TelNet.

Взаємодія рівнів загалом має такий вигляд:

- Застосування передає транспортному рівневі повідомлення (message) певної семантики та розміру.

- Транспортний рівень розрізає, в разі потреби, повідомлення на пакети (packet), які передаються міжмережному рівню.
- Міжмережний рівень, тобто протокол IP, формує свої IP-пакети (IP-дейтаграми) та упаковує їх у формати, що відповідають певному фізичному середовищу передавання. Такі апаратнозалежні пакети називають кадрами, або фреймами.

Маршрутизація в IP-мережах

Термін маршрутизація (routing) означає передавання дейтаграм від одного вузла іншому. "Пряма" маршрутизація (direct routing) здійснюється між вузлами однієї підмережі. В цьому випадку вузол-відправник знає конкретну фізичну адресу отримувача й інкапсулює IP-дейтаграму у відповідний фрейм мережі. "Непряма" маршрутизація (indirect routing) означає передавання дейтаграм між вузлами різних (під)мереж, що здійснюється маршрутизатром. Виявивши розходження немаскованої (мережної) частини IP-адрес, вузол-відправник направляє фрейм з IP-дейтаграмою за фізичною адресою маршрутизатора. Маршрутизатор (спеціалізований пристрій або комп'ютер) зберігає таблиці маршрутизації за допомогою яких, якщо відома адреса призначення пакета, можна визначити адресу іншого маршрутизатора або іншої (під)мережі. Після аналізу IP-адреси отримувача маршрутизатор направляє дейтаграму в одну з безпосередньо під'єднаних до нього (під)мереж, або ж - наступному маршрутизатору. Для забезпечення міжмережного обміну всі вузли мережі (зокрема і маршрутизатори) повинні мати списки IP-адрес доступних маршрутизаторів.

Розташовані на межі локальної (кампусної) та глобальної мереж маршрутизатори називають граничними (Border Gateway). Його таблиці маршрутизації містять інформацію як про внутрішні, так і про зовнішні мережі. Використання граничних маршрутизаторів дає змогу зменшити розміри таблиць внутрішніх маршрутизаторів та підвищити ефективність їхньої роботи.

Протоколи маршрутизації бувають статичними та динамічними. У статичних протоколах зміни в таблицях маршрутизації робить адміністратор мережі, у динамічних цей процес відбувається автоматично.

Список літератури

1. Администратор сетевой операционной системы NetWare v.3.11.– К.: АО "Квазар-Микро", 1994. – 191 с.

2. Баня Е.Н. Компьютерные сети. – К.: Світ, 1999. – 112 с.

3. Буров Є. Комп'ютерні мережі. – Львів: БаК, 1999. – 468 с.

4. Галіцин В.К., Левченко Ф.А. Багатокористувацькі обчислювальні системи та мережі: Навч. посібник. – К.: КНЕУ, 1998. – 360 с.

5. Гук М. Локальные сети Novell. Карманная энциклопедия. – СПб: Питер, 1996. – 288 с.

6. Кулаков Ю.А., Луцкий Г.М. Компьютерные сети. – К.: Юниор, 1998. – 384 с.

7. Рикалюк Р.Є., Стягар О.М., Данчак П.В. Вступ до комп'ютерних мереж. Текст лекцій. – Львів: Ред.-вид. відд. Львів. ун-ту, 1996. – 60 с.

8. Фролов А.В., Фролов Г.В. Сети комп'ютеров в вашем офисе. – М.: Диалог-МИФИ, 1995. – 272 с.

Серія науково-методичних матеріалів
"Побудова та адміністрування Intranet-мереж"
складається з таких частин:

1.Основи мережних технологій.
2.Адміністрування мереж Windows NT.