

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
імені ІВАНА ФРАНКА

Р.Є.Рикалюк

# **КОМП'ЮТЕРНІ МЕРЕЖІ**

## **Текст лекцій**

Рекомендовано до друку  
кафедрою програмування  
Протокол № від

Львів ЛНУ 2015

Рикалюк Р.Є. Комп'ютерні мережі: текст лекцій.  
Видавн. центр Львів. ун-ту, 2015. - 158 с.

У конспекті лекцій викладено основи комп'ютерних мереж і комунікацій, модель взаємодії відкритих інформаційних систем, моделі топологій, принципи функціонування конкретних сучасних мереж та програмного забезпечення.

Для студентів факультету прикладної математики та інформатики, економічного та факультету електроніки університету.

Рецензенти:

©Р.Є.Рикалюк, 2015

Кінець другого тисячоліття і початок третього ознаменував перехід до ери інформаційного суспільства. Цілі галузі, зокрема страхові і банківські компанії, фірми з мільярдними доходами мають справу не з матеріалізованими товарами, а з інформацією, обробляти яку і керувати якою допомагають комп'ютери.

Комп'ютерна революція торкнулася всіх сфер життя, і комп'ютер став чи не найважливішим інструментом у наукових дослідженнях, сучасних технологіях та дослідженнях космічного простору. За кілька останніх років комп'ютерні технології докорінно змінили безліч професій та створили багато нових. Комп'ютери стали необхідним допоміжним засобом у виробництві, бізнесі, сфері обслуговування, у побуті. Однак дуже швидко комп'ютери самі по собі перестали задовільняти людей, і якщо людям для обміну інформацією потрібні телефони, то комп'ютерам – мережі. Хоч з моменту появи перших комп'ютерних мереж минуло трохи більше 30 років, сьогодні мережі перетворились з диковинки в мільярдний бізнес. Кожного разу, коли Ви користуєтесь телефоном для міжміської розмови чи замовляєте квиток для подорожі авіалініями чи залізницею, Ви довіряєтесь комп'ютерній мережі.

Останніми роками введено в експлуатацію мережі, які дають змогу комп'ютерам обмінюватися інформацією зі швидкістю приблизно 10-12 Гбіт/с. Це еквівалентно передаванню за одну секунду 5 000 000 сторінок тексту, надрукованого через один інтервал. Є експериментальні мережі, здатні передати всю інформацію Британської енциклопедії за лічені секунди. Лабораторні дослідження підтверджують можливість систем зв'язку з швидкістю кількох терабіт/с на віддаль 100 км без підсилення. У 2007 р. фірми Fujitsu та Heinrich Herz встановили рекорд у швидкості передавання даних через оптоволоконні мережі 2,56 Тбіт/с на віддаль 160 км.

Сьогодні вчений, користуючись комп'ютером, може надіслати через мережу колезі з іншого кінця країни або світу тривимірний графік результатів проведеного експерименту упродовж лічених хвилин. Швидкий обмін даними дає змогу скоротити тривалість проведення експерименту до кількох днів замість колишніх тижнів, і працювати разом з колегами

навіть тоді, коли їх розділяють тисячі кілометрів, не втрачаючи часу на переїзди.

Ми також намагаємось увійти у світовий інформаційний простір. Цей процес, очевидно, триватиме довго. Однак уже сьогодні маємо змогу вчитися і працювати на ліпших світових зразках комп'ютерних мереж. В Україні є багато локальних мереж, які, на жаль, дуже різні і поки що нема потужних центрів, навколо яких вони могли б об'єднуватись. У затяжній стадії реалізації проект міжвузівської та наукової мережі URAN, хоч паралельно існує вже багато років мережа UARNET. Сподіваємось, що ситуацію в значній мірі вдасться виправити, залучивши широке коло користувачів наукових та дослідницьких установ України до мережі GEANT, яка є частиною мережі Internet.

## I. АРХІТЕКТУРА РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

### 1.1 Виникнення комп'ютерних мереж

Уже з початку розвитку комп'ютерної техніки ситуація склалася так, що потреби були більші, ніж можливості. У 60-х роках це зумовило концепцію об'єднання кількох ЕОМ, віддалених одна від одної, в єдину систему шляхом з'єднання їх спеціальними каналами зв'язку.

Це був прообраз комп'ютерної мережі. Можливості перших мереж, як і самих комп'ютерів, були скромними. Всеволод Бурцев [40] згадує про створення першої глобальної комп'ютерної мережі у колишньому Радянському Союзі для реалізації проблеми протиракетної оборони. Така мережа була створена (цілком таємно) у 1961 році на полігоні у Казахстані, на захід від озера Балхаш.

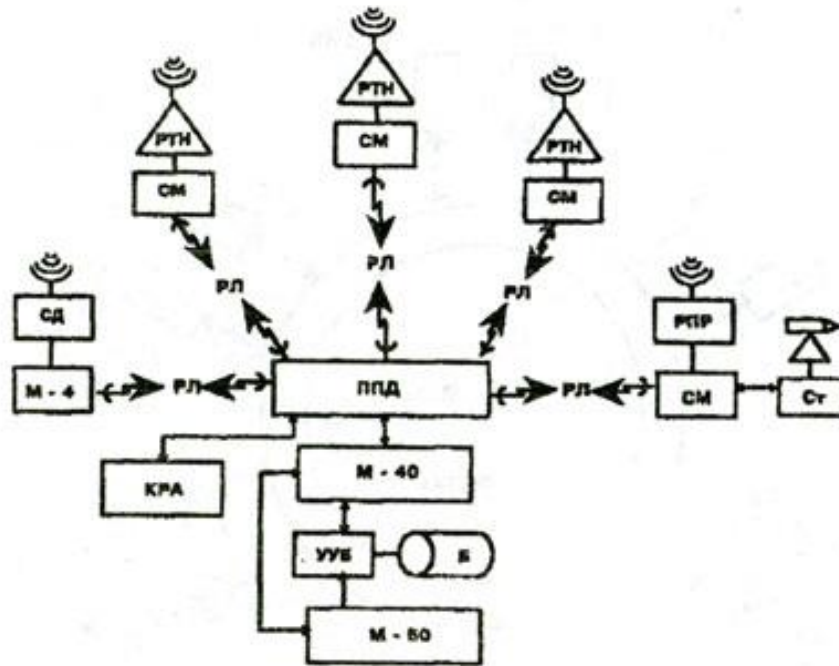


Схема обчислювальної мережі експериментальної системи ПРО, розгорнутої в 1959-1960 рр. в Казахстані.

Позначення: РТН – радіолокатори точного наведення, СМ – спеціальні обчислювальні машини, СД – станція дальнього пошуку, РПР – радіолокатор протиракет (передача сигналів на протиракету), СТ – мобільна стартова установка протиракет, ППД – процесор приймання і передавання даних, М-4, М-40 і М-50 – електронні обчислювальні машини, Б – запам'ятовуючий пристрій на магнітному барабані, УУБ – пристрій керування барабаном, КРА – контрольно-реєструвальне обладнання, РЛ – радіорелейні лінії зв'язку.

Така мережа працювала на частоті 1 МГц, включала кілька обчислювальних машин різної потужності, у тому числі на мобільній (!) платформі, сполучених між собою у бездротову (!) мережу, яка могла працювати на віддалі до 200 км. (Бездротові мережі для загального використання у світі отримали поширення лиш в 1980-і роки).

На американському континенті однією з перших була мережа Cybernet, створена фірмою Control Data Corporation (CDC) у 1969 році. Спочатку вона мала два центри (кластери) з багатомашинною структурою. Кожна з машин кластерів могла працювати самостійно або в комплексі над якоюсь громіздкою задачею. Кластери були з'єднані між собою швидкісною лінією зв'язку. Від них відходили лінії зв'язку до обчислювальних центрів (ОЦ) в інших містах, де були слабші ЕОМ, ніж ті, що в кластерах (фірма CDC). На периферійному обладнанні цих машин працювали користувачі. Якщо задача

користувача не потребувала великих ресурсів, то її обробляла місцева ЕОМ. Якщо ж вона не справлялась, то пересилала задачу в кластер, а результати – назад в місцеву ЕОМ. Це була трирівнева система обробки на відстані, чи телеобробки. Сама ідея телеобробки передбачала розміщення термінального обладнання користувача на відстані від ОЦ і з'єднання його з ЕОМ за допомогою телефонних ліній. Під час передавання даних у модемах (модулятор-демодулятор) цифрова інформація (байт) перетворювалася в послідовне кодування з частотною або амплітудно-частотною модуляцією. На це покладали багато надій (ресурси були зосереджені в одному місці, інформація теж. Набирай звідки-небудь код по телефону і з'єднуйся). Власне такий тип обчислювальних мереж демонструвався в Нью-Йорку в 1965р.(центральна машина CDC-6600, перший суперкомп'ютер Сеймура Крея). Для 60-70-х років апаратна частина комп'ютерів була дуже дорогою, тому зосередження та обробка інформації у великих вузлах системи була цілком виправданою. Режим телеобробки виявився ефективним для невеликих віддалей (в межах однієї будівлі чи установи). Так було організовано віддалений доступ термінального обладнання до каналів ЕОМ серії ЕС (див. рис.1.). Докладніше про телекомунікаційний метод доступу див. у [13].

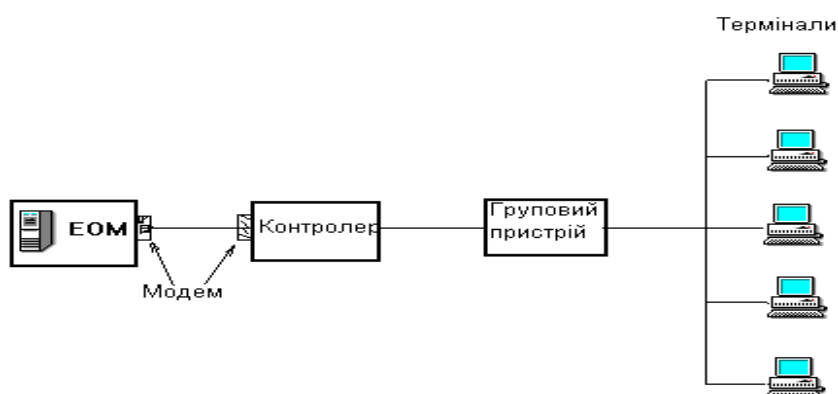


Рис.1. Мережа з телекомунікаційним зв'язком.

Однак цей спосіб побудови мереж дуже швидко виявився неперспективним. Причини: неефективність роботи внаслідок низької швидкодії та інформативності обміну;

дорожнеча телефонних розмов; захист переданої інформації від несанкціонованого доступу майже відсутній. Тому до концепції мережі підійшли з іншого боку, а власне з інформаційного, оскільки відомо, що сьогодні інформація є одним з найцінніших продуктів суспільства. Її розташовують на магнітних носіях ЕОМ, створюють спеціальні структури – бази даних (БД), якими керують системи керування базами даних (СКБД). Сотні організацій, фірм, державних структур мають потребу в інформації. Питання як і звідки її одержати? Найпростіше – розробити в себе інформаційні бази даних та супроводжувати їх для власного використання. Проте це не завжди можливо з різних причин. БД – "жива структура", яка періодично змінюється, тому треба мати відповідну службу для їх обслуговування. Найкраще, коли розробкою та супроводжуванням БД займаються організації, які вміють це робити фахово, а інші звертаються до них і користуються БД. Так ми підійшли до концепції розподілених БД: кожна організація веде БД за своєю тематикою і водночас має доступ до БД інших організацій. Як же отримати цей доступ? Очевидно, це залежить від обсягу інформації, засобів приймання та передавання тощо. Інформацію у вигляді файлів можна передавати за допомогою пристроїв флеш-пам'яті, магнітних дисків або стрічок, дискет, а також у формі графіків, телефонограм та ін. Однак найліпше мати безпосередній доступ до самої БД за допомогою швидкісних каналів зв'язку, щоб використати її у своїй локальній ЕОМ, бо кінцева мета не тільки отримати інформацію, але скористатися нею в розрахунках. Отже, виникає потреба поєднати інформаційну мережу з обчислювальною, тобто створити інформаційно-обчислювальну мережу. Більшість існуючих мереж є власне такими.

Історія розвитку комп'ютерних мереж дуже добре проглядається через історію розвитку найбільшої на сьогодні інформаційної мережі Інтернет. Ще у 1958 році при Міністерстві оборони США було створено Агентство Передових Дослідницьких Проектів — Advanced Research Projects Agency (ARPA). Головним завданням ARPA були дослідження в області забезпечення безпеки зв'язку і комунікацій в ході обміну ядерними ударами. У 1963 році керівником комп'ютерної лабораторії ARPA Джоном Ліклідером (J.C.R.Licklider) була запропонована детально розроблена концепція комп'ютерної

мережі а у 1967 році Ларрі Робертс (Larry Roberts), розпочав практичні роботи з реалізації теоретичних ідей Ліклідера. Через два роки поспіль ARPANET запрацював. До мережі приєднуються комп'ютери провідних університетів, лабораторій та дослідницьких центрів США. У 1968 працюють сумісно чотири станції, а у 1969 прийнято перший RFC (Request for Comment) "Програмне забезпечення вузла" Steve Crocker.

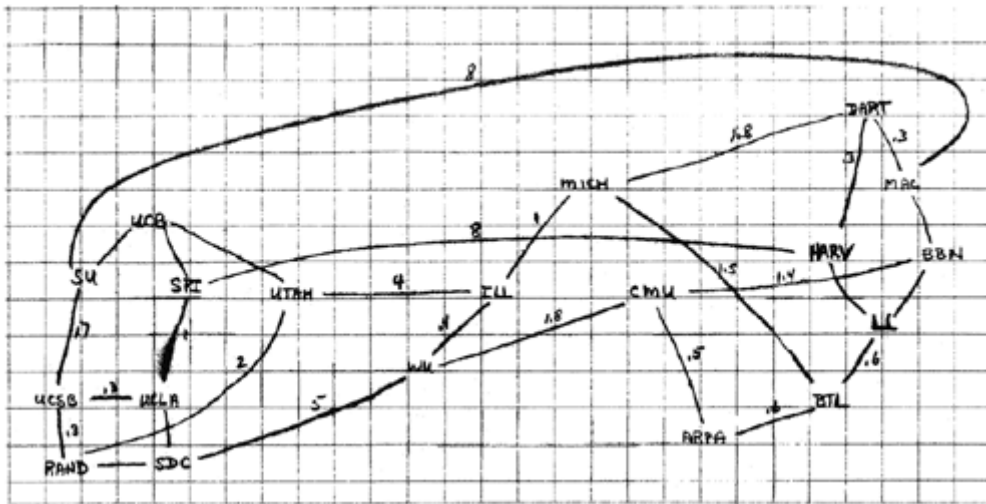


Рис. 1.2. Схема ARPAnet наприкінці 60-х років.

Вже у 1972 році в мережі працює 40 ЕОМ, а через десять років мережа стає стандартом — приймається протокол обміну інформаційними пакетами та протокол адресування, які знайомі нам сьогодні як сімейство TCP/IP.

Перший сервер ARPANET був встановлений 2 вересня 1969 року в Каліфорнійському університеті в Лос-Анджелесі. Комп'ютер Honeywell DP-516 мав 24 Кб оперативної пам'яті. 29 жовтня 1969 в 21:00 між двома першими вузлами мережі ARPANET, що знаходяться на відстані в 640 км - в Каліфорнійському університеті Лос-Анджелеса (UCLA) і в Стенфордському дослідницькому інституті (SRI) - провели сеанс зв'язку. Чарлі Клайн (Charley Kline) намагався виконати віддалене підключення до комп'ютера в SRI. Успішну передачу кожного введенного символу його колега Білл Дювалль (Bill Duvall) з SRI підтверджував по телефону.

У перший раз вдалося відправити всього три символи «LOG», після чого мережа перестала функціонувати. LOG повинно було бути словом LOGON (команда входу в систему). У робочий стан систему повернули вже до 22:30 і наступна спроба виявилася успішною. Саме цю дату можна вважати днем народження Інтернету.

































До 1971 року була розроблена перша програма для відправки електронної пошти по мережі. Ця програма відразу стала дуже популярна. У 1973 році до мережі були підключені через трансатлантичний телефонний кабель перші іноземні організації з Великобританії та Норвегії, мережа стала міжнародною.

У 1974 році відкрита перша комерційна версія ARPANET - мережа Telenet. Реальним прообразом сьогоденішнього Інтернету, напевно, можна вважати об'єднання у 1986 році шести великих американських IP-мереж у єдину наукову мережу NSFNET, яка у 1989 році налічувала більше 10 тисяч хостів і зберігала провідну роль впродовж десяти років.



Причиною переродження мережі у сучасний Інтернет стала запропонована у 1992 році Тімом Бернерсом-Лі з Європейського Центру ядерних досліджень в Женеві (CERN), технологія представлення інформації за допомогою веб-сторінок — протокол World Wide Web (WWW). Вже у 1993 році число приєднаних серверів перейшло мільйонну позначку, а у 1996 році число хостів налічувало 12,8 мільйонів і 500 тисяч веб-сторінок (сайтів). Через десять років, тобто у 2006 році число користувачів мережі Інтернет перейшло мільярдну межу, а у 2011 -- 2-мільярдну. Зараз в Європі налічується понад 476 млн користувачів Інтернет, що становить 58.3% усього населення континенту або 22.7% користувачів світу. За період 2000—2011 число користувачів Всесвітньої мережі зросло майже у три з половиною рази, тобто на червень 2011 року їх кількість становила 353.1% від кількості 2000 року. Розподіл Інтернет-користувачів у Європі подано у таблиці:

Місце	Країна	Кількість користувачів (тис. осіб)	Частка населення
1	 <a href="#">Німеччина</a>	65 125.0	79.9%
2	 <a href="#">Росія</a>	59 700.0	43.0%
3	 <a href="#">Велика Британія</a>	51 442.1	82.0%
4	 <a href="#">Франція</a>	45 262.0	69.5%
5	 <a href="#">Туреччина</a>	35 000.0	44.4%
6	 <a href="#">Італія</a>	30 026.4	49.2%
7	 <a href="#">Іспанія</a>	29 094.0	62.2%
8	 <a href="#">Польща</a>	22 452.1	58.4%
9	 <a href="#">Україна</a>	19 700.0	43.5%
10	 <a href="#">Нідерланди</a>	14 872.2	88.3%
11	 <a href="#">Швеція</a>	8 397.9	92.4%
12	 <a href="#">Бельгія</a>	8 113.2	77.8%
13	 <a href="#">Румунія</a>	7 786.7	35.5%
14	 <a href="#">Чехія</a>	6 680.8	65.6%
15	 <a href="#">Угорщина</a>	6 176.4	61.9%
16	 <a href="#">Швейцарія</a>	6 152.0	80.5%
17	 <a href="#">Австрія</a>	6 143.6	74.8%
18	 <a href="#">Португалія</a>	5 168.8	48.0%
19	 <a href="#">Греція</a>	4 970.7	46.2%
20	 <a href="#">Данія</a>	4 750.5	85.9%
21	 <a href="#">Фінляндія</a>	4 480.9	85.2%
22	 <a href="#">Білорусь</a>	4 436.8	46.3%
23	 <a href="#">Норвегія</a>	4 431.1	94.4%

Місце	Країна	Кількість користувачів (тис. осіб)	Частка населення
24	 <a href="#">Сербія</a>	4 107.0	56.2%
25	 <a href="#">Словаччина</a>	4 063.6	74.2%
26	 <a href="#">Азербайджан</a>	3 689.0	44.1%
27	 <a href="#">Болгарія</a>	3 395.0	47.9%
28	 <a href="#">Ірландія</a>	3 042.6	65.1%
29	 <a href="#">Хорватія</a>	2 244.4	50.1%
30	 <a href="#">Литва</a>	2 103.5	59.5%
31	 <a href="#">Латвія</a>	1 503.4	68.2%
32	 <a href="#">Боснія і Герцеговина</a>	1 441.1	31.2%
33	 <a href="#">Вірменія</a>	1 396.6	47.1%
34	 <a href="#">Молдова</a>	1 333.0	30.9%
35	 <a href="#">Албанія</a>	1 300.0	43.4%
36	 <a href="#">Грузія</a>	1 300.0	28.3%
37	 <a href="#">Словенія</a>	1 298.5	64.9%
38	 <a href="#">Македонія</a>	1 057.4	50.9%
39	 <a href="#">Естонія</a>	971.9	75.7%
40	 <a href="#">Кіпр</a>	482.4	43.1%
41	 <a href="#">Люксембург</a>	424.5	84.3%
42	 <a href="#">Косово</a>	377.0	20.7%
43	 <a href="#">Чорногорія</a>	303.5	45.9%
44	 <a href="#">Ісландія</a>	301.6	97.0%
45	 <a href="#">Мальта</a>	240.6	58.9%
46	 <a href="#">Андорра</a>	67.2	79.2%
47	 <a href="#">Гернсі</a>	78.3	74.2%
48	 <a href="#">Джерсі</a>	45.8	48.6%
49	 <a href="#">Фарерські острови</a>	37.5	76.1%
50	 <a href="#">Острів Мен</a>	35.6	42.1%
51	 <a href="#">Монако</a>	29.8	97.6%
52	 <a href="#">Ліхтенштейн</a>	23.0	65.3%
53	 <a href="#">Гібралтар</a>	20.2	69.8%
54	 <a href="#">Сан-Марино</a>	17.0	53.4%
55	 <a href="#">Ватикан</a>	0.5	57.7%

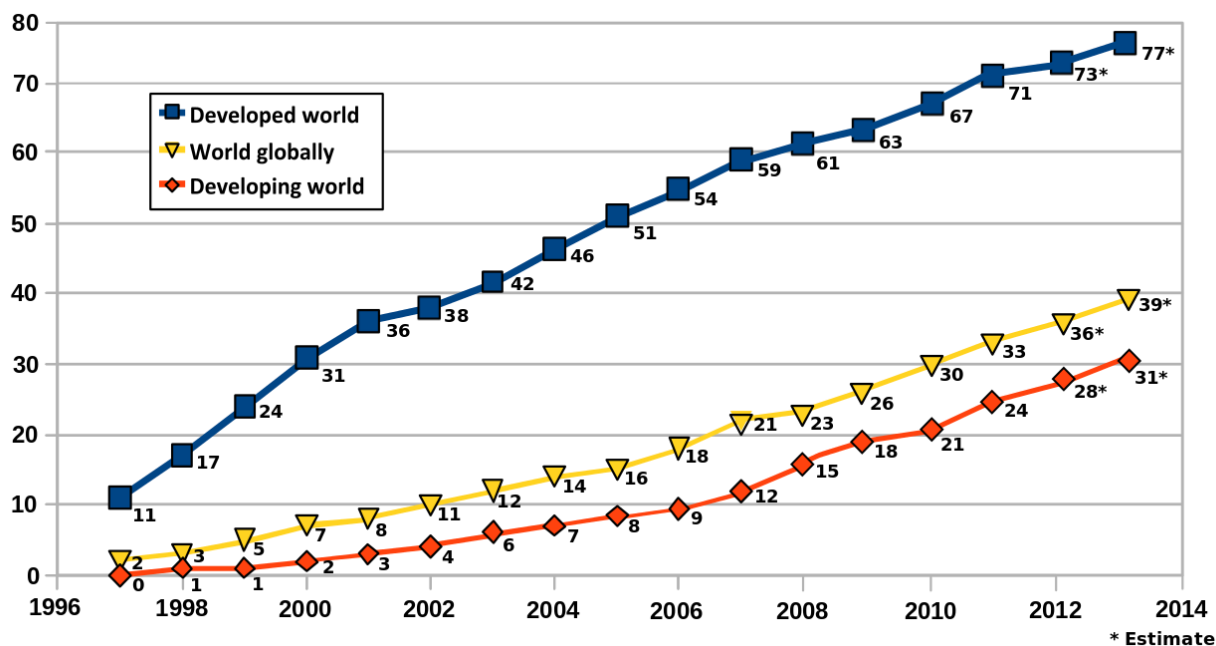


Рис. 1.3. Зростання кількості користувачів мережі Інтернет у світі.

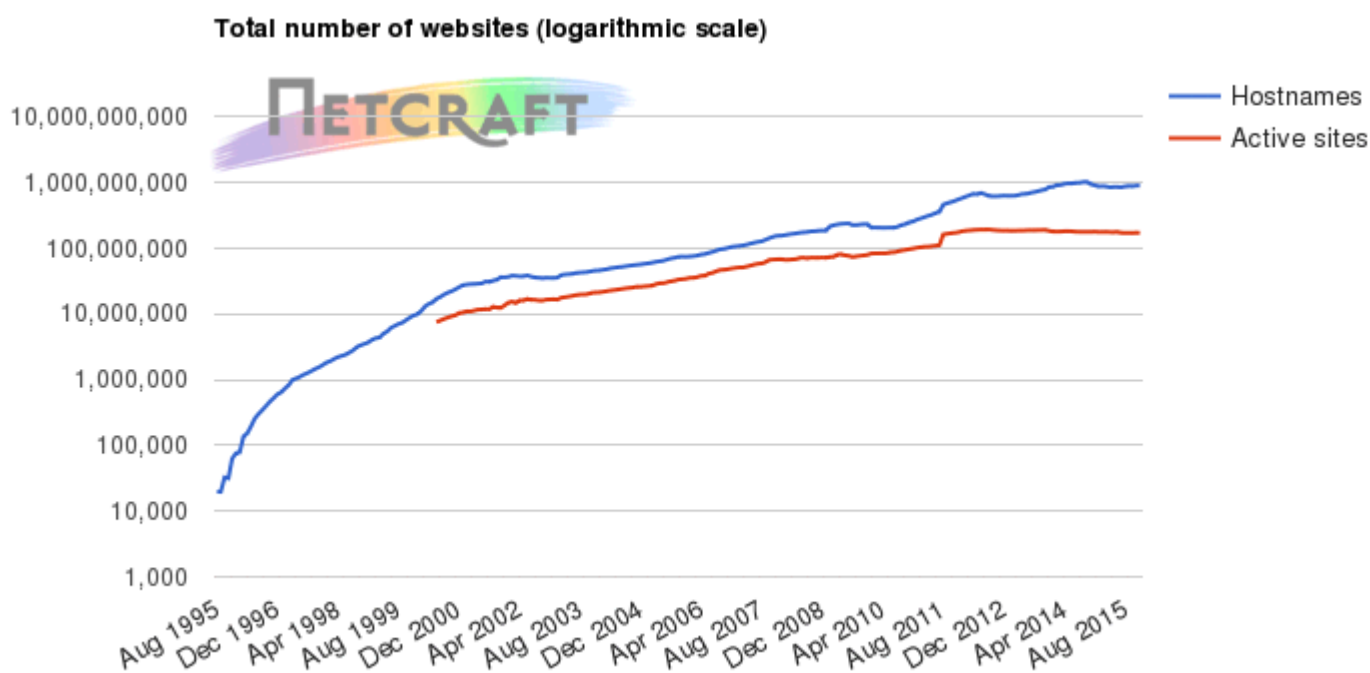


Рис.1.4. Зростання числа вузлів WWW в період 1994-2015 роки

Існують побоювання, що мережі може забракнути пропускної здатності для передавання постійно зростаючих обсягів інформації (тут є дві причини — ріст кількості користувачів і зростання відеонаповнення мережі), тому розробляються нові технології, які здатні будуть замінити “старий Інтернет”, розширити його функції або створити національні комп’ютерні мережі.

Заради справедливості необхідно відзначити, що мережа Інтернет є дуже великою інформаційною мережею, але не єдиною.

\* **Ще у 1980 році письменник** і політичний аналітик Алвін Тоффлер (Alvin Toffler) опублікував книгу "Третя хвиля" (The Third Wave), у якій описав постіндустріальний світ, в якому "першу скрипку" відіграють інформаційні технології. Тоффлер передбачив, зокрема, розвиток комп'ютерних мереж, які здатні будуть об'єднати весь світ, надавши людям набагато більше можливостей у ділянці телекомунікацій, ніж звичайні радіо і телебачення.

Існує два підходи до означення комп'ютерної мережі. Перший, більш теоретизований, належить міжнародній організації стандартів ISO: **комп'ютерною мережею називається послідовне біт орієнтоване передавання інформації між пов'язаними один з одним незалежними пристроями**. Другий підхід, що базується практичному використанні, має таке формулювання: **комп'ютерною мережею називається сукупність вузлів (ПК, робочі станції, майнфрейми, пристрої введення та виведення інформації), які взаємодіють між собою за допомогою апаратних засобів та спеціального програмного забезпечення**.

## 1.2 Класифікація мереж

Попередньо ми вже зробили перший крок до класифікації сучасних мереж, поділяючи їх за функціональним призначенням — обчислювальні, інформаційні та інформаційно-обчислювальні. Крім цього існує ще декілька критеріїв, серед яких найбільш важливими є такі:

- 1) розміри або протяжність мережі:
  - персональні PAN (Personal Area Network);
  - локальні LAN (Local Area Network);
  - міські MAN (Metropolitan Area Network);
  - кампусні CAN (Campus Area Network);
  - WAN (Wide Area Network);
  - глобальні GAN (Global Area Network).
- 2) спосіб взаємодії вузлів:
  - однорангові;
  - розподілені;
  - мережі з централізованим управлінням.
- 3) доступ до середовища передавання:
  - мережі з розподіленим середовищем передавання;
  - мережі з комутацією.

4) спільність операційних систем:

- гомогенні мережі;
- гетерогенні мережі.

5) пропускна здатність мережі:

- низька (до 10 Мбіт/с);
- середня (до 100 Мбіт/с);
- висока (більше 100 Мбіт/с).

Часто для визначення швидкості передавання даних в мережі використовують *бод*. **Baud (бод)** — одиниця швидкості передавання сигналу, яку вимірюють числом дискретних переходів або подій за секунду. Якщо кожна подія буде представлена одним бітом, то бод буде еквівалентним одному біт/сек (в реальних комунікаціях це виконується не завжди).

6) смуга пропускання каналу:

- вузькосмугові;
- широкосмугові.

Глобальні мережі зв'язують абонентів у межах країни, континенту чи всієї планети. Тут на першому плані організація засобів зв'язку. Основним видом зв'язку є супутниковий, радіорелейний або оптоволоконний. Приклади: міжнародна мережа авіакомпаній для замовлення квитків, інформаційна мережа Internet.

Міські мережі з'єднують абонентів у межах міста, області, групи закладів чи підприємств, інститутів та ін. Приклади: АСУ міста Львова (проекти), інформаційна мережа в межах міністерства (поки що нереалізований проект).

WAN (*wide Area Network*) – це глобальна мережа, яка покриває великі географічні регіони, включає в себе як локальні мережі, так і інші телекомунікаційні мережі і пристрої. Прикладом може слугувати мережа з комутацією пакетів (Frame relay), засобами котрої можуть з'єднуватись між собою різні комп'ютерні мережі.

Існує також термін "*корпоративна мережа*", який подібно до *кампусної* також використовується в літературі для позначення об'єднання кількох мереж, кожна з яких може бути побудована на різних технічних, програмних та інформаційних принципах.

У глобальній та міській мережах основні види робіт – інформаційні. Обчислювальні машини не об'єднують обчислювальні ресурси в динаміці, через мережу, а обмінюються файлами програм і даних.



Локальні обчислювальні мережі (ЛОМ), або локальні комп'ютерні мережі (ЛКМ), об'єднують ЕОМ, які розташовані на площах, обмежених одним навчальним закладом, підприємством або будівлею. Відстані малі, отже лінії з'єднання дешевші (у кілька разів від регіональних чи глобальних мереж). Тому можна досягти більших швидкостей передавання інформації, застосовуючи спеціальні лінії передач, наприклад, коаксіальні чи оптоволоконні кабелі. Для порівняння наведемо деякі цифри: швидкості передавання через телефонні лінії становлять 56-115 Кбіт/с, коаксіальних та оптоволоконних – 1-1000 Мбіт/с, тобто на 2-4 порядки більше. Такі швидкості співвимірні зі швидкодією каналів ЕОМ (портів ПЕОМ). Це дає змогу використовувати ЛКМ не тільки як інформаційну мережу, але й для об'єднання обчислювальних ресурсів (наприклад побудови кластерів). Майже всі ЛКМ є інформаційно-обчислювальними, а їх архітектура є одним з видів архітектури обчислювальної системи. Приклади: наша навчальна ЛКМ, локальні мережі банківських організацій, податкових служб.

*Персональна мережа*— це найменша за розміром мережа, яка обмежена зв'язком між пристроями, що знаходяться у безпосередній близькості до окремої особи або контролера пристрою (наприклад, в одній кімнаті, офісі або автомобілі). Такі мережі покликані об'єднувати усе персональне електронне обладнання користувача (телефони, КПК, ноутбуки, гарнітури і т. д.). Для зручності більшість персональних мереж бездротові (використовується абревіатура WPAN). Такими стандартизованими мережами в наш час є [Bluetooth](#), [ZigBee](#), [Piconet](#).

### **1.3. Організація передавання повідомлень у мережах. Методи передавання даних**

Є три основні типи організації багатоточкового зв'язку: комутація ліній, повідомлень та пакетів.

З *комутацією ліній* ми ознайомлені давно, це телефонний зв'язок, який відбувається за такою схемою:

 тел1  $\Leftrightarrow$  лінія  $\Leftrightarrow$  станція  $\Leftrightarrow$  група комутаційних блоків  
[  $\Leftrightarrow$  лінія  $\Leftrightarrow$  група комутаційних блоків  $\Leftrightarrow$  станція ]  $\Leftrightarrow$  лінія  $\Leftrightarrow$   
тел2 

У мережі попередньо встановлюється фізичне з'єднання між адресатами, яке називають каналом (у наведеному прикладі лінії зв'язку та комутаційні блоки станцій). При цьому задіяні для передавання ділянки каналів недоступні для передавання іншими користувачами. Використовують у випадках вимоги збереження часової послідовності передавання інформації, що є перевагою даного методу. Недолік — низький коефіцієнт корисної дії, високий рівень завад.

У методі *комутації повідомлень* інформація проходить шляхом запам'ятовування у проміжних вузлах комутації між пунктами відправлення та прийняття. Для цього створюються так звані віртуальні канали. Метод дає змогу збільшити пропускну здатність мережі та зменшити затримки у передаванні інформації.

*Комутація пакетів* передбачає постійний зв'язок абонентів. Лінії закріплені за мережею, а інформація передається певними порціями — пакетами\*. Під *пакетом* розуміємо блок даних фіксованої довжини, який має таку структуру:

Заголовок	Інформаційний блок	Контрольна сума
-----------	--------------------	-----------------

заголовок (службові поля, де зазначені адреси в мережі, пункт джерела пакета, пункт споживача, номер повідомлення та ін.);  
інформаційний блок;  
контрольна сума пакета.

Кожний пакет передається незалежно один від одного. У вузлах мережі, через які передається пакет, формується *повідомлення* — повний обсяг інформації, що передається за одне звертання до мережі, згідно з наведеним вище принципом. Для такого пересилання цей вузол буде джерелом. Пакети відправляють у мережу через найближчий вільний вузол у потрібному напрямку. Вони можуть проходити через кілька вузлів, а у вузлі призначення формується повідомлення і передається адресату.

\* Технологію, здатну розбивати файли на куски і передавати їх різними шляхами через мережу, запропонував у **1961 році** студент Массачусетського Технологічного Інституту (Massachusetts Institute of Technology) Леонард Клейнрок (Leonard Kleinrock).

#### **1.4 Теоретичні основи передачі даних. Перетворення Фур'є. Модуляція сигналу. Мультиплексування. Розділення середовища**

## 1.5. Мережа з маршрутизацією пакетів

Розглянемо деяку мережу з чотирма вузлами (див. рис.2). Частина з них з'єднана між собою каналами зв'язку. У вузлах розташовані абонентські системи, що складаються з ЕОМ (зовнішня пам'ять, периферія, термінали). Абонентські ЕОМ в таких мережах називаються "хост" (англ. host - господар).

Вузлова ЕОМ формує повідомлення, ділить його на пакети, перевіряє пакети, додає заголовок, відправляє по найменш завантажених маршрутах, тобто керує завантаженням комунікаційної підмережі.

У принципі комунікаційна підмережа може мати свою архітектуру, що не збігається з архітектурою "Хоста". Тому можливі перетворення даних. Щоб звільнити від цієї роботи „Хости“, в мережу вводять міні-ЕОМ, які виконують функції програмованого *адаптера* мережі. Вони, образно кажучи, одним боком повернуті до "Хоста", а іншим – до мережі, і навпаки.

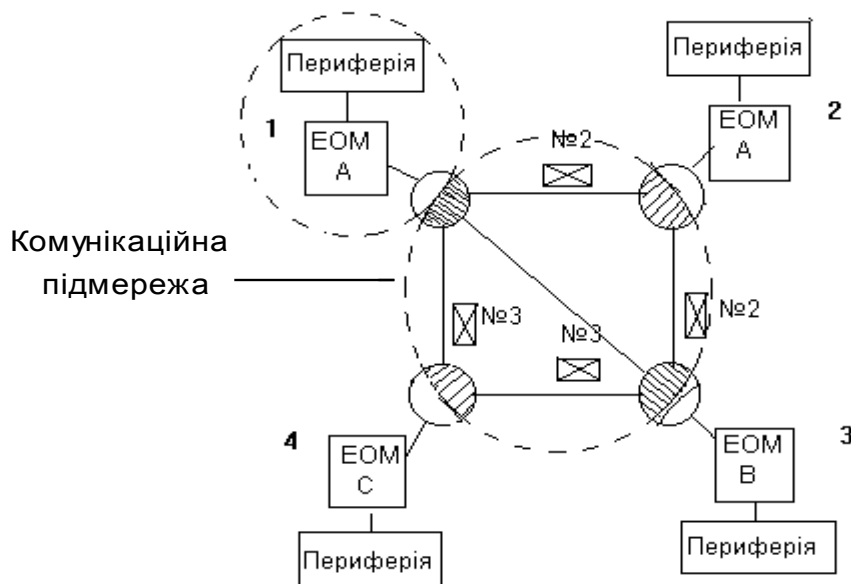


Рис.2. Мережа з маршрутизацією пакетів.

Розглянемо роботу такої мережі на прикладі. Нехай потрібно передати повідомлення з першого вузла в третій.



- 1) "Хост"А сформує чотири пакети і передасть у міні-ЕОМ першого вузла;
  - 2) міні-ЕОМ переведе пакети в структуру комунікаційної мережі і почне розсилати пакети;
  - 3) пакет №1 буде послано по діагональній ланці 1-3;
  - 4) поки перша міні-ЕОМ очікує підтвердження від третьої міні-ЕОМ, другий пакет направляється по ланці 1-2-3 у вузол №2;
  - 5) третій пакет відправляється по ланці 1-4-3 в третій вузол;
  - 6) надходить підтвердження про прибуття пакету №1.
- Лінія звільнилась, і по ній посилається пакет №4.  
Передача повідомлення закінчена.

Повідомлення, що передається окремими пакетами без їхнього сортування на приймальному вузлі за порядком посилянь, називається *данограмою*, або *дейтаграмою* (англ. datagram).

Після отримання підтвердження про правильність пересилання пакета №4 починається обробка повідомлення в третьому вузлі. Сортується пакет за номерами, міні-ЕОМ звільняє пакети від службової інформації, пов'язаної з пересиланням, перекодовує інформацію пакета зі структури комунікаційної мережі в структуру „Хосту”В, і пересилає в „Хост”В.

Так працює мережа з маршрутизацією пакетів. Її продуктивність визначається в основному максимальною пропускнуою здатністю ліній зв'язку та швидкодією міні-ЕОМ.

## **1.6. Мережа із селекцією пакетів**

Тепер ознайомимося з принципово іншою мережею: пакети розсилаються всім абонентам без винятку, а адресат відбирає адресований йому пакет (решту ігнорує). Така мережа називається мережею із *селекцією пакетів*.

На початку 70-х років була спроектована така експериментальна мережа на пропозицію професора Гавайського університету Нормана Абрамсона. Мережа отримала назву "Алоха", що в перекладі з гавайської означає любов, порозуміння. Центральною "ланкою" цієї мережі став геостаціонарний супутник зв'язку, який виконував функцію ретранслятора сигналів, а абонентами - університети на

Гавайських островах, Японії, США, Австралії. Абоненти були обладнані радіопередавачами та приймачами, антени яких напрямлені на супутник (7 комп'ютерів на 4-х островах).

Розглянемо принцип роботи такої мережі. Нехай перший абонент надіслав повідомлення четвертому абоненту. Воно потрапить до всіх абонентів, у тому числі й до першого (для контролю). Якщо в цей же час пошле повідомлення і другий абонент, то воно зіпсує повідомлення першого, але це побачить другий абонент і подасть своє повідомлення вдруге. Час затримання для повторного посилення вибирається згідно з законом випадкових чисел (переважно це від 3 до 30 тривалості повного посилення повідомлення). Отже, ймовірність неспотворення повідомлення залежить від навантаження в мережі. У мережі "Алоха" ситуація, коли повідомлення не проходить зовсім, виникало при 18% завантаження. Це можна поправити, ввівши синхронізацію. Така мережа досить дешева. Конус, утворений з вершиною-антеною, є ніби загальним каналом зв'язку, а засобами зв'язку — передавач, приймач і антена. Таке загальнопередавальне середовище називається *моноканалом*. Пізніше цей принцип передавання даних (протокол) було реалізовано у мережі Езернет.

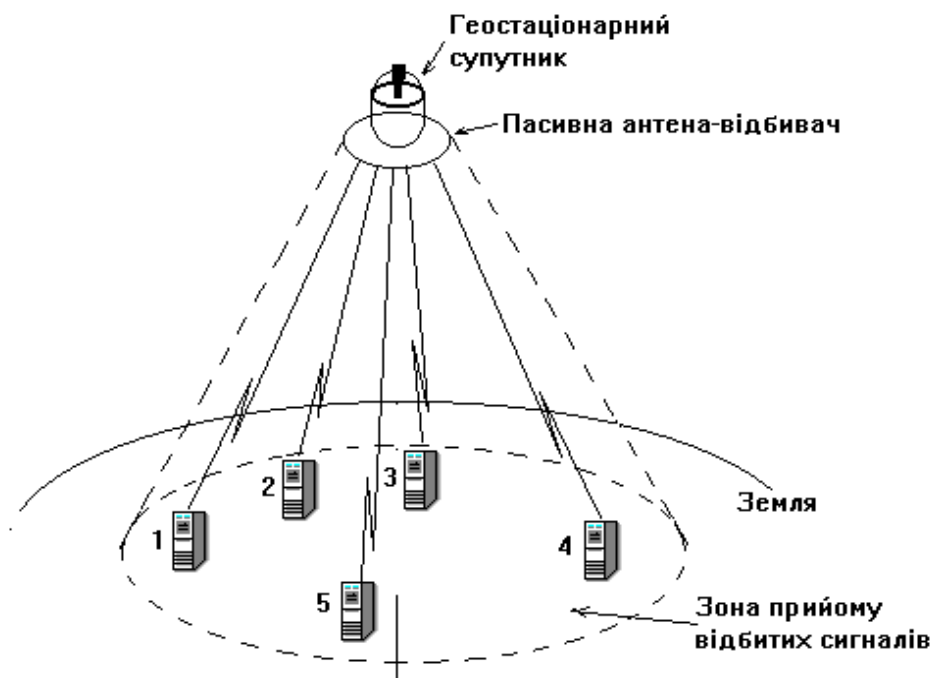


Рис.3. Мережа з селекцією пакетів.

Мережу, подібну до "Алохи" дуже зручно використовувати для роботи електронної пошти та нарад у мережі.

*Електронна пошта* (e-mail) - одна із головних функцій мережі, яка полягає у передаванні між абонентами будь-яких повідомлень, в тому числі текстів, графіків, мовограм. Передавання по e-mail ідуть із зазначенням адреси абонентів (селективний режим) або всім абонентам мережі (режим телеконференцій, циркулярних повідомлень). Обмін не пов'язаний з реальним масштабом часу. Подібно до організації передавання кореспонденції звичайною поштою, електронна пошта також оперує поняттям "поштова скринька" — певним чином організованою областю пам'яті комп'ютера.

**1971 рік.** Рей Томлісон (Ray Tomlison), програміст з комп'ютерної фірми Bolt Beranek and Newman, розробив систему електронної пошти і запропонував використовувати для розділення імені і назви домена значок @ (комерційне «і», або, вульгарно "собака").

Новини мережі Usenet (*телеконференції*) — це другий за розповсюдженістю сервіс Інтернет. Якщо електронна пошта передає повідомлення по принципу «від одного — одному», то новини мережі передають повідомлення «від одного — багатьом». Механізм передачі кожного повідомлення схожий на передачу пліток: кожен вузол мережі, який отримав якусь нову інформацію (тобто нове повідомлення), передає її на всі знайомі вузли, тобто всім тим вузлам, з якими обмінюється новинами. .

## **1.7. Стандарти інформаційно-обчислювальних мереж**

Було б добре, якби всі комп'ютери, які використовують у мережах, були однотипні, а засоби зв'язку (комунікації) "розуміли" кожного з них і могли порозумітися між собою. Але насправді це не зовсім так. Низка проблем надзвичайно утруднює процес передавання даних, а саме:

розподіл функцій між хостами і комунікаційними пристроями;

різні фізичні засоби передавання даних;

різні режими роботи хостів: пакетний, діалоговий, передавання файлів тощо;

потреби в об'єднанні мереж.

Усе це потребує введення певних стандартів на інформаційно-обчислювальні мережі. Що ж стандартизувати: архітектуру хостів, фізичні засоби зв'язку? Ні. А от процес

перетворення інформації від прикладного рівня до рівня передавання даних по інформаційних каналах, мабуть можна. Цим зайнялася в 1977 році Міжнародна організація стандартів (International Standards Organization, ISO).

Зрозуміло, що ввести загальний стандарт на всю зону взаємодії систем (під системою розуміємо обчислювальну машину, програмне забезпечення та штат операторів, здатний обробляти інформацію) важко. Тому цю зону розділяють на кілька ( $n$ ) рівнів. Еталонна модель взаємодії відкритих інформаційних систем визначає сім рівнів, кожен з яких є достатньо автономним і виконує одне чітке завдання. В стандарті відкритої мережі блоки даних фіксуються в тому вигляді, у якому вони представляються на певному  $n$ -ному рівні. **Сукупність правил і форматів, які визначають взаємодію об'єктів на  $n$ -рівні під час виконання ними всіх функцій цього рівня, називається  $n$ -протоколом.** Протоколи і є одним з головних об'єктів стандартизації.

Протоколи мають три складові: синтаксис, семантику і синхронізацію.

**Синтаксис** протоколу визначає розміри полів протокольних блоків (наприклад, 16-байтне поле для адресів, 32-бітне поле для контрольних сум, 512 байт для даних).

**Семантика** протоколу надає цим полям значення (наприклад, якщо адресне поле складається з усіх адрес, то це так званий "широкосмутовий" пакет).

Складова **синхронізація** визначає швидкість передавання даних у бітах за секунду. Це важливо як на нижніх, так і на верхніх рівнях протоколів.

## Модель OSI

Абонент-ська служба	7	Прикладний ( <b>A</b> pplication)	Форми взаємодії прикладних процесів (керування терміналом, файлами, завданнями, системою, е-пошта)
	6	Відображення ( <b>P</b> resentation)	Рівень відображення даних (шифрування, стискання, кодові перетворення)
	5	Сеансовий ( <b>S</b> ession)	Організація та проведення діалогу (дуплекс, напівдуплекс, синхронізація передавання даних)
Транспортна служба	4	Транспортний ( <b>T</b> ransport)	Надання наскрізних (прозорих) з'єднань (з контролем чи без)
	3	Мережний ( <b>N</b> etwork)	Прокладання з'єднань між системами (мережна маршрутизація, комутація)
	2	Канальний ( <b>D</b> ata <b>L</b> ink)	Передавання даних між суміжними системами (термінал і обладнання мережі)
	1	Фізичний ( <b>P</b> hysical)	Спряження систем з фізичними засобами з'єднань

Після публікації моделі взаємодії відкритих систем (OSI) Міжнародна організація стандартів розробила протоколи для семи рівнів цієї моделі. Як і під час розв'язування подібних інших задач такого масштабу, багато часу було витрачено на визначення й узгодження цих стандартів. Для прискорення цього процесу, а також для сприяння використанню протоколів OSI було схвалено також низку стандартів, розроблених Інститутом інженерів з електроніки і електротехніки (Institute of Electrical and Electronic Engineers, IEEE) та Міжнародним Консультативним Комітетом з телеграфного і телефонного зв'язку (Comite Consultatif Internationale de Telegraphique et Telephonique, CCITT).

Рівні Моделі OSI	
Дані	
Дані	<u>Прикладний</u> доступ до мережних служб
Дані	<u>Представлення</u> представлення і кодування даних
Дані	<u>Сеансовий</u> керування сеансом зв'язку
Блоки	<u>Транспортний</u> безпечне та надійне з'єднання «точка - точка»
Пакети	<u>Мережний</u> визначення маршруту та IP (логічна адресація)
Кадри	<u>Канальний</u> MAC та LLC (фізична адресація)
Біти	<u>Фізичний</u> кабель, сигнали, бінарна передача

## OSI-протоколи

Два нижні рівні — фізичний і канальний — стосуються стандартних типів ЛКМ, таких як CSMA/CD, Token Ring і Token Bus (про них мова піде пізніше). **Фізичний** рівень відповідає за тип фізичного середовища, тип передавання, метод кодування і швидкість передавання даних для різних типів мереж. Забезпечує як синхронну так і асинхронну (послідовну) роботу комп'ютерної мережі. [Є.Буров]. Для фізичного рівня визначений докладний список рекомендацій до вжитку з'єднань, напр.: 25-контактне роз'єднання для порту RS-232, 34-контактне роз'єднання для широкосмугового модема під протоколом V.35, коаксіальний кабель з хвильовим опором 50 Ом, скручена пара дротів для передавання даних на швидкості 10 Мбіт/с чи 100 Мбіт/с (екранована, неекранована), волоконно-оптичний кабель та ін.

Цифрова передача даних вимагає виконання кількох обов'язкових операцій:

- синхронізації тактової частоти передавача і приймача;
- перетворення послідовності бітів в електричний сигнал;
- зменшення частоти спектру електричного сигналу за допомогою фільтрів;

- передачі урізаного спектра по каналу зв'язку;
- посилення сигналу і відновлення його форми приймачем;
- перетворення аналогового сигналу в цифровий.

Розглянемо взаємозв'язок тактової частоти і бітової послідовності. Бітовий потік передається зі швидкістю, яка визначається числом біт в одиницю часу. Іншими словами біти в секунду - це число дискретних змін сигналу в одиницю часу. Тактова частота, вимірювана в герцах, це число синусоїдальних змін сигналу в одиницю часу.

Дана очевидна відповідність породила помилкове уявлення про адекватність значень герц і біт в секунду. На практиці все складніше. Швидкість передачі даних, як правило, вище тактової частоти. Для збільшення швидкості передачі сигнал може йти паралельно по декількох парах дротів. Дані можуть передаватися бітами або байтами. Кодований сигнал може мати два, три, п'ять і більше рівнів. Деякі методи кодування сигналів вимагають додаткового кодування даних або синхронізації, які зменшують швидкість передачі інформаційних сигналів. Для прикладу розглянемо код RZ.

**RZ** - це трирівневий код, що забезпечує повернення до нульового рівня після передачі кожного біта інформації. Його так і називають: кодування з поверненням до нуля (Return to Zero). Логічному нулю відповідає додатний імпульс, логічній одиниці - від'ємний (див.рисунок).

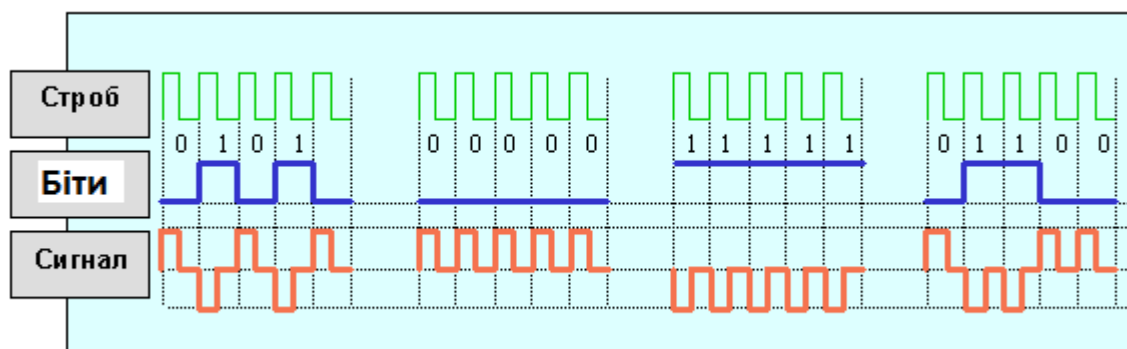


Рис.. Трирівневий код RZ

Інформаційний перехід здійснюється на початку біта, повернення до нульового рівня - в середині біта. Особливістю коду RZ є те, що в центрі біта завжди є перехід (позитивний або негативний). Отже, кожен біт позначений. Приймач може виділити синхроімпульс (той що стрибає), що має частоту проходження імпульсів, з самого сигналу. Прив'язка

проводиться до кожного біта, що забезпечує синхронізацію приймача з передавачем.

Недолік коду RZ полягає в тому, що він не дає виграшу в швидкості передачі даних. Для передачі зі швидкістю 10 Мбіт/с потрібно частота несучої 10 МГц. Крім того, для розрізнення трьох рівнів необхідно краще співвідношення сигнал / шум на вході приймача, ніж для дворівневих кодів.

Найчастіше код RZ використовується в оптоволоконних мережах. При передачі світла не існує позитивних і негативних сигналів, тому використовують три рівні потужності світлових імпульсів.

### **Код Манчестер-II**

Код Манчестер-II або манчестерський код набув найбільшого поширення в локальних мережах. Він також відноситься до самосинхронізованих кодів, але на відміну від коду RZ має не три, а тільки два рівні, що забезпечує кращу завадозахищеність.

Логічному нулю відповідає перехід на верхній рівень в центрі бітового інтервалу, логічній одиниці - перехід на нижній рівень. Логіка кодування добре видна на прикладі передачі послідовності одиниць і нулів. При передачі бітів, що чергуються, частота проходження імпульсів зменшується в два рази.

Інформаційні переходи в середині біта залишаються, а граничні (на межі бітових інтервалів) - при чергуванні одиниць і нулів відсутні. Це виконується за допомогою послідовності забороняючих імпульсів. Ці імпульси синхронізуються з інформаційними та забезпечують заборону небажаних граничних переходів.

Зміна сигналу в центрі кожного біта дозволяє легко виділити синхросигнал. Самосинхронізація дає можливість передачі великих пакетів інформації без втрат через відмінності тактової частоти передавача і приймача.



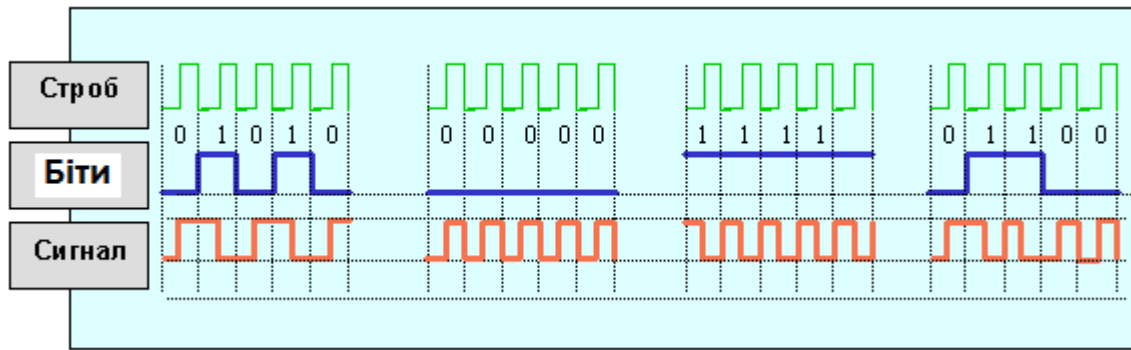


Рис.. Дворівневий код Манчестер-II

Велика перевага манчестерського коду - відсутність постійної складової при передачі довгої послідовності одиниць нулів. Завдяки цьому гальванічна розв'язка сигналів виконується найпростішими способами, наприклад, за допомогою імпульсних трансформаторів.

Частотний спектр сигналу при манчестерському кодуванні включає тільки дві несучі частоти. Для десятимегабітного протоколу - це 10 МГц при передачі сигналу, що складається з одних нулів або одних одиниць, і 5 МГц - для сигналу з чергуванням нулів і одиниць. Тому за допомогою смугових фільтрів можна легко відфільтрувати всі інші частоти.

Код Манчестер-II знайшов застосування в оптоволоконних і електропровідних мережах. Найпоширеніший протокол локальних мереж Ethernet 10 Мбіт/с використовує саме цей код.

Рівень 2 — **канальний** — складається з двох підрівнів. Нижній з них — керування засобами доступу (Media Access Control, MAC) — є частиною фізичного стандарту мережі. Специфіковані різні варіанти з такими стандартами як 802.3, 802.4 і 802.5. Вища секція рівня 2 — керування логічним зв'язком (Logical Link Control, LLC) — охоплюється стандартом IEEE 802.2. Фактично LLC було розроблено для забезпечення багатократного зв'язку між багатьма станціями ("багато з багатьма") в єдиній фізичній мережі. Ця частина стандарту стосується програмного забезпечення, хоча розміщена, як звичайно, в апаратній частині (наприклад, програми в мікросхемах (МС) постійної пам'яті (ROM) на АКМ-картах). Є два суттєво різних класи LLC.

Клас I є формою комунікації без попереднього налагодження логічного зв'язку. При ньому не налагоджується попередній логічний зв'язок (handshaking), немає підтверджень про прийом блоків даних, управління потоку та

корекції помилок. Протокольні блоки даних канального рівня називають кадрами (frames). До сервісів на канальному рівні відносять різні види індикації, запити та відповіді про уведенні/виведення інформації.

Клас II здійснює протоколо-залежну комунікацію. Перед передаванням даних встановлюється логічний зв'язок між блоками керування логічним зв'язком. Цей логічний зв'язок забезпечує керування потоком даних та корекцію помилок. Через порівняно низький рівень помилок локальні мережі використовують, як звичайно клас I LLC. Клас II суттєво знижує ефективну пропускну здатність мережі внаслідок перевантаження її керуванням, підтвердженнями та корекцією помилок. Керування зв'язком переноситься в першому випадку на транспортний рівень (рівень 4) моделі OSI.

Для організації передавання даних у глобальних мережах на канальному рівні застосовують протокол HDLC (Higt-level Data Link Control), який забезпечує функціонування двоточнової системи.

Наступні два рівні — мережний і транспортний — також мають як безконтактні, так і контактні-орієнтовані протоколи. Загалом ці дві форми комунікації можна визначити так:

безконтактний протокол дає змогу передавати через мережу блоки даних (данограми). Попереднього контакту між передавальним та приймальним пристроями нема. Данограми можуть надходити у будь-якому порядку або навіть бути втраченими — безконтактного протоколу це не стосується;

контактно-залежний протокол потребує, щоб до початку передавання даних був налагоджений логічний зв'язок між передавальним та приймальним пристроями. Після цього послідовно передають дані. Про помилки сповіщається перед тим, як почне передаватися наступний блок даних.

Третій рівень — **мережний** — у локальних мережах як звичайно ґрунтується на контактній-незалежній протоколі керування мережею без налагодження логічного зв'язку (Connection Less Network Service, CLNS). Це не що інше, як мережна маршрутизація, тобто сполучення кількох станцій з проміжними вузлами опрацювання даних або локальної мережі з іншою мережею для передавання блоків даних, тобто пакетів. Перевага його є в тому, що завдяки низькому рівню

помилки у локальних мережах не виникає перевантаження мережі, пов'язаного з налагодженням зв'язку та керування даними. У помилкових ситуаціях немає потреби у відновленні зв'язку, отже спрощується рестарт, зберігається час і збільшується пропускна здатність. Історично перші протоколи були розроблені для глобальних мереж, які є багатовузловими і ефективна маршрутизація є головною проблемою у їхній роботі. Розрізняють дві стратегії передавання пакетів: данограмну та віртуальних каналів. [Є.Буров]. Типові протоколи цього рівня – X.25/3 і IP (Internet Protocol).

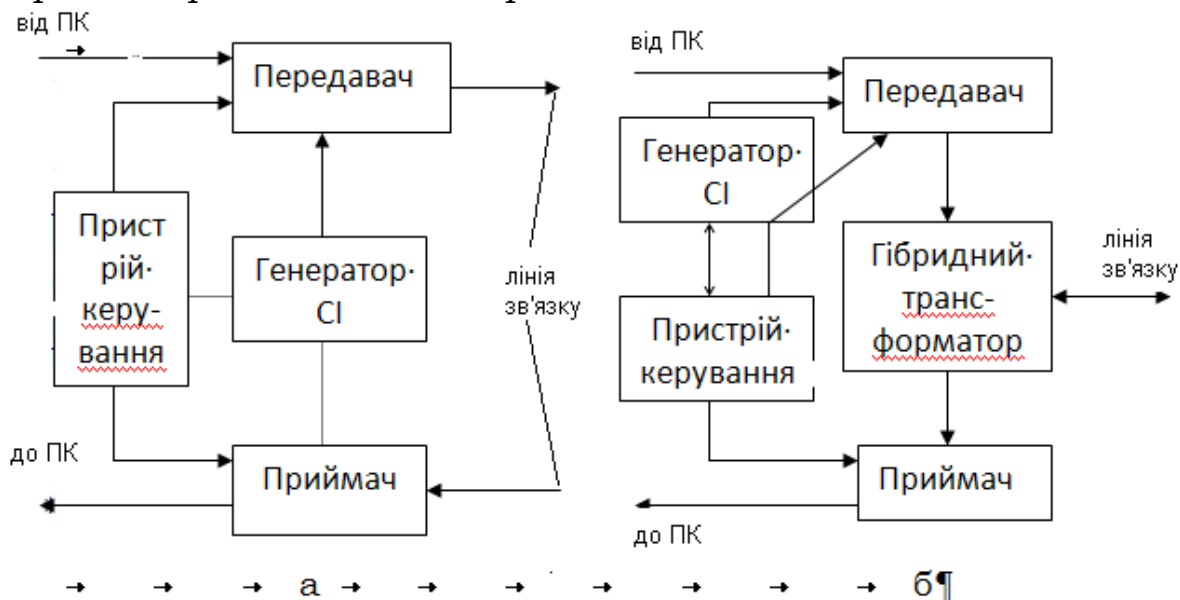
Четвертий рівень — **транспортний** — у локальних мережах реалізований, як звичайно, на контактнорієнтованому протоколі, який називається транспортним протоколом 4 (Transport Protocol 4, TP4). Він використовує всі можливості CLNS і просто порівнює дані під час їх отримання, упорядковує данограми, перевіряє їх на наявність помилок та, якщо потрібно, посиляє запити на повторне передавання (ретрансмісію). У випадку використання цього методу зв'язком керують комп'ютери, які посиляють чи отримують інформацію, але жодної службової інформації, призначеної для керування контактом (зв'язком), через мережу не передається, за винятком запитів на ретрансмісію, якщо є помилки, мінімізуючи таким чином завантаження мережі. Подібний до нього протокол TCP, про що скажемо пізніше.

Транспортний рівень має 5 класів сервісу:

- 0 – для використання у найкращих системах, налагоджує транспортні сполучення і керує ними (без перевірки передавання даних, відсутнє мультиплексування та виправлення помилок);
- 1 – крім функцій 0-го класу включає контроль за передаванням інформації, виявлення та виправлення помилок;
- 2 – властивості класу 0 і здійснення мультиплексування;
- 3 – 1 клас + 2 клас;
- 4 – властивості всіх попередніх класів + данограмний режим роботи.

**Сеансовий рівень** (п'ятий) та рівень відображення даних (шостий) мають визначені контактнорієнтовані протоколи. Ці протоколи розроблені швидше як інтерфейс між прикладними програмами, ніж як компоненти мережі. Тому їхня реалізація більше залежить від того, як використовують мережу, ніж як вона функціонує. Прикладами цих рівнів у до-

OSI операційному середовищі є Telnet та Netbios. Сеансовий рівень відповідає за режим передавання та встановлення точок синхронізації (точки всередині діалогу). (С.Шатт: діалог двох японських бізнесменів – “хай – хай”). Типові діалоги – дуплекс та напівдуплекс (див. Рис.). На цьому рівні вирішують питання про відновлення чи не відновлення зв'язку після його втрати та режим його завершення.



Схеми реалізації дуплексного (а) та напівдуплексного (б) зв'язку.

Рівень **відображення** даних відповідає за фізичне відображення інформації, зокрема шифрування даних. Наявність протоколів цього рівня є характерне для мереж з не однотипними комп'ютерами. Типові протоколи – XML, частково FTP.

Сьомий рівень — **прикладний**. Це рівень, де відбуваються основні міжмережні зв'язки користувача. Сьомий рівень моделі OSI має дуже багато стандартів, зокрема: X.400 (електронна пошта), X.500 (служба керування директоріями), віртуальний термінал та служба передавання файлів, доступу до файлів та керування файлами (File Transfer, Access and Management, FTAM). Вони є основними складовими, що дають змогу різним прикладним програмам співпрацювати між собою без будь-якого узгодження чи перепрограмування.

Основними спробами реалізації OSI до цього часу були MAP, TOP та GOSIP.

MAP — протокол автоматизації виробництва (Manufacturing Automation Protocol) — розробила компанія General Motors у 1983р. Спочатку це була спроба об'єднати в мультимережу електронне обладнання виробничих приміщень. Однак випуск у 1987р. MAP 3.0 забезпечив широкий набір протоколів для комерційної реалізації. Очікують, що він стане базою майбутнього розвитку стандартів для комунікації між автоматизованими засобами виробництва.

Набір стандартів з визначень OSI вибрали як найбільш вдалий для потреб автоматизації виробництва. Він містив кільцеву локальну мережу Token Bus (802.4) і доданий до набору OSI протокол прикладного рівня, що називається "Стандарт формату виробничих повідомлень" (Manufacturing Message Format Standard, MMFS).

TOP — технічний та офісний протокол (Technical and Office Protocols), подібний до MAP. Запропонований компанією Boeing Computer Services. Дотримується стандарту OSI і пов'язаний з обміном діловими документами та графікою у пакеті форматів міжнародних стандартів. Обидва протоколи, MAP і TOP мають подібне призначення, але для різних середовищ. Можливо, що обидві ці ідеї зіллються і утворять єдиний набір стандартів для обміну діловою інформацією.

GOSIP — державний опис відкритих інформаційних систем (Government Open Systems Information Profile). Започаткований урядом Великобританії і визначав низку стандартів та описів OSI, що їх повинні були наслідувати всі розробники та постачальники систем для державного сектора. Зараз GOSIP схвалений багатьма державами світу. Кожен уряд визначає свої власні конкретні вимоги в рамках моделі OSI, хоч різні національні описи GOSIP починають зливатися.

Протоколи ISO найчисельніші і всеохоплюючі, їх відомо близько 50. Ось деякі з них:

646 - функціонування процесів системи OSI в семибітному коді для інформаційного взаємообміну;

8802 - система обробки інформації в ЛКМ з мультистанційним доступом з виявленням зіткнень. Канальний протокол;

8802-3=IEEE802.3 (описаний далі в тексті);

8802-4=IEEE802.4 (описаний далі в тексті);

8802-5=IEEE802.5 (описаний далі в тексті);

8881 - система обробки інформації для обміну даних DC (data communication) під протоколом пакетного рівня X.25 в ЛКМ.

9040,41 - система обробки інформації OSI для обслуговування віртуальних терміналів.

Тепер варто ознайомитися з протоколами інших, уже згадуваних вище організацій.

### **Приклади протоколів Міжнародного Консультаційного Комітету з телеграфу і телефону ССІТТ**

(з 1995 року цей комітет офіційно називається **ITU-T** - ([англ.](#) *International Telecommunication Union - Telecommunication sector*) сектор стандартизації електрозв'язку Міжнародного союзу електрозв'язку.):

X.21 — інтерфейс загального призначення між DTE (обладнання кінцевої станції (терміналу)) і DCE (аппаратура передавання даних або обладнання мережі) для синхронізації операцій під час передавання даних у мережі;

X.25 — один з найпопулярніших протоколів, який забезпечує інтерфейс між DTE та DCE для керування терміналами в пакетному режимі передавання даних у мережі. Згідно з наведеною вище моделлю це протокол третього рівня, причому створений ще у 1976р. до опублікування стандарту відкритої мережі, дуже добре з ним узгоджений і структурно перекриває протоколи трьох нижніх рівнів;

X.400 — служба специфікацій для зв'язку пристроїв у режимі передавання повідомлень з проміжним зберіганням (a store and forward). Типовий протокол сьомого рівня. Використовується для робочих станцій e-mail;

X.500 — служба директорій для зв'язку пристроїв, що працюють у режимі передавання повідомлень з проміжним зберіганням.

**Протоколи IEEE** (Інститут інженерів з електротехніки та електроніки):

IEEE802.1 — Керування мережею. Цей стандарт відповідає моделі OSI;

IEEE802.2 — Керування логічними з'днаннями;

IEEE802.3 — відомий як Ethernet (Езернет)-протокол керування передаванням даних у мережі з мультистанційним доступом з виявленням колізій (зіткнень) типу CSMA/CD. Цей тип протоколу працює в мережі, що використовує baseband communication (пряма немодульована передача даних) зі швидкістю 10 Мбіт/с за допомогою коаксіального кабелю з деревоподібною шинною структурою. Подібні перетворення для мережі Apple Talk називаються CSMA/CA ( CA — уникнення колізій ).

IEEE802.4 — маркерна шина (Token Bus). Цей протокол поєднує шинну структуру Ethernet-подібних мереж з системою передавання маркера в естафетних кільцевих мережах (token ring).

IEEE802.5 — маркерне кільце (Token Ring). Функціонування TR ґрунтується на ідеї закритої петлі. Стандартно специфікації стосуються виті пари зі швидкістю передавання даних 4 Мбіт/с.

IEEE802.6 – див. [DQDB](#), відповідає [ISO8802/6](#)

IEEE802.7 – широкосмстові мережі (технології)

IEEE802.8 – оптоволоконні мережі

IEEE802.9 - s. [IVDLAN](#) (Integrated Voice Data [LAN](#) , 4MBit/s)

IEEE802.11 - [MAC](#) i [PHY](#)-Protokoll, 2MBit/s, 2,4GHz ([WLAN](#))

IEEE802.11a - [PHY](#)-Protokoll, 54MBit/s, 5,2GHz , [OFDM](#) ([WLAN](#))

IEEE802.11b - [PHY](#)-Protokoll, 11MBit/s, 2,4GHz ([WLAN](#))

IEEE802.11e - [QoS](#) для [WLANs](#)

IEEE802.11f - [IAPP](#)-Protokoll f. [Roaming](#) in [WLANs](#)

IEEE802.11g - [PHY](#)-Protokoll , 54MBit/s, 2,4GHz,[OFDM](#) ([WLAN](#))

IEEE802.11h - [PHY](#)-Protokoll, 54MBit/s, 2,4GHz або 5,2GHz з регулюванням потужності сигналу ([WLAN](#))

IEEE802.11i - [WLAN](#)- протокол з використанням шифрування.

IEEE802.12 - відповідає [100BaseVG](#), стандарт 100 Мбіт/с [Ethernet](#) для передачі через чотири пари проводів



категорії 3 UTP (відомих як голосовий клас ([англ.](#) *voice grade*), звідси і "VG"). Він також відомий, як 100VG-AnyLAN

Ще задовго до прийняття стандартної моделі взаємодії відкритих систем робота в комп'ютерних мережах регламентувалася в основному протоколом TCP/IP. Протокол керування передаванням/міжмережний протокол (Transmission Control Protocol/Internet Protocol, TCP/IP) і сьогодні є складовою набору протоколів Internet (Internet Protocol Suite), програмного забезпечення, що функціонує в мережі для забезпечення комунікації.

Протокол TCP/IP виник з розробок та з експериментів з пакетним радіозв'язком, які проводила у 70-х роках агенція передових досліджень міністерства оборони Америки (ARPA, який на кілька років випередив стандарт OSI, хоча і використовував багаторівневу структуру, подібну до моделі OSI. Коли комерційні організації почали розробляти мережі, вони наштовхнулися на ті ж проблеми, що й розробники ARPANET. Проте для них уже були готові вирішення проблеми, оскільки протоколи TCP/IP були повністю протестовані. Використанню TCP/IP сприяло включення його в контракти американського уряду, а також прийняття його операційною системою UNIX для зв'язку між робочими станціями.

TCP/IP не є сумісним з OSI, він діє паралельно з моделлю OSI. Технічно він складається з двох протоколів (TCP та IP), а назва TCP/IP використовується для позначення загальної назви набору протоколів та утиліт. Протокол Internet (IP) подібний до мережного протоколу без налагодження логічного зв'язку стандарту ISO (ConnectionLess Network Service, CLNS), (ISO 8473). Протокол керування передаванням (TCP) подібний до четвертого класу транспортного рівня стандарту ISO (Transport Layer Class 4, ISO 8073). TCP забезпечує протоколо-залежну службу передавання для прикладних програм з корекцією помилок. Він перевіряє в основному всі дані, що IP передає мережі, змінює порядок даних, шукає помилки, а також дає запит на повторне передавання пошкоджених або втрачених даних.

Перевагою TCP/IP є його історичний статус як стандарту де-факто для операцій у мережах. Тому він забезпечує більшу гнучкість для об'єднання мереж (мультимережі) і сумісність, ніж будь-який інший не сумісний з стандартом ISO протокол.



Недоліком є те, що він не відповідає моделі взаємодії відкритих систем OSI і був початково створений для роботи в глобальних мережах (ГКМ) (Wide Area Network), а не в ЛКМ. ГКМ мають, як звичайно, значно вищий рівень помилок, ніж ЛКМ внаслідок нижчої якості з'єднань у мережі. Тому TCP/IP витрачає багато часу на перевірки, що знижує продуктивність, хоча в останніх версіях цей недолік суттєво зменшений.

Давно очікували, що TCP/IP буде витіснитися OSI, але, як показала практика, його застосовують і, очевидно, ще будуть застосовувати тривалий час, і всі мережі повинні мати міжмережний інтерфейс (шлюз, gateway) для приєднання до існуючих мереж, що застосовують TCP/IP.

Головною причиною широкого його використання було і є те, що TCP/IP містить низку прикладних протоколів *вищого* рівня, або утиліт, що їх стали широко використовувати розробники мереж. Наведені нижче три з них є невеликим набором з усіх доступних, які, мабуть, використовуються найширше.

TELNET – протокол, який забезпечує інтерфейс віртуального ASCII терміналу. Для терміналу він дає змогу приєднуватися до віддаленої головної машини (host) з іншої машини або з термінал-сервера. Для host-машини він емулює безпосередньо приєднаний термінал. TELNET може працювати у двох режимах: командному та введення рядка. Якщо набрано команду TELNET без аргументів, то це означає командний режим. Якщо ж набрати команду TELNET з аргументами, то виконується підкоманда *open* з цими аргументами, і відбувається перехід до режиму введення рядка.

Протокол передавання файлів File Transfer Protocol (FTP) дає змогу передавати файли як у кодах американського стандарту для обміну інформацією (American Standard Code for Information Interchange, ASCII), так і у формі образів (IMAGE form). Слід зауважити, що ASCII визначає стандартний набір кодів для зображення літеро-цифрових символів.

Файл можна передати з машини, що використовує розширений двійково-десятковий код для обміну інформацією (Extended Binary Coded Decimal Interchange Code, EBCDIC) машині, що працює у стандарті ASCII, і навпаки. IMAGE-

формат є більш машинно-залежним форматом, тому при передаванні перетворень не відбувається; таким чином, використання IMAGE-файлів залежить від того, чи обидві машини використовують сумісні формати файлів. (Не слід плутати IMAGE- формат і двійковий (BINARY) - це різні формати).

До протоколів *середнього* рівня крім TCP/IP чи Netbios відносять також протоколи SPX/IPX, які фірма Novell застосовує для організації обміну данограмами (IPX) та для обміну в сеансах (SPX).

Протокол IPX (Internetwork Packet Exchange – Міжмережний обмін пакетами) відповідає мережному рівню моделі OSI і виконує функції адресації, маршрутизації та переключення у процесі передавання пакетів повідомлень. Саме цей протокол використовує ОС NetWare при обміні службовими повідомленнями з файл-сервером. Відсутня гарантія доставки повідомлень.

Протокол SPX (Sequenced Packet Exchange – Послідовний обмін пакетами) працює на мережному рівні і має деякі функції сеансового рівня. Для обміну пакетами попередньо потрібно встановити логічний зв'язок між учасниками діалогу. Гарантує правильну доставку пакетів, тому використовується для доступу до внутрішніх функцій управління та діагностики мережі.

Крім цих дуже часто використовуються протоколи SMTP та SNMP.

Простий протокол передавання електронної пошти (Simple Mail Transfer Protocol, SMTP) дозволяє передавати "з рук в руки" електронну пошту через мережу. Текст повідомлення готується за допомогою звичайного текстового редактора. Передавання здійснюється за допомогою команди UNIX *sendmail*.

Простий протокол керування мережею (Simple Network Management Protocol, SNMP) є стандартним набором правил, який дозволяє з одного пристрою керувати іншими пристроями, що підтримують цей протокол.

Відповідність інших протоколів рівням моделі OSI (не завжди повна) подана у наступній таблиці.

Рівень	OSI Протоколи
Прикладний	HTTP, gopher, Telnet, DNS, SMTP, SNMP, CMIP, FTP, TFTP, SSH, IRC, AIM, NFS, NNTP, NTP, SNTP, XMPP, FTAM, APPC, X.400, X.500, AFP, LDAP, SIP, IETF, RTP, RTCP, ITMS, ModbusTCP, BACnet IP, IMAP, POP3, SMB, MFTP, BitTorrent, e2k, PROFIBUS
Відображення	ASN.1, XML, TDI, XDR, NCP, AFP, ASCII, Unicode
Сеансовий	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone Information Protocol, SSL, TLS, SOCKS, PPTP
Транспортний	TCP, UDP, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP, STP, TFTP
Мережний	IPv4, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPsec, ARP, SKIP
Канальний	ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token Ring, PPP, PPPoE, StarLan, WiFi, PPTP, L2F, L2TP, PROFIBUS
Фізичний	RS-232, RS-422, RS-423, RS-449, RS-485, ITU-T, RJ-11, T-carrier (T1, E1), модифікації стандарту Ethernet: 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-TX, 1000BASE-SX



### 2.1. Основні поняття. Топологія мереж

Усе, про що йшлося вище, крім деяких протоколів, стосувалося глобальних та регіональних мереж, які свого часу виникли як обчислювальні, потім переродились в інформаційно-обчислювальні. Це пов'язано з тим, що затримки в лініях передавання регіональних та глобальних мереж роблять нераціональним об'єднання їх для використання обчислювальних ресурсів.

А от локальні мережі набули і продовжують набувати що раз більшого поширення. Що ж ми розуміємо під локальною мережею? Переважно *локальною мережею* називається деяка кількість незалежних комп'ютерів, з'єднаних між собою комунікаційним обладнанням. У цьому випадку прикладне програмне забезпечення, що працює на цих комп'ютерах, повинно мати достатньо надійні, прості та швидкодіючі засоби передавання даних через наявне комунікаційне обладнання.

Комп'ютери такої мережі переважно розташовані на невеликих відстанях (приблизно до 1 км), часто в межах однієї будівлі чи установи, що, власне, і забезпечує "локальність" мережі.

З чого складається ЛКМ? По-перше, — комп'ютер, по-друге, — комунікаційне обладнання. Сюди відносять спеціалізовані *адаптери* мережі, які вставляють у вільні *слоти* (розняття всередині ПК). Це не що інше, як блоки доступу окремого комп'ютера до фізичного середовища передавання даних. Варто зазначити, що об'єднанню підлягають тільки однотипні адаптери.

По-третє, — це лінії зв'язку та розняття, що часто називають *інтерфейсом*. І, безумовно, програмне забезпечення.

Це все стосується апаратної частини мережі. А тепер розглянемо мережу з погляду її використання. Традиційно ЛКМ розвивалися як засіб розподілу дорогих ресурсів та як засіб керування складними процесами, які відбуваються в режимі реального часу. Основні ресурси, що підлягають розподілу, це дискова пам'ять та друкарські пристрої. Зрозуміло, що основне навантаження в мережі

зосереджується на тих комп'ютерах, які виділяють у мережу свої ресурси. Тому комп'ютери поділяють на ті, що виділяють свої ресурси в мережу (*сервери*), і ті що споживають їх (*робочі станції*).

Слід зауважити, що в літературі трапляється і трохи інше визначення терміна *станція*, — а саме – міжпроцесорний пристрій, що стикує абонента з комунікаційною підмережею. Згідно з моделлю ISO така станція повинна виконувати функції значної частини нижніх рівнів, аж до транспортного. Якщо така станція реалізує функції фізичного і канального рівнів, то вона називається *канальною станцією*, або *контролером*. Станції, що беруть на себе функції мережного чи транспортного рівнів, називають відповідно *мережними* і *транспортними*. Це можуть бути спеціалізовані процесори або потужні комп'ютерні системи.

Окрім розподілу ресурсів у ЛКМ є важливим розподіл навантаження та розподілене опрацювання даних. До головних функцій локальної мережі відносять:

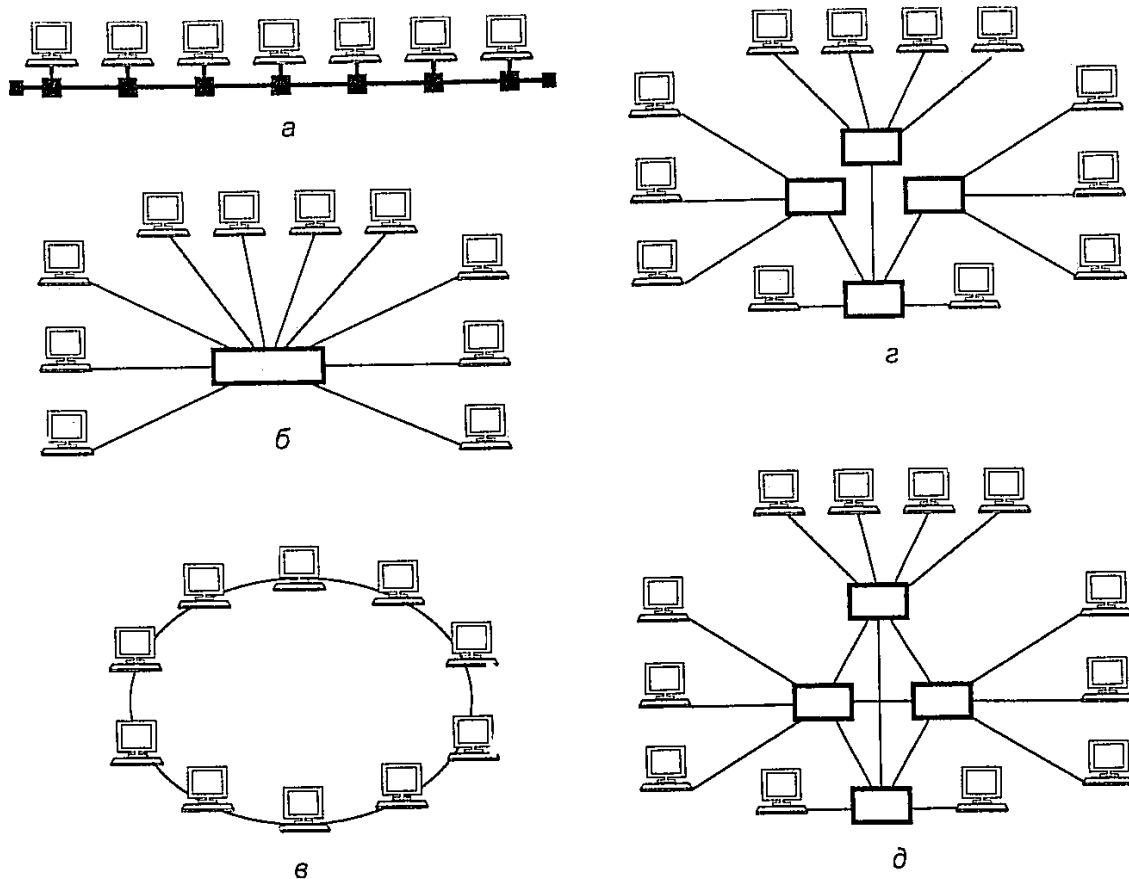
1. розподілене використання файлів, тобто багато користувачів отримують доступ до одного файла;
2. передавання файлів (швидке копіювання файлів довільних розмірів без застосування дискретних носіїв інформації);
3. багато станційний доступ до інформації та файлів (включаючи запуск прикладних програм з будь-якої станції);
4. розподілене використання прикладних програм;
5. одночасне введення даних у прикладні програми (напр., записи у бухгалтерські книги). Ця функція працює тільки з спеціальними програмами;
6. розподілене використання принтера;
7. передавання службових повідомлень у текстовому форматі (електронна пошта).

Про обладнання, функції та математичне забезпечення сервера чи файл-сервера йтиметься згодом. А зараз кілька слів про те, як можуть комп'ютери з'єднуватись у мережі, тобто яка *топология* локальних мереж?

В основному мережеву топологію (від грец. Τόπος, - місце) - розглядають як спосіб опису конфігурації мережі, схему розташування з'єднань мережевих пристроїв. Проте, мережева топологія може бути:

- *фізичною* - описує реальне розташування і зв'язки між вузлами мережі.
- *логічною* - описує проходження сигналу в рамках фізичної топології.
- *інформаційною* - описує напрямки потоків інформації, переданих по мережі.
- *управління обміном* - це принцип передачі права на користування мережею.

ЛКМ будують з комунікаційною підмережею, яка має ідеологію *моноканалу*. Така підмережа може мати різні топології: зірка, кільце, шина, деревоподібна, та змішана.



а) шина; б) зірка; в) кільце; г) деревоподібна; д) змішана.

1. *Зірка*. Приклад: мережа "Алоха"(С.10-11) а також окремі ділянки мережі Fast Ethernet. Типове розташування абонентів мережі показано на рис.4.

Переваги: зручне розташування центрального пристрою контролю за станом мережі та збору статистики.

Недоліки: велика протяжність і кількість ліній зв'язку. (Крім супутникового зв'язку).



Рис.4. Мережа зіркоподібного типу.

## 2.Кільце (циклічна мережа)



Рис.5. Мережа кільцевого типу, або однорангова кільцева топологія.

Для того, щоб робота кільцевого моноканалу була засинхронізована, в адаптери або в кабелі включають лінії затримки і все кільце стає ніби динамічною пам'яттю на лініях затримки. Довжина кабелю, на якому розташовується блок даних фіксованої довжини, називається *сегментом*. Кількість сегментів повинна бути завжди цілою! Якщо такого узгодження нема, то монітор (сервер) вставляє в спеціальний регульовальний сегмент або знімає з нього деяку кількість нулів.

У кожному сегменті розташовується кадр інформації - ніби скринька, в яку закладається міні-пакет. Отже, в кільці з постійною швидкістю циркулює певна, постійна кількість "скриньок" (подібно до чортового колеса, чи підйомника в горах).

Структура кадру така, що в "голові" відмічено, чи є в ньому міні-пакет (повний він чи порожній), а в "хвості" — місце для відмітки адресата про отримання міні-пакета. В міні-пакеті зазначають номери станцій адресата і відправника. Коли повз станцію з блоком доступу проходить "порожній" кадр, вона може вкласти в нього міні-пакет, змінивши відповідну ознаку на "новий". Коли кадр проходить повз станцію отримувача, то вона списує вміст міні-пакета і в кінці кадру ставить відмітку про те, прийняла вона пакет чи ні.

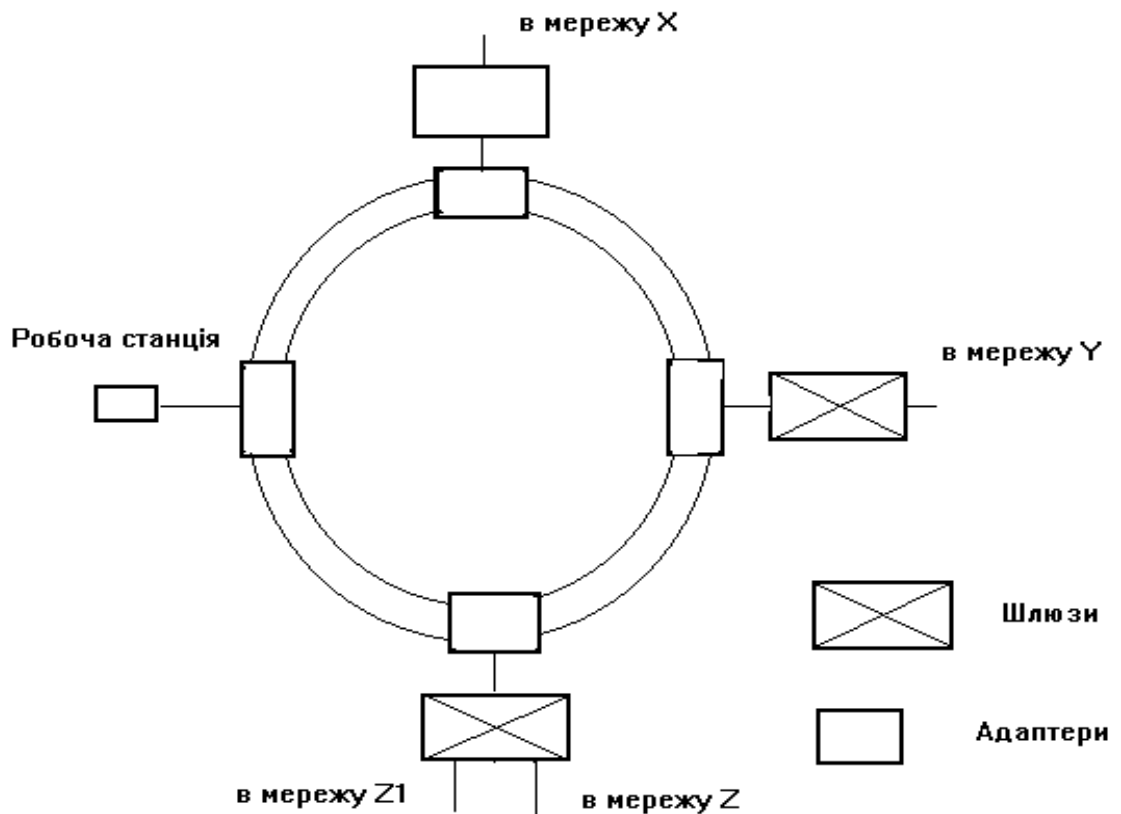


Рис.6. Схема передавання інформації у мережі кільцевого типу.

Коли кадр пройде повний круг, він знову досягне станції відправника, станція знімає з нього ознаку "повний", звіряє його з надісланим і перевіряє наявність відмітки про отримання. Якщо така відмітка є, то все гаразд, якщо ні — повторює посилку, дочекавшись вільного кадру (бо старий уже



пішов). Інформаційна місткість кільця невелика, тому міні-пакети роблять такими, що об'єм корисних даних 2-4 байти. Збільшити місткість можна шляхом збільшення робочої частоти або затримки. Тому кільцеву топологію ЛКМ застосовують у малих локальних мережах з можливістю виходу в інші мережі, більш потужні (див. рис.6).

Обладнання для передавання даних з однієї мережі в іншу називається *шлюзом*.

Недоліком такої мережі є ще й те, що у випадку виходу з ладу кільця на одній ділянці втрачається можливість роботи у всій мережі. Частково цього уникають у модифікованих кільцевих мережах, так званих петлеподібних.

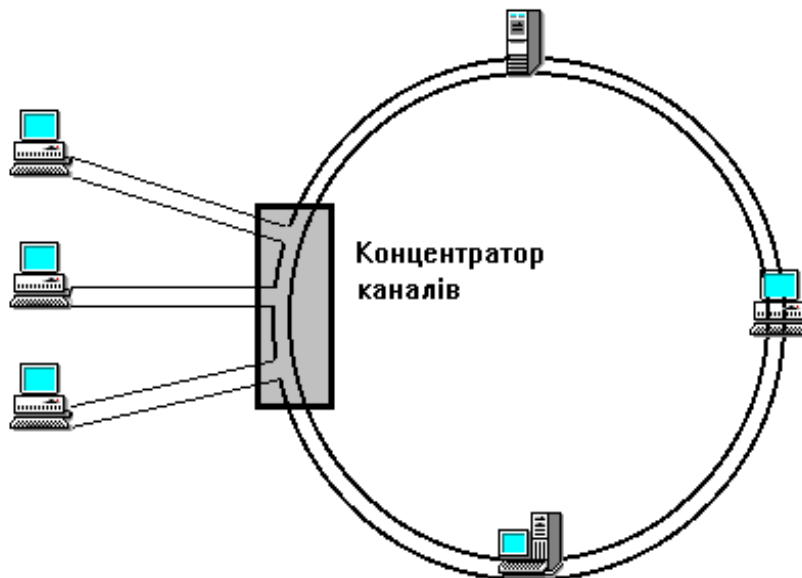


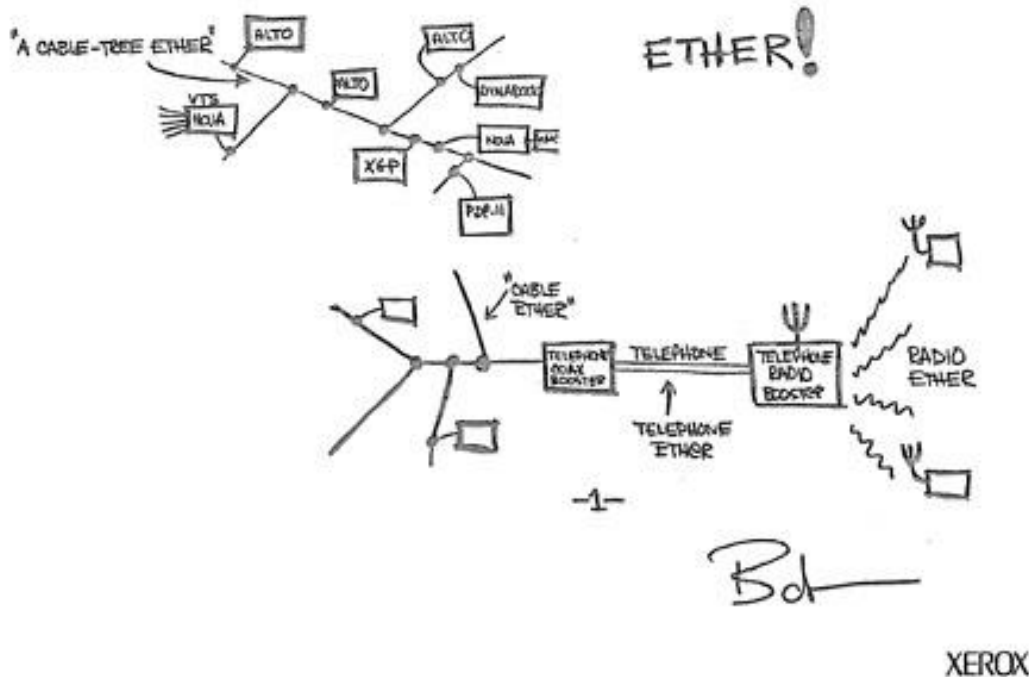
Рис.7. Кільцева петлеподібна мережа, або зірково-кільцева топологія.

У мережу (див. рис.7) вмикають *концентратори каналів* — керувально-контрольні центри, які ведуть статистику, контролюють роботу мережі, а головне — блокують несправну ділянку (шунтують).

3. *Шинна та лінійна топології* — пряма аналогія магістральних шинних архітектур міні та мікро-ЕОМ. Однією з найпоширеніших мереж шинної, чи деревоподібної архітектури є мережа Ethernet (Езернет), яку розробили провідні фірми XEROX, а потім DEC та INTEL. Іноді цю мережу позначають DIX. Уже згадуваний IEEE адаптував і

модифікував DIX V.2, уклав для її роботи протокол IEEE 802.3, який повністю збігається з ISO 8802.3, про що вже згадувалось.

**1973 рік.** Роберт Меткалф (Robert Metcalfe) і Давид Боггс (David Boggs), співробітники дослідницької лабораторії компанії Xerox, створили Ethernet - першу локальну комп'ютерну мережу. Швидкість передачі - 2.94 Мбіт/с. За аналогією до закону Мура (Gordon Moore, засновник Intel), Р.Меткалф передбачив експоненційний ріст мереж.



Ескіз технології Ethernet (Р.Меткалф)

Джерело: <http://www1.chapman.edu/soe/faculty/piper/teachtech/history.htm>

Як приклад, наведемо CSMA/CD деревоподібну структуру мережі Ethernet (рис.8). Тут мережа складається з чотирьох лінійних ділянок, які називаються сегментами. За допомогою спеціальних пристроїв сегменти під'єднуються до головної шини, утворюючи у такий спосіб деревовидну структуру. Така структура дозволяє будувати багатосерверні мережі, бо кожний з сегментів може мати свій сервер. Характерною особливістю таких мереж є узгодження хвильових опорів інформаційних шин (коаксіальних кабелів) за допомогою спеціальних пристроїв — термінаторів (“заглушок”). У випадку мережі Езернет – це звичайний резистор величиною 50 Ом.

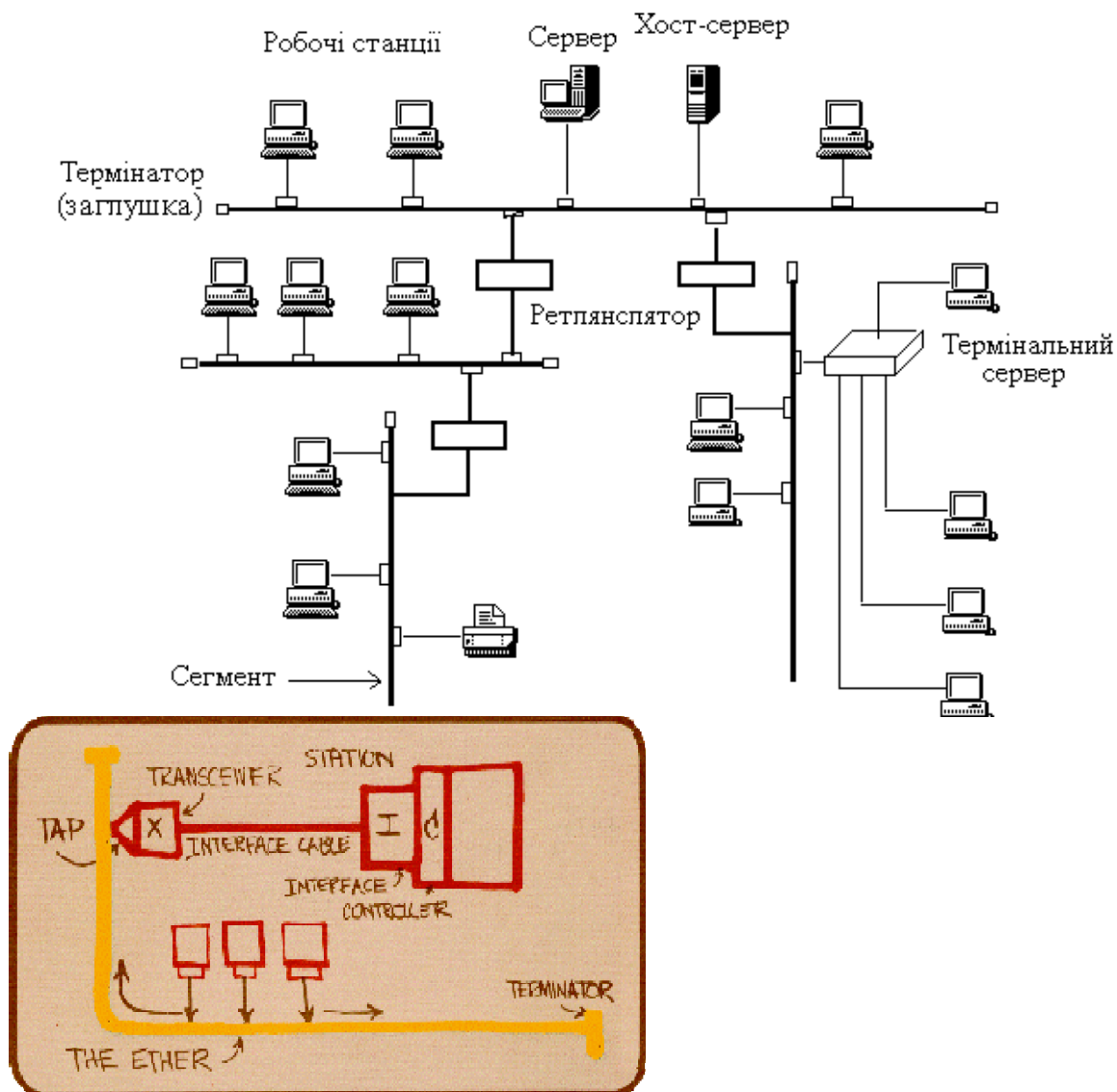
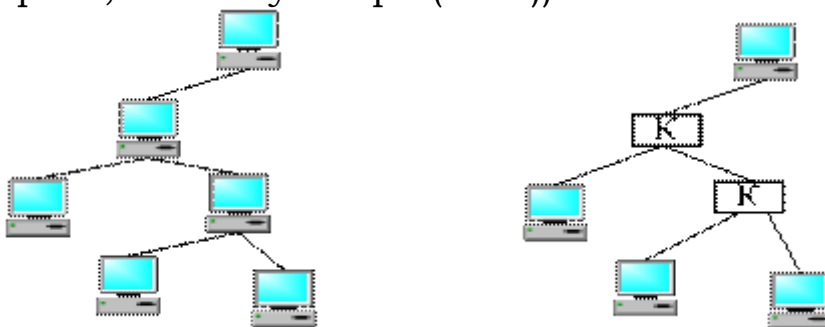


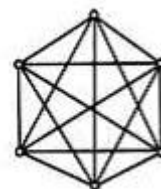
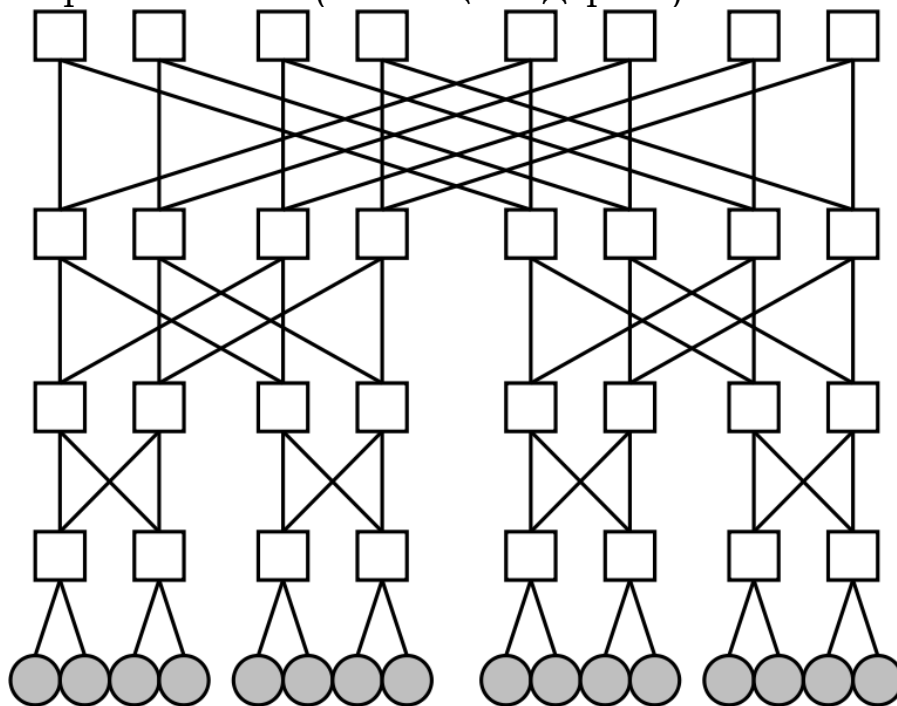
Рис.8. Шинна топологія (Мережа типу "Езернет" на коаксіальному кабелі).

4. *Топологія деревовидна.* Сучасний спосіб організації приєднання робочих станцій до мережі (активне та пасивне дерево, К – комутатори (хаби)).

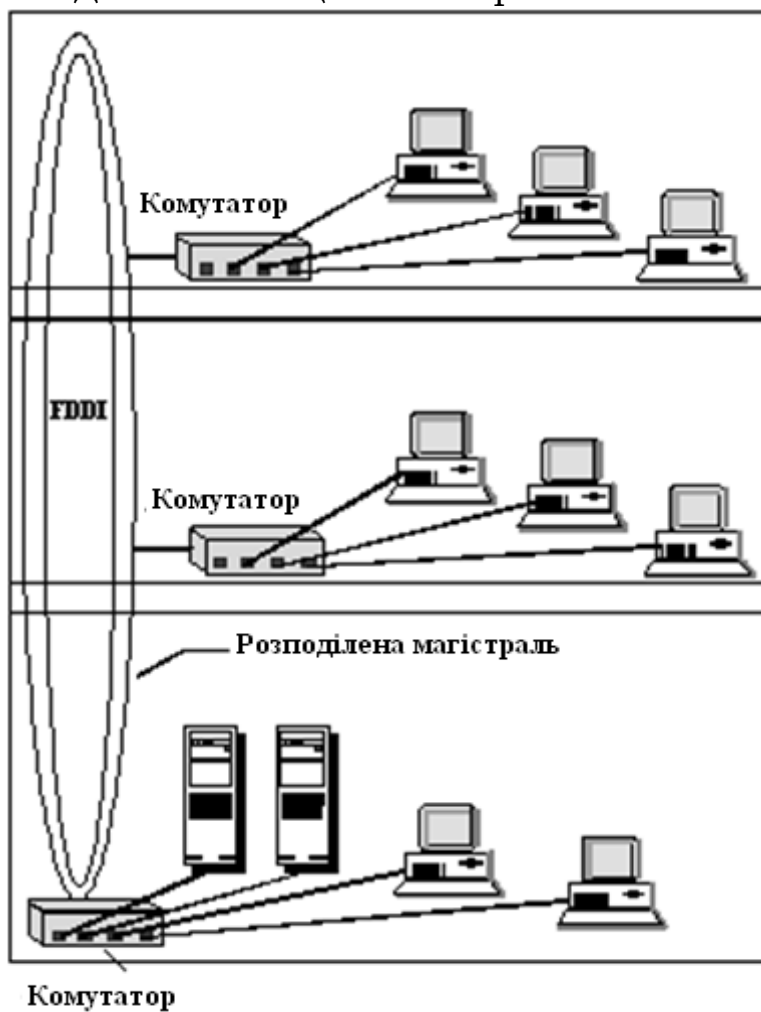


5. *Складні (змішані) топології.*

Мережа fat tree (потовщене дерево) -



Поєднання кільцевої та зіркової топології:



## 2.2 Основні типи ЛКМ, їх характеристики.

Ми вже згадували про те, що робота ЛКМ має два аспекти: фізичний та логічний (принцип передавання і перетворення даних). Про перший ітиметься дещо пізніше і, може, більш стисло, а другий аспект розглянемо детальніше. З погляду програмістів чи спеціалістів з інформатики він є важливіший. З самого початку відзначимо, що всі ЛКМ базуються на пакетно-орієнтованому передаванні: це означає, що всі дані "вставляються" в пакети, у заголовках яких містяться відповідні адреси для ідентифікації пристрою, з яким потрібно налагодити зв'язок.

Сучасний ринок пропонує кілька типів мереж. Найпоширенішою сьогодні є мережа Ethernet, з якою ми тільки що ознайомилися. На її основі прийнято відповідні стандарти Міжнародної Організації Стандартів (ISO) та Інституту інженерів з електротехніки і радіоелектроніки (IEEE). Цей стандарт дає змогу приєднувати комп'ютери практично всіх платформ: на основі процесорів Intel x86, Macintosh, систем RISC 9000 тощо.

**a. Ethernet** - мережа з мультистанційним доступом з контролем несучої частоти та виявленням колізій (зіткнень). "Ethernet" - один з найвідоміших термінів у технології мереж.

Під час обговорення протоколів наводились параметри швидкодії (10 Мбіт/с). Топологія Ethernet є розгалуженою деревоподібною структурою зі сполученими між собою сегментами (рис.8.). Кожен сегмент може мати у найкращому випадку довжину до 500 м з максимальною кількістю 100 вузлів мережі на сегмент. Щоб продовжити довжину або кількість пристроїв понад максимум, сегменти сполучають між собою за допомогою повторювачів (repeaters) або напівповторювачів (half-repeaters). Вони просто збільшують довжину мережі, регенеруючи (повторюючи) сигнали. Повторювач з'єднує два сусідні сегменти мережі. Напівповторювач здійснює передавання між двома сегментами, забезпечуючи таким чином більшу відстань між ними. Є обмеження в чотири повторювачі або напівповторювачі, що можуть підтримуватися між будь-якими двома точками мережі. Для подальшого розширення мережі треба використовувати мости (bridges) та маршрутизатори чи рутери (routers).

Відомо три модифікації мережі, залежно від якості кабелювання. Перша з них, що називається 10 BASE 5, використовує високоякісний коаксіальний, так званий "жовтий кабель", і забезпечує пропускну здатність у 10 Мбіт/с при максимальній довжині сегмента 500 м. Друга, 10 BASE 2, використовує значно дешевший "тонкий" кабель типу RG 058 і забезпечує пропускну здатність у 10 Мбіт/с при довжині сегмента 200м. Третя, 10 BASE T використовує для з'єднань скручену пару дротів. При 10Мбіт/с довжина сегмента не перевищує 100 м і є одне відгалуження, тоді як 10 BASE 2 дає змогу мати до 30 відгалужень. 10 BASE 2 часто називають Cheapernet (cheap - дешевий).

### Як працює Ethernet? (Алгоритм CSMA/CD)

Усі пристрої в ЛКМ можуть налагоджувати зв'язок, як тільки виникне потреба, без будь-якого пріоритету і порядку. Вони використовують пряме (немодульоване) передавання даних (baseband communication) (тобто в кабелі в кожен момент може бути тільки один сигнал) на швидкості 10 Мбіт/с. Пристрій, що хоче надіслати повідомлення, "прослуховує" мережу (це і є контроль несучої частоти), і, якщо жоден інший пристрій у мережі не виконує передавання, починає передавати його. Ймовірно, що й інший пристрій може почати передавання в той самий момент (бо доступ мультистанційний), отже, пристрої перевіряють канал на відсутність зіткнень (колізії) різних посилок. Якщо зіткнення сталося, то пристрої припиняють роботу на деякий час, що визначається з певного інтервалу розподілу випадкових чисел, після чого передавання відновлюється. Алгоритм передбачає 16 таких спроб. Всі пристрої постійно "прослуховують" мережу, копіюючи та підтверджуючи всі пакети даних, що адресовані до них. При виявленні колізії в середовище передається спеціальний сигнал (jam-послідовність). Див.діаграму:

**Довжина кабельної системи вибирається так, щоб за час передачі кадра мінімальної довжини сигнал колізії встигав би поширитися до найдальшого вузла мережі. Між двома послідовно передаваними через спільну шину кадрами інформації повинна витримуватися пауза (IPG) в 96 тактів (9.6 мкс для швидкості 10 Мбіт/сек); ця пауза потрібна для приведення у вихідний стан мережних адаптерів вузлів, а також для запобігання монопольного захоплення середовища передачі даних однією станцією.**



Pre+SFD	DA	SA	T L	LLC data	(Pad)	FCS
Преамбула+SFD	Адреса призначення	Адреса джерела	Тип або довжина кадра	Дані верхніх рівнів	Поле заповнення	Контрольна сума

**Pre** - преамбула (7 байт 10101010) для синхронізації на приймаючій стороні

**SFD** - початковий обмежувач кадра (Starting Frame Delimiter, 10101011)

**DA** - адреса призначення (Destination Address, 6 байт - MAC адреса)

**SA** - адреса джерела (Source Address, 6 байт - MAC адреса)

**T** - тип кадра, 2 байти (для кадра **Ethernet II**)

**L** - довжина кадра, 2 байти (для кадрів **Ethernet 802.3**, **Ethernet 802.2**, **Ethernet SNAP**)

**LLC data** - 0-1500 байт, інформація з заголовками верхніх рівнів

**Pad** - поле заповнення, якщо поле **LLC data** менше 46 байт

**FCS** - контрольна сума кадра (Frame Check Status, 4 байти, циклічний надлишковий код по всіх полях, крім Pre+SFD і FCS)

Загальна довжина кадра Ethernet - **64-1518** байт, довжина заголовкової і трейлерної частин (без преамбули) - 18 байт.

Типи MAC-адрес:

- **Unicast**

Кожний термінальний комунікаційний пристрій, як правило, має унікальну адресу каналного рівня. Перший біт шестибайтової послідовності завжди =0.

- **Multicast**

Така адреса ідентифікує станції, що виділені в групу адміністратором. Перший біт - 1, решта будь-які, крім всіх 1. Не може бути адресою відправника SA.

- **Broadcast**

Всі біти адреси виставляються в 1, тобто адрес має вигляд FF-FF-FF-FF-FF-FF. Кадр з такою адресою призначений для усіх станцій в мережі.

**6. Token Ring (маркерне (естафетне) кільце).** Мережа TR є типовою мережею кільцевого типу. Для прикладу можна привести схему мережі IBM Token Ring (рис.10).

Token Ring базується на концепції замкнутих кілець, так що станція має змогу отримувати своє власне повідомлення. Робота мережі пов'язана з поняттям маркера.

*Маркером* називається спеціальна коротка послідовність, що циркулює по кільці. Для мережі Token Ring довжина такого маркера має три байти (рис.11).



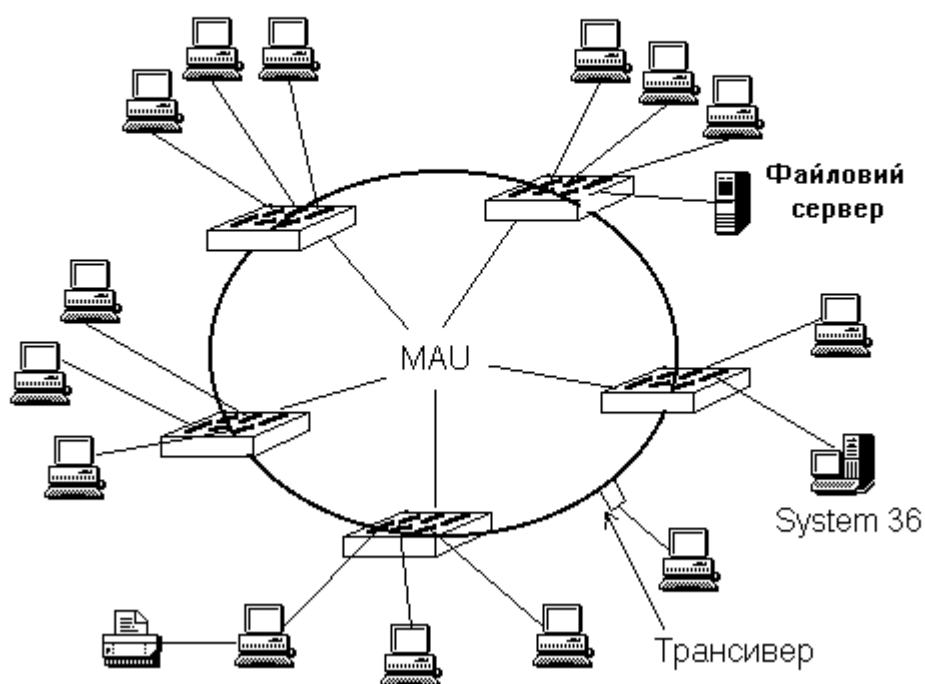


Рис.10. IBM структура Token Ring - найвідоміша з мереж.

Початковий розділювач (Start Delimiter)	Контроль доступу (Access Control)	Кінцевий розділювач (End Delimiter)
1 байт	1 байт	1 байт
0 0 0 0 1 1 1 1	P P P T M R R R	E

Рис.11. Структура маркера мережі Token Ring.

Байт контролю доступу поділено на чотири області: PPP - біти пріоритету, Т - біт маркера (якщо Т=1, то це ознака не зайнятого маркера, Т=0 - за маркером є пакет), RRR - біти резервування. М - біт монітора, який встановлюється в "1", якщо пакет передано активним монітором і дорівнює "0" у протилежному випадку. Початковий та кінцевий розділювачі є унікальними послідовностями електричних імпульсів.

Кожна станція отримує і регенерує маркер. Коли станція збирається передавати дані, вона чекає на маркер, додає адресну інформацію і дані, помічає маркер зайнятим і посилає його наступній станції. Всі станції мережі

продовжують отримувати і регенерувати пакети, але коли станція збирається передати дані, вона повинна зачекати, поки маркер стане вільним. Станція, що отримала маркер, адресований їй, копіює дані і регенерує пакет. Можливо, що станція отримає свій власний зайнятий пакет. Тоді вона вилучає своє повідомлення, а посилає вільний маркер, надаючи змогу передавання наступній станції.

Щоб підвищити ефективність мережі, з'явилась нова форма передавання маркера, яка називається "раннє звільнення маркера" і дає змогу звільнити маркер зразу ж, коли кадр даних передано. Це зменшує затримку, оскільки станції вже не чекають повернення свого власного повідомлення, що може зайняти значний час у мережі з багатьма станціями.

Існує багато типів мереж, що застосовують стандарт IEEE 802.5 (Token Ring). Найвідомішою є система IBM Token Ring, що працює на швидкості 4 Мбіт/с. Останній варіант IBM Token Ring використовує швидкість передавання 16 Мбіт/с.

Стандартна специфікація використовує немодульоване передавання на швидкості 4 Мбіт/с через скручену пару. Це дає перевагу у вартості перед Ethernet, яка функціонує на коаксіальному кабелі, оскільки кабелювання скрученою парою є значно дешевшим. Але повна специфікація IBM передбачає кабелювання екранованим кабелем, що значно дорожче. Введення стандарту Ethernet 10 BASE T (Ethernet, що функціонує на скрученій парі) суттєво вирівняло цю різницю, давши змогу передавання по неекранованому кабелі.

Хоча Token Ring є мережею з архітектурою цього типу, мережа IBM Token Ring не мусить фізично мати кільцеву топологію. Пристрої, що називаються пристроями мультистанційного доступу (Multi-station Access Unit, MAU), діють як радіальні центри кільцевої топології. На відміну від Ethernet, Token Ring не є природно стійкою мережею, і видалення станції з кільця може спричинити зупинку передавання даних. Щоб запобігти цьому, MAU опитує всі приєднані пристрої і відновлює кільце, якщо трапляються розриви. MAU дає змогу приєднати до себе певну кількість пристроїв (як звичайно, сім) а також приєднуватися до інших MAU, що працюють в мережі. MAU може підтримувати одне або кілька підкілець на будь-якому своєму з'єднанні, а не тільки окремий пристрій. Тому мережні повторювачі

CSMA/CD можна використовувати для розширення мережі, можливо, між двома будівлями, хоч повторювачі і не збільшують максимальної кількості пристроїв, які може підтримувати кожна мережа.

Як зазначено раніше, основним недоліком кільцевої топології є припинення функціонування всієї мережі при "розриві" кільця. MAU весь час підтримує активну конфігурацію, виявляючи і негайно обходячи будь-яку аварію. Мережа відновлює роботу і всі станції, за винятком секції, що зазнала аварії, не припиняють роботи. Одним з наслідків помилок цього типу є втрата маркера внаслідок аварії пристрою чи від'єднання, коли у нього був маркер. Пристрій може також зазнати аварії після передавання "зайнятого" маркера і таким чином бути нездатним звільнити його. В обох випадках за виявлення аномальних умов і прийняття коректувальних дій відповідає арбітр. Кільце може мати до 33 MAU і 260 станцій.

Там, де не використовують MAU, пристрої, через які до мережі приєднують інші пристрої, виконують ті самі відновлювальні функції, що й MAU.

Основним обмеженням топології є максимальна відстань між станціями 100 м, хоча її можна збільшити, використовуючи мости і рутери для сполучення кілець між собою.

Перевагою Token Ring є те, що кожна станція може "тримати" маркер тільки визначений відрізок часу, даючи таким чином усім станціям змогу регулярно передавати інформацію, незалежно від завантаженості мережі. Іншою перевагою перед CSMA/CD або Ethernet є те, що в мережі не існує колізій, отже, продуктивність знижується лінійно зі зростанням завантаження мережі.

**в. Token Bus (маркерна (естафетна) шина).** Token Bus поєднує шинну структуру мереж типу Ethernet і систему передавання маркера мережі Token Ring. Стандартна форма комунікації – ширококутовий зв'язок по коаксіальному кабелю. Такий зв'язок виділяє сигналам різні смуги частот, даючи змогу передавати по кабелю одночасно кілька сигналів. Це можна порівняти з використанням коаксіального кабелю для передавання одночасно сигналів кількох телевізійних програм. Сигнали генеруються звичайно парами і кабель

може підтримувати кілька різних пар. Передавання сигналу модульоване, "вперед" і "назад" на різних несучих частотах. Такий спосіб передавання потребує спеціальних пристроїв – трансиверів для під'єднання ПК до мережі. Термінатори, що в Ethernet є просто резисторами, тут повинні бути складними пристроями, які здатні регенерувати сигнали на іншій несучій частоті. Кабелювання такої мережі значно дорожче, ніж Ethernet.

Можна використовувати різні швидкості передавання: або чотири пари на швидкості 1 Мбіт/с, або одна пара на швидкості 5 Мбіт/с, або одна пара на швидкості 10 Мбіт/с. Найуживанішою формою до недавнього часу була вита пара на швидкості 5 Мбіт/с.

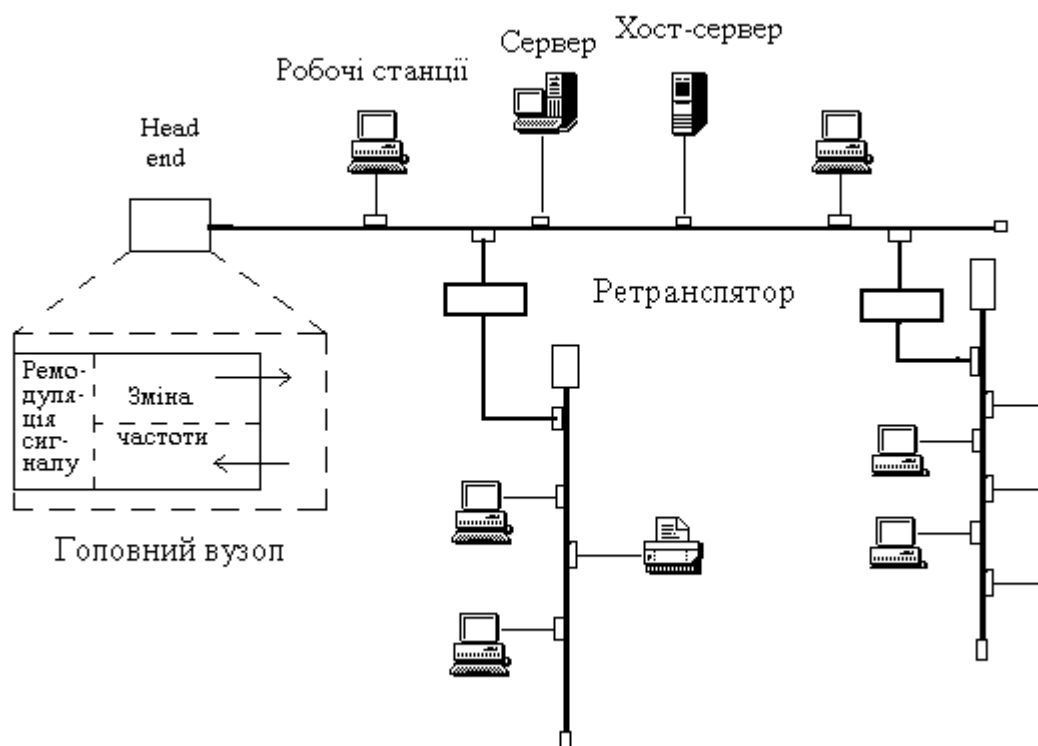


Рис.12. Мережа Token Bus.

Принцип передавання інформації в мережі ТВ. Для того, щоб забезпечити можливість передавання сигналу до кожної станції, приєднаної до шини, вони передаються в різних частотних діапазонах і таким чином реалізовано два канали - "вперед" і "назад". Коли сигнал досягає так званого головного вузла мережі, він ремодулюється (змінюється несуча частота) і транслюється в мережу по іншому частотному каналу. Це дає змогу кожній станції передавати інформацію до будь-якої

іншої станції незалежно від її розташування в мережі. І хоч мережа не має форми фізичного кільця, фактично реалізоване логічне кільце. Застосовується логічна адресація станцій у мережі і кожна станція передає маркер за наступною логічною адресою в шині.

Використання широкосмугового передавання потребує складнішої системи зв'язку і певного типу модемів для приєднання кожного пристрою до мережі. Мережа потребує також пристрою, що називається головним вузлом (head end) для ремодуляції і регенерації сигналів. Тому вона є дорожчою і складнішою для реалізації, ніж мережа з немодульованим передаванням.

Перевагою Token Bus є те, що кабелювання тут значно легше, ніж у випадку кільцевої топології. Крім того, уникаючи колізій, можна досягти значно вищої продуктивності, ніж у CSMA/CD, бо використовується передавання маркера. Однак, оскільки застосовується логічне кільце, то маркер повинен бути перехоплений і регенований перш ніж його передадуть наступному пристрою в логічному кільці, що надлишково перевантажує мережу. Щоб зменшити ці накладні витрати, можна застосувати багатократне передавання під час захоплення маркера пристроєм. Проте це лиш частково розв'язує проблему, оскільки маркер можна затримати лише обмежений період часу.

#### **г. Оптоволоконний розподільний інтерфейс, Fibre Distributed Data Interface (FDDI)**

FDDI є стандартом, зареєстрованим Американським національним інститутом стандартів (ANSI) і має назву X3T9.5. Він ґрунтується на оптоволоконних лініях, методі доступу з передаванням маркера та кільцевій топології. Це дуже ефективна кільцева мережа з передаванням маркера, хоч реалізації FDDI ще не повністю відповідають стандартам IEEE та OSI. Мережа може мати довжину до 100 км і працювати зі швидкістю передавання інформації 100 Мбіт/с.

При максимальній дистанції 100 км ця мережа не відповідає терміну локальна комп'ютерна мережа. Її можна віднести швидше до базових мереж, що з'єднують будівлі і центральні ресурси та серії малих дешевших мереж у

кожному відділі чи на кожному поверсі. Потужні, розраховані на великі дистанції базові мережі часто зачисляють до метропольних (чи міських) мереж (Metropolitan Area Networks, MANs). Робота цих метропольних мереж підпорядкована протоколу IEEE 802.6. Інше застосування FDDI може бути в новітніх, спеціалізованих станціях, наприклад тих, які використовують на конструкторських автоматизованих робочих місцях (Computer Aided Design, CAD), де постійно з центрального комп'ютера до терміналів передаються величезні масиви інформації.

FDDI дає кілька важливих переваг перед звичайними мережними архітектурами. По-перше, принцип передавання інформації передбачає подвійне проходження оптичного кільця, що збільшує відмовостійкість для кільця та приєднаних до нього вузлів. По-друге, по мережі в кожен момент часу може проходити більше одного пакета, що дає змогу ефективніше використовувати її потужність. По-третє, це дає змогу збільшити максимальний розмір пакетів порівняно з іншими типами мереж, що значно збільшує ефективність передавання даних, особливо для пристроїв, що потребують передавання до них особливо великих масивів інформації, як, наприклад, графічні станції тощо. По-четверте, оскільки

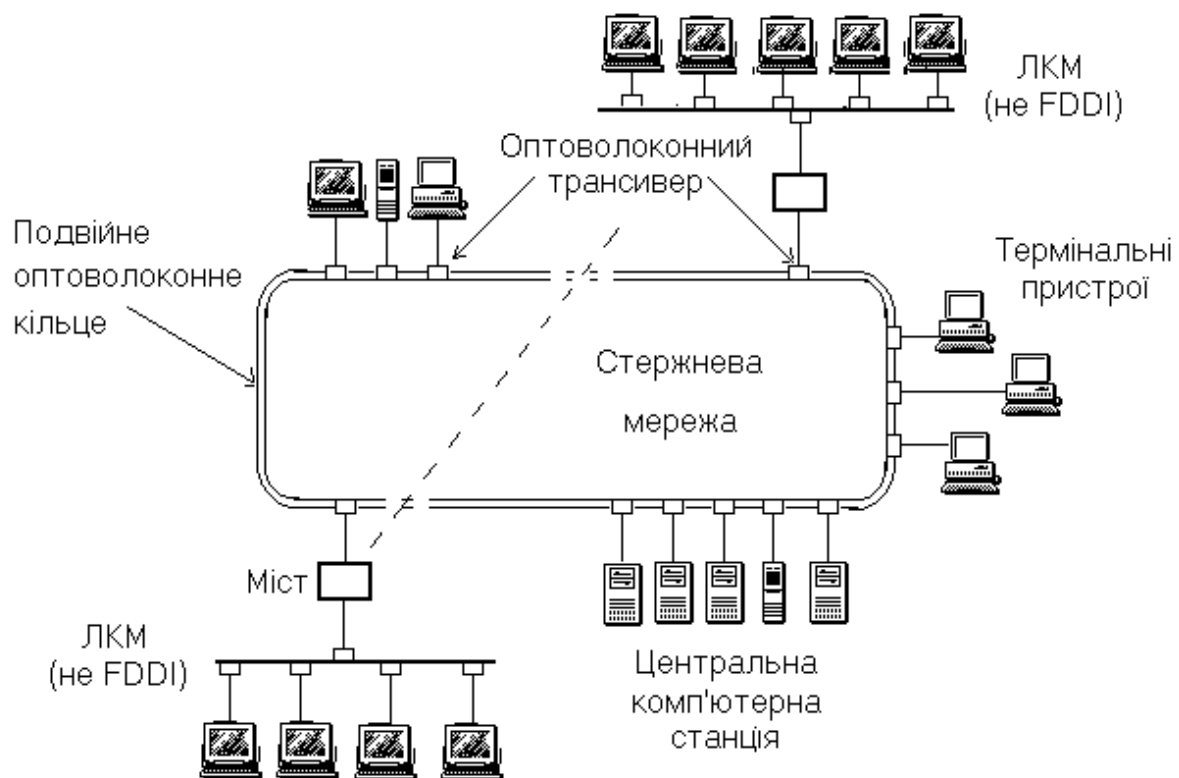


Рис.13. Мережа з оптоволоконним інтерфейсом.

оптоволоконний кабель використовує для передавання інформації світло, він вільний від усіх звичайних електричних завад. Кількість помилок під час передавання інформації значно зменшується, отже значно зменшується і кількість необхідних повторних передавань. Внаслідок цього збільшується пропускна здатність для приєднаних пристроїв. Нарешті, використання передавання маркера дає змогу уникнути проблем, пов'язаних з колізіями. Цей принцип, розвинений далі, дає змогу різним пристроям мати пріоритети у використанні мережі, тобто ключовим пристроям, а також тим, що передають надвеликі масиви інформації, можна надати пріоритет, усуваючи можливі затримки.

Сьогодні вартість FDDI є досить високою, в основному завдяки вартості оптоволоконного кабелю та передавально-приймальних пристроїв. Однак, зі збільшенням кількості даних та появою нових пристроїв FDDI ставатиме найбільш популярним. Про це свідчить новий стандарт, що називається FDDI II. Надалі працюючи на швидкості 100 Мбіт/с, він, використовуючи схему пріоритетів, дає змогу поряд з передаванням числових даних передавати в реальному часі аудіо- та відео інформацію.

**д. Мережа Apple Talk** є власним мережним протоколом, розробленим фірмою Apple Computer. Вона доступна для всіх користувачів комп'ютерами типу Makintosh. Коли Apple вперше випустила Apple Talk, термін охоплював протоколи всіх рівнів, у тім числі й фізичні засоби. Згодом Apple перевизначила фізичний рівень як LokalTalk, а вищі рівні – як Apple Talk. Потім фірма реалізувала Ethernet, вийшла мережа EtherTalk, а недавно ще й Token Ring, і вийшла TokenTalk.

LokalTalk використовує шинну топологію та немодульоване передавання інформації. Кабелювання роблять скручено парою, швидкість передавання 230 Кбіт/с, максимальна довжина мережі 300 м. Метод доступу до шини є варіант CSMA/CD, що називається у даному випадку Мультистанційним доступом з контролем несучої частоти з уникненням колізій (CSMA/CA).

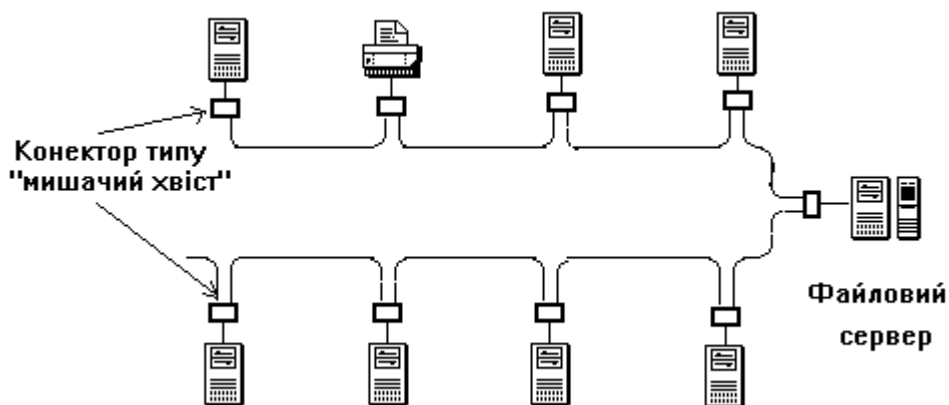


Рис.14. Мережа Apple Talk.

Таку мережу легко встановити, оскільки кожний комп'ютер Apple обладнаний усім необхідним для комунікації в мережі. До кожної системи додають і необхідне програмне забезпечення. Для об'єднання в мережу потрібно тільки з'єднати пристрої, що їх називають "мишачий хвіст" ("Rat's Tail"), та кабель (скручена пара).

EtherTalk та TokenTalk потребують вмонтування в комп'ютер Makintosh додатково LAN-карти. Швидкість передавання інформації в мережі збільшується до 10 та 4 Мбіт/с відповідно. Ethernet дає змогу реалізувати стандарти OSI для мереж Makintosh.

#### **е.Мережа ARCnet (Attached Resource Computer net)**

Цю мережу розробила корпорація Datapoint, вона є її власною ЛМ. ARCnet з'явилася у 1977 р. і була першою комерційною локальною мережею. Мережа використовує немодульоване передавання даних на швидкості 2,5 Мбіт/с. Методом доступу є естафетне передавання маркера, який згодом було прийнято як міжнародний стандарт IEEE 802.4-85. Може використовуватись як кільцева, так і шинна топологія. Спочатку систему розробили для передавання інформації через тонкий коаксіальний кабель, але внаслідок розвитку система пізніше стала включати підтримку скрученої пари та оптоволоконного кабелю.

Мережа порівняно дешева у інсталяції і оскільки вона першою з'явилася на ринку, то мала велику кількість користувачів. Однак сьогодні її популярність значно знизилася. Мережа не повністю підтримує запроваджені стандарти і є дещо повільнішою від сучасних.



Розмір пакета не перевищує 0.5 Кбайт, причому до 508 байт відводиться під дані, решта використовується під адреси станції-приймача, станції-передавача та іншу службову інформацію. Кожна плата ARCnet-контролера станції має свою унікальну фізичну адресу в діапазоні від 0 до 255. Застосовуються концентратори каналів (HUB) двох типів: активні (дозволяють з'єднувати станції до 600 м) і пасивні (до 30 м), або їх комбінацію.

У випадку застосування коаксіального кабелю і використання шинної топології об'єднують по 4, 8, 16 і так далі станцій. У такій мережі на обидвох кінцях шини вмонтовують термінатори (резистори з номінальним опором 93 Ом) для узгодження хвильового опору кабелю.

### **ж. Мережа Fast Ethernet**

У травні 1995 комітет IEEE прийняв специфікацію Fast Ethernet як стандарт **802.3u**.

Відмінності FE від E насамперед обумовлені використанням різних варіантів кабельних систем та електричних параметрів імпульсів, а також способом кодування сигналів і кількістю використовуваних в кабелі провідників.

Стандартом Fast Ethernet IEEE 802.3u установлені чотири типи фізичного інтерфейсу : 100Base-FX, 100Base-TX , 100Base-T4 і 100Base-T2 .

Специфікація Ethernet	Швидкість передачі, baud	Кодування	Кабельна система	Можливість роботи в дуплексному режимі
10Base-T	10 Mbd	Manchester II	2 пари UTP 3 кат.	+
100Base-TX	125 Mbd	4B/5B, MLT-3	2 пари UTP 5 кат., STP 1	+
100Base-T4	33 Mbd	8B/6T	4 пари UTP 3 кат.	-
100Base-T2	25 Mbd	PAM-5	2 пари UTP 3 кат.	+
100Base-FX	125 Mbd	4B/5B, NRZI	оптоволокну	+

Фізичний рівень складається з трьох підрівнів:

- 1) підрівень узгодження (reconciliation sublayer)
- 2) Незалежний від середовища інтерфейс (Media Independent Interface, МІІ, внутрішній і зовнішній (40 Pin, 1m, 5v)) - підтримує незалежний від фізичного середовища спосіб обміну даними між MAC-підрівнем і підрівнем РНУ. Подібний на АUI, тільки АUI між РНУ (там завжди однакове кодування) і РМА
- 3) Пристрій фізичного рівня (Physical layer device, РНУ) - забезпечує кодування даних, які поступають від MAC-підрівня для передачі їх по кабелю певного типу, синхронізацію передаваних даних, а також приймання і декодування даних у вузлі-приймачі

### **Підтримка VLAN**

VLAN - Virtual Local Area Networks, можливість створення віртуальних локальних мереж на комутаторах (1998 рік).

Технологія комутації кадрів дозволяє створити логічну конфігурацію локальної мережі незалежною від її фізичної інфраструктури.

Мета:

1. Забезпечити засоби підтримки додатків, критичних до часу затримки і стабільності пропускну здатності;
2. дозволити об'єднати станції в незалежні логічні групи, забезпечити комунікацію всередині групи, розмежувавши внутрішній та зовнішній трафіки;
3. спростити конфігурування локальних мереж.

### **3. Мережа Gigabit Ethernet**

1000BASE-T, IEEE 802.3ab — Стандарт Ethernet 1 Гбіт/с. Скручена пара категорії 5е або категорії 6. В передачі даних задіяні всі 4 пари. Швидкість передачі даних — 250Мбіт/с через одну пару.

1000BASE-TX, — Стандарт Ethernet 1 Гбіт/с, використовує тільки скручену пару категорії 6. Практично не використовується.

1000Base-X — загальний термін для позначення технології Гігабіт Ethernet, що використовує як середовище передачі даних оптоволоконний кабель, включає в себе 1000BASE-SX, 1000BASE-LX і 1000BASE-CX.

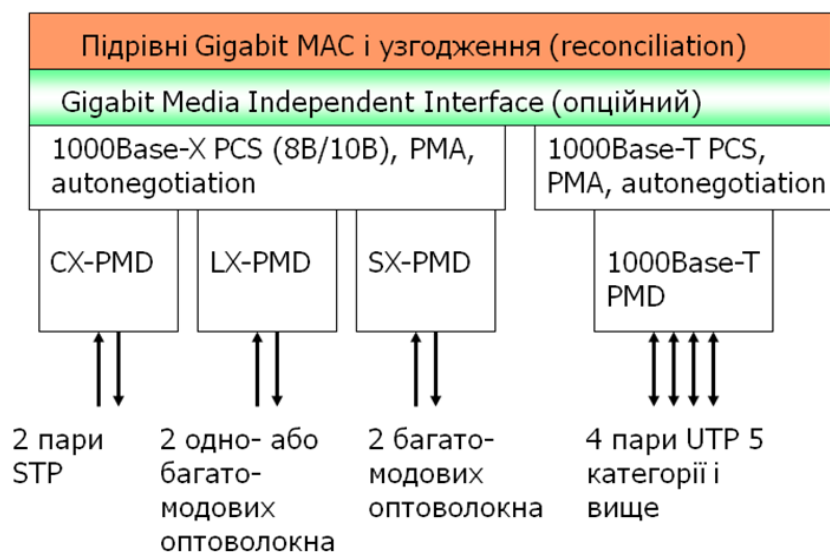
[1000BASE-SX](#), IEEE 802.3z — 1 Гбіт/с Ethernet технологія, використовує багатомодове волокно дальність проходження сигналу без повторювача до 550 метрів.

[1000BASE-LX](#), IEEE 802.3z — 1 Гбіт/с Ethernet технологія, використовує багатомодове волокно дальність проходження сигналу без повторювача до 550 метрів. Оптимізована для далеких віддалей, при використанні одномодового волокна (до 10 кілометрів).

[1000BASE-CX](#) — Технологія Гігабіт Ethernet для коротких віддалей (до 25 метрів), використовує спеціальний мідний кабель (екранована вита пара (STP)) з хвильовим опором 150 Ом. Замінений стандартом 1000BASE-T, і зараз не використовується.

[1000BASE-LH](#) (Long Haul) — 1 Гбіт/с Ethernet технологія, використовує одномодовий оптичний кабель, дальність проходження сигналу без повторювача до 100 кілометрів.

## Gigabit Ethernet



**Кодування 8B/10B (8 бітів → 10 бітів)** застосовується також в Fibre Channel.

Характеристики:

- введена надлишковість (256 станів кодуються в 1024);
- Надлишковість дозволяє відновлювати неправильно переданий сигнал без повторної передачі;

- можливість самосинхронізації за рахунок фронтів імпульсів, які часто зустрічаються;
- ліквідовано дизбаланс між кількістю "0" і "1" порівняно з 4b/5b (нема залежності нагрівання лазерів від передаваних даних, підвищено стабільність, а також нема накопичення потенціалу для електропровідних ліній);
- Кодування дозволяє відрізнити дані від управляючих сигналів.

Перехід від Fast Ethernet до продуктивніших мереж (напр., Gigabit Ethernet) відбувається або заміною обладнання (комутаторів, репітерів), або завдяки використанню агрегації каналів (можливість паралельного пересилання даних між комутаторами по кількох скручених парах одночасно).

З метою уникнення неповного використання каналу передачі використовують ущільнення кадрів. Перший кадр передається, якщо є потреба, з розширенням, а замість міжкадрових проміжків (IFG\*), коли станція повинна "мовчати", вона видає в середовище символи розширення (для того, щоб інші станції не захопили середовище), а потім після першого IFG\* йдуть інші кадри, але вже без розширення (проміжки між кадрами знову заповнюються символами розширення). У такий спосіб смуга пропускання використовується значно практичніше.

<b>MAC кадр з розширенням</b>	<b>IFG*</b>	<b>MAC кадр</b>	<b>IFG*</b>	<b>MAC кадр</b>
-------------------------------	-------------	-----------------	-------------	-----------------

## **i. Мережа 10 Gigabit Ethernet**

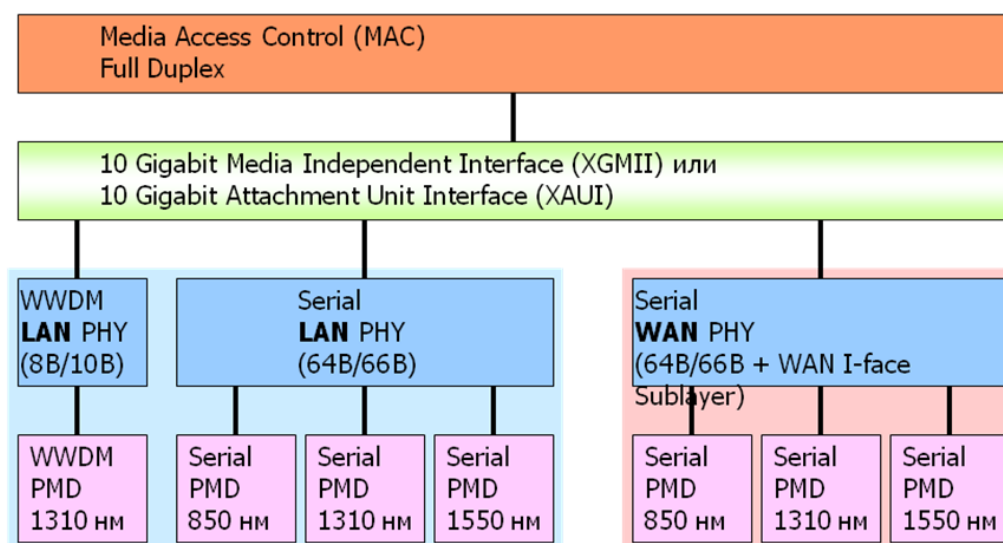
10 Gigabit Ethernet Alliance -> IEEE 802.3ae

Роботу над стандартом почато в 1999 р., завершено в середині 2002.

Особливості 10GE:

- а) збережено формат кадра (MAC підрівень);
- б) передача тільки в повнодуплексному режимі;
- в) використання оптоволокна (переважно одномодового) як середовища передавання (для специфікацій на міді гарантується підтримка 100 метрових сегментів для скрученої пари 7 категорії, 55-100 метрів для 6 категорії);
- г) метод доступу CSMA/CD не потрібний!.

# Стек 10 Gigabit Ethernet



Дві специфікації пристроїв фізичного рівня: **LAN** і **WAN** для використання в локальних і глобальних мережах відповідно.

## 2.3. Компоненти та устаткування ЛКМ. Вибір типу файл-сервера, інтерфейси.

У попередніх розділах ми вже ознайомилися з основними компонентами мережі персональних комп'ютерів. Тепер трохи розширимо ці поняття з погляду технічного забезпечення ЛКМ. Про програмний аспект цього питання йтиметься в окремому розділі. Отже, компоненти ЛКМ:

- робоча станція, або кінцевий термінальний пристрій. У переважній більшості випадків це автономний персональний комп'ютер, який обов'язково має свій процесор, оперативну пам'ять, монітор та клавіатуру. Наявність твердих і гнучких дисків не обов'язкова. Іноді така конфігурація робочих станцій навіть корисна, тому що підвищує стійкість мережі до зараження вірусами;
- хост-сервер (головний сервер) — термін, який в основному вживається для UNIX - мереж. Це спеціальний комп'ютер, побудований на базі процесора не нижче Intel 80486, з великою місткістю оперативної та зовнішньої пам'яті та можливістю їхнього розширення. Переважно цим терміном називають великий потужний комп'ютер мережі, однак іноді це поняття переносять і на файл-сервер;

- файл-сервер. З погляду вимог до технічного забезпечення файл-сервер нічим не відрізняється від перелічених вище для хост-сервера, але функції файл-сервера обмежуються тим, що забезпечують зберігання даних (файлів) і спільний доступ до них усіх користувачів мережі, координують зв'язок між робочими станціями і керують пристроями введення/виведення інформації;
- засоби доступу мережі до ПК: LAN-карти, адаптери, порти;
- принтер;
- спеціальне обладнання (плотери, дигітайзери та ін.).

Устаткування мереж:

- репітери, або ретранслятори чи повторювачі;
- концентратори (hub), комутатори;
- мости;
- маршрутизатори (рутери);
- шлюзи.

Які функції виконує те чи інше устаткування добре видно зі схеми (рис.15), де мережі зображені у вигляді двох взаємодіючих відкритих інформаційних систем:

Мережа 1	Обладнання для з'єднань	Мережа 2
Прикладний (Application)	Шлюз (Gateway)	Прикладний (Application)
Представницький (Presentation)		Представницький (Presentation)
Сеансовий (Session)		Сеансовий (Session)
Транспортний (Transport)		Транспортний (Transport)
Мережний (Network)	Маршрутизатор (Router)	Мережний (Network)
Канальний (Data Link)	Міст (Bridge)	Канальний (Data Link)
Фізичний (Physical)	Ретранслятор (Repeater), Концентратор (hub)	Фізичний (Physical)

Рис.15. Схема взаємодії двох інформаційних систем.

## **Сервери в локальних мережах**

Дуже часто у рамках однієї ЛКМ може використовуватися кілька виділених серверів. За своїм функціональним призначенням розрізняють кілька типів серверів (сервісів):

- файловий сервер;
- сервер друку;
- сервер додатків;
- сервер бази даних;
- комунікаційний сервер і т.д.

**Файловий сервер** - комп'ютер, який виконує функції управління ЛКМ, відповідає за комунікаційні зв'язки, зберігає файли, що розділяються в ЛКМ, і надає доступ до спільно використовованого дискового простору.

**Сервер друку** (Принт - сервер) - комп'ютер, програма або спеціальний пристрій, що забезпечує доступ станціям мережі до центрального принтера. Запити на друк надходять від кожної робочої станції до сервера друку, який розділяє їх на індивідуальні завдання принтера, створює чергу друку. Завдання зазвичай обробляються в порядку їх надходження. У функції сервера друку входить також управління принтером.

**Комунікаційний сервер** (сервер віддаленого доступу) дозволяє працювати з різними протоколами (правилами передачі інформації в мережі) і дозволяє станціям розділяти модем або вузол зв'язку з великою ЕОМ. Це дає можливість отримати інформацію, що зберігається в мережі, практично з будь-якого місця, де є телефон, модем і комп'ютер.

**Сервери додатків.** На серверах додатків виконуються прикладні частини клієнт - серверних додатків, а також знаходяться дані, доступні клієнтам. Якщо в файл-сервері файл або дані цілком копіюються на комп'ютер користувача, то в сервері додатка на запит комп'ютера пересилаються тільки результати запиту.

**Поштові сервери** зберігають та управляють передачею електронних повідомлень між користувачами мережі.

**Факс сервери** управляють потоком вхідних і вихідних факсимільних повідомлень через один або кілька факс-модемів.

Один виділений комп'ютер в мережі може одночасно виконувати функції файл-сервера, сервера друку, додатків і т.д.

### *Потужність і продуктивність сервера*

Для сервера необхідно використовувати досить потужний і надійний комп'ютер. Чималу роль відіграє можливість розширення і модернізації сервера. Це дозволить забезпечити необхідну продуктивність не тільки в даний час, але і в майбутньому.

Підвищення продуктивності здійснюється за рахунок використання швидких і потужних процесорів (в т.ч. і багатопроцесорних систем), високошвидкісних інтерфейсів (особливо для дискових підсистем), збільшення кількості оперативної пам'яті і кеш-пам'яті. Широке поширення отримали RAID-підсистеми і «гаряча» заміна дискових накопичувачів. RAID (Redundant Array of Inexpensive Disks-«надлишковий масив недорогих дисків»).

RAID має три основні ознаки:

1. це набір дисків, доступних користувачам як один або кілька логічних дисків.
2. дані розподіляються по набору дисків певним чином.
3. додається надлишкова ємність і, відповідно, надлишкова інформація для можливості відновлення даних у разі відмови.

Матриця дисків RAID оснащена спеціалізованим контролером з власним процесором і кешуванням декількох дисків. В цьому випадку для ОС і користувача кілька дисків представляють один великий диск. Виграш у швидкодії досягається за рахунок розпаралелювання запитів на читання / запис між дисками матриці, застосування великий кеш-пам'яті і використання власного процесора для обробки операцій читання / запису, який розвантажує центральний процесор сервера.

Матриці дисків дозволяють також істотно підвищити відмовостійкість дискової підсистеми за рахунок можливості продовжувати роботу при виході з ладу будь-якого одного диска. Відмовостійкість досягається за рахунок запису на диски матриці додаткової надлишкової інформації, яка використовується для автоматичного відновлення даних у разі відмови одного з дисків. Надлишкова інформація становить до 25%, що дає виграш і в вартості в порівнянні з повним «задзеркалюванням» дисків. При «задзеркалюванні» дисків інформація одного повністю дублюється на іншому, тобто надлишкова інформація дубльованих ділянок підсистем становить 50%. Висока надійність серверів досягається



шляхом повного або часткового дублювання підсистем (як для розглянутої вище дискової підсистеми).

Для збільшення надійності ЛОМ застосовують також і дублювання («задзеркалювання») серверів. В цьому випадку обидва сервери повністю дублюють функції іншого, і в разі поломки або виключення будь-якого з них, робота в мережі може бути продовжена.

Для збільшення відмовостійкості системи обов'язково використовують безперебійні джерела живлення (UPS). Ці пристрої забезпечують захист сервера від перепадів напруги, промислових перешкод і повного відключення електроживлення. Додаткове апаратно програмне забезпечення дозволяє через мережу зі станції адміністратора здійснювати моніторинг живлення, температури UPS, а в разі необхідності коректно закрити файловий сервер. Крім UPS для сервера передбачають спеціальні пристрої для захисту мережевих адаптерів. Це необхідно, оскільки в кабелі для передавання даних можуть виникати імпульси високої напруги, які можуть призвести до пошкоджень системної плати або адаптерів.

Для підвищення надійності сервери мають вбудовані засоби діагностики, а також засоби архівування та резервного копіювання даних.

## **2.4 Поняття про корпоративні мережі**

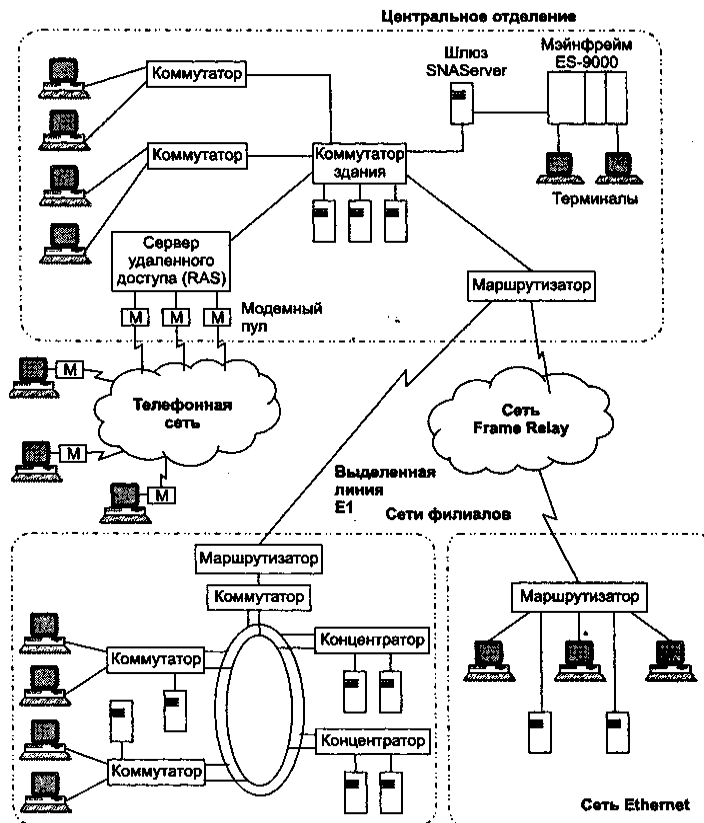
Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам. Залежно від масштабу підприємства, а також від складності і різноманіття вирішуваних завдань розрізняють мережі відділу, мережі кампусу і корпоративні мережі (термін «корпоративні» в даній класифікації набуває вузького значення — мережу великого підприємства).

Використання обчислювальних мереж дає підприємству наступні можливості:

- розділення дорогих ресурсів;
  - вдосконалення комунікацій;
  - поліпшення доступу до інформації;
  - швидке і якісне ухвалення рішень;
- свобода в територіальному розміщенні комп'ютерів.

Концептуальною перевагою корпоративних мереж є **здатність виконувати паралельні обчислення**. За рахунок цього в системі з декількома оброблювальними вузлами в принципі може бути досягнута продуктивність, що перевищує максимально можливу на даний момент продуктивність будь-якого окремого, скільки завгодно потужного процесора.

Ще одна очевидна і важлива гідність розподілених систем — це їх принципово **вища відмовостійкість**. Під відмовостійкістю розуміється здатність системи виконувати свої функції (можливо, не в повному обсязі) при відмовах окремих елементів апаратури і неповної доступності даних. Основою підвищеної відмовостійкості розподілених систем є надмірність. Надмірність оброблювальних вузлів (процесорів в багатопроцесорних системах або комп'ютерів в мережах) дозволяє при відмові одного вузла перепризначувати приписані йому завдання на інші вузли. З цією метою в розподіленій системі можуть бути передбачені процедури динамічної або статичної реконфігурації. У обчислювальних мережах деякі набори даних можуть дублюватися на зовнішніх пристроях запам'ятовування декількох комп'ютерів мережі, так що при відмові одного їхніх дані залишаються доступними.



Мал. 16. Приклад корпоративної мережі

Використання територіально розподілених обчислювальних систем більше відповідає **розподіленому характеру прикладних завдань** в певних областях, таких як автоматизація технологічних процесів, банківська діяльність і тому подібне. У всіх цих випадках є розосереджені по деякій території окремі споживачі інформації — співробітники, організації або технологічні установки. Ці споживачі автономно вирішують свої завдання, тому раціонально надавати їм власні обчислювальні засоби, але в той же час, оскільки вирішувані ними завдання логічно тісно взаємозв'язані, їх обчислювальні засоби повинні бути об'єднані в єдину систему. Адекватним рішенням в такій ситуації є використання обчислювальної мережі.

Для користувача розподілені системи дають ще, окрім вище названих, і такі переваги, як **можливість сумісного використання даних і пристроїв**, а також можливість гнучкого розподілу робіт по всій системі. Подібне розділення дорогих периферійних пристроїв, таких як дискові масиви великої ємкості, кольорові принтери, графічні пристрої, модеми, оптичні диски, у багатьох випадках є основною причиною розгортання мережі на підприємстві.

Останнім часом почав переважати інший спонукальний мотив розгортання мереж, набагато важливіший в сучасних умовах, чим економія засобів за рахунок розділення між

співробітниками корпорації дорогої апаратури або програм. Цим мотивом стало прагнення забезпечити співробітникам **оперативний доступ до обширної корпоративної інформації**. В умовах жорсткої конкурентної боротьби в будь-якому секторі ринку виграє, врешті, та компанія, співробітники якої можуть швидко і правильно відповісти на будь-яке питання клієнта — про можливості їх продукції, про умови її застосування, про вирішення будь-яких можливих проблем і тому подібне. На великому підприємстві навіть хороший менеджер навряд чи знає всі характеристики кожного з продуктів, що випускаються, тим більше що їх номенклатура може оновлюватися кожного кварталу, якщо не місяць. Тому дуже важливо, щоб менеджер мав можливість зі свого комп'ютера, підключеного до корпоративної мережі, скажемо У Львові, передати питання клієнта на сервер, розташований в центральному відділенні підприємства в Києві, і оперативно отримати якісну відповідь, що задовольняє клієнта. У такому разі клієнт не звернеться в іншу компанію, а користуватиметься послугами даного менеджера і надалі.

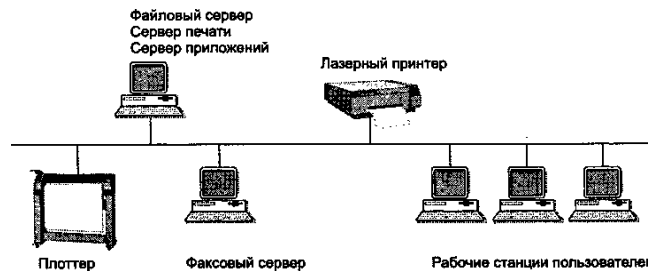
Наявність мережі приводить до **вдосконалення комунікацій** між співробітниками підприємства, а також його клієнтами і постачальниками. Мережі знижують потребу підприємств в інших формах передачі інформації, таких як телефон або звичайна пошта. Корпоративна мережа, яка інтегрує дані і мультимедійну інформацію, може використовуватися для організації аудіо- і відеоконференцій, крім того, на її основі може бути створена власна внутрішня телефонна мережа.

Залежно від масштабу виробничого підрозділу, в межах якого діє мережа, розрізняють мережі відділів, мережі кампусів і мережі підприємств.

**Мережі відділів** — це мережі, які використовуються порівняно невеликою групою співробітників, що працюють в одному відділі підприємства. Вважається, що відділ може налічувати до 100-150 співробітників.

Головною метою мережі відділу є розділення локальних ресурсів, таких як додатки, дані, лазерні принтери і модеми. Зазвичай мережі відділів мають один або два файлові сервери, не більше тридцяти користувачів (мал. 17) і розділяються на підмережі. У цих мережах локалізується велика частина трафіку підприємства. Мережі відділів зазвичай створюються на основі якої-небудь однієї мережевої

технології — Ethernet, Token Ring. Для такої мережі характерний один або максимум два типи операційних систем. Невелика кількість користувачів бачать можливим використання в мережах відділів однорангових мережевих ОС, таких, наприклад, як Windows 98.

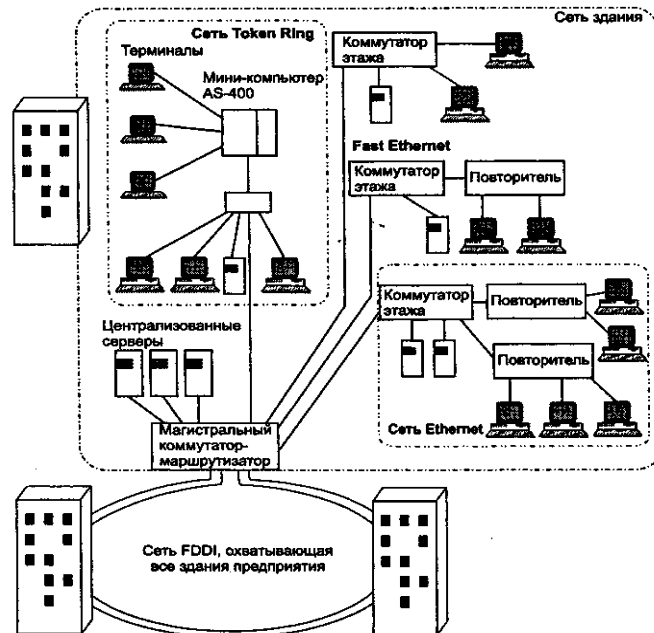


Мал. 17. Приклад мережі масштабу відділу

Існує і інший тип мереж, близький до мереж відділів, — **мережі робочих груп**. До таких мереж відносять зовсім невеликі мережі, що включають до 10-20 комп'ютерів. Характеристики мереж робочих груп практично не відрізняються від описаних вище характеристик мереж відділів. Такі властивості, як простота мережі і однорідність, тут виявляються найбільшою мірою, тоді як мережі відділів можуть наближатися в деяких випадках до наступного по масштабу типу мереж — мереж кампусів.

**Мережі кампусів** отримали свою назву від англійського слова **campus** — студентське містечко. Саме на території університетських містечок часто виникала необхідність об'єднання декількох дрібних мереж в одну велику мережу. Зараз цю назву використовують для позначення мереж будь-яких підприємств і організацій.

Головними особливостями мереж кампусів є те, що вони об'єднують безліч мереж різних відділів одного підприємства в межах окремої будівлі або в межах однієї території, що покриває площу в декілька квадратних кілометрів. При цьому глобальні з'єднання в мережах кампусів не використовуються. Важливою службою, що надається мережами кампусів, стає доступ до корпоративних баз даних незалежно від того, на яких типах комп'ютерів вони розташовуються.



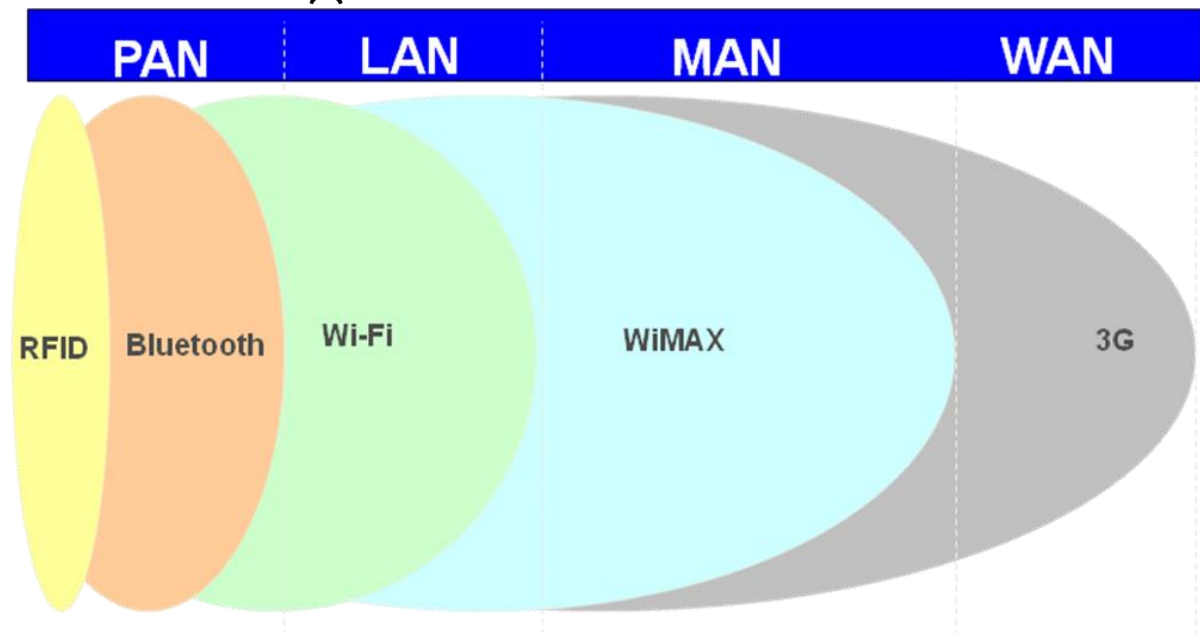
Мал. 18. Приклад мережі кампусів

Корпоративні мережі називають також мережами масштабу підприємства. **Мережі масштабу підприємства** (корпоративні мережі) об'єднують велику кількість комп'ютерів на всіх територіях окремого підприємства. Вони можуть бути складно зв'язані і покривати місто, регіон або навіть континент. Число користувачів і комп'ютерів може вимірюватися тисячами, а число серверів — сотнями, відстані між мережами окремих територій можуть виявитися такими, що використання глобальних зв'язків стає необхідним. Неодмінним атрибутом такої складної і великомасштабної мережі є високий ступінь неоднорідності (гетерогенності) — не можна задовольнити потреби тисяч користувачів за допомогою однотипних програмних і апаратних засобів. У корпоративній мережі обов'язково використовуються різні типи комп'ютерів — від мейнфреймів до персональних, декілька типів операційних систем і безліч різних застосувань. Неоднорідні частини корпоративної мережі повинні працювати як єдине ціле, надаючи користувачам по можливості зручний і простий доступ до всіх необхідних ресурсів.

Поява корпоративних мереж — це хороша ілюстрація відомого філософського постулату про перехід кількості в якість. При об'єднанні окремих мереж крупного підприємства, що має філії в різних містах і навіть країнах, в єдину мережу багато кількісних характеристик об'єднаної мережі перевершують деякий критичний поріг, за яким починається нова якість. У цих умовах існуючі методи і підходи до вирішення традиційних завдань мереж менших масштабів

для корпоративних мереж виявилися непридатними. На перший план вийшли такі завдання і проблеми, які в мережах робочих груп, відділів і навіть кампусів або мали другорядне значення, або взагалі не виявлялися. Прикладом може служити просте (для невеликих мереж) завдання ведення облікових даних про користувачів мережі.

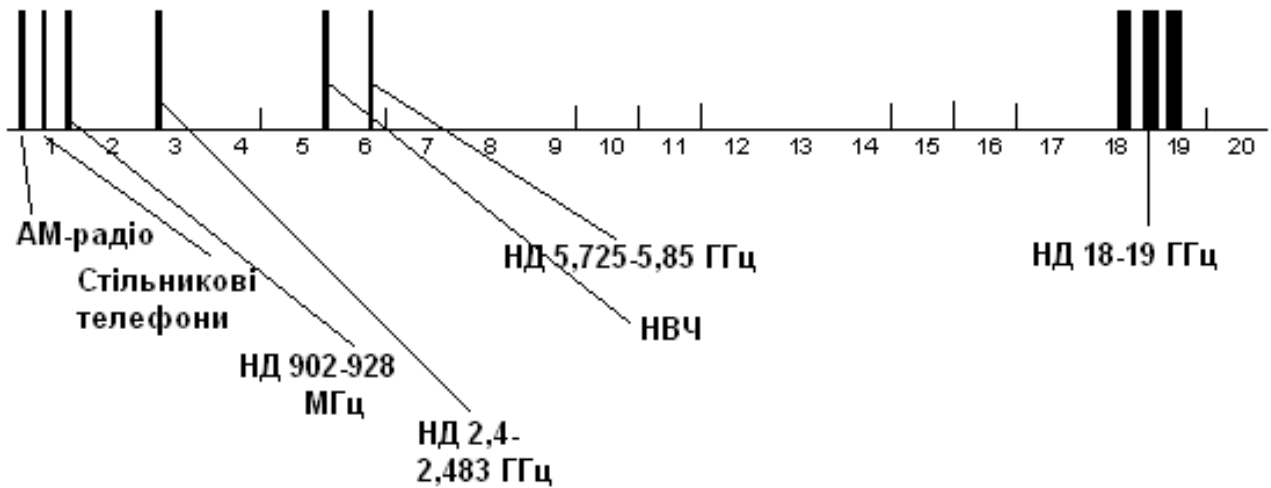
## 2.5. БЕЗПРОВОДОВІ МЕРЕЖІ



Існуючі бездротові технології.

**Залежно від технології передавання розрізняють такі класи мереж:**

- Лазерні (інфрачервоні системи)
- З використанням радіосигналів
  - а) з розподіленим спектром
  - б) з вузькосмуговим спектром
- Мікрохвильові (надвисокі частоти)
- Стільникові (аналогові PDS, GSM та цифрові CDMA, LTE, WiMAX)
- Радіорелейні
- З системою SST (Spread Spectrum Technology)
- системи VSAT (Very Small Aperture Terminal) 260 суп.
- Системи з використанням низькоорбітальних супутників LEO (Low Earth Orbit)



Частотні діапазони для бездротових мереж.

Розглянемо мережу WiFi (**Wi-Fi**, **WiFi** (від англ. *Wireless Fidelity*) — торгова марка, що належить Wi-Fi Alliance. Загальновживана назва для стандарту бездротового (радіо) зв'язку передачі даних, який об'єднує декілька протоколів та ґрунтується на сімействі стандартів IEEE 802.11)

### Реалізовані стандарти:

#### 802.11b

- частотний діапазон — 2,4 ГГц;
- число частотних каналів, які не перетинаються — 3;
- модуляція — ССК (Complementary Code Keying), 22 МГц на канал, одна несуча;
- метод доступу — CSMA/CA;
- максимальна швидкість передачі даних — 11 Мбіт/с.

#### 802.11a

- частотний діапазон — 5 ГГц;
- число частотних каналів, які не перетинаються — 8;
- модуляція — OFDM (Orthogonal Frequency Division Multiplexing), 20 МГц на канал, кілька несучих;
- метод доступу — CSMA/CA;
- максимальна швидкість передачі даних — 54 Мбіт/с.

**802.11g** — використовує модуляцію OFDM в діапазоні 2,4 ГГц (ця специфікація повністю включає в себе 802.11b).

**802.11n** . Максимальна теоретична пропускна здатність — 600 Мбіт/сек. Приріст продуктивності досягається за рахунок системи «безліч входів, безліч виходів» MIMO (паралельне використання декількох приймачів і передавачів для обміну даними по бездротових каналах). Така реалізація дозволяє домогтися кращого охоплення покриття в порівнянні з попередніми стандартами.



- Решта специфікацій визначають:
- 802.11c — таблиці маршрутизації для бездротових «мостів»;
  - 802.11d — міжнародний роумінг у бездротових мережах;
  - 802.11e — технологія QoS (Quality of Service) в застосуванні до бездротових мереж;
  - 802.11f — протоколи для обміну даними між точками доступу (базовими станціями);
  - 802.11h — додаткові вимоги (стосуються європейського регіону);
  - 802.11i — покращені порівняно з базовими стандартами технології захисту даних.
- 802.11a, b, g, n стосуються фізичного рівня середовища передавання; 802.11d, 802.11e, 802.11i та 802.11h — MAC-рівня, решта два — більш високих рівнів (модель OSI).

На даний момент Wi-Fi працює на частоті 2,4 та 5 гігагерц. У вересні 2009 року була офіційно представлена остаточна версія стандарту 802.11n з максимальною швидкістю передачі даних до 600 мегабіт на секунду (802.11g – 54 мегабіт за секунду).

### **Фізичний рівень протоколу 802.11. Технологія DSSS**

- При потенціальному кодуванні інформаційні біти передаються прямокутними імпульсами напруг.
- $\Delta T = 1 / \Delta F$ .
- в технології DSSS в кожний передаваний інформаційний біт (логічний 0 або 1) вмонтовується послідовність так званих чіпів. Кожний окремий чіп — це також прямокутний імпульс, однак його тривалість в декілька разів менша за тривалість інформаційного біта. Оскільки тривалість одного чіпа в  $n$  раз менша за трив. інформаційного біта, то і ширина спектру перетвореного сигналу буде в  $n$ -раз більша від ширини спектру початкового сигналу. При цьому і амплітуда сигналу зменшиться в  $n$  разів.
- Чіпові послідовності називають шумоподібними кодами (PN-послідовностями). Такі сигнали важко відрізнити від природнього шуму.

## Коди Баркера

Сигнали Баркера - це фазо-модульовані сигнали, які можна визначити так:

$$s(t) = \sum_{k=0}^{N-1} q_k f_k(t),$$

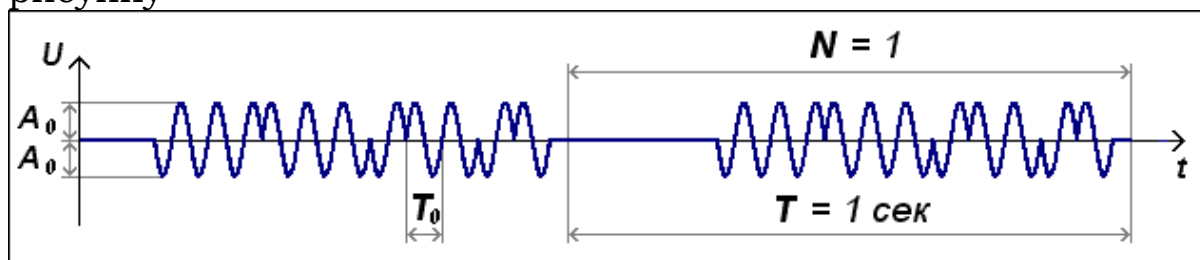
де  $q_k = \pm 1$  (при  $k$  от 0 до  $N-1$ ).

$$f_k(t) = A_0 \sin(\omega t),$$

де  $\omega = 2\pi/T$  – фаза сигналу

$A_0$  – амплітуда сигналу

- Для  $N=11$  сигнал Баркера має форму, показану на рисунку



На MAC-рівні протоколу 802.11 визначено два типи колективного доступу до середовища передавання даних:

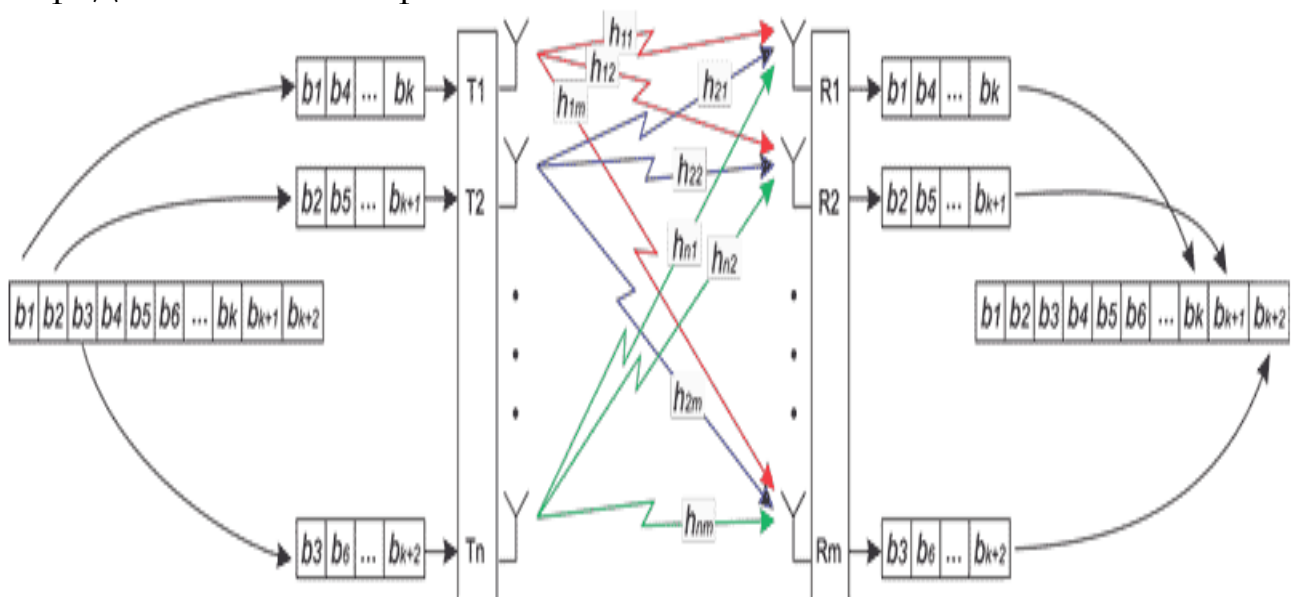
- **функція розподіленої координації (Distributed Coordination Function, DCF).** Базується на методі колективного доступу з виявленням несучої та механізмом уникнення колізій (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA).
- **функція централізованої координації (Point Coordination function, PCF).** Один з вузлів мережі (точка доступу) є центральним і називається центром координації (Point Coordinator, PC), головним завданням якого є задача управління колективним доступом всіх решти вузлів до середовища передачі даних на основі певного алгоритму опитування або керуючись пріоритетами вузлів мережі. Колізії неможливі, і гарантовано пріоритетний доступ до середовища.

Стандарт IEEE 802.11n заснований на технології OFDM-MIMO. Дуже багато реалізовані в ньому технічні деталі запозичені зі стандарту 802.11a, проте в стандарті IEEE 802.11n передбачається використання як частотного діапазону, прийнятого для стандарту IEEE 802.11a, так і частотного діапазону, прийнятого для стандартів IEEE 802.11b/g. Тобто пристрої, що підтримують стандарт IEEE 802.11n, можуть працювати в частотному діапазоні або 5, або 2,4 ГГц, причому конкретна реалізація залежить від країни. Збільшення швидкості передачі в стандарті IEEE 802.11n досягається, по-перше, завдяки подвоєнню ширини каналу з 20 до 40 МГц, а по-друге, за рахунок реалізації технології MIMO.

Технологія MIMO (Multiple Input Multiple Output) припускає застосування декількох передаючих і приймаючих антен. За аналогією традиційні системи, тобто системи з однієї передавальної і однієї приймаючої антеною, називаються SISO (Single Input Single Output).

Теоретично MIMO-система з  $n$  передавальними і  $n$  приймаючими антенами здатна забезпечити пікову пропускну здатність у  $n$  разів більшу, ніж системи SISO. Це досягається за рахунок того, що передавач розбиває потік даних на незалежні послідовності біт і пересилає їх одночасно, використовуючи масив антен. Така техніка передачі називається просторовим мультиплексуванням. Відзначимо, що всі антени передають дані незалежно один від одного в одному й тому ж частотному діапазоні.

Розглянемо, наприклад, MIMO-систему, що складається з  $n$  передавальних і  $m$  приймаючих антен.



- Передавач в такій системі посилає  $n$  незалежних сигналів, застосовуючи  $n$  антен. На приймальному боці кожна з  $m$  антен отримує сигнали, які є суперпозицією  $n$  сигналів від всіх передавальних антен. Таким чином, сигнал  $R_1$ , приймається першим антеною, можна представити у вигляді:

$$R_1 = h_{11}T_1 + h_{21}T_2 + \dots + h_{n1}T_n$$

Записуючи подібні рівняння для кожної прийомної антени, отримаємо наступну систему:

$$\begin{cases} R_1 = h_{11}T_1 + h_{21}T_2 + \dots + h_{n1}T_n; \\ R_2 = h_{12}T_1 + h_{22}T_2 + \dots + h_{n2}T_n; \\ \dots \\ R_m = h_{1m}T_1 + h_{2m}T_2 + \dots + h_{nm}T_n. \end{cases}$$

Або, переписавши даний вираз в матричному вигляді:

- $[R] = [H] \cdot [T]$

де  $[H]$  - матриця переносу, що описує MIMO-канал зв'язку.

Для того щоб на приймальній стороні декодер міг правильно відновити всі сигнали, він повинен перш за все визначити коефіцієнти  $h_{ij}$ , які характеризують кожний з  $m$  х  $n$  каналів передачі. Для визначення коефіцієнтів  $h_{ij}$  в технології MIMO використовується преамбула пакета. Визначивши коефіцієнти матриці переносу, можна легко відновити переданий сигнал:

$$[T] = [H]^{-1} \cdot [R]$$

де  $[H]^{-1}$  - обернена матриця переносу.

- Важливо відзначити, що в технології MIMO застосування декількох передаючих і приймаючих антен дозволяє підвищити пропускну здатність каналу зв'язку за рахунок реалізації кількох просторово рознесених підканалів, при цьому дані передаються в одному і тому ж частотному діапазоні.

Технологія MIMO ніяк не зачіпає метод кодування даних і в принципі може використовуватися в поєднанні з будь-

якими методами фізичного та логічного кодування даних.

У стандарті 802.11n передбачено **два режими передачі**: стандартний режим передачі (**L**) і режим з високою пропускнуою здатністю (High Throughput, **HT**). У традиційних режимах передачі використовуються 52 частотних OFDM-підканали (піднесучих частот), з яких 48 задіюється для передачі даних, а решта - для передачі службової інформації. У режимах з підвищеною пропускнуою здатністю при ширині каналу в 20 МГц застосовуються 56 частотних підканалів, з яких 52 задіюється для передачі даних, а чотири канали є пілотними. Таким чином, навіть при використанні каналу шириною 20 МГц збільшення частотних підканалів з 48 до 52 дозволяє підвищити швидкість передачі на 8%. При застосуванні каналу подвоєної ширини, тобто каналу шириною 40 МГц, в стандартному режимі передачі мовлення фактично ведеться на здвоєному каналі. Відповідно кількість частот, збільшується вдвічі (104 підканали, з яких 96 є інформаційними). Завдяки цьому швидкість передачі збільшується на 100%.

При використанні 40-мегагерцевого каналу та режиму з високою пропускнуою здатністю застосовуються 114 частотних підканалів, з яких 108 підканалів - інформаційні, а шість - пілотні. Відповідно це дозволяє збільшити швидкість передачі вже на 125%.

Від використовуваної антенної конфігурації напряду залежить швидкість обміну інформацією:

- Конфігурація "4x4" при використанні модуляції 64-QAM забезпечує швидкість до 600 Мбіт/с,
- конфігурація "3x3" при використанні модуляції 64-QAM забезпечує швидкість до 450 Мбіт/с,
- конфігурація "2x3" забезпечить швидкість до 300 Мбіт/с,
- конфігурація "1x2" забезпечить швидкість до 150 Мбіт/с.

## 2.6. Оптичні мережі

#### 3.1. Архітектура програмних засобів. Структура мережевої операційної системи

Як звичайно, описуючи ЛКМ найчастіше розглядають питання пов'язані з обладнанням: адаптерами, файл-серверами, комунікаційним обладнанням тощо. Однак продуктивність їхньої роботи значно залежить і від особливостей програмного забезпечення, тобто від типу операційного середовища (ОС) і наявності спеціальних програмних засобів, що поліпшують роботу мережі. Власне ці програмні засоби дають змогу розділювати ресурси, обмінюватися повідомленнями, аналізувати ситуації у випадках збою та усувати їх, отримувати статистичні дані про завантаженість обладнання, захищати інформацію від несанкціонованого доступу.

Архітектура програмних засобів визначається можливостями апаратних засобів та вибором протоколів передавання даних у мережі. Для побудови глобальних мереж переважно застосовують мережну архітектуру TCP/IP, X.200 та ISO. У регіональних мережах програмне забезпечення в основному також ґрунтується на архітектурі протоколу TCP/IP а також IPX/SPX, XNS та VINES. Програмне забезпечення локальних мереж зорієнтоване на роботу з протоколами TCP/IP, IPX/SPX, PC (IBM), 3COM, LAT та ін.

**Мережева операційна система** лежить в основі будь-якої обчислювальної мережі. Кожен комп'ютер у мережі значною мірою автономний, тому під **мережевою операційною системою** у широкому значенні розуміють сукупність операційних систем окремих комп'ютерів, котрі взаємодіють із метою обміну повідомленнями й розподілу ресурсів за єдиними правилами – протоколами. У вузькому значенні **мережева ОС – це операційна система окремого комп'ютера, яка забезпечує йому можливість працювати у мережі.**



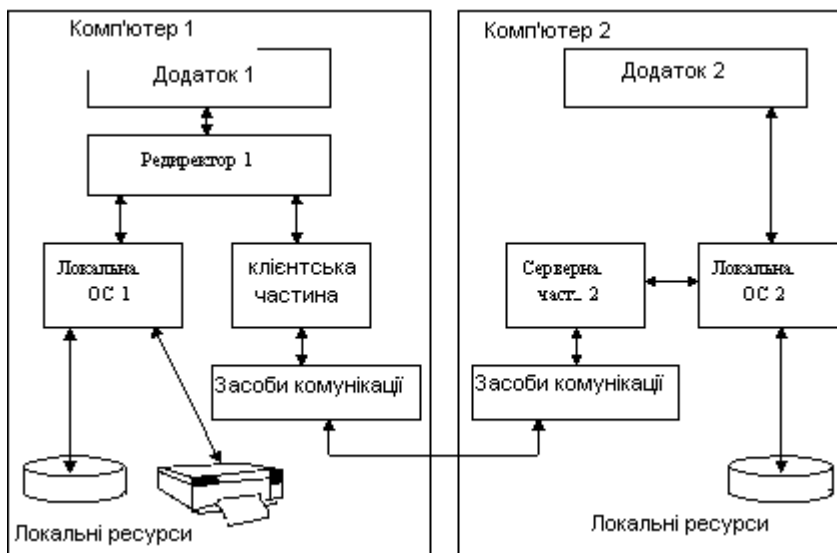
Мал. 3.1. Структура мережної ОС

У мережевій операційній системі окремої машини можна виокремити декілька частин (мал. 3.1):

- Засоби управління локальними ресурсами комп'ютера: функції розподілу оперативної пам'яті між процесами, планування і диспетчеризації процесів, управління процесорами в мультипроцесорних машинах, управління периферійними пристроями та інші функції управління ресурсами локальних ОС.
- Засоби надання власних ресурсів немає і послуг у загальне користування - серверна частина ОС (сервер). Ці засоби забезпечують, наприклад, блокування файлів і записів, що потрібно для їх спільного використання; ведення довідників імен мережеских ресурсів; обробку запитів віддаленого доступу до власної файлової системи та бази даних; управління чергами запитів віддалених користувачів до своїх периферійним пристроїв.
- Засоби запиту доступу до віддалених ресурсів і послуг та його використання – клієнтська частина ОС (редиректор). Ця частина виконує розпізнавання і перенапрявлення до мережі запитів до віддалених ресурсів від додатків і користувачів, при цьому запит йде від додатків у локальної формі, а передається до мережі в іншій формі, яка відповідає вимогам сервера. Клієнтська частина також здійснює прийом відповідей від серверів і перетворення в локальний формат, тобто для додатків виконання локальних та віддалених запитів нерозрізнено.
- Комунікаційні засоби ОС, з допомогою яких відбувається обмін повідомленнями у мережі. Ця частина забезпечує адресацію і буферизацію повідомлень, вибір маршруту передачі повідомлення через мережу, надійність передачі й т.п., тобто є способом транспортування повідомлень.

Залежно від функцій, покладених на конкретний комп'ютер, у його операційній системі може бути відсутня або клієнтська, або серверна частини.

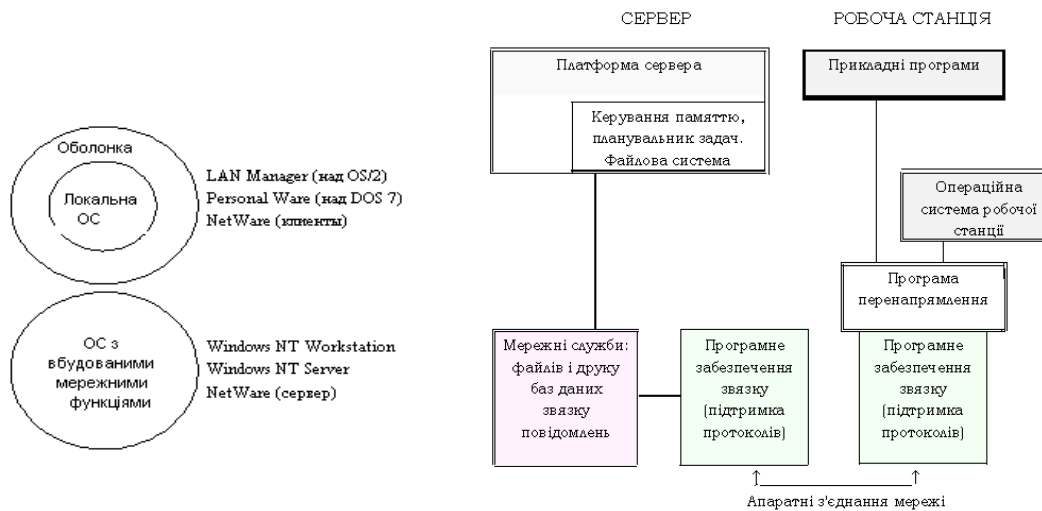
На малюнку 3.2 показана взаємодія мережевих компонентів. Тут комп'ютер 1 виконує роль "чистого" клієнта, а комп'ютер 2 - роль "чистого" сервера, відповідно на першій машині відсутня серверна частина, а в другій – клієнтська. На малюнку окремо показаний компонент клієнтської частини – редиректор. Саме редиректор перехоплює всі запити, які поступають від додатків, і аналізує їх. Якщо видано запит до ресурсу даного комп'ютера, він переадресовується до відповідної підсистеми локальної ОС. Якщо ж це запит до віддаленого ресурсу, він переправляється до мережі. При цьому клієнтська частина перетворює запити з локальної форми в мережевий формат і передає його до транспортної підсистеми, що відповідає за доставку повідомлень зазначеному серверу. Серверна частина ОС комп'ютера 2 приймає запит, перетворює його й передає до виконання своєї локальної ОС. Після отримання результату, сервер звертається до транспортної підсистеми і направляє відповідь клієнту, який видав запит. Клієнтська частина перетворює результат у відповідний формат і адресує його додатку, який видав запит.



Мал. 3.2. Взаємодія компонентів ОС при взаємодії комп'ютерів

На практиці склалося кілька підходів побудови мережевих операційних систем (мал. 3.3).





а) загальний підхід  
ОС Novell

б) приклад архітектури

Мал. 3.3. Варіанти побудови мережевих ОС

Перші мережеві ОС виглядали як сукупність існуючої локальної ОС і надбудованої до неї **мережевої оболонки**. Причому у локальну ОС вбудовували мінімум мережевих функцій, необхідних для роботи мережевої оболонки, яка виконувала основні функції мережі. Прикладом такого підходу є використання у кожній машині мережі ОС MS DOS (починаючи з її третьої версії з'явилися такі вбудовані функції, як блокування файлів і записів, необхідних спільного доступу до файлів). Принцип побудови мережевих ОС як мережевої оболонки над локальною ОС використовують і у пізніших ОС, таких, наприклад, як LANtastic чи Personal Ware.

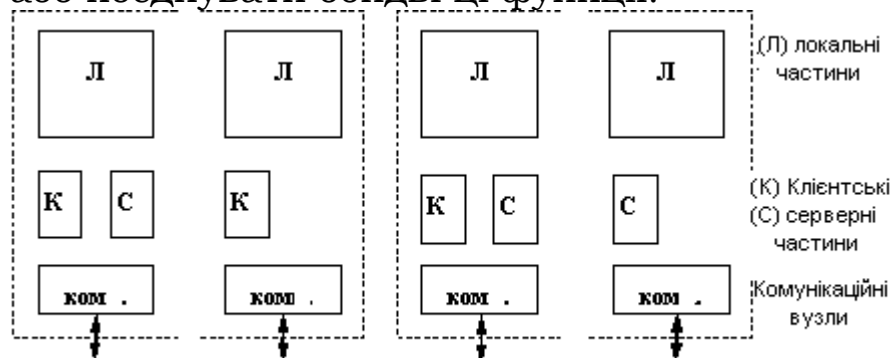
Однак більш ефективним є шлях розробки операційних систем, які спеціально призначені для роботи у мережі. Мережеві функції у ОС подібного типу глибоко вмонтовані в основні модулі системи, що забезпечує їх логічну стрункість, простоту експлуатації і модифікації, а також високу продуктивність. Прикладом такої ОС є система Windows NT фірми Microsoft, яка з допомогою вбудованості мережевих засобів забезпечує вищі наведені показники продуктивності і захищеності інформації у порівнянні з мережевою ОС LAN Manager тієї ж фірми (спільне вироблення з IBM), що є надбудовою над локальною операційною системою OS/2.

### Однорангові мережеві ОС і ОС з виділеними серверами

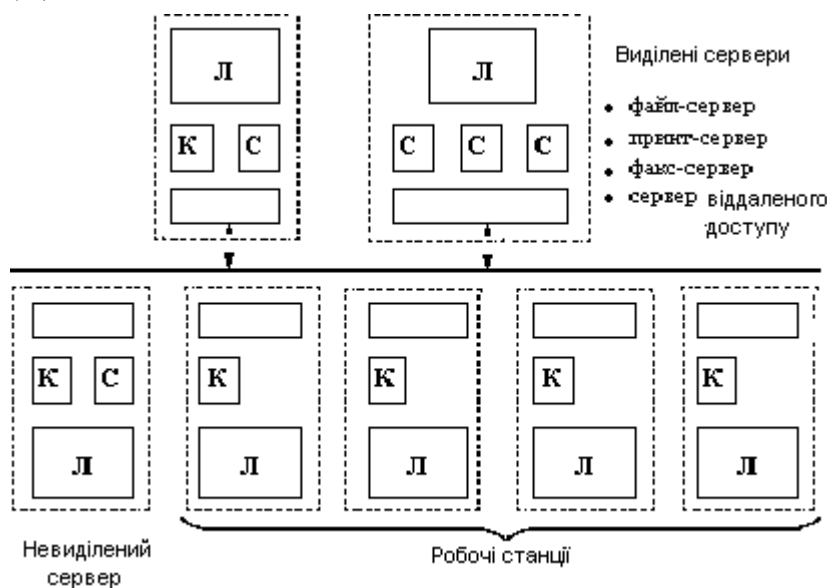
Залежно від того, як розподілені функції між комп'ютерами мережі, мережеві операційні системи, а отже, і мережі

діляться на два класи: однорангові і з виділеними серверами (мал. 3.4).

**Якщо комп'ютер надає свої ресурси іншим користувачам мережі, то він виконує функцію сервера. При цьому комп'ютер, який звертається до ресурсів іншої машини, є клієнтом.** Як було зазначено, комп'ютер, що працює у мережі, може виконувати функції або клієнта, або сервера, або поєднувати обидві ці функції.



(а)



(б)

Мал. 3.4. (а) - однорангова мережа, (б) – мережа з виділеним сервером

Якщо виконання будь-яких серверних функцій є основним призначенням комп'ютера (наприклад, надання файлів для загального користування решті користувачам мережі або організація спільного використання факсу, чи надання всім користувачам мережі можливості запуску на цьому комп'ютері своїх додатків), такий комп'ютер називається **виділеним сервером**. Залежно від того, який ресурс сервера є

поділюваним, він називається файл-сервером, факс-сервером, принт-сервером, сервером додатків тощо.

У виділених серверах бажано встановлювати ОС, спеціально оптимізовані до виконання тих чи інших серверних функцій. Тож у мережах із виділеними серверами найчастіше використовують мережеві операційні системи, до складу яких входить кілька варіантів ОС, що відрізняються можливостями серверних частин. Наприклад, мережева ОС Novell NetWare має серверний варіант, оптимізований до роботи на ролі файл-сервера, а також варіанти оболонок для робочих станцій з різними локальними ОС, причому ці оболонки виконують виключно функції клієнта. Іншим прикладом ОС, яка орієнтована на побудову мережі з виділеним сервером, є операційна система Windows NT. На відміну від NetWare, обидва варіанти даної мережевої ОС – Windows NT Server (для виділеного сервера) і Windows NT Workstation (для робочої станції) - можуть підтримувати функції і клієнта і сервера. Але серверний варіант Windows NT має більші можливості надання ресурсів свого комп'ютера іншим користувачам мережі, оскільки може виконувати ширший набір функцій, підтримує більше одночасних з'єднань з клієнтами, реалізує централізоване управління мережею, має більш розвинені засоби захисту.

Виділений сервер не бажано використовувати для завдань, які не пов'язані з його основним призначенням, оскільки це може зменшити продуктивність його роботи, як сервера. У зв'язку з такими міркуваннями в ОС Novell NetWare для серверної частини можливість виконання звичайних прикладних програм взагалі не передбачена, тобто сервер зовсім позбавлений клієнтської частини, а в робочих станціях відсутні серверні компоненти. Однак у інших мережевих ОС функціонування на виділеному сервері клієнтської частини цілком імовірно. Наприклад, під керівництвом Windows NT Server можуть запускатися звичайні програми локального користувача, які можуть вимагати виконання клієнтських функцій ОС у разі запитів до ресурсів інших комп'ютерів мережі. У цьому робочі станції, у яких встановлено ОС Windows NT Workstation, можуть виконувати функції невиділеного сервера.

Важливо зрозуміти, що попри те, що у мережі з виділеним сервером всі комп'ютери можуть виконувати одночасно ролі й сервера, і клієнта, ця мережа функціонально не симетрична: апаратно і програмно у ній реалізовані два типи комп'ютерів - одні, більшою мірою зорієнтовані на виконання серверних функцій під керівництвом спеціалізованих серверних ОС, інші - переважно виконують клієнтські функції під керівництвом відповідного цьому призначенню варіанта ОС. Функціональна несиметричність, зазвичай, викликає і несиметричність апаратури — для виділених серверів використовують потужніші комп'ютери з більшими обсягами оперативної та зовнішньої пам'яті.

У однорангових мережах всі комп'ютери рівні у правах доступу до ресурсів один одного. Кожен користувач може за власним бажанням оголосити будь-який ресурс свого комп'ютера поділюваним, після чого інші користувачі можуть його експлуатувати. У цих мережах на усіх комп'ютерах встановлюється одна й та сама ОС, що надає всім комп'ютерам у мережі потенційно рівні можливості. Однорангові мережі можуть бути побудовані, наприклад, на базі ОС LANtastic, Personal Ware, Windows for Workgroup, Windows NT Workstation.

У однорангових мережах може виникнути функціональна несиметричність: одні користувачі не бажають розділяти свої ресурси з іншими, і у такому випадку їхні комп'ютери виконують роль клієнта: за іншими комп'ютерами адміністратор закріпив лише функції організації спільного використання ресурсів, отже вони є серверами: у третьому випадку, коли локальний користувач не заперечує використання ресурсів і сам він не виключає можливості звернення до решти комп'ютерів, ОС, що встановлена на його комп'ютері, повинна мати і серверну, і клієнтську частини. На відміну від мереж з виділеними серверами, в однорангових мережах відсутня спеціалізація ОС залежно від переважаючої функціональної спрямованості – клієнта чи сервера. Усі варіації реалізуються засобами конфігурування одного й того ж варіанта ОС.

Однорангові мережі простіші у створенні і експлуатації, але вони застосовуються переважно для об'єднання невеликих груп користувачів, без особливих вимог до обсягів

збереженої інформації, її захищеності від несанкціонованого доступу і до швидкості доступу. При підвищених вимогах до цих характеристик кращими є мережі з виділеним сервером, оскільки його апаратура й мережева операційна система спеціально спроектовані для цієї мети.

## **ОС для робочих груп і ОС для мереж масштабу підприємства**

Мережеві операційні системи мають різні властивості залежно від того, чи призначені вони для мереж масштабу робочої групи (відділу), для мереж масштабу кампусу чи для мереж масштабу підприємства.

- *Мережі відділів* - використовуються невеликою групою співробітників, що вирішують спільні завдання. Головна мета мережі відділу є поділ локальних ресурсів, як-от додатки, дані, лазерні принтери і модеми. Мережі відділів звичайно не поділяються на підмережі.
- *Мережі кампусів* - з'єднують кілька мереж відділів всередині окремої будівлі всередині однієї території підприємства. Ці мережі є все ще локальними мережами, хоч і можуть покривати територію у кілька квадратних кілометрів. Сервіси таких мереж включають взаємодія між мережами відділів, доступ до баз даних підприємства, доступ до факс-серверів, високошвидкісних модемів і високошвидкісних принтерів.
- *Мережі підприємства (корпоративні мережі)* - об'єднують усі комп'ютери всіх територій окремого підприємства. Вони можуть покривати місто, регіон і навіть континент. У цих мережах користувачам надається доступ до інформації та додатків, які є у інших робочих групах, інших відділах, підрозділах і штаб-квартирах корпорації.

Головне завдання ОС, яка використовується у мережі масштабу відділу, є організація поділу ресурсів (додатки, дані, лазерні принтери і, можливо, низькошвидкісні модеми). Зазвичай мережі відділів мають один чи два файлових сервери і не більше 30 користувачів. Завдання управління лише на рівні відділу відносно прості. До завдань адміністратора входить додавання нових користувачів, усунення простих відмов, інсталяція нових вузлів і установка

нових версій програмного забезпечення. Операційні системи мереж відділів добре відпрацьовані й досить різноманітні, як і самі мережі відділів, віддавна застосовувані і налагоджені. Така мережа зазвичай використовує одну чи максимум дві мережні ОС. Найчастіше це мережі з виділеним сервером NetWare4.x чи Windows NT, Windows 2000 або ж однорангова мережа, наприклад мережа Windows for Workgroups .

Наступним кроком у еволюції мереж є об'єднання локальних мереж кількох відділів у єдину мережу будівлі чи групи будинків. Такі мережі називають мережами кампусів. Мережі кампусів можуть сягати кількох кілометрів, і при цьому глобальні сполучення не потрібні.

Операційні системи, які використовують у мережі кампусу, мають забезпечувати для співробітників одних відділів доступ до деяких файлів та адміністративних ресурсів мереж інших відділів. Послуги, надані ОС мереж кампусів, не обмежуються простим поділом файлів і принтерів, а часто надають доступ і до серверів інших типів, наприклад, до факс-серверів і до серверів високошвидкісних модемів. Важливим сервісом, наданих операційними системами даного класу, є доступ до корпоративних баз даних, незалежно від того, розташовуються вони на серверах баз даних чи мінікомп'ютерах.

На рівні мережі кампусу починаються проблеми інтеграції. У загальному випадку, відділи вже вибрали собі типи комп'ютерів, мережного устаткування й мережеві операційні системи. Наприклад, інженерний відділ може використовувати операційну систему UNIX та мережеве устаткування Ethernet, відділ продажів може використовувати операційні середовища DOS/Novell й устаткування Token Ring. Найчастіше мережа кампусу з'єднує різноманітні комп'ютерні системи, тоді як мережі відділів використовують однотипні комп'ютери.

Корпоративна мережа з'єднує мережі всіх підрозділів підприємства, що є на великих відстанях. Корпоративні мережі використовують глобальні зв'язки (WAN links) для сполучення локальних мереж чи окремих комп'ютерів.

Поруч із базовими сервісами, пов'язані з поділом файлів і принтерів, мережева ОС, яка розробляється для корпорацій,

повинна підтримувати ширший набір сервісів, куди зазвичай входять поштова служба, засоби колективної роботи, підтримка віддалених користувачів, факс-сервіс, обробка голосових повідомлень, організація відеоконференцій та інших.

Особливого значення набули завдання подолання гетерогенності - у мережі з'явилися численні шлязи, щоб забезпечити узгоджену роботу різних ОС і мережевих системних додатків.

До ознак корпоративних ОС можна віднести також такі особливості.

**Підтримка додатків.** У корпоративних мережах виконуються складні додатки, які потребують для виконання значних обчислювальних потужностей. Такі додатки поділяються на кілька частин, наприклад, на одному комп'ютері виконується додаток, що пов'язаний з виконанням запитів до бази даних, на іншому - запитів до файлового сервісу, а в клієнтських машинах - частина, реалізує логіку обробки даних докладання і організує інтерфейс з користувачем. Обчислювальна частина спільних для корпорації програмних систем може бути об'ємною і непідйомною для робочих станцій клієнтів, тому додатки виконуватимуть ефективніше, якщо найбільш складні в обчислювальному відношенні частини перенести на спеціально готовий до цього потужний комп'ютер - *сервер додатків*.

ОС сервера додатків мають забезпечувати високу продуктивність обчислень, отже підтримувати багатониткову обробку, витісняючи багатозадачність, мультипроцесування, віртуальну пам'ять і найпопулярніші прикладні середовища (UNIX, Windows, MS-DOS, OS/2). У цьому плані мережеву ОС NetWare складно зарахувати до корпоративних продуктів, позаяк у ній відсутні майже всі вимоги, які пред'являються до сервера додатків. У той самий час хороша підтримка універсальних додатків у Windows NT власне і дозволяє їй претендувати на місце у світі корпоративних продуктів.

**Довідкова служба.** Корпоративна ОС повинна мати здатність зберігати інформацію про користувачів і ресурси в такий спосіб, щоб забезпечувалося управління нею з однієї центральної точки. Подібно великій організації, корпоративна

мережа потребує централізованого зберігання максимально повної довідкової інформації про себе (починаючи з даних про користувачів, серверах, робочих станціях і закінчуючи даними про кабельної системі). Природно організувати цю інформацію як бази даних. Дані з цієї бази можуть бути затребуваними багатьма мережними системними додатками, насамперед системами управління і адміністрування. Крім цього, така база корисна з організацією електронної пошти, систем колективної роботи, служби безпеки, служби інвентаризації програмного і апаратного забезпечення мережі, та й практично будь-якого великого бізнес-дodatка.

У ідеалі мережева довідкова інформація мусить бути реалізована як єдина база даних, а не бути набіром баз даних, що спеціалізуються з зберіганні інформації того чи іншого виду, як це часто буває у реальних операційних системах. Наприклад, в Windows NT є п'ять різних типів довідкових баз даних. Головний довідник домену (NT Domain Directory Service) зберігає інформацію про користувачів, що використовується з організацією їх логічного входу до мережі. Дані про тих самих користувачів можуть утримуватися в іншому довіднику, використовуваному електронною поштою Microsoft Mail. Ще три бази даних підтримують дозвіл низкорівневих адрес: WINS - встановлює відповідність Netbios-імен IP-адресам, довідник DNS - сервер імен домену - виявляється корисним при підключенні NT-мережі до Internet, і, нарешті, довідник протоколу DHCP використовується для автоматичного призначення IP-адрес комп'ютерів мережі. Ближче до ідеалу перебувають довідкові служби, що їх поставляє фірма Banyan (продукт Streetwork III) і фірмою Novell (NetWare Directory Services), які пропонують єдиний довідник всім мережевим додаткам. Наявність єдиної довідкової служби для мережевої ОС - одне з найважливіших ознак її корпоративності.

**Безпека.** Особливої важливості для ОС корпоративної мережі набувають питання безпеки даних. З одного боку, у великомасштабній мережі об'єктивно існують більші можливості для несанкціонованого доступу - через децентралізацію даних, і велику розподіленість "законних" точок доступу, через велике число користувачів, про благонадійність яких важко сказати, і навіть через великі числа можливих точок несанкціонованого підключення до неї.



З іншого боку, корпоративні бізнес-додатки працюють із даними, які мають життєво важливе значення на шляху успішної роботи корпорації у цілому. І для захисту таких даних в корпоративних мережах поруч із різноманітними апаратними засобами використовують увесь спектр засобів захисту, наданий операційною системою: вибірні чи мандатні права доступу, складні процедури аутентифікації користувачів, програмна шифрація.

До недавнього часу мережеві операційні середовища орієнтувалися на роботу з операційними системами робочих станцій DOS або UNIX.

У DOS-орієнтованих ОС можливе розділення обчислювальних ресурсів (принтерів, твердих дисків); у цьому випадку кожний ПК мережі може користуватися ресурсами будь-якої робочої станції. Це підвищує гнучкість, але погіршує адміністрування і відновлення роботи після збоїв. Недоліком також є те, що ОС займає багато місця в оперативній пам'яті робочої станції (іноді до 400 К).

Функціональні можливості цих ОС майже однакові: меню для вибору режиму, засоби організації черг (однак майже завжди нема e-mail, збору статистики, засобів адміністрування мережі, засобів відновлення). Проте, в ОС 10NET децю з цих засобів є.

UNIX-орієнтовані ОС працюють з несуміщеним файл-сервером (ПК, на якому завантажено тільки ядро ОС). Отже, все навантаження з організації черг, роботи з груповими операціями (транзакціями) під час організації системи обробки даних, блокування ресурсів (локування), припадає власне на ядро ОС, вивільнюючи від цього мережне матзабезпечення робочої станції. В цих ОС матзабезпечення робочих станцій є достатньо простим і займає мало місця в ОП, однак програмне забезпечення файл-сервера порівняно складніше. UNIX - орієнтовані ОС працюють значно швидше від DOS-орієнтованих. Крім того, UNIX-орієнтовані ОС мають більше функціональних можливостей, наприклад: e-mail, підтримку віддалених робочих станцій, роботу з мостами і шлюзами, відновлення роботи після збоїв.

Розглянемо роботу мережного ОС на прикладі ОС фірми NOVELL (рис.16).

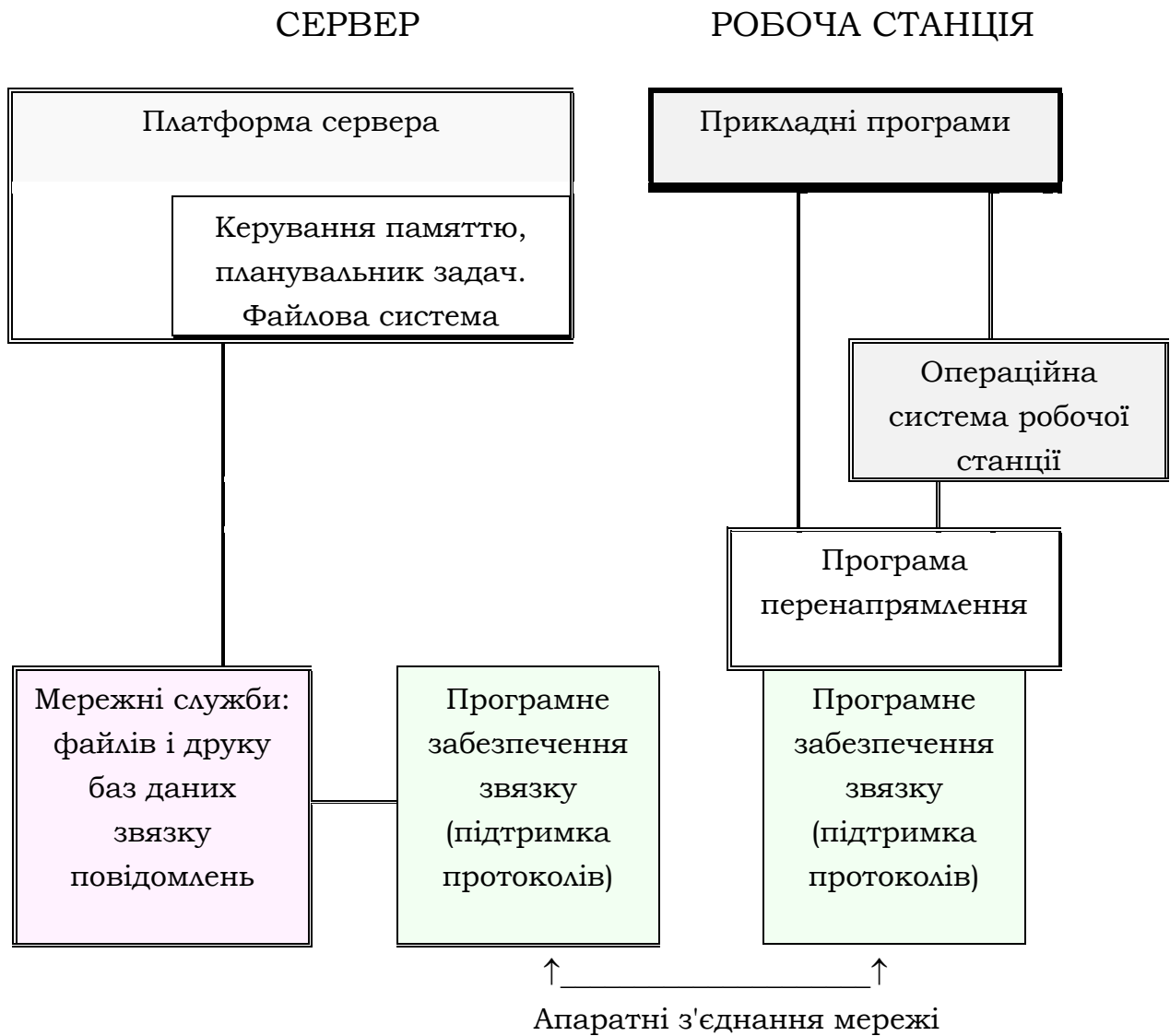


Рис. 16. Архітектура ОС мережі фірми NOVELL.

Компоненти операційного середовища:

- операційна система сервера;
- прикладні програми клієнт-сервера;
- програмне забезпечення зв'язку робочих станцій.

Ці компоненти, взаємодіючи між собою, організовують мережне середовище, яке забезпечує користувачам доступ до засобів мережі.

ОС сервера забезпечує виконання базових функцій, необхідних для підтримки основних операцій мережі (підтримка файлової системи, керування пам'яттю, планування задач).

Прикладні програми клієнт-сервера виконуються в середовищі ОС сервера, забезпечуючи мережу додатковими функціональними можливостями (блокування файлів та

записів, підтримка запитів мови SQL до сервера баз даних та ін.).

Зв'язок між ОС робочої станції і мережною ОС сервера відбувається за допомогою мережного комунікаційного обладнання, яке використовує апаратні засоби мережі для налагодження зв'язку з іншими вузлами і серверами цієї мережі. Комунікаційне програмне забезпечення підтримує протоколи зв'язку, які дають змогу передавати по мережі запити і приймати відповіді на них. Користувачі та прикладні програми одержують доступ до серверів за допомогою програм забезпечення зв'язку, які виконуються на робочих станціях.

Програмне забезпечення зв'язку з мережею встановлюють на робочих станціях користувачів разом з ОС робочими станціями (DOS, OS/2, UNIX, Windows, Macintosh). Звертання прикладних програм і команди користувачів передають за допомогою мережних протоколів. Мережні протоколи можна розділити на три групи: протоколи середовища передавання, транспортні протоколи і протоколи клієнт-сервера. Всі вони працюють взаємопов'язано. Детальніше про основні з них див. §1.7.

### **3.2. Головні мережеві операційні середовища**

Кількість ОС приблизно така ж, як і кількість ЛКМ. Точної відповідності не існує, оскільки ОС є більш гнучкими середовищами і можуть функціонувати в мережах різного типу. Основними характеристиками ОС мереж є: взаємне використання та розподіл ресурсів, наявність суміщеного чи несуміщеного файл-серверів, віддаленого доступу, інтерфейсу ПК з різними ОС.

У 90-і роки минулого століття практично всі операційні системи, що займають помітне місце на ринку, стали мережевими. Мережеві функції вбудовуються в ядро ОС, будучи її невід'ємною частиною. У ОС використовуються засоби мультиплексування декількох стеків протоколів, за рахунок якого комп'ютери можуть підтримувати одночасну роботу з різнорідними серверами і клієнтами. З'явилися спеціалізовані ОС, наприклад, мережева ОС IOS компанії Cisco System, що працює в маршрутизаторах. У другій половині 90-х років усі виробники ОС посилили підтримку засобів роботи з інтерфейсами. Крім стека протоколів TCP / IP

в комплект поставки почали включати утиліти, що реалізують популярні сервіси Інтернету: telnet, ftp, DNS, Web та ін

Особлива увага приділялася в останньому десятилітті і приділяється в даний час корпоративним мережевим операційним системам. Це одне з найбільш важливих завдань у найближчому майбутньому. Корпоративні ОС повинні добре і стійко працювати у великих мережах, які характерні для великих організацій (підприємств, банків тощо), що мають відділення в багатьох містах і, можливо, в різних країнах. Корпоративна ОС повинна без проблем взаємодіяти з ОС різного типу і працювати на різних апаратних платформах. Зараз визначилася літери у класі корпоративних ОС - це MS Windows 2000/2003/2008/2012 ([Server 2003](#) · [Server 2008](#) ([Server 2008 R2](#) · [HPC Server 2008](#)) · [Home Server](#) ([Home Server 2011](#)) · [Essential Business Server](#) · [MultiPoint Server](#) · [Small Business Server](#)), UNIX і Linux-системи, а також Novell NetWare 6.5. Розглянемо деякі з них.

**Мережні операційні системи ОС Unix.** UNIX є дуже потужна, гнучка і динамічна операційна система, котра може обробляти будь-яке запропоноване користувачем завдання. Володіє широким набором запропонованих засобів, з допомогою яких можна вирішити більшість проблем, які виникають при роботі з інформаційними технологіями. Перевагою UNIX є потужність роботи, стабільність і надійність, повна автоматизація, і навіть підтримка безлічі мов програмування.

Ця операційна система пропонує оптимальні рішення роботи з Internet, зокрема доступу до ресурсів Web, Telnet, FTP, баз даним тощо. Оскільки система UNIX створювалася спеціально для обробки великих масивів даних, і повної інтеграції з мережевим середовищем, вона практично завжди перевершує по швидкодії будь-яку іншу комбінацію апаратного та програмного забезпечення. Linux є версією UNIX, адаптованою для процесорів Intel.

**ОС NetWare фірми Novell.** Novell була однією із перших компаній, які почали створювати ЛКМ. У якості файлового сервера в NetWare можна використовувати звичайний ПК, мережева ОС якого здійснює управління роботою ЛКМ. Функції управління включають координацію робочих станцій та регулювання процесу поділу файлів і принтера в ЛКМ. Мережеві файли всіх робочих станцій зберігаються на

жорсткому диску файлового сервера, а не на дисках робочих станцій. Найкращими вважаються продукти NetWare 6.x

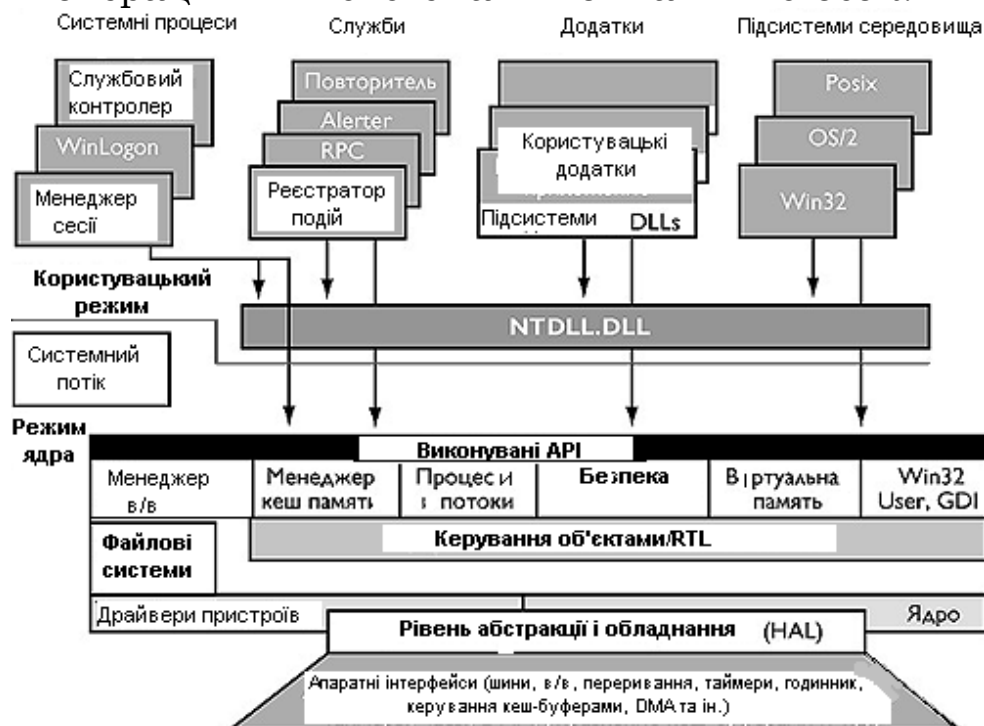
Основна відмінність NetWare 6 від попередніх версій пов'язано з портуванням в ядро NetWare більшого обсягу POSIX - коду з метою портування на платформу NetWare 6 популярних UNIX програм, таких як WEB Server [Apache](#) , SQL сервера [MySQL](#) , [Php](#) , [SSH](#) та інших додатків. Саме це дозволило зрушити нарешті історію операційної системи з мертвої точки. З випуском в жовтні [2001](#) NetWare 6, зміни були продовжені: була додана поліпшена підтримка симетричної багатопроцесорної обробки ( [SMP](#) - кілька процесорів в одному сервері), iFolder (синхронізація файлів локальної папки з сервером та надання захищеного доступу до них в локальній мережі і через Інтернет ), iManager (веб-утиліта адміністрування NetWare та інших продуктів), Native File Access Pack (NFAP - компонент, що надають доступ до ресурсів сервера NetWare клієнтам Windows, Macintosh і [UNIX](#) -подібних систем за протоколами відповідних мереж), NetDrive (утиліта, що дозволяє призначати букви дисків на [HTTP](#) - і [FTP](#) -ресурси, а також на сервери iFolder), а також веб-сервер за замовчуванням був замінений з Netscape Enterprise Server на [Apache](#) .

У 2005 році Novell була запущена серія мережевої операційної системи [Open Enterprise Server](#) (OES), щоб допомогти безболісно мігрувати численним користувачам NetWare на сучасну ОС. OES включає в себе Novell NetWare, [SUSE Linux Enterprise Server](#) і набір мережевих служб. Продукт був розроблений таким чином, щоб обидві операційні системи могли взаємодіяти одна з одною, а клієнти могли створювати змішані середовища для оптимального задоволення своїх потреб. У тому числі створювати змішані кластери, в яких ресурси при збої можуть переміщатися з сервера NetWare на сервер Linux і навпаки.

Тестування ОС за допомогою спеціальних тестів (створення, послідовний запис, випадкове читання і випадковий запис великого файла) засвідчило, що найбільші функціональні можливості і добрі часові характеристики має ОС NetWare. Не дивно, що власне ця ОС викликає найбільший інтерес (у Львівському університеті ім.І.Франка на початку функціонування локальної мережі була встановлена власне така ОС, спочатку v.3.11, потім v.3.12 та v.4.10).

## Мережеві ОС фірми Microsoft.

**Мережева ОС Windows NT.** Спочатку Windows NT існувала двох версіях: **Windows NT Advanced Server** встановлювалася на серверах мережі NT, а **Windows NT Workstation** являла собою потужну настільну операційну систему з функціональними можливостями. Наступна версія Windows NT, призначена для використання на серверах, було перейменована в Windows NT Server. Висока продуктивність і поліпшена підтримка додатків зробили її однією з найбільш популярних операційних систем. Windows NT 4.0 об'єднувала у собі поліпшену інтеграцію з Internet і корпоративними мережами, підвищену продуктивність, відмінну сумісність з іншими операційними системами компанії Microsoft.



Мал.1.5. Структурна схема ОС Windows NT .

## Сімейство програмних продуктів Microsoft Windows 2000 Server

Сімейство програмних продуктів Windows 2000 Server – є наступним поколінням серії операційних систем **Windows NT Server**, у якому надійні, зручні до роботи в Інтернеті служби каталогу, мережеві служби й служби додатків, поєднані з потужним комплексним управлінням.

**Windows 2000 Server** - для серверів робочих груп, і відділів.

**Windows 2000 Advanced Server** - для додатків і більш надійних серверів відділів.

**Windows 2000 Datacenter Server** - для найвідповідальніших систем обробки даних.

### **Сімейство програмних продуктів Windows Server 2003**

Сімейство програмних продуктів Windows Server 2003 є наступним поколінням серверних операційних систем Windows. Windows Server 2003 продовжена в Windows 2000 Server. Вона є платформою високої продуктивності для підтримки зв'язаних додатків, мереж, і веб-служб XML для робочих груп, відділів будь-якого розміру.

Склад Windows Server 2003: **Windows Server 2003 Standard Edition** - це мережева операційна система підприємств бізнесу і окремих підрозділів організації.

**Windows Server 2003 Enterprise Edition** покликана задовольнити загальні ІТ-потреби.

**Windows Server 2003 Datacenter Edition** призначена для рішення відповідальних завдань, які потребують дуже високого рівня масштабованості, доступності та надійності.

**Windows Server 2003 Web Edition** – це операційна система для Web-серверів.

**Microsoft Windows Server 2008.** Windows Server 2008 — це операційна система нової генерації. У основу Windows Server 2008 покладено операційна система Windows Server 2003. Вона розроблена для забезпечення користувачів найбільш продуктивною платформою, що дозволяє розширити функціональність додатків, мереж, і веб-служб, від робочих груп до центрів даних. При спільному використанні клієнтських комп'ютерів Windows Vista і серверів під Windows Server 2008 значно підвищується продуктивність, надійність мережі.

**Windows Small Business Server 2011 Essentials** (SBS 2011 Essentials) - це нове, просте у використанні рішення для компаній, які купили перший сервер, тобто невеликим компаніям, чисельність користувачів в яких не перевищує 25 осіб. Це рішення можна легко інтегрувати з такими службами, як Office 365 і рішення хмарного резервного копіювання даних і управління хмарою.

SBS 2011 Essentials забезпечує технології корпоративного класу для вирішення завдань резервного копіювання і відновлення даних, забезпечення віддаленого доступу, надання спільного доступу до файлів і принтера, а також



швидке підключення до хмари в одному інтегрованому рішенні.

**Windows Server 2012** (кодове ім'я «Windows Server 8») — версія серверної операційної системи від Microsoft, що вийшла у 2012 році на заміну [Windows Server 2008 R2](#). Windows Server 2012 — перша версія Windows Server починаючи з [Windows NT 4.0](#), яка не підтримує Itanium процесори. Windows Server - провідна серверна операційна система, на якій побудована робота багатьох найбільших центрів обробки даних - надає широкі можливості підприємствам будь-якого розміру по всьому світу. Продовжуючи найкращі традиції, Windows Server 2012 містить сотні нових і вдосконалених функцій, які дозволяють трансформувати ІТ-середовища віртуалізації і хмарних обчислень з метою скорочення витрат на ІТ та збільшення цінності для бізнесу. У Windows Server 2012 реалізовані вражаючі інновації в області віртуалізації, мережових технологій, систем зберігання даних і зручності роботи.

*Основні удосконалень:* новий користувацький інтерфейс **Metro UI**. 2300 нових команд [Windows PowerShell](#). Вдосконалений Диспетчер завдань. Тепер Server Core рекомендований варіант установки, а перемикання між режимами з класичним робочим столом і режимом Server Core може бути виконано без перевстановлення сервера. Нова роль IPAM (IP address management) для управління і аудиту адресним простором IP4 і IP6. Удосконалень в службі [Active Directory](#). Нова версія Hyper-V. Нова файлова система ReFS (Resilient File System). Нова версія IIS 8.0 (Internet Information Services).

Одним з нововведень нової Windows Server 2012 є *нова розробка корпорації - Storage Spaces*, яка пропонує можливість системним адміністраторам, що працюють з цією ОС, керувати великим числом систем зберігання даних, підключеними через інтерфейс SAS. Цікаво, що завдяки Storage Spaces немає необхідності використовувати додаткове програмне забезпечення. Технологія Storage Spaces дає можливість об'єднання більше 10 жорстких дисків в єдиний пул з можливістю поділу вмісту цього пулу дисків на численні віртуальні диски.

У нової серверної ОС додана служба *Dynamic Access Control*. Робота даної служби спрямована на поліпшення централізованого захисту на рівні доменів файлів, а також на



забезпечення безпеки папок поверх всіх наявних дозволів файлів.

**МАШТАБОВАНІСТЬ.** Windows server 2012 підтримує наступне апаратне забезпечення

<b>Spec</b>	<b>Windows Server 2012</b>	<b>Windows Server 2008 R2</b>
Фізичних <a href="#">процесорів</a>	64	64
Логічних процесорів з вимкненим Hyper-V	640	256
Логічних процесорів з увімкненим Hyper-V	320	64
<a href="#">ОЗП</a>	4 <a href="#">ТБ</a>	2 <a href="#">ТБ</a>
Failover cluster nodes	64	16

Windows Server 2012 має 4 редакції: Foundation, Essentials, Standard и Datacenter

З добрими часовими характеристиками є **ОС NEXOS**, яка з'явилася на європейському ринку в 1990 р. Поставляє її американська фірма Carolina Microelectronic System (CMS). Вона, як і NetWare, є файл-сервер-орієнтованою і подібна до неї за ідеологією. Користувачі NetWare мають змогу безпосередньо звертатись до файл-сервера, що працює під керуванням ОС NEXOS.

Засоби комунікації ОС NEXOS підтримують протоколи TCP/IP, X.25, дають змогу працювати з асинхронним шлюзом. ОС допускає використання робочої станції без "вінчестерів" (завантаження відбувається з мікросхеми адаптера мережі BOOTROM). ОС NEXOS просто встановлювати і вона дешевша від NetWare. Цю ОС можна ефективно використовувати для невеликих ЛКМ, де не потрібні великі потужності NetWare, але потрібні високі швидкості обробки інформації і нема достатньо кваліфікованого обслуговуючого персоналу.

**VINES-4.0** на базі ОС UNIX створила компанія Banyan. Вона добре підходить до великої мережі з багатьма серверами або коли потрібно з'єднувати між собою територіально віддалені ЛКМ. Основою такої мережі є міжмережний

протокол VIN (VINES Internet Protocol), який використовує датаграмний принцип передавання пакетів.

Характерною відмінністю для VINES-4.0 є наявність Street Talk (розподілу імен), що робить її апаратно незалежною, а також нова підсистема підвищення ефективності роботи з каталогами Directory Assistance. Служба Street Talk розподіляє єдину базу даних користувачів, груп та ресурсів між усіма серверами ЛКМ, так що Вам не потрібно робити будь-які зміни в правах доступу до мережі більше одного разу (навіть переїхавши в інше місто, вводите дані зі стримера у файл-сервер і продовжуєте роботу з того місця, де вона була перервана).

Служба Directory Assistance забезпечує ведення в кожній мережі копії повного каталогу Street Talk для всієї глобальної мережі (якщо немає зв'язку між мережами, то повідомлення запам'ятовується і буде передане, як тільки зв'язок відновиться).

Недоліки мережі VINES:

- 1) система не передбачає можливості дублювання - резервування накопичувача сервера для страхування від збоїв;
- 2) малий резерв оперативної пам'яті, оскільки драйвери мережі займають багато місця (108 Кбайт). Детальніше див.[1, 16, 18].

На закінчення зазначимо, що в міру того, як бізнес стає щораз менше ієрархічним, він потребує щораз гнучкіших обчислювальних систем, які здатні задовольняти вимоги клієнтів, а не жорстких систем, під які повинні підлаштовуватись самі користувачі.

Якщо ресурси розташовані на сервері, то користувачам необхідно знати, де є кожний ресурс, до якого вони хочуть доступити. Функції керування, "прив'язані до сервера", також обмежують свободу доступу до ресурсів головних систем. Ці обмеження саме стали причиною переходу до технології розподіленої обробки даних — мережних обчислень.

### **3.3. Мережні обчислення**

Типове сучасне велике підприємство використовує головні системи, які ґрунтуються на ОС VMS фірми DEC, VM чи MVS фірми IBM, UNIX, а також сервери, подібні до

Netware. Робочі станції використовують ОС DOS, Windows, OS/2, MacOS і UNIX.

Мережні обчислення забезпечують інтеграцію головних і настільних систем користувача в єдину логічну мережу.

Мета — забезпечити прозорість розподілу інформації і обчислювальних функцій між усіма користувачами організації, незалежно від місця їхнього знаходження.

Першою конкретною реалізацією системи мережних обчислень є система NCS (Network Computing Systems) фірми APOLLO. NCS містить визначення протоколів, планувальник (location broker) і компілятор.

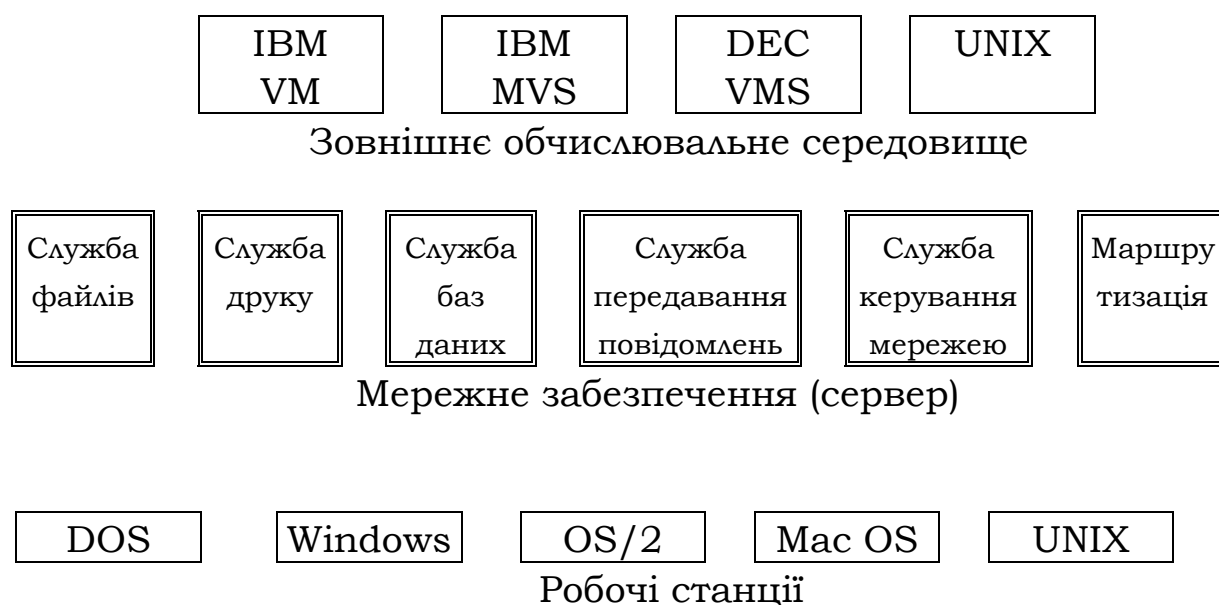


Рис.17. Схема забезпечення взаємодії різних операційних середовищ.

#### 4. СІМ'Я ОПЕРАЦІЙНИХ СЕРЕДОВИЩ NETWARE

##### 4.1 Загальні відомості

ОС Netware розробила фірма NOVELL для мережі NOVELL S-Net з топологією зірки і файл-сервера на базі мікропроцесора MC6800. З появою IBM PC виявилось, що його легко можна перенести на Intel 8088. Перша версія ОС Netware з'явилася на ринку в 1983 р., потім була V 1.0, а в 1986 р. – вже версія 2.0 на базі Intel 286, яка давала змогу використовувати пам'ять понад 1 Мбайт, додаткові (VAP) процеси, а також приєднувати різні мережі через комп'ютери (мости). У 1987 р. з'явилася версія SFT Netware,

в якому вже були засоби захисту від збоїв, тоді ж виникла версія 2.1 з розширеною можливістю адміністрування мережі, а в 1988 р. випущені версії 2.15 і Macintosh. Останні версії давали змогу приєднувати до сервера чи робочої станції до 16 принтерів, причому один принтер можна було використовувати в кількох мережах (принт-сервер).

З вересня 1989 р. у продажі є V3.0 (Intel 386). Цю систему NOVELL розробила як майбутній стандарт для великих локальних мереж і користувачів, які активно працюють. Може працювати і на процесорах Intel 486. У 1990 р. з'явилася V3.1, яка дає змогу адмініструвати віддалені мережі. Дещо вдосконалені версії ОС, які зараз в основному експлуатують – V3.11 та V3.12. В стадії активного впровадження версія 4.10.

Є розробки для великих машин: ОС Netware for VMS для сім'ї VAX фірми DEC, ОС Portable Netware для EOM під керуванням UNIX, VMS чи OS/2.

#### **4.2 Програмне забезпечення файл-сервера та робочих станцій. Багатосерверні мережі.**

а) Програмне забезпечення файл-сервера. Є кілька варіантів програмного забезпечення файл-сервера. Їхня класифікація залежить від двох ознак: які засоби вони надають до використання і які їхні функціональні можливості. Найпоширеніші на сьогодні в основному дві версії Netware: — v.3.11(3.12) та v.4.10. Netware v.3.11 як і її попередниця v2.2 ідеально підходить для дрібних та середніх підприємств а також для робочих груп всередині великих компаній. Програмне забезпечення працює на PC з процесором Intel 386 та іншими, що програмно сумісні з ним.

Якщо ОП є достатньо (1,5 Мбайт і більше), то на файл-сервері в основній пам'яті може працювати паралельно з ОС користувач в DOS. Такий сервер називається *невиділеним*. Якщо на файл-сервері не передбачена паралельна робота користувача з ОС файл-сервера, то такий сервер називається *виділеним*. Зрозуміло, що на виділеному файл-сервері є більш серйозна система захисту даних. В обох випадках ОС працює краще, коли пам'яті виділено більше 2 Мбайт.

Паралельно до ядра ОС (функції керування мережею, передаванням даних, маршрутизації, служби баз даних, файлів, друку) на файл-сервері можуть виконуватися

додаткові процеси (VAR-процеси), які розробляють за спеціальними правилами. Ці процеси стартують під час завантаження програмного забезпечення файл-сервера і дають змогу ядру прикладної програми клієнт-сервера виконуватися на сервері Netware. В ОС v 3.11 прикладні програми клієнт-сервера виконуються як завантажувальні модулі Netware (NLM), і var-процеси не підтримуються.

У багатьох організаціях ще продовжують експлуатувати ОС Netware v.2.15 для ПК з Intel 286. За можливостями воно мало відрізняється від v.2.20. Важливо те, що воно потребує трохи менше ОП, але в цьому випадку менш надійно працює. Формати запису інформації на диск цих систем збігаються, що дає змогу, якщо потрібно, легко перейти на вищу версію.

Поява потужніших ПК (386,486) зумовила потребу і в оновленні ОС. Кульмінацією цих систем стало ОС Netware V 3.11 (пізніше модифіковане як 3.12), яке забезпечило перехід від мереж робочих груп і відділів до більших мереж, здатних підтримувати сотні користувачів на одному сервері (конфігурації 20, 100, 250 користувачів). Ця система не передбачає роботи користувача на файл-сервері в MS DOS, тобто працює тільки як виділений сервер. Формати драйверів адаптерів мережі і дисків не збігаються з Netware 286 всіх версій. Але ця система набагато ефективніша як за рахунок внутрішньої організації, так і за рахунок використовуваних можливостей 386 процесора. Для нормального функціонування такого ОС потрібно більше ОП (понад 4 Мбайти). ОС Netware V3.11 забезпечує об'єднання в одну мережу міні-ЕОМ, мережних серверів на основі IBM-сумісних ПК, а також робочих станцій під керуванням DOS, WINDOWS, OS/2, UNIX і ОС Macintosh.

В ОС V 3.11 підтримуються протоколи OSI, SPX/IPX, NETBIOS, TCP/IP, AppleTalk та інші. NLM-процеси (NetWare Loadable Module) більш гнучкі в роботі, ніж VAR-процеси, їх можна знімати і запускати в будь-який момент роботи файл-сервера. За технологією NLM-процеси побудовані як драйвери для NetWare386. Підтримка Macintosh в середовищі Netware V 3.11 також реалізована на основі NLM-процесів.

Під керуванням програмного забезпечення файл-сервера можуть працювати і додаткові сервери мережі. Таким додатковим сервером є, наприклад, сервер друку (принт-сервер), який може працювати як на самому файл-сервері,

так і на окремій робочій станції мережі. Він може керувати пристроями, які приєднані як до портів типу LPT і COM сервера, до робочих станцій користувачів мережі так і безпосередньо в мережу через відповідне обладнання.

В одній мережі можуть працювати кілька файл-серверів, причому різних версій і потужностей. Кожний файл-сервер повинен мати своє унікальне ім'я (наприклад, ABC) і серійний номер. Серійний номер унікальний для кожної купленої копії ОС Netware. Два сервери в одній мережі з одним серійним номером працювати не зможуть. Користувач може працювати одночасно з кількома файл-серверами. Щоб приєднатись до іншого файл-сервера, не від'єднуючись від Вашого файл-сервера, достатньо набрати

ATTACH <ім'я сервера>/<ваше ім'я на цьому ф-с>  
<ENTER>

Ресурси кожного сервера користувач отримує незалежно від інших файл-серверів. Це означає, що він повинен пройти незалежну процедуру реєстрації, після чого отримує свої права (доступу до диску, черг друку, права оператора, чи супервізора тощо).

Зазначимо, що NetWare V3.11 – перше мережне ОС, яке підтримує служби файлів і друку на робочих станціях DOS, Macintosh, Windows, OS/2 і UNIX.

б) Програмне забезпечення робочих станцій. Робочі станції у комп'ютерній мережі використовуються як звичайні ПК, а для комунікації з файл-серверами застосовується програмне забезпечення, яке складається з оболонки і протоколу (або драйвера комунікації низького рівня). Це вже відомий нам IPX-протокол, який фактично є мовою, за допомогою якої робочі станції комунікують з файл-серверами. Оболонка NetWare є кількох версій: NET3, NET4, які розраховані на роботу у версіях DOSy V.3.XX і V4.XX відповідно, та NETX, EMSNETX, XMSNETX. Програма NETX працює у всіх версіях MS-DOS і подібних до неї систем.

Оболонка спрямовує запити робочої системи до DOS або до NetWare. Наприклад, якщо запит є команда DOS DIR (перелік файлів у локальній директорії), то його адресують DOSy, якщо запитом є друкування завдання на принтері мережі, то цей запит обслуговує NetWare. (Дія оболонки

подібна до залізничної стрілки, яка скеровує поїзди в потрібному напрямку).

Одне з основних завдань, яке вирішує оболонка, – це відображення дисків мережі на пристрої робочої станції. Варто згадати, що вся інформація в мережі зберігається на жорсткому диску файл-сервера. Ця система зберігання інформації має файлову структуру, яка включає в себе:

- 1) файл-сервери, яких є один або більше;
- 2) томи, які можуть міститися на кількох жорстких дисках і відповідно поділяються на:
- 3) директорії, які можуть містити піддиректорії;
- 4) файли.

Цю файлову систему можна порівняти з шафою-каталогом (сейфом) де сейф – файл-сервер; шухляди, ящики – томи; папки – директорії. Їх можна створювати і знищувати, так само, як Ви виймаєте чи вкладаєте папки до шухляди; піддиректорії – конверти всередині папки – ніби ділять директорії на частини; і нарешті директорії містять файли, так само, як у конвертах є певні документи.

Кожний том має свою незалежну файлову систему, яка зовнішньо подібна до файлової системи MS DOS в розділах локального вінчестера. Але томи файл-сервера мають символні імена, на відміну від розділів MS DOS, які називають буквами латинського алфавіту (C, D, E тощо). Перший том диска файл-сервера переважно називають "SYS:", решта можуть називатися довільно (формується під час створення тома). Кожний файл-сервер має незалежну структуру томів, а тому для вказання унікального дискового тому в мережі застосовують комбінацію імен:

**< сервер > \ < том > :**

Наприклад :   UNI\SYS: - том для системних файлів;  
                  UNI\APPL: - том для прикладних програм;  
                  UNI\HOME:       - том для конкретного користувача.

Однак програмне забезпечення MS DOS орієнтоване на роботу з буквенними ідентифікаторами дискових пристроїв (A, B, C...). Тому для того, щоб ці програми без переробки могли працювати з мережею, оболонка NetWare на робочій станції робить прив'язку імен конкретних томів на файлі-сервері до букв дискових пристроїв на робочій станції. Ця

процедура називається *відображенням* (MAPPING). Наприклад, том UNI\SYS: прив'язується до букви J:. За рахунок такого відображення досягається "прозорість" використання мережі прикладними програмами.

Пояснення: під фразою "відображення дискового тому мережі на букву дискового пристрою робочої станції" потрібно розуміти задання відповідності між іменем тому мережі і буквою дискового пристрою. Це відображення досягається імітацією наявного диска на машині користувача, тому операції прямого читання і записування секторів для такого диска не підтримуються.

### **4.3.Адресація в мережі. Маршрутизація**

Досі ми уявляли собі, що всі машини в мережі приєднані до деякого спільного кабелю і за передавання інформації від машини до машини (наприклад, між файл-сервером і робочою станцією) відповідає апаратна частина мережі. Але може бути й по іншому: Ви маєте різні адаптери мережі, які можуть працювати тільки в незалежних частинах мережі, або ЛКМ має дві незалежні частини (сегменти), які фізично розділені між собою.

ОС NetWare підтримує роботу з такими мережами. У цьому випадку на комп'ютерах, чи спеціальних пристроях, які об'єднують ці сегменти, встановлюють спеціальне програмне забезпечення, яке спільно з апаратною частиною виконує функції *моста* або *маршрутизатора*. Функції маршрутизатора може виконувати безпосередньо і файл-сервер, якщо до нього приєднати не більше чотирьох сегментів. У середині кожного сегмента адреса станції визначається апаратно заданою адресою адаптера мережі (так звана адреса вузла). Адреси адаптерів у середині сегмента повинні бути унікальними. Так само унікальними повинні бути і номери сегментів у всій мережі. Порушення цього правила призводить до збоїв у мережі. Якщо є кілька сегментів у мережі, то апаратні адреси комп'ютерів можуть повторюватися, а тому для однозначної адресації використовують комбінацію

**< номер сегменту >: < адреса вузла >.**

Можлива ситуація, коли на кожному комп'ютері мережі працює кілька програм, яким потрібний незалежний доступ



до мережі. Для того, щоб інформація, яка надходить у комп'ютер, не переплуталася, до адреси комп'ютера (чи робочої станції) в мережі додають номер так званого *гнізда* (socket). Гніздо є умовним числовим ідентифікатором виду інформації, яка передається чи приймається на конкретний комп'ютер в мережі.

Використання гнізд дещо подібне до багатоканального передавання інформації. Переважно певна кількість гнізд фіксована для різного роду робіт. Наприклад, одне з N гнізд задіяне для запитів оболонки NetWare до файл-сервера, друге — для діагностики мережі, третє — для спілкування файл-серверів між собою і т.д.

#### **4.4 Можливості Netware (основні).**

ОС Netware дає змогу користувачу виконувати два завдання: спільне використання дисків і спільне використання пристроїв виведення інформації, що приєднуються до файл-сервера. Пристрої можуть приєднуватись до портів COM, LPT для виведення на них організованих черг. Користувач може керувати цими чергами а в певних межах, і пристроями сервера. Для програм, що виводять інформацію безпосередньо на локальний принтер, є засоби перескерування цієї інформації на друкарський пристрій файл-сервера. Спільне використання дисків відбувається в прозорому для DOS режимі. Це означає, що прикладне програмне забезпечення може працювати з дисками мережі через звертання до MS DOS так само, як воно працює з локальними дисками комп'ютера користувача. Отже, в мережі можна експлуатувати прикладні програми, не призначені для мережі, без змін (але з деякими обмеженнями).

Використовувати ресурси мережі можуть не тільки користувачі MS DOS, але й користувачі Macintosh, OS/2, Windows та ін.

В ОС Netware добре розвинута система керування доступом. Певний набір прав визначає тип користувача:

- а. *звичайні користувачі* пропускають програми і працюють з файлами згідно з наданими їм правами;

б. *оператори* (оператори файл-сервера, оператор друку, оператор принт-сервера) - це звичайні користувачі, яким надано деякі додаткові права.

в. *менеджери*, або керівники - це користувачі, які відповідають за створення і керування іншими користувачами. Груповий менеджер може створювати і керувати користувачем, менеджер обліку – керувати, але не реєструвати користувачів.

г. *аудитор*

д. *адміністратор мережі* (супервізор) відповідає за нормальне функціонування мережі в цілому, стежить за програмним забезпеченням, змінює його, якщо потрібно.

Однією з найважливіших функцій мережі є система захисту інформації, яку реалізують такі засоби:

1) система охорони входу в мережу (система реєстрації), яка забезпечується завдяки:

- існуванню імен та паролів користувачів;
- криптуванню паролів при передачі їх по мережі;
- керуванню обмеженнями на роботу станції (термін дії пароля, термін реєстрації та ін.);

2) система прав (чи система повноважень) користувача, яка визначає:

- до яких файлів чи директорій можна доступати;
- що з ними можна робити;

3) система атрибутів, що призначається директоріям та файлам і визначає:

- чи можна директорію або файл знищувати, копіювати, переглядати або виконувати в них записи;
- тип доступу до користування — колективний чи виключний.

Для виконання задач NetWare існує велика кількість утиліт (обслуговуючих програм). Усі утиліти поділяють на діалогові (меню-утиліти) та утиліти командного рядка. Меню-утиліти надають весь необхідний сервіс під час безпосередньої роботи користувача за екраном комп'ютера, мають розвинутий віконний інтерфейс.

Утиліти командного рядка дають змогу всі необхідні параметри передати безпосередньо під час виклику з командного рядка. Це дає змогу включати їх у bat-файли і в

цей спосіб переналагоджувати роботу прикладних програм з мережею.

Основні утиліти загального використання розташовані переважно в каталозі SYS:\PUBLIC. Детальніше про функції утиліт та практичну роботу в мережі NetWare див.[13, 15, 21-25].

#### **4.5. Структура серверного диска**

Серверний диск містить DOS-розділ, який необхідний для оперативного керування мережею, і розділ Netware, який і свою чергу містить томи:

- SYS: том для системних файлів (LOGIN, PUBLIC, SYSTEM, MAIL)
- APPL: том для прикладних програм
- HOME: для індивідуального використання конкретними користувачами.

На томі SYS: окрім ОС мережі з відповідними каталогами та файлами не повинно бути жодної іншої інформації. Правда на SYS: зберігаються утиліти керування мережею, до котрих має доступ лише супервізор. Це такі утиліти:

- антивірусне програмне забезпечення
- оболонка користувача з системним інтерфейсом (NC, Norton Utilites)
- дружня оболонка, яка зорієнтована на користувача (наприклад Office)
- резервне програмне забезпечення
- сервер-орієнтовані засоби роботи і задокументування (наприклад tool)

На томі APPL: повинні бути розташовані тільки системні файли програмного забезпечення для користувачів. Том може вести не тільки супервізор, але й спеціаліст з прикладного забезпечення, чи адміністратор мережі. Користувачу на APPL: достатньо прав Read(читати), Search(шукати) і Open(відкривати).

Том HOME: містить робочі каталоги користувачів. Вони повністю надаються користувачам. Власники каталогів на цьому томі можуть отримувати всі права. Все це можливо тільки тоді, коли для кожного користувача створено робочий каталог у мережі, причому кожен користувач може

маніпулювати тільки своїми даними, і не може обробляти чужі. Так створюється том по замовчуванню. Потім власник файлів чи адміністратор можуть по потребі змінювати права доступу.

#### **4.6. Обслуговування сервера. Команди супервізора.**

Ці команди подібні до звичайних команд Netware. В принципі вони можуть застосовуватися з будь-якої робочої станції. Однак зважаючи на те, що виконання таких команд може суттєво вплинути на роботу мережі і безпеку даних, їх включають в каталог SYSTEM (на відміну від PUBLIC для інших), доступ до якого отримує Супервізор, чи довірене йому особа.

Утиліта (команда) CPM OFF (cpmoff) позбавляє користувача відкривати файли. Діє до того часу, коли не буде команди CPM ON (cpmon), або поки не буде перевантажена робоча станція мережі.

Команда EOJ OFF (eojoff) запобігає можливість закриття файлів системою зразу через EOJ (end of job). Використовувати слід обережно - файли можуть закриватися неправильно. А тому можуть бути втрачені. По замовчуванню встановлюється команда EOJ ON (eojon).

Команда HIDEFILE (hilefile<ім'я файла>) робить файл, який заданий, як параметр, невидимим. Він не відображається на екрані при роздруку вмістимого каталогу. За допомогою DOSy Ви не зможете його ні скопіювати, ні стерти. Однак невидимі файли можуть запускатись, як виконувані, оскільки їх імена відомі. Крім того, за допомогою type ім'я файла можна роздрукувати на екрані вміст невидимого у каталозі файла. Команда відміни SHOWFILE (showfile <ім'я файла>)

Команда HOLDON (holdon) здійснює захоплення (перехоплення) файлів при звертанні до них. При цьому файл не може бути використаний ще одним користувачем.

NetWare по замовчуванню відносно файлів є non-share-able, тобто не розділювані і read only, тобто тільки для читання. Внаслідок цього одночасне використання файлів кількома користувачами неможливе. Однак існують прикладні програми, які дозволяють (мають необхідність) кільком користувачам одночасно доступитися до файлів. Для цього власне існує команда NetWare holdon, яка на час модифікації даних блокує доступ іншого користувача.

Команда holdoff знімає обмеження команди holdon.

### **Команди консолі NetWare.**

Запускаються тільки з консолі сервера. Призначені для трьох видів обробки:

- конфігурування мережі
- електронної пошти
- керування друком.

#### ***а. Конфігурування мережі.***

CLEAR STATION - (clear station № станції) - позбавляє робочу станцію наданих ресурсів мережі.(наприклад, робоча станція від'єдналась від мережі, а файли залишились відкриті)

CONFIG (config) - видає лістинг таблиць контролерів мережі, які під'єднані до файл-сервера, їх тип і версію NetWare.

Наприклад:

CONSOLE - (console) - за допомогою цієї команди сервер, що працює в DOS-режимі переходить у режим консолі. Тільки в цьому режимі можуть виконуватись консоль-команди. Зворотня дія- повернення до DOSy.

DISABLE LOGIN - (disable login) - дає можливість відмовити у приєднанні робочої станції до файл-сервера. Команда відміни - enable login.

DISK - (disk) - перевіряє фізичний стан жорсткого диска файл-сервера. Видається інформація про порядковий номер файл-сервера, канал, контролер, статус дисководу, помилки вводу-виводу, кількість вільних блоків, кількість зайнятих блоків та ін.

DOWN - (down). Підготовляє файл-сервер до вимкнення: вміст кеш-пам'яті з віртуального диска (псевдодиска) переноситься на жорсткий диск, відкриті файли закриваються, зберігаються директорії і FAT-таблиці. Закриваються також і ті файли, які були під'єднані до р.с. без потреби. Якщо р.с. до цього часу ще не від'єднана від мережі, то видається відповідне повідомлення.

Після цього ф.с. повідомляє:

Server ABC has been shut-down.

Please Re-boot to Restart.

MONITOR - (monitor). Викликає спеціальний екран ф.с. - дисплей-монітор. На цьому екрані може бути відображена діяльність в мережі до шести ф.с.

Відображуються значення:

util (utilisation) - завантаженість мережі (в %)

pend (pending - в стані очікування) - показує число блоків кеш-пам'яті, які зазнали змін на псевдодиску і ще не переписані на жорсткий диск ф.с. Після номера станції показується останній запит з цього робочого місця до ф.с. В колонці File відображуються оброблювані файли, а в колонці Status - стан цих файлів.

Командою NAME - (name) на монітор можна вивести ім'я ф.с.

Обернена команда до MONITOR - OFF вимикає зображення на моніторі.

Окрім того для конфігурування мережі використовують команди TIME та SET TIME для перегляду та модифікації часу і поточної дати; REMIRROR та UNMIRROR для організації "дзеркального відображення" дисків (тільки для SET режиму); VAP для видання інформації про VAP-процеси у давніших версіях; lock—блокує клавіатуру файл-сервера.

## **б. Електронна пошта**

BROADCAST (broadcast<повідомлення.>) дозволяє передавати повідомлення на всі р.с. (повідомлення може містити не більше 60 алфавітно-цифрових знаків). Повідомлення на р.с. можна видалити з екрана комбінацією <Ctrl+Enter>.

Якщо робоча станція захищена командою caston, то повідомлення не буде прийняте.

Повідомлення можна переслати і за допомогою команди SEND--(send <"повідомлення"> to <список р.с.>). "Повідомлення" обов'язково повинно бути поміщено у лапки, а список робочих станцій можна взяти з userlist.

## **в. Керування друком.**

QUEUES--(queues)—видає на екран всю чергу завдань на друк, яку обслуговує файл сервер.

Команда `QUEUE CHANGE JOB PRIORITY ( q ім'я черги № to новий №)` дає змогу змінити послідовність завдань на друк в черзі. Переглянути послідовність завдань можна за допомогою команди `list queue contents`.

Для створення нової черги служить команда `QUEUE CREATE`. Після створення нової черги її необхідно скерувати принтеру за допомогою команди `queue to printer`.

За допомогою команди `QUEUE JOBS ( q <ім'я черги>)` можна переглянути всі завдання, що стоять у черзі, а команда `QUEUE DELETE JOB ( q <ім'я черги> d)` видалить всі завдання на друк, що є всередині черги.

Є ще одна команда, яка видаляє завдання з черги - це `QUEUE DESTROY (q <ім'я черги> destroy)`, при чому вона виконується беззастережно.

Вмістиме буфера для спулінга можна роздрукувати за допомогою команди `SPOOL`.

Окремо про команди принтера :

- `PRINTER - (printer або p)` - роздруковує інформацію про всі принтери, які під'єднані до файл-сервера з вказанням їх стану.

- `PRINTER REWID - (p <№принтера> rewid <к-ть сторінок>)` - може припинити друкування, якщо виявилось, що не все потрібно друкувати. Можна також друкувати задану кількість сторінок.

- `PRINTER START - (p <№принтера> start)` - вмикає принтер після дії команд `Stop printer`, `delete all jobs in queue` чи ін.

Інші команди обслуговування принтера:

`PRINTER STOP - (p <№принтера> stop)`

`PRINTER FORM FEED - (p <№принтера> form feed)`

`PRINTER MOUNT FORM - (p <№принтера> form <№форми>)`

`PRINTER DELETE QUEUE (p <№принтера> del <№черги>).`

Обернена до неї команда `add queue to printer`.

`PRINTER ADD QUEUE PRIORITY (p <№принтера> add <черга> at priority <пріоритет>).` Найвищим вважається пріоритет з числом 1.

Якщо Ви працюєте з локальним принтером і маєте потребу скористатися принтером, під'єднаним до файл-сервера, то необхідно використати команду `CAPTURE`, яка буде діяти тільки на момент під'єднання до даного сервера. Навіть до завершення від'єднання від мережі Ви можете перейти на локальний принтер за допомогою команди `end cap`.

(матеріал для ознайомлення в історичному плані)

Вже згадувалося, що у однорангових ЛКМ передбачається такий режим роботи, що кожна робоча станція може одночасно бути і файл-сервером. Звичайно, що затрати на організацію такої ЛКМ будуть відносно невеликими, однак при збільшенні числа робочих станцій ефективність роботи такої мережі різко впаде. Тому однорангові ЛКМ застосовуються для невеликих робочих груп, де зменшення продуктивності робочих станцій є не єдиною проблемою. Тут маємо можливість втрати файлів при збоях робоча станція - файл-сервер, проблема з резервним копіюванням, розподіл функцій між файл-сервером та ін.

Розглянемо принцип функціонування кількох ОС однорангових ЛКМ .

### **5.1. Мережне ОС LANtastic.**

До недавнього часу це ОС фірми Artisoft було лідером на ринку однорангових ЛКМ за популярністю та числом продаж. LANtastic, хоч і не володіє високим показником швидкодії, проте має прекрасні можливості розділення принтера, організації звукової електронної пошти, розділення накопичувачів на CD-ROM, невимоглива до великого об'єму пам'яті, має можливість працювати з ПК різних платформ (зокрема, Macintosh ), прекрасно сумісна з Windows (після випуску у 1991 р. версії 4.0 )

З 1993 р. продається версія 5.0, де є засоби для організації роботи LANtastic у ЛКМ Netware на базі файл-серверів а також можливість для розділення у ЛКМ графічних і текстових даних прикладних програм Windows. Особливістю 6-ї версії є збільшення швидкодії а також можливість використання утиліт Windows для керування ресурсами ЛКМ.

У версії 6.0 є навіть шлюз до цифрового пейджеру, а також передбачені засоби для роботи з факсами у ЛКМ (факс-апарат під'єднується до сервера). Окремо слід відзначити таку особливість LANtastic, як контроль використання ОП. Версія 6.0 містить навіть свій модуль SHARE.EXE, який є більш швидкодіючим, ніж відповідний DOSівський.

Кількість ПК, які можуть працювати у ЛКМ під управлінням LANtastic - від 2 до кількох сотень. Однак при



збільшенні числа ПК Artisoft пропонує виділити 1 ПК для файл-сервера .

Як і відома ОС Netware , LANtastic має добре розвинену систему утиліт, як меню так і командного рядка. Є також засоби для організації діалогу між користувачами ЛКМ за допомогою клавіатури, а також електронна пошта і засоби для адміністрування мережі. Резидентна програма LANPUP дає можливість за допомогою "гарячих клавіш" керувати системою меню-утиліт.

*а) меню-утиліти.*

Система меню ОС LANtastic активізується при запуску команди NET без параметрів і містить такі опції:

1. мережні накопичувачі і принтери.
2. керування чергами друку.
3. поштова служба.
4. переговори з іншими користувачами
5. приєднання / вихід з системи
6. керування реєстрацією користувачів
7. огляд дій сервера

Пояснення опцій:

**перша опція** дає можливість вибрати файл-сервер і дозволити /заборонити розділення жорстких дисків чи мережного принтера;

**друга опція** дозволяє здійснювати контроль роботи принтера чи переглядати черги друку. Тут можливі певні привілеї;

**третя опція** надає можливість переглянути на файл-сервері чергу поштових повідомлень, а також передати власне повідомлення (якщо встановлено відповідне обладнання, то і звукове);

**четверта опція** дає можливість "поговорити" з іншими користувачами за допомогою клавіатури;

**п'ята опція** є для початку і закінчення сеансу роботи у ЛКМ;

**шоста опція** дозволяє кожному змінити свій пароль, відмінити псевдонім чи переглянути свій статус;

**сьома опція** дає можливість визначити користувачів, які під'єднані до ЛКМ, а також файли, до яких вони звертаються

*б) утиліти командного рядка*

Ці утиліти запускаються з командного рядка ДОС. Для цього потрібно ввести команду NET<параметр>, де параметром і є власне утиліта, чи команда. Наприклад: NET ATTACH, NET DIR, NET COPY, NET HELP та інші

Таких команд є кілька десятків (~30). Для прикладу приведемо кілька з них:

Команда	Функція
ATTACH	Виділити всі диски на сервері, які передбачені як розділювальні
AUDIT	Помістити контрольну інформацію в log-файл
CHangepw	Змінити пароль
CLOCK	Засинхронізувати годинник робочої станції з годинником файл-сервера
COPY	Копіювати файл з сервера на робочу станцію
EXPAND	Визначити повний шлях до файла
LOGIN/LOG OUT	Розпочати (закінчити) сеанс в локальній комп'ютерній мережі
MAIL	Передати поштове повідомлення
PRINT	Аналогічна PRINT в DOS
QUEUE	Команди управління спулерам друку
HALT	
PAUSE	
RESTART	
STATUS	
RUN	Запустити DOS-програму на вказаному сервері
SEND	Послати повідомлення іншому користувачеві в локальній мережі
SHOW	Показати конфігурацію робочої станції в локальній комп'ютерній мережі, до яких серверів вона під'єднана і показати список серверів, які є в локальній комп'ютерній мережі

Продуктивність LANtastic зростає, якщо застосувати систему кешування (LANcache).

Починаючи з версії 6.0 в систему додані засоби автоматичного відновлення зв'язку робочої станції з сервером після його перевантаження.

ОС LANtastic досить проста у встановленні та адмініструванні. Має багатофункціональну систему захисту даних від несанкціонованого доступу.

Потрібні права і дозволи можна надати кожному користувачеві після його реєстрації у вікні системи Windows. Цю ж процедуру можна виконати за допомогою команди NETMGR. У обох випадках Ви повинні мати привілей системного адміністратора. Команда NETMGR вимагає системного паролю, який рекомендують час від часу змінювати.

Ще один рівень захисту даних – надання прав доступу до певних директорій на файл-сервері. Можна встановити певні дні тижня і навіть години, коли користувачі з певними псевдонімами можуть отримувати доступ до файлів ЛКМ.

## **5.2. Мережне ОС POWERLan**

Надзвичайно цікава і найшвидкодійоюча ОС для однорангових ЛКМ. Мережу, яка працює під POWERLan можна легко під'єднати до мережі під управлінням UNIX, LANServer, LANManager. Якщо ви працюєте в ОС POWERLan, яка входить у склад великої мережі під Netware, то Ви маєте доступ як до серверів POWERLan так і Netware. Один з варіантів POWERLan - використання NetBios.

ОС POWERLan - це набір резидентних програм (модульна система), що дозволяє будувати її структуру залежно від потреб.

ОС має добре розвинуту систему збереження інформації при збоях по живленню (сигнал від UPS до файл-сервера). Як і попередня дозволяє розділення накопичувачів CD-ROM.

ОС має просту у використанні систему керування завданнями для друку (перегляду черги, відсутності паперу у принтері, зміна пріоритету завдань, відміна друку завдання).

ОС POWERLan має спеціальний модуль, який дозволяє працювати всередині Netware, а використання модуля NetBios дозволяє під'єднання до мережі робочих станцій, які працюють під OS/2.

ОС має розвинену систему утиліт (меню і командного рядка). Система меню і діалогових панелей є результатом

функціонування текстового інтерфейсу користувача, який відповідає специфікаціям фірми IBM.

ОС POWERLan має низку засобів захисту даних:

- права запису, читання і створення для накопичувачів і директорій (але не для файлів)
- дозвіл і заборона декількох одночасних під'єднань до ЛКМ
- паролі для використання принтерів
- перевірка серверами процедури під'єднання кожної станції до серверів мережі
- шифрування паролів при передаванні їх через кабелі мережі

паролювання команд сервера

- обмеження під'єднання користувачів певними днями, годинами

ОС POWERLan може використовуватись також у ЛКМ з виділеним файл-сервером. Тоді варто встановити програму для кешування диску (може використовувати до 32 Мб ), що значно підвищує продуктивність.

### **5.3. ОС NetWare Lite і Personal NetWare**

Фірма Novell, прагнучи завоювати ще й ринок однорангового програмного забезпечення у 1991р. випустила Netware Lite (під DOS). Через два роки фірма переробила свій продукт і назвала його Personal Netware. Однак ще довгий час продовжувала випускати і попередній продукт. Вартість цього програмного продукту невелика (99 доларів за одну станцію), тому фірма запровадила захист від несанкціонованого копіювання за принципом і при запуску ПЗ на одній з Р.С. автоматично відбувається перевірка всієї ЛКМ на предмет наявності копії програми на іншій Р.С. Якщо появиться ще одне ПЗ, то робота тієї РС буде заблокована (порівняйте з роботою NW v.3.12 чи 4.10).

#### **Можливості ОС Personal Netware.**

Кількість ПК - від 2 до 25. Для сервера необхідно наявність жорсткого диску. ОП в межах 640 К. Для кожної робочої станції окреме ПЗ, свій адаптер з кабелями, роз'ємними, термінаторами і драйверами до адаптерів.

Personal Netware може працювати сумісно з NW v. 2.2, 3.12 і 4.0.

Система команд (меню і рядка) забезпечує виконання таких дій:

- виконувати перепризначення мережних накопичувачів за допомогою буквенних позначень;
- здійснювати створення та модернізацію мережних директорій;
- показувати контрольний список користувачів у ЛКМ та записувати контрольний список у файл;
- вмикати чи вимикати режим контролю;
- синхронізація системного годинника на всіх робочих станціях;
- показувати помилки при при'єднанні до ЛКМ;
- передавати та приймати повідомлення;
- встановлювати паролі;
- створювати, модифікувати і знищувати Ваш псевдонім;
- конфігурувати мережні принтери;
- перенаправляти друк з порту на мережний принтер;
- створювати резервні копії;
- змінювати конфігурацію файл-сервера, показувати його статус;

Як і у інших ОС для виконання різних команд необхідно мати різний статус. Наприклад, право дати команду NET DOWN для зупинення роботи сервера може тільки особа, якій дозволено керувати сервером.

Якщо говорити про продуктивність ОС Personal NW, то краще це подивитись у таблиці, де приведено час доступу до файлів:

	PowerLan 3.0	NWLite 1.1	Personal NW
А. На локальному вінчестері робочої станції			
Чит.	10.20	11.03	10.95
Зап.	8.60	8.95	8.15
Б. На диску файл-сервера при доступі з робочої станції			
Чит.	17.90	25.40	26.25
Зап.	12.05	15.43	15.00
В. При одночасній роботі двох робочих станцій			
Чит.	29.10	41.09	38.85
Зап.	18.90	34.78	34.12

Фірма Novell пояснює дещо повільнішу роботу свого продукту тим, що він проектувався з метою максимального спрощення роботи з ним навіть ціною зменшення продуктивності

Характерною рисою NWLite і Personal NW є підтримка протоколів NetBIOS та IPX, що якісно вирізняє їх від інших однорангових ОС.

Обидва ОС сумісні з програмним пакетом Windows а також прекрасно працює у складі XW.

До особливостей NWLite і Personal NW слід віднести також можливість розділяти CD-ROM, Personal NW може працювати на бездисковій робочій станції.

Захист даних у моделі NetwareLite і PersonalNetware застосовний той самий, що і в регулярних версіях Netware. Як видно з переліку системи команд існує можливість надання чи відміни привілейованого доступу через надання прав, реєстрування і паролювання.

Для кожної директорії можна вказати права доступу по замовчуванню і виділити користувачів з особливими правами. У ОС PersonalNetware можна відмінити захист даних взагалі, тобто всі користувачі отримують повний доступ до всіх розподілюваних ресурсів сервера мережі.

Вимоги до пам'яті:

	NetwareLite	PersonalNetwar e
<i>На сервері</i>	<b>95.8 К</b>	<b>151 К</b>
<i>На р.с.</i>	<b>26.8 К</b>	<b>80 К</b>

Причому всі модулі пам'яті можна завантажити у верхній області пам'яті.

## **6.1. Стек протоколів TCP/IP**

### **Історія та перспективи стека TCP/IP**

*Transmission Control Protocol/Internet Protocol (TCP/IP)* - це промисловий стандарт стека протоколів, розроблений для глобальних мереж.

Стандарти TCP/IP опубліковано у серії документів, названих Request for Comment (RFC). Документи RFC описують внутрішню роботу мережі Internet. Деякі RFC описують мережні сервіси чи протоколи та його реалізацію, тоді як інші узагальнюють умови застосування. Стандарти TCP/IP завжди публікуються у вигляді документів RFC, але визначають стандарти не RFC.

Стек розробили з ініціативи Міністерства оборони США (Department of Defence, DoD) у 1969 році для забезпечення зв'язку експериментальної мережі ARPAnet з іншими сателітними мережами як набір загальних протоколів для різноманітного обчислювального середовища. У мережі ARPA зв'язок між двома комп'ютерами здійснювався з допомогою протоколу Internet Protocol (IP).

Вагомий внесок у розвиток стека TCP/IP вніс університет Берклі, реалізувавши протоколи стека у своїй версії ОС UNIX. Широке поширення ОС UNIX призвело і до широкого поширення протоколу IP та інших протоколів стека. На цьому стекові працює всесвітня інформаційна мережа Internet, а підрозділ Internet Engineering Task Force (IETF) вносить основний внесок у вдосконалення стандартів стека, які публікує у вигляді специфікацій RFC.

На сьогодні стек TCP/IP поширений не тільки у мережах із ОС UNIX, але й у останніх версіях мережесистемних операційних системах для персональних комп'ютерів (Windows NT 3.5, NetWare 4.1, Windows 95, XP, Vista).

Роль стека TCP/IP, як лідера, пояснюється такими його властивостями:

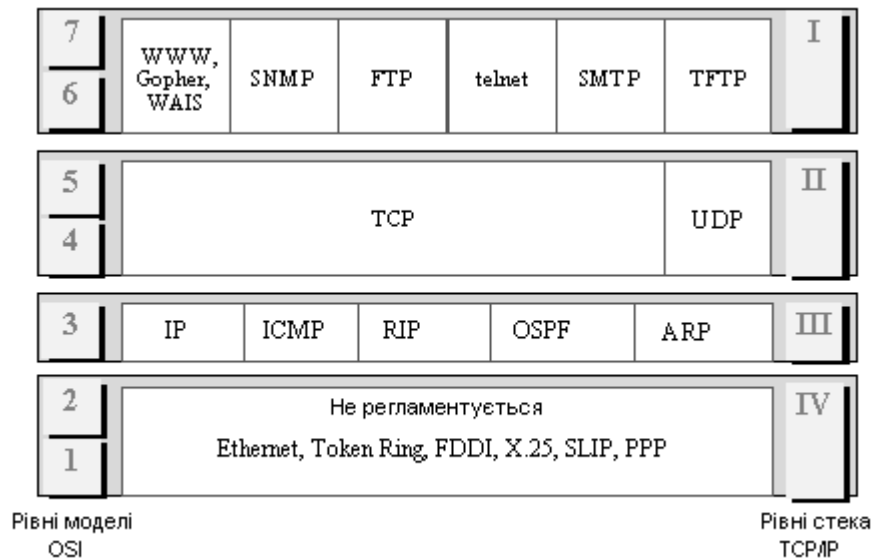
- Це найбільш завершений стандартний й водночас популярний стек мережевих протоколів, що має багаторічну історію.
- Майже всі великі мережі передають основну частину свого трафіку з допомогою протоколу TCP/IP.
- Це метод отримання доступу до Internet.
- Цей стек є підставою до створення intranet – корпоративної мережі, яка використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet.
- Усі сучасні операційні системи підтримують стек TCP/IP.
- Це гнучка технологія для сполучення різномірних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів.
- Це стійке масштабоване міжплатформенне середовище для додатків клієнт-сервер.

### **Структура стека TCP/IP. Коротка характеристика протоколів**

Оскільки стек TCP/IP розробили до появи моделі взаємодії відкритих систем ISO/OSI, то хоч він і має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделі OSI є досить умовною.

Структуру протоколів TCP/IP приведено на мал. 6.1. Протоколи TCP/IP утворюють 4-рівневу структуру.





Мал.6.1. Стек TCP/IP

Найбільш нижній (**рівень IV**) відповідає фізичному і каналному рівням моделі OSI. Цей рівень у протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного і каналного рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальних мереж - протоколи сполучень "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay. Розроблена також спеціальна специфікація, яка визначає використання технології ATM. Зазвичай у разі появи нової технології локальних чи глобальних мереж вона швидко входить у стек TCP/IP завдяки розробці відповідного RFC, яким визначають метод інкапсуляції пакетів IP у її кадри.

Наступний рівень (**рівень III**) - це рівень міжмережевої взаємодії, котрий займається передачею пакетів з різних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку й т. п.

Основним протоколом мережного рівня (в термінах моделі OSI) в стеці використовується протокол **IP**, що завжди проектувався як протокол передачі пакетів в складних мережах, які складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює у мережах зі складною топологією, раціонально використовуючи присутність у них підсистем й економно витрачаючи пропускну спроможність низькошвидкісних ліній зв'язку.

Протокол IP є дейтаграмним протоколом, тобто не гарантує доставку пакетів до вузла призначення.

До рівня міжмережної взаємодії належать також всі протоколи, пов'язані з упорядкуванням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації **RIP** (Routing Internet Protocol) і **OSPF** (Open Shortest Path First), а також протокол міжмережних керуючих повідомлень **ICMP** (Internet Control Message Protocol). Останній протокол призначений обмінюватись інформацією про помилки між маршрутизаторами мережі й вузлом — джерелом пакета. З допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості складання пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилки та певного типу обслуговування, про стан системи тощо.

Наступний рівень (**рівень II**) називається основним. На цьому рівні функціонують протокол керування передаванням **TCP** (Transmission Control Protocol) і протокол дейтаграм користувача **UDP** (User Datagram Protocol). Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами з допомогою створення віртуальних сполучень. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і IP, і виконує лише функції сполучної ланки між мережним протоколом і численними прикладними процесами.

Верхній рівень (**рівень I**) називається прикладним. За довгі роки використання їх у мережах різноманітних країн і організацій стек TCP/IP нагромадив дуже багато протоколів і сервісів прикладного рівня. До них належать такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, вживаний у електроній пошті мережі Internet, гіпертекстові сервіси доступу до віддаленої інформації, такі як WWW і ще ін.. Зупинимось докладніше на деяких із них.

Протокол передавання файлів **FTP** (File Transfer Protocol) реалізує віддалений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує у ролі транспорту протокол з встановленням сполучень - TCP. Крім пересилки файлів протокол FTP пропонує також інші послуги. Так, користувачеві дають можливість інтерактивної роботи з

віддаленою машиною, наприклад, можна роздрукувати вміст її каталогів. Нарешті, FTP виконує аутентифікацію користувачів. Перш, ніж одержати доступ до файлу, відповідно до протоколу користувачі повинні повідомити своє ім'я і пароль. Для доступу до публічних каталогів FTP-архівів Internet паролі аутентифікація не потрібна, і його обходять з допомогою спрямування такого доступу до визначеного імені користувача Anonymous.

У стеці TCP/IP протокол FTP пропонує найширший набір послуг до роботи з файлами, проте є й найбільш складним для програмування. Додатки, які не потребують всіх можливостей FTP, можуть використати інший, економічніший протокол – простий протокол пересилки файлів **TFTP** (Trivial File Transfer Protocol). Цей протокол реалізує лише передачу файлів, причому у ролі транспорту використовує простіший, ніж TCP, протокол без встановлення сполучень – UDP.

Протокол **telnet** забезпечує передачу потоку байтів між процесами, і навіть між процесом і терміналом. Найчастіше цей протокол використовується для емуляції терміналу віддаленого комп'ютера. З використанням сервісу telnet користувач фактично управляє віддаленим комп'ютером, як і локальний користувач, тому такий вид доступу вимагає хорошого захисту. Тому сервери telnet завжди використовують принаймні аутентифікацію за паролем, а іноді й потужніші засоби захисту, наприклад, систему Kerberos.

Протокол **SNMP** (Simple Network Management Protocol) використовується для організації мережного управління. Спочатку протокол SNMP розробили для віддаленого контролю та управління маршрутизаторами Internet, котрі традиційно часто називають також шлюзами. Зі збільшенням популярності протокол SNMP почали застосовувати також для управління будь-яким комунікаційним устаткуванням – концентраторами, мостами, мережними адаптерами тощо. Проблема управління у протоколі SNMP поділяється на два завдання.

Перше завдання пов'язане з передачею інформації. Протоколи передачі керуючої інформації визначають процедуру взаємодії SNMP-агента, що працює у керованому устаткуванні, і SNMP-монітора, що працює у комп'ютері адміністратора, який часто називають також консоллю управління. Протоколи передачі

визначають формати повідомлень, якими обмінюються агенти і монітор.

Друге пов'язане з контрольованими змінними, котрі характеризують стан керованого пристрою. Стандарти регламентують, які дані повинні зберігатися і накопичуватися в пристроях, імена цих даних, і синтаксис цих імен. У стандарті SNMP визначена специфікація інформаційної бази даних управління мережею. Ця специфікація, відома як база даних MIB (Management Information Base), визначає ті елементи даних, які керований пристрій має зберігати, і які над ними допустимі операції.

**TCP (Transmission Control Protocol)** - протокол контролю передачі, протокол TCP застосовується в тих випадках, коли потрібно гарантована доставка повідомлень. Перша і остання версія TCP - [RFC-793](#) (Transmission Control Protocol J. Postel Sep-01-1981). Основні особливості:

- Встановлюється з'єднання.
- Дані передаються **сегментами**. Модуль TCP нарізає великі повідомлення (файли) на пакети, кожен з яких передається окремо, на приймачі навпаки файли збираються. Для цього потрібен **порядковий номер (Sequence Number - SN)** пакета.
- Надсилає запит на наступний пакет, вказуючи його номер у поле "**Номер підтвердження**" (**AS**). Тим самим, підтверджуючи отримання попереднього пакета.
- Робить перевірку цілісності даних, якщо пакет «битий» - посилає повторний запит.



Структура дейтаграми TCP. Слова по 32 біти.

**Довжина заголовка** - задається словами по 32біти.

**Розмір вікна** - кількість байт, які готовий прийняти одержувач без підтвердження.

**Контрольна сума** - включає псевдозаголовок, заголовок і дані.

**Показчик терміновості** - вказує останній байт термінових даних, на які треба негайно реагувати.

**URG** - ознака терміновості, включає поле "Показчик терміновості", якщо = 0 то поле ігнорується.

**ACK** - ознака підтвердження, включає поле "Номер підтвердження, якщо = 0 то поле ігнорується.

**PSH** - ознака вимагає виконання операції push, модуль TCP повинен терміново передати пакет програмі.

**RST** - ознака переривання з'єднання, використовується для відмови у з'єднанні

**SYN** - ознака синхронізації порядкових номерів, використовується при встановленні з'єднання.

**FIN** - ознака закінчення передачі з боку відправника вказує останній байт термінових даних, на які треба негайно реагувати.

**Додаткові параметри або опції** - зарезервовано на майбутнє і в заголовку може бути відсутнім, його розмір змінний і доповнюється до кратного 32-біт за допомогою поля **заповнення**. На тепер визначені опції:

- Кінець списку опцій.
- Жодних операцій. Використовується для заповнення поля опції до числа октетів, кратного 4.
- Максимальний розмір сегмента (MSS).

Поле **дані** може мати змінну довжину, верхня його межа задається значенням **MSS** (Maximum Segment Size). Значення MSS може бути задане при встановленні з'єднання кожної зі сторін незалежно. Для Ethernet MSS = 1452 байта.

Для встановлення коректної TCP сесії з віддаленим хостом має дотримуватися така умова:

$$\text{MSS} + \text{заголовок TCP} + \text{заголовок IP} \leq \text{MTU}$$

Термін **maximum transmission unit (MTU)** у [комп'ютерних мережах](#) означає максимальний розмір корисного блоку даних одного [пакета](#) ([англ. payload](#)), який може бути переданий [протоколом](#) без фрагментації. Зазвичай заголовки протоколу не входять в MTU, але в деяких системах в деяких протоколах заголовки можуть враховуватися. Коли говорять про MTU, зазвичай мають на увазі протокол канального рівня [мережевої моделі OSI](#). Однак, цей термін може застосовуватися і для інших рівнів.

Отже, максимальний розмір

$$\text{MSS} = \text{MTU} - \text{розмір заголовка IPv4} - \text{розмір заголовка TCP}.$$

Так кожен хост на IPv4 вимагає доступності для MSS останніх 536 октетів (= 576 - 20 - 20) а на IPv6 - 1220 октетів (= 1280 - 40 - 20).

Зазвичай конкретне значення MSS визначається [операційною системою](#) під час встановлення контакту TCP з цільовим хостом виходячи зі значень MTU або PMTUD (Path MTU Discovery).

## Встановлення TCP-з'єднань

Для організації надійної передачі даних передбачається встановлення логічного з'єднання між двома прикладними процесами. Коли прикладний процес починає використовувати TCP, то модуль TCP на машині клієнта і модуль TCP на машині сервера починають спілкуватися. Ці два кінцевих модуля TCP підтримують інформацію про стан з'єднання, яке називають віртуальним каналом. Цей віртуальний канал споживає ресурси обох кінцевих модулів TCP. Канал є дуплексним: дані можуть одночасно передаватися в обох напрямках. Один прикладний процес пише дані в TCP - порт, вони проходять по мережі, і інший прикладний процес читає їх зі свого TCP-порту. У рамках з'єднання здійснюється обов'язкове підтвердження

правильності прийому для всіх переданих повідомлень, і при необхідності виконується повторна передача.

З'єднання в протоколі TCP ідентифікується парою повних адрес обох взаємодіючих процесів (кінцевих точок). Адреса кожної з кінцевих точок включає IP- адресу (номер мережі і номер комп'ютера) і номер порту. Одна кінцева точка може брати участь у кількох з'єднаннях.

Встановлення з'єднання виконується в наступній послідовності:

- При встановленні з'єднання одна зі сторін є ініціатором. Вона посилає запит до протоколу TCP на відкриття порту для передачі (active open ).
- Після відкриття порту протокол TCP на стороні процесу - ініціатора надсилає запит процесу, з яким потрібно встановити з'єднання.
- Протокол TCP на приймальній стороні відкриває порт для прийому даних ( passive open ) і повертає квитанцію, що підтверджує прийом запиту.
- Для того щоб передача могла вестися в обидві сторони, протокол на приймальній стороні також відкриває порт для передачі ( active port ) і також передає запит до протилежної сторони.
- Сторона- ініціатор відкриває порт для прийому і повертає квитанцію.
- З'єднання вважається встановленим. Далі відбувається обмін даними в рамках даного з'єднання.

## **Призначення портів у TCP**

За номером порту транспортні протоколи визначають, яким додатком передати вміст пакетів. Порти можуть приймати значення від 0-65535 (два байти  $2^{16}$ ). Номери портів присвоюються таким чином: є стандартні номери (наприклад, номер 21 закріплений за сервісом FTP, 23 - за telnet, 80 - за HTTP), а менш відомі програми користуються довільно вибраними локальними номерами (як правило, більше  $> 1024$ ), деякі з них також зарезервовані.

Деякі задані порти [RFC-+1700](#) (одна тисяча дев'ятсот дев'яносто чотири)

Порт	Служба	Опис
0	- -	Зарезервовано
13	Daytime	Синхронізація часу
20	ftp-data	Канал передачі даних для FTP
21	ftp	Передача файлів
23	telnet	Мережний термінал
25	SMTP	Передача пошти
37	time	Синхронізація часу
43	Whois	Служба Whois
53	DNS	Доменні імена
67	bootps	BOOTP і DHCP - сервер
68	bootps	BOOTP і DHCP - клієнт
69	tftp	Спрощена передача пошти
80	HTTP	Передача гіпертексту
109	POP2	Отримання пошти
110	POP3	Отримання пошти
119	NNTP	Конференції
123	NTP	Синхронізація часу
137	netbios-ns	NETBIOS - імена
138	netbios-dgm	Service NETBIOS Datagram Service
143	imap2	Отримання пошти
161	SNMP	Протокол управління
210	z39.50	Бібліотечний протокол
213	IPX	IPX - протокол
220	imap3	Отримання пошти
443	HTTPs	HTTP з шифруванням
520	RIP	Динамічна маршрутизація
<b>Діапазон 1024-65535</b>		
1024	- -	Зарезервовано
6000-6063	X11	Графічний мережевий термінал

## Концепція квітування

У рамках з'єднання правильність передачі кожного сегмента повинна підтверджуватися квитанцією одержувача. Квітування - це один з традиційних методів забезпечення надійного зв'язку. Ідея квітування полягає в наступному:



Для того, щоб можна було організувати повторну передачу спотворених даних відправник нумерує одиниці даних, що відправляються (далі для простоти звані кадрами). Для кожного кадру відправник очікує від приймача так звану позитивну квитанцію - службове повідомлення, що сповіщає про те, що вихідний кадр був отриманий і дані в ньому виявилися коректними. Час цього очікування обмежений - при відправці кожного кадру передавач запускає таймер, і якщо по його закінченню позитивна квитанція не отримана, то кадр вважається загубленим. Так як ТСП - канал є дуплексним, то підтвердження для даних, що йдуть в одному напрямку, можуть передаватися разом з даними, що йдуть в протилежному напрямку. У деяких протоколах приймач, у разі отримання кадру з перекрученими даними повинен відправити негативну квитанцію - явну вказівку того, що даний кадр потрібно передати повторно.

### **Реалізація ковзаючого вікна в протоколі ТСП**

У протоколі ТСП реалізовано різновид алгоритму квітуння з використанням вікна. Особливість цього алгоритму полягає в тому, що, хоча одиницею переданих даних є сегмент, вікно визначено на безлічі нумерованих байт неструктурованого потоку даних, що надходять з верхнього рівня і буферизованих протоколом ТСП.

Квитанція надсилається тільки у разі правильного прийому даних, негативні квитанції не посилаються. Таким чином, відсутність квитанції означає або прийом спотвореного сегмента, або втрату сегмента, або втрату квитанції.

Як квитанцію одержувач сегмента відсилає відповідь повідомлення (сегмент), в яке поміщає число, що на одиницю перевищує максимальний номер байта в отриманому сегменті. Якщо розмір вікна дорівнює  $W$ , а остання квитанція містила значення  $N$ , то відправник може посилати нові сегменти до тих пір, поки в черговий сегмент не потрапить байт з номером  $N + W$ . Цей сегмент виходить за рамки вікна, і передачу в такому випадку необхідно призупинити до приходу наступної квитанції.

## **Вибір тайм- ауту**

Тайм-аут не повинен бути занадто коротким, щоб по можливості виключити надлишкові повторні передачі, які знижують корисну пропускну здатність системи. Але він не повинен бути і занадто великим, щоб уникнути тривалих простоїв, пов'язаних з очікуванням неіснуючої або "заблудшої" квитанції.

При виборі величини тайм-ауту повинні враховуватися швидкість і надійність фізичних ліній зв'язку, їх протяжність і багато інших подібних факторів. У протоколі ТСП тайм- аут визначається за допомогою досить складного адаптивного алгоритму, ідея якого полягає в наступному. При кожній передачі засікається час від моменту відправлення сегмента до приходу квитанції про його прийом (час обороту). Одержувані значення часів обороту усереднюються з ваговими коефіцієнтами, зростають від попереднього виміру до наступного. Це робиться для того, щоб посилити вплив останніх вимірів. Як тайм - аут вибирається середній час обороту, помножене на деякий коефіцієнт. Практика показує, що значення цього коефіцієнта повинно перевищувати 2 . У мережах з великим розкидом часу обороту при виборі тайм-ауту враховується і дисперсія цієї величини.

## **Реакція на перевантаження мережі**

Варіюючи величину вікна, можна вплинути на завантаження мережі. Чим більше вікно, тим більшу порцію непідтверджених даних можна послати в мережу. Якщо мережа не справляється з навантаженням, то виникають черги в проміжних вузлах - маршрутизаторах і в кінцевих вузлах - комп'ютерах.

При переповненні приймального буфера кінцевого вузла "перевантажений" протокол ТСП, відправляючи квитанцію, поміщає в неї новий, зменшений розмір вікна. Якщо він зовсім відмовляється від прийому, то в квитанції вказується вікно нульового розміру. Після прийому квитанції з нульовим значенням вікна протокол-відправник час від часу робить контрольні спроби продовжити обмін даними. Якщо протокол-приймач вже готовий приймати інформацію, то у відповідь на

контрольний запит він посилає квитанцію із зазначенням ненульового розміру вікна.

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

Наостанок зазначимо: протокол TCP розбиває потік байтів на пакети; він не зберігає меж між записами. Наприклад, якщо один прикладний процес робить 5 записів в TCP - порт, то прикладний процес на іншому кінці віртуального каналу може виконати 10 читань для того, щоб отримати всі дані. Але цей же процес може отримати всі дані відразу, зробивши тільки одну операцію читання. Не існує залежності між числом і розміром записуваних повідомлень з одного боку і числом і розміром зчитувальних повідомлень з іншого боку.

**Про сокети.** Динамічні номери портів призначаються мережевими програмами - додатками на комп'ютері - робочій станції, причому різні додатки на різних комп'ютерах можуть використовувати одні й ті ж номери портів, так як будь-який додаток на будь-якому комп'ютері може бути ідентифіковано за допомогою комбінації IP адреси комп'ютера і номера порту програмного додатка.

Ось ця комбінація і називається сокетом (socket), наприклад, 192.1.1.1:25 - це адреса SMTP сервера на комп'ютері з адресою 192.1.1.1.

## **Протокол UDP**

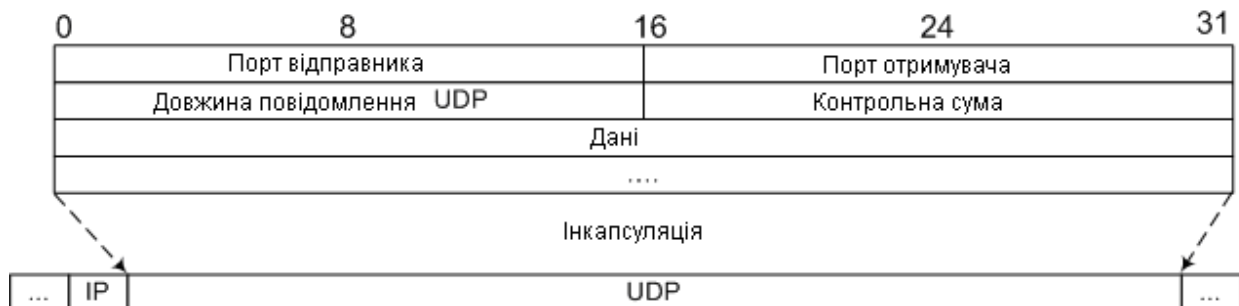
**UDP (Universal Datagram Protocol)** - універсальний протокол передачі даних, більш полегшений транспортний протокол, ніж TCP.

Перша і остання версія UDP - [RFC-768](#) (User Datagram Protocol J. Postel Aug-28-1980).

Основні відмінності від TCP:

- Відсутнє з'єднання між модулями UDP.
- Не розбиває повідомлення для передачі
- При втраті пакету запит для повторної передачі не надсилається

UDP використовується якщо не потрібно гарантована доставка пакетів, наприклад, для потокового відео і аудіо, DNS (тому що дані невеликих розмірів). Якщо перевірка контрольної суми виявила помилку або якщо процесу, підключеного до потрібного порту, не існує, пакет ігнорується (знищується). Якщо пакети надходять швидше, ніж модуль UDP встигає їх обробляти, то ці пакети також ігноруються.



Структура данограми UDP. Слова по 32 біта.

Не всі поля UDP-пакета обов'язково повинні бути заповнені. Якщо посилається дейтаграма, яка не передбачає відповіді, то на місці адреси відправника можуть поміщатися нулі.

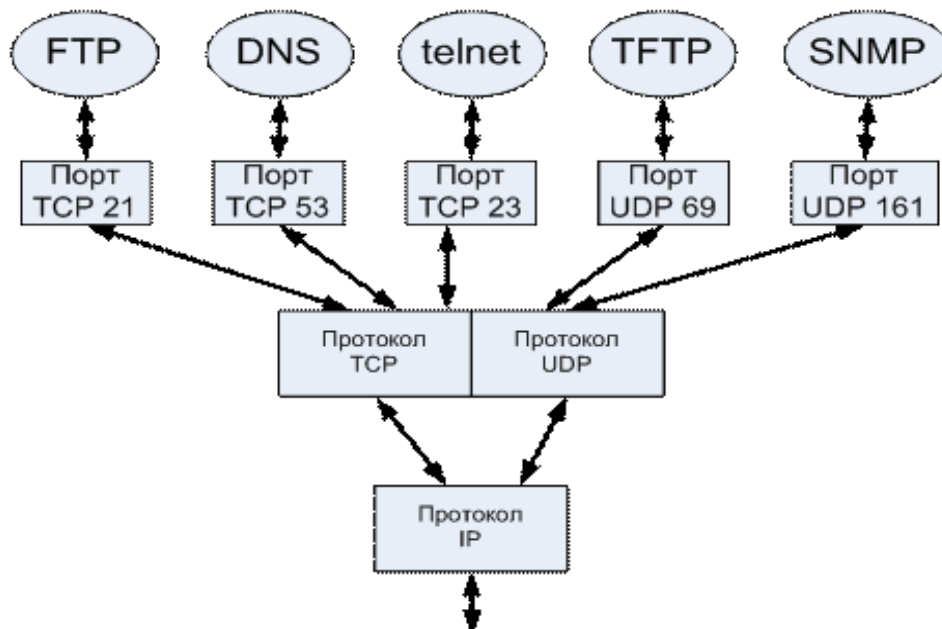
### Довжина данограми

Поле, що задає довжину всієї дата грами (заголовок і даних) в байтах. Мінімальна довжина дорівнює довжині заголовка - 8 байт. Теоретично, максимальний розмір поля - 65 535 байт для UDP - данограми (8 байт на заголовок і 65527 на дані). Фактична межа для довжини даних при використанні IPv4 - 65507 (крім 8 байт на UDP - заголовок потрібно ще 20 на IP-заголовок).

На практиці також слід враховувати, що якщо довжина IPv4 пакету з UDP перевищуватиме MTU (для Ethernet за замовчуванням 1500 байт), то відправка такого пакета викличе його фрагментацію, що може призвести до того, що він взагалі не зможе бути доставлений, якщо проміжні маршрутизатори або кінцевий хост не підтримуватимуть фрагментовані IP пакети. Також в RFC791 вказується мінімальна довжина IP пакета не менше 576 байт і рекомендується відправляти IP пакети більшого розміру тільки в тому випадку якщо ви впевнені, що приймаюча сторона може прийняти пакети такого розміру. Отже, щоб уникнути фрагментації UDP пакетів (і можливої їх втрати), розмір даних в UDP не повинен перевищувати:  $MTU - (Max\ IP\ Header\ Size) - (UDP\ Header\ Size) = 1500 - 60 - 8 = 1432$  байт. Для того щоб бути впевненим, що пакет буде прийнятий будь-яким хостом, розмір даних в UDP не повинен перевищувати: (мінімальна довжина IP пакета) - (Max IP Header Size) - (UDP Header Size) =  $576 - 60 - 8 = 508$  байт.

У Jumbogram'мах IPv6 пакети UDP можуть мати більший розмір. Максимальне значення становить 4294967295 байт ( $2^{32} - 1$ ), з яких 8 байт відповідають заголовку, а решта 4294967287 байт - даним.

Процедура прийому даних протоколами TCP і UDP, що надходять від декількох різних прикладних служб, називається **мультиплексуванням**. Зворотня процедура - процедура розподілу протоколами TCP і UDP пакетів, які надходять від мережевого рівня між набором високорівневих служб - називається демультимплексування.



Мал.. Мультиплексування і демультиплексування на транспортному рівні.

Крім цього у стеку протоколів часто використовують:

### **Протокол реального часу RTP**

**RTP (Real Time Protocol)** - транспортний протокол для додатків реального часу.

**RTCP (Real Time Control Protocol)** - транспортний протокол зворотного зв'язку для програми RTP.

## **6.2. Маршрутизація. Протокол IP**

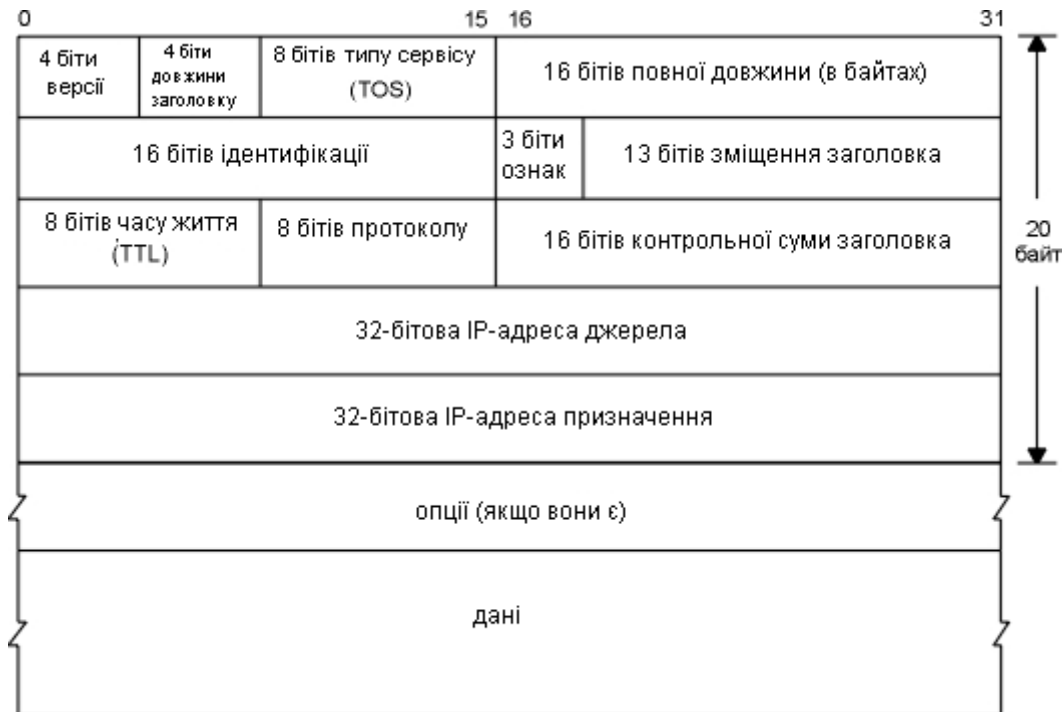
У попередньому розділі вже згадувалось, що зв'язок між двома комп'ютерами, починаючи з мережі **ARPA**, а потім і в інших мережах, здійснювався з допомогою протоколу Internet Protocol (IP).

Сьогодні цей мережевий протокол використовують як для зв'язку комп'ютерів всесвітньої мережі, так і у переважній більшості корпоративних мереж.

Нині використовується версія протоколу IP, відома як **IPv4**. Розглянемо стандартну схему адресації і сучасні методи

раціонального використання адресного простору, запроваджені в результаті виявлених недоліків у реалізації протоколу IP.

Стандартний розмір IP заголовка складає 20 байт, якщо відсутні опції. Структура заголовка показана на мал.6.2.



Мал 6.2. IP данограма, поля IP заголовка.

Подамо короткий опис полів заголовка.

Поточна версія протоколу - 4, тому IP іноді називається IPv4.

Довжина заголовка (header length) вказує кількість 32-бітових слів в заголовку, включаючи і опції. Оскільки це поле 4-бітове, то воно обмежує розмір заголовка в 60 байт. Це обмеження іноді впливає на деякі опції, зокрема, на опцію запису маршруту. Зазвичай значення поля рівне 5 (коли відсутні опції).

Поле типу сервісу (TOS - type-of-service) складається з 3-бітового поля приставки (що часто ігнорується), 4 бітів TOS і невикористовуваного біта, що дорівнює 0. 4 біти TOS такі: мінімальна затримка, максимальна пропускна здатність, максимальна надійність і мінімальна вартість. Одночасно може бути встановлений в одиницю лише один із цих 4 біт. Якщо всі 4 біти дорівнюють 0, то це звичайний сервіс.

Діалогові додатки, такі як Telnet і Rlogin, вимагають мінімізації затримок, оскільки їх використовують користувачі інтерактивно і здійснюють невеликі передачі даних. Передача файлів з допомогою FTP, з іншого боку, вимагає максимальної пропускну здатності. Максимальна надійність необхідна для мережного управління (SNMP) й у протоколів маршрутизації. Новини Usenet (NNTP) це єдиний додаток, що потребує мінімізації вартості.

Характеристика TOS, нині, більшістю реалізацій TCP/IP не підтримується, проте її включено для нових систем, починаючи з 4.3BSD Reno. Деякі протоколи маршрутизації, такі як OSPF і IS-IS, мають можливість приймати рішення щодо маршрутизації з урахуванням цього поля.

Поле повної довжини (total length) містить повну довжину IP данограми в байтах. Завдяки цьому полю і полю довжини заголовка, знаємо, від якого місця починаються дані в IP данограмі та його довжину. Оскільки це поле складається з 16 біт, максимальна величина IP данограми становить 65535 байт.

Попри те, що є можливість відправити данограму розміром 65535 байт, більшість каналних рівнів поділять таку данограму на фрагменти (кадри). Більше того, від хоста непотрібно приймати данограму розміром більше, ніж 576 байт. TCP ділить користувацькі дані на частини, тому це обмеження звичайно не впливає на TCP. Що ж до UDP, послугами якого користуються додатки, наприклад (RIP, TFTP, BOOTP, DNS, SNMP), то він обмежує себе 512 байтами користувацьких даних, що менше обмеження в 576 байт. Більшість додатків у даний час (особливо ті, які підтримують NFS - Network File System) дозволяють використовувати IP данограму розміром 8192 байти.

Поле повної довжини потрібно у IP заголовку деяким каналам (як, наприклад, Ethernet), який доповнює маленькі фрейми до мінімальної довжини. Попри те що мінімальний розмір фрейму Ethernet становить 46 байт, IP данограма може бути й меншою. Якщо поле повної довжини не було представлено, то IP рівень не буде знати, скільки 46-байтових фреймів Ethernet вийде з IP данограми.

Поле ідентифікації (identification) унікально ідентифікує кожну данограму, відправлену хостом. Значення, що зберігається у



полі, зазвичай збільшується на одиницю із посиленням кожної данограми.

Поле ознак (flags) і поле усунення фрагментації (fragmentation offset) стосуються особливого режиму передавання данограм з використанням фрагментації.

Поле часу життя (TTL - time-to-live) містить максимальне число пересилань (маршрутизаторів), через які може пройти данограма. Це поле обмежує тривалість життя данограми. Значення встановлюється відправником (зазвичай 32 чи 64) і зменшується на одиницю кожним маршрутизатором, який обробляє данограму. Коли значення поля досягає 0, данограма видаляється, а відправник повідомляється про це з допомогою ICMP повідомлення. Такий алгоритм запобігає зацикленню пакетів в петлях маршрутизації. Спостерігати за проходженням пакетів данограми можна за допомогою програми Traceroute.

Поле протоколу (protocol) вказує, який протокол відправив дані через IP.

Контрольна сума заголовка (header checksum) розраховується лише для IP заголовка. Вона не включає у себе дані, що слідує за заголовком. Протоколи ICMP, IGMP, UDP і TCP мають контрольні суми у власних заголовках, що охоплюють їх заголовки і дані.

Якщо виявляється помилка контрольної суми, IP відкидає прийняту данограму. Повідомлення про помилку не генерується. У завдання верхніх рівнів входить визначити, що данограма відсутня, й забезпечити повторну передачу.

Кожна IP данограма містить IP адресу джерела (source IP address) і IP адресу призначення (destination IP address). Це 32-бітові значення, які ми опишемо далі.

І останнє поле - поле опцій (options), це список додаткової інформації змінної довжини. На сьогодні опції визначено так:

- безпека продукції та обробка обмежень (для військових додатків),
- запис маршруту (запис кожного маршруту та його IP адреси),

- тимчасова марка (запис кожного маршруту, його IP адреса і час),
- вільна маршрутизація джерела (вказує список IP адрес, якими повинна пройти данограма),
- жорстка маршрутизація джерела (теж саме, що у попередньому пункті, проте IP данограма повинна пройти лише крізь вказані у списку адреси.

Ці опції рідко використовують і не усі хости чи маршрутизатори підтримують всі опції.

Поле опцій завжди обмежено 32 бітами. Байти заповнення, значення яких дорівнюють 0, додаються в разі потреби. Завдяки цьому IP заголовок завжди кратний 32 бітам (як і потрібно для поля довжини заголовка).

## Адреси протоколу IPv4

Відповідно до специфікації протоколу, кожному вузлу, приєднаному до IP-мережі, присвоюється унікальний номер. Вузлом може бути комп'ютер, маршрутизатор, міжмережевий екран та ін. Якщо якийсь вузол має низку фізичних підключень до неї, то кожному підключенню може бути присвоєно свій унікальний номер.

Цей номер, чи інакше **IP-адреса**, має довжину чотири октети, і складається з двох частин. Перша частина визначає мережу, до якої підключено вузол, а друга — унікальну адресу самого вузла всередині мережі.


Номер мережі			Номер вузла
11011100	11010111	00001110	00010110

У класичній реалізації протоколу першу частину адреси називають "мережним префіксом", оскільки він однозначно визначає мережу. Однак у сучасній реалізації мережу ідентифікують в інший спосіб, про що мова йтиме нижче.

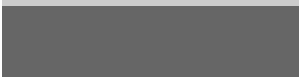
## Класова адресна схема протоколу IP

Класова модель передбачає поділ адресного простору на п'ять класів: А, В, С, D та Е. Кожен клас однозначно ідентифікувався першими бітами лівого байта адреси, а самі класи відрізнялися розмірами мережної і вузлової частин. Знаючи клас адреси, легко визначити межу між його мережною і вузловою частинами.


### Клас А

Номер біта	0	8	16	24	31
Адреса	0.....	.....	.....	.....	
Мережева частина					

### Клас В

Номер біта	0	8	16	24	31
Адреса	10.....	.....	.....	.....	
Мережева частина					

### Клас С

Номер біта	0	8	16	24	31
Адреса	110.....	.....	.....	.....	
Мережева частина					

### Клас D

Номер біта	0	8	16	24	31
Адреса	1110....	.....	.....	.....	

### Клас Е

Номер біта	0	8	16	24	31
Адреса	1111....	.....	.....	.....	

Рис. 6.3.

**Клас А** орієнтовано на дуже великі мережі. Усі адреси, що належать до цього класу, мають 8-бітовий мережевий префікс, на що вказує перший біт лівого байта адреси. Відповідно, на ідентифікацію вузла відведено 24 біти й кожна мережа може містити до  $2^{24}-2$  вузлів. Дві адреси необхідно забрати, оскільки адреси, які містять у правому октеті всі нулі (ідентифікує зазначену мережу) і всі одиниці (широкосмугову адресу) використовують зі службовою метою.

Самих мереж у класі А може бути  $2^7-2$ . Знову ми віднімаємо двійку, але вже дві службових мережі: 127.0.0.0 і 0.0.0.0.

Бачимо, що клас А містить всього  $2^7 * 2^{24} = 2^{31}$  адрес, або половину всіх можливих IP-адрес.

**Клас В** призначений для мереж великого й середнього розмірів. Адреси цього класу ідентифікуються двома старшими бітами, рівними відповідно 1 і 0. Мережний префікс класу складається з шістнадцяти біт або перших двох октетів адреси.

Оскільки два перших біти мережного префікса зайняті ключем для визначення класу, отримуємо лише  $2^{14}$  різних мереж. Вузлів ж у кожній мережі можна визначити до  $2^{16}-2$ .

Провівши обчислення, аналогічні наведених для класу А, побачимо, що клас В займає чверть адресного простору протоколу IP.

**Клас С**, найуживаніший клас мереж — має 24 бітний мережевий префікс, визначається старшими бітами, установлених у 110, і може ідентифікувати до  $2^{21}$  мереж. Клас С дозволяє адресувати до  $2^8-2$  вузлів. Займає восьму частину адресного простору протоколу IP.

Останні два класи займають решту адрес, що залишилися у адресному просторі і призначені для службового (**клас D**) і експериментального (**клас E**) використання. Для класу D старші чотири біти адреси рівні 1110, для класу E -- 1111. Сьогодні клас D використовується для передавання даних за груповими адресами.

Оскільки довгі послідовності з одиниць і нулів важко запам'ятати, IP адреси зазвичай записують у десяткової формі (кожен октет адреси представляється як десяткове число).

Поміж себе октети відокремлюються крапкою. Іноді октети позначаються як **w.x.y.z** і називаються "**z-октет**", "**y-октет**", "**x-октет**" і "**w-октет**".

Представлення IP-адреси, як чотирьох десяткових чисел розділених крапками, називається "крапково-десятьковою нотацією".

Окетт	W	X	Y	Z
Номер біта	0	8	16	24 31
Адреса	11011100	11010111	00001110	00010110
	220	215	14	22
Крапково-десятьковий формат	220.215.14.22			

**Рис. 6.4**

Підсумуємо інформацію про класи мереж в таблиці:

Клас	Кількість мереж	Кількість вузлів	Десятковий діапазон
<b>A</b>	$2^7 - 2$ (126)	$2^{24} - 2$ (2 147 483 648)	1.xxx.xxx.xxx - 126.xxx.xxx.xxx
<b>B</b>	$2^{14}$ (16 384)	$2^{16} - 2$ (65 534)	128.0.xxx.xxx- 191.255.xxx.xxx
<b>C</b>	$2^{21}$ (2 097 152)	$2^8 - 2$ (254)	192.0.0.xxx - 223.255.255.xxx
<b>D</b>	-	-	224.0.0.xxx - 239.255.255.xxx
<b>E</b>	-	-	240.0.0.xxx - 254.255.255.xxx

**Рис. 6.5.**

## Зарезервовані адреси

Як зазначалося, в адресній схемі протоколу виділяють особливі IP-адреси.

Якщо біти всіх октетів адреси рівні нулю, він позначає адресу того вузла, який згенерував даний пакет. Це використовують

у окремих випадках, наприклад, у деяких повідомленнях протоколу IP.

Якщо біти мережного префікса рівні нулю, то це значить, що вузол призначення належить до тієї ж мережі, що і джерело пакета.

Коли біти всіх октетів адреси рівні двійковій одиниці, пакет доставляється всім вузлам, що належить до тієї ж мережі, що і відправник пакета. Таке розсилання називається обмеженим **широкомовленням**.

Якщо в одиниці встановлені всі біти адреси вузла призначення, то такий пакет розсилається всім вузлам зазначеної мережі. Це називається **широкомовленням (broadcast)**.

Спеціальне значення має, також, і адреса мережі 127/8. Її використовують для тестування програм, та взаємодії процесів у межах однієї машини. Пакети, відправлені на цей інтерфейс, обробляються локально, як вхідні. Тому адреси з цієї мережі не можна присвоювати фізичним мережним інтерфейсам.

## **Організація підмереж**

Дуже рідко в локальну обчислювальну мережу входять більше як 100-200 вузлів: навіть розглядаючи мережу з значною кількістю вузлів, багато мережних середовищ накладають обмеження, наприклад, в 1024 вузли. Виходячи з цього, доцільність використання мереж класу А і В є сумнівною. Та й використання класу С для мереж, які складаються з 20-30 вузлів, є також марнотратством.

Для вирішення проблем в дворівневу ієрархію IP-адрес (мережа – вузол) було запроваджено нова складова — *підмережа*. Ідея полягає у "запозиченні" кількох бітів з вузлової частини адреси для визначення підмережі.

Повний префікс мережі, що складається з мережного префікса і номера підмережі, отримав назву розширеного мережного префікса. Двійкове число, та його десятковий еквівалент, що містить одиниці в розрядах, які стосуються розширеного мережного префікса, а інших розрядах -- нулі, назвали *маскою підмережі*.

		Мережний префікс		підмережа	вузол
IP адреса	144.144.19.22	10010000	10010000	00010011	00010110
Маска	255.255.255.0	11111111	11111111	11111111	00000000
		Розширений мережевий префікс			

**Мал.6.6. Префікси та маска мережі**

Але маску в десятковому поданні зручно використовувати буде лише тоді, коли розширений мережевий префікс закінчується на межі октетів, в інших випадках її розшифрувати складніше. Припустимо, що у прикладі на мал. 4 ми хотіли б для підмережі використовувати не 8 біт, а десять. Тоді, у останньому (z-му) октеті ми мали би не нулі, а число 11000000. У десятковому поданні отримуємо 255.255.255.192. Очевидно, що таке уявлення не дуже зручне. Нині частіше використовують позначення виду ".../xx", де xx – кількість бітів у розширеному мережному префіксі. Отже, замість вказівки: "144.144.19.22 з маскою 255.255.255.192", ми можемо записати: 144.144.19.22/26. Як бачимо, таке уявлення є більш компактним і зрозумілішим.

### **Маска підмережі змінної довжини VLSM (Variable Length Subnet Mask)**

Проте невдовзі зрозуміли, що підмережі, попри всі їхні переваги, мають і недоліки. Так, визначивши одного разу маску підмережі, доводиться використовувати підмережі фіксованих розмірів. Скажімо, ми маємо мережу 144.144.0.0/16 з розширеним префіксом /23.

		Мережний префікс		Підмережа	Вузол
144.144.0.0/23	<-->	10010000	10010000	00000000	0 00000000
		Розширений мережевий префікс			

**Мал. 6.7**

Така схема дозволяє створити  $2^7$  підмереж площею  $2^9$  вузлів кожна. Це наближається до випадку, коли є багато підмереж з великою кількістю вузлів. Але якщо серед мереж є такі,

кількість вузлів у яких в межах сотні, то для кожної з них буде пропадати близько 400 адрес.

Вирішення проблеми полягає у тому, щоб для однієї мережі вказувати більше, ніж один розширений мережний префікс. Таку мережу називають мережею з маскою підмережі змінної довжини (VLSM).

Справді, якщо для мережі 144.144.0.0/16 використовувати розширений мережний префікс /25, то це більше підходило б для мереж з розмірами близько сотні вузлів. Якщо припустити використання обох масок, це б значно збільшило гнучкість застосування підмереж.

Загальна схема розбивки мережі на підмережі з масками змінної довжини така: мережу ділять на підмережі максимально необхідного розміру. Потім деякі підмережі ділять на дрібніші, і рекурсивно далі, до того часу, поки це необхідно.

Крім того, технологія VLSM, шляхом приховання частини підмереж, дозволяє зменшити обсяг даних, що їх передають маршрутизатори. Тож якщо мережа 12/8 конфігурується з розширеним мережним префіксом /16, після чого мережі 12.1/16 і 12.2/16 розбиваються на підмережі /20, то маршрутизатору у мережі 12.1 не потрібно знати про підмережі 12.2 з префіксом /20, йому досить знати маршрут на мережу 12.1/16.

### **Проблеми класичної схеми**

У 1980-х роках Internet вперше зіштовхнувся з проблемою переповнення таблиць магістральних маршрутизаторів. Рішення, проте, було знайдено – підмережі усунули проблему на кілька років. Але вже на початку 90-х до проблеми великої кількості маршрутів додалася нестача адресного простору. Обмеження у 4 мільярди адрес, закладене у протоколі, і що здавалося недосяжною величиною, виявилось дуже відчутним.

Для розв'язання проблеми були водночас запропоновані два підходи – один на найближче майбутнє, інший комплексний і довгостроковий. Перше рішення — це впровадження протоколу безкласової маршрутизації (CIDR), до якого пізніше приєдналася система NAT (Network Address Translation).



Довгострокове рішення — це протокол IP наступної версії IPv6, чи IPng (Internet Protocol next generation). У реалізації цього протоколу довжина адреси збільшена до 16-ти байтів (128 bit!), виключені деякі елементи чинного протоколу, які виявилися невикористаними.

IPv6 забезпечить, як люблять вказувати, щільність в 3 911 873 538 269 506 102 IP адрес на один квадратний метр Землі.

Але те, що до 2000-го року протокол проходив стандартизацію, і те, що протокол CIDR разом із системою NAT виявилися ефективним рішенням, дає підстави думати, що перехід із IPv4 на IPng триватиме ще значний час.

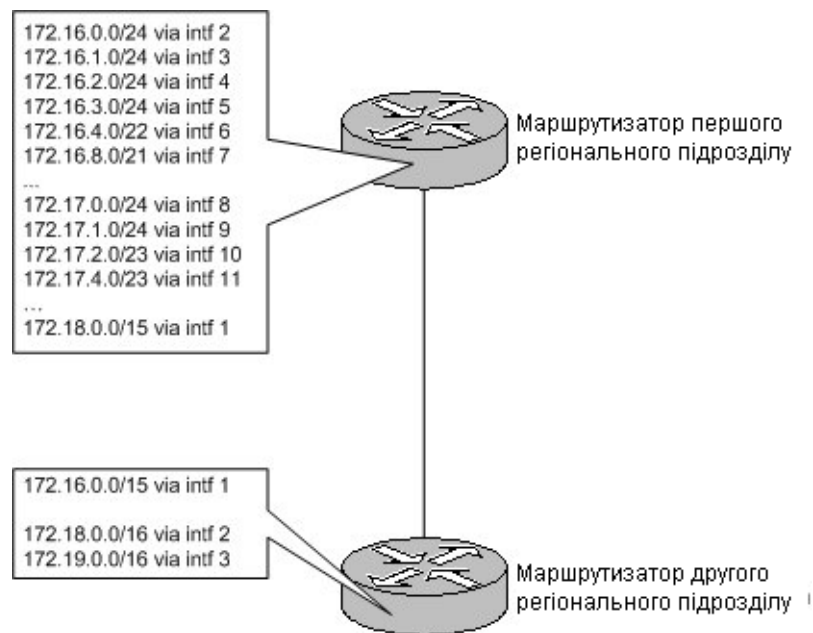
### **Безкласова міждоменна маршрутизація CIDR (Classless Inter-Domain Routing)**

Поява цієї технології викликана різким збільшенням обсягу трафіка у Internet і як наслідок, збільшенням кількості маршрутів на магістральних маршрутизаторах. Тож, якщо у 1994 році, до розгортання CIDR, таблиці маршрутизаторів містили до 70 000 маршрутів, то після запровадження їх число зменшилося до 30 000. На вересень 2002, кількість маршрутів перевищила оцінку 110 000! Уявляєте собі, скільки маршрутів потрібно було б тримати в таблицях сьогодні, якби не було CIDR!

Що ж являє собою ця технологія? Вона дозволяє уникнути класової схеми адресації, ефективніше використовувати адресний простір протоколу IP. З іншого боку, CIDR дозволяє збирати (агрегувати) маршрутні записи. Одним записом в таблиці маршрутизатора описуються шляхи до багатьох мереж.

Суть технології CIDR у тому, кожному постачальнику послуг Internet (чи, для корпоративних мереж, якомусь структурно-територіальному підрозділу) може бути призначений нерозривний діапазон IP-адрес. Вводиться поняття узагальненого мережного префікса, що визначає загальну частину всіх призначених адрес. Відповідно, маршрутизація на магістральних каналах може реалізовуватися з урахуванням узагальненого мережного префікса. Результатом є агрегування маршрутних записів, зменшення розміру таблиць маршрутних записів і підвищення швидкості обробки пакетів.

*Приклад:* центральний офіс компанії виділяє одному своєму регіональному підрозділу мережі 172.16.0.0/16 і 172.17.0.0/16, іншому – 172.18.0.0/16 і 172.19.0.0/16. Кожен регіональний підрозділ має свої обласні філії і з отриманого адресного блоку їм виділяються підмережі різних розмірів. Використання технології безкласової маршрутизації дозволяє з допомогою лише одного запису на маршрутизаторі другого підрозділу адресувати всі мережі й підмережі першого підрозділу. І тому вказується маршрут до неї 172.16.0.0 з узагальненим мережним префіксом 15. Вони повинні вказувати на маршрутизатор першого регіонального підрозділу (Мал.6.8).



**Рис. 6.8**

За своєю суттю технологія CIDR споріднена з VLSM. Тільки, якщо у випадку VLSM є можливість рекурсивного розподілу на підмережі, невидимі ззовні, то CIDR дозволяє рекурсивно адресувати цілі адресні блоки.

Використання CIDR дозволило розділити Internet на адресні домени, всередині яких передається інформація виключно про внутрішні мережі. Поза доменом використовується тільки спільний префікс мереж. В результаті багатьом мережам відповідає один маршрутний запис.

## Приклади

Наведемо деякі практичні приклади адресації. Проектування адресної схеми вимагає від фахівця скрупульозного опрацювання багатьох чинників, обліку можливого зростання і розвитку мережі.

Почнемо з прикладу розбивки мережі на підмережі. При будь-якому плануванні треба знати, скільки підмереж необхідно сьогодні і скільки може знадобитися завтра, скільки вузлів перебуває у найбільшій підмережі сьогодні й скільки можливо буде, у майбутньому.

З іншого боку, слід розробити хоча б схематичну топологію мережі із зазначенням всіх маршрутизаторів і шлюзів. Хорошою практикою є резервування ресурсів у майбутнє. Тож якщо у найбільшій підмережі є 60 вузлів, то не варто виділяти підмережу розмірністю у  $2^6 - 2 (=62)$  вузли! Не скупіться, вартість рішення можливої проблеми буде більшою, ніж вартість виділення вдвічі більшого блоку адрес. Однак не варто впадати й у іншу крайність.

### Приклад 1

*Організації виділено блок адрес 220.215.14.0/24. Розбити блок на 4 підмережі, найбільша з яких налічує 50 вузлів. Врахувати можливе зростання на 10%.*

На першому етапі необхідну кількість підмереж заокругляємо у більшу сторону до найближчого степеня числа 2. Оскільки у даному прикладі число необхідних підмереж дорівнює 4, округляти не потрібно. Визначимо кількість бітів, потрібних для організації 4 підмереж. Для цього представимо 4 як степінь двійки:  $4 = 2^2$ . Степінь – і є кількість бітів, відведених для номера підмережі. Оскільки мережевий префікс блоку дорівнює 24, то розширений мережевий префікс дорівнюватиме  $24 + 2 = 26$ .

Мережний префікс			Підмережа	Вузол
0	8	16	24 25	31
220.215.14.0/26 <-->	10010000	10010000	00001110	0 0
000000				
Розширений мережевий префікс				

Решта  $32 - 26 = 6$  біт використовуватимуться для номера вузла. Перевіримо, скільки вузлів може бути задано 6-ма бітами:  $2^6 - 2 = 62$  вузлів. Чи достатньо це, враховуючи 10% зростання? 10% від 50 вузлів -- це 5 вузлів, а 55 вузлів менше можливих 62-х. Отже, два біти для номера підмережі нас влаштовують.

Наступний етап — знаходження підмереж. Для цього двійкове представлення номера підмережі, починаючи від нульового, підставляється в біти, відведені для номера підмережі.

Основна мережа	11011100	11010111	00001110	00	000000	220.215.14.0/24
Підмережа 0(00)	11011100	11010111	00001110	00	000000	220.215.14.0/26
Підмережа 1(01)	11011100	11010111	00001110	01	000000	220.215.14.64/26
Підмережа 2(10)	11011100	11010111	00001110	10	000000	220.215.14.128/26
Підмережа 3(11)	11011100	11010111	00001110	11	000000	220.215.14.192/26
Розширений мережевий префікс						

Для перевірки правдивості наших обчислень, працює просте **правило: десяткові номери підмереж повинні бути кратними номеру першої підмережі**. На цьому правилі можна побудувати й інше, яке спрощує розрахунок підмереж: досить обчислити адресу першої підмережі, а адреси наступних визначаються множенням першої адреси на відповідний номер підмережі. У прикладі ми легко можемо встановити адресу третьої підмережі, просто помноживши  $64 * 3 = 192$ .

Як згадувалося, крім адреси підмережі, де всі біти вузлової частини рівні нулю, є ще одна службова адреса – широкомовна. Особливістю широкомовної адреси є те, що всі біти вузлової частини рівні одиниці. Розрахуємо широкомовні адреси наших підмереж:

підмережа |

ШМА підмережі 0 (00) | 11011100.11011100.00001110.00 111111 | 220.215.14.63/26  
 ШМА підмережі 0 (01) | 11011100.11011100.00001110.01 111111 | 220.215.14.127/26  
 ШМА підмережі 0 (10) | 11011100.11011100.00001110.10 111111 | 220.215.14.191/26  
 ШМА підмережі 0 (11) | 11011100.11011100.00001110.11 111111 | 220.215.14.255/26  
 | Розширений мережний префікс | Вузлова частина = всі 1

Легко помітити, що широкомовною адресою є найбільша адреса підмережі. Тепер, отримавши адреси підмереж та його широкомовні адреси, ми можемо побудувати таблицю використовуваних адрес:

№ підмережі	Найменша адреса підмережі	Найбільша адреса підмережі
0	220.215.14.1 - 220.215.14.62	
1	220.215.14.65 - 220.215.14.126	
2	220.215.14.129 - 220.215.14.190	
3	220.215.14.193 - 220.215.14.254	

Це і розбивка, що задовольняє умові.

## Приклад 2

У першому прикладі підмережі були однакового розміру -- по 6 розрядів. Часто зручніше мати підмережі різного розміру. Припустимо, одна підмережа потрібна для задання адрес двох маршрутизаторів, пов'язаних за схемою "точка-точка". У цьому випадку використовується лише дві адреси.

Розглянемо тепер випадок, коли компанії виділено блок адрес 144.144.0.0/16. Потрібно розбити адресний простір на три частини, виділити адреси для двох пар маршрутизаторів і залишити певний резерв.

Розділимо мережу 144.144.0.0/16 на чотири рівні частини, виділивши два біти для номера підмережі:

Октет	W	X	Y	Z	
Підмережа 0(00)	10010000	10010000	00	000000	00000000 144.144.0.0/18
Підмережа 1(01)	10010000	10010000	01	000000	00000000 144.144.64.0/18
Підмережа 2(10)	10010000	10010000	10	000000	00000000 144.144.128.0/18
Підмережа 3(11)	10010000	10010000	11	000000	00000000 144.144.192.0/18

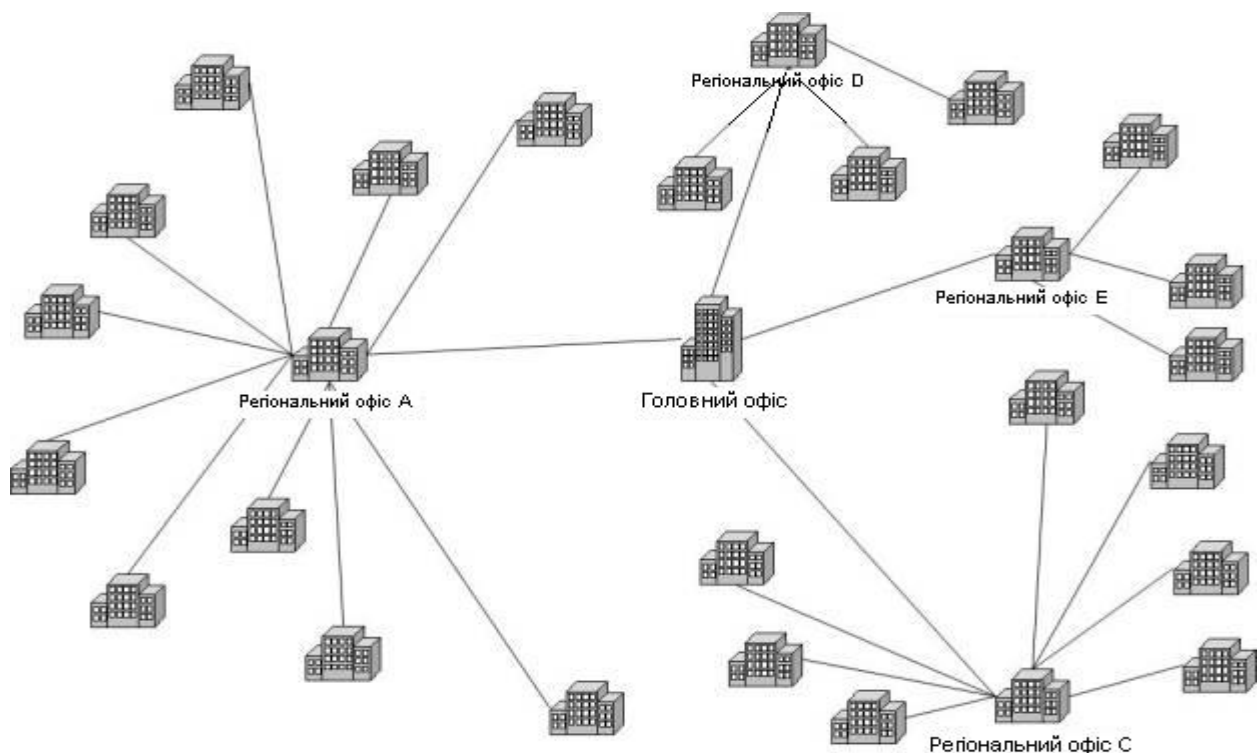
Усередині третьої підмережі виділимо дві підмережі розміром у чотири адреси:

		Підмережа № 3				№ вузла	
Підмережа 0(0)	10010000	10010000	11	000000	000000	00	144.144.192.0/30
Підмережа 1(1)	10010000	10010000	11	000000	000001	00	144.144.192.4/30
				Номер підмережі			

Отримані дві мережі використовуватимемо для адресації інтерфейсів маршрутизаторів. Адресний простір, що залишився, буде резервом, із якого виділятимемо адресні блоки за потребою. З решти адрес можна, наприклад, утворити 62 мережі розмірності класу С та ще декілька, трохи менших розмірів.

### Приклад 3

Компанія організовує корпоративну мережу. Схема розташування філій і канали, що їх пов'язують, наведено малюнку 6.9.



Мал.6.9.

Є чотири регіональних офіси, які пов'язані каналами з центральним офісом. До регіональних офісів, в свою чергу, підключені обласні філії цього регіону.

*Вирішено використовувати мережу 10/8 для корпоративної мережі. Потрібно скласти схему **IP-адресації** компанії. Домовимося відразу обирати спосіб адресації, найкращий з погляду маршрутизації.*

Для визначення розмірів регіональних офісів, складемо таблицю кількості підключених обласних філій до кожного регіональному офісу.

Регіональний офіс	Включено обласних філій	Відсоток
A	10	36%
C	7	25%
D	3	11%
E	3	11%

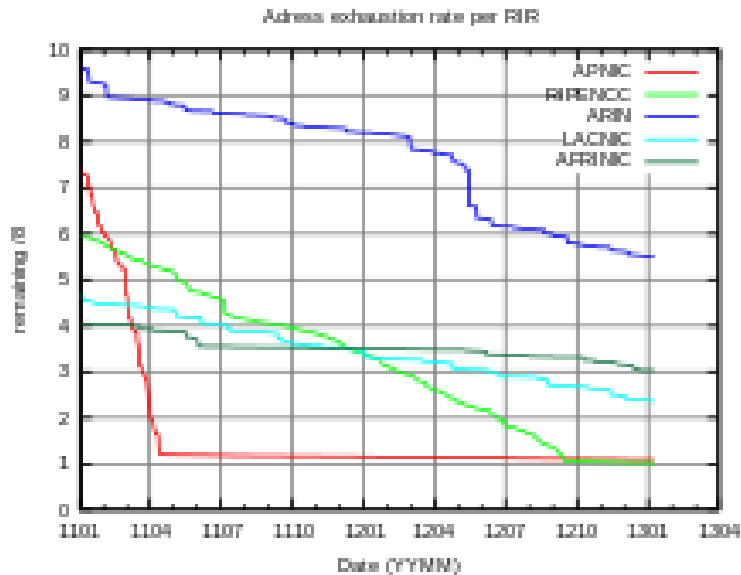
Відповідно до цієї таблиці розділимо адресний простір так (відразу ж зазначимо послідовні діапазони адресного простору):

Регіональний офіс	Відсоток адресного простору	Діапазон адрес	Блок виділених адрес
A	25%	<b>10.0-63.x.x</b>	10.0.0.0/10
C	25%	<b>10.64-127.x.x</b>	10.64.0.0/10
D	12,5%	<b>10.128-159.x.x</b>	10.128.0.0/11
E	12,5%	<b>10.160-191.x.x</b>	10.160.0.0/11
Резерв	25%	<b>10.192-255.x.x</b>	10.192.0.0/10

От ми й використали різні маски підмережі одній й тої ж мережі 10/8. Чому ми використовували для кожного офісу нерозривний адресний простір? А для того, щоб на центральному маршрутизаторі, шлях до всіх підмереж (читай: обласних офісів цього регіону) вказувався одним рядком!

Для повноти схеми, залишається визначити, як краще адресувати районні офіси. Можливо, досить віддати кожному офісу одну мережу /16. Цього буде досить навіть для великих офісів. Надлишок мереж поміщаємо у резерв.

Незважаючи на усі перелічені заходи запас IP адрес вичерпується і у 2012 р. запропоновано повністю перехід на версію протоколу IPv6.



Вичерпування запасу  
IP адрес регіональними реєстраторами у 2011 році.



## СПИСОК ЛІТЕРАТУРИ

1. *Беленькая Н.М., Сченснович В.В.* Операционные системы для локальных вычислительных сетей на базе персональных компьютеров //Интеркомпьютер, 1991, №1-2, С.28-34.
2. *Бертсекас Д., Галлагер Р.* Сети передачи данных. М.: Мир, 1989.
3. *Богуславская Л.Б.* Управление протоколами данных в сетях ЭВМ. М.: Энергоатомиздат, 1984.
4. *Буров Є.* Комп'ютерні мережі. – Львів.: БаК, 2002. –584с.
5. *Бурцев В. С.* Московская научная школа академика С. А. Лебедева в развитии вычислительной техники. /«Информационные технологии и вычислительные системы», 2002. №3.
5. *Веттис Д.* Novell NetWare/ Пер. с нем. К.: Торгово-издательское бюро BHV, 1993. –528с.
6. *Вудвард Дж.* Введение в систему NetWare. Рязань: Versus Ltd., 1992.
7. *Галицин В.К., Левченко Ф.А.* Багатокористувацькі обчислювальні системи та мережі: навч.посібник. – К.: КНЕУ, 1998. –360с.
8. *Довгаль С.И., Литвинов Б.Ю., Сбитнев А.И.* Персональные ЭВМ: ТурбоПаскаль V6.0. Объектное программирование. Локальные сети. К.: Информсистема сервис, 1993.
9. *Зайцев С.С.* Описание и реализация протоколов сетей ЭВМ. М.: Наука, 1989.
10. Каталог продуктов фирмы NOVELL. //КомпьютерПресс, 1992, № № 3-5,7.
11. *Кролл Э.* Все об ИНТЕРНЕТ. –К.: BHV, 1995
12. *Кукуруза П.В.* Концепция клиент/сервер. //Компьютеры + Программы, 1993, №7(8).
13. *Кулаков Ю.А., Луцкий Г.М.* Компьютерные сети: Учеб.пособие.–К.: Юниор, 1998.–384с.
14. *Лазарев В.Г.* Сетевые протоколы и управление в распределенных вычислительных сетях. М.: Наука, 1986.
15. Локальные сети от А до Я: Курс обучения. //КомпьютерПресс, 1990-1991.
16. Локальные сети NetWare. Пособие для начинающего пользователя. Рига: О.О.О.БИС, 1994.
17. *Лоренс Б.* Novell NetWare 4.1 в подлиннике. BHV - Санкт-Петербург, 1989. –720с.
18. *Лоу Д.* Компьютерные сети для "чайников". К.: Диалектика, 1995.

19. *Лауристон Р.* Сетевые ОС: пальма первенства у Netware. // Мир ПК, 1991, №3, С.95-104.
20. *Нанс Б.* Компьютерные сети /Пер.з англ. М.: БИНОМ, 1996.
21. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы (4-е издание). . –С.-П., М., Харк., Минск: Питер, – 2010.
22. Организация локальных сетей на базе персональных компьютеров.М.: И.В.К.–СОФТ, 1991.
23. *Осадчук.А.* Сетевые архитектуры современных информационно-вычислительных систем. // Компьютер Пресс, 1995, №15, С112-116.
24. *Смирнов А.А.* Архитектура вычислительных систем. М.: Наука, 1990.
25. *Спортак М., Паппас Ф., Рензинг Э.* Высокопроизводительные сети. Энциклопедия пользователя. - К.: DiaSoft, 1998. –432с.
26. *Страхарчук А.Я., Страхарчук В.П.* Інформаційні технології в економіці: навч.посібник. –К.:НМЦ "Укооспосвіта", 1999. – 357с.
26. *Стягар О.М., Рикалюк Р.Є.,Гудзь Р.В.* Методичні вказівки до застосування локальної комп'ютерної мережі NetWare V.3.11(основні поняття). –Львів, ЛДУ, 1995.
27. *Шатт С.* Мир компьютерных сетей. К.: Торгово-издательское бюро BHV, 1996.
28. *Флинт Д.* Локальные сети ЭВМ. Архитектура, принципы построения, реализация. М.: Финансы и статистика, 1986.
29. *Фигурнов В.Э.* IBM PC для пользователя. 6-е изд. М.: Инфра-М, 1996.
30. ЭВМ и вычислительные сети. Под ред.В.Н.Криушина. М.: Статистика, 1980.
31. *Рикалюк Р.Є.,Стягар О.М., Данчак П.В.* Вступ до комп'ютерних мереж.Текст лекцій. –Львів, ЛДУ, 1996.–60с.
32. *Горлач В.М.,Макар В.М.* Побудова та адміністрування INTRANET- мереж. Ч.1. Основи мережних технологій:Тексти лекцій. –Львів, Видавн. центр ЛДУ, 1999.–45с.
33. *Горлач В.М.,Макар В.М.* Побудова та адміністрування INTRANET- мереж. Ч.2. Адміністрування мереж WindowsNT:Тексти лекцій. –Львів, Видавн. центр ЛДУ, 1999.– 40с.
34. *Кульгин М.* Технологии корпоративных сетей. Энциклопедия. –С.-П., М., Харк., Минск: Питер, 2000.

35. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.
36. Peterson L., Davie B. Computer Networks: a system approach. МК, San Francisco, 2000.
37. Е. Неммет, UNIX. Керівництво системного адміністратора.
38. Д. Шиндлер, Основы комп'ютерних мереж
39. И. Песин. Повесть об IP-адресации  
[http://gazette.linux.ru.net/rus/articles/povest\\_ob\\_ip](http://gazette.linux.ru.net/rus/articles/povest_ob_ip).
40. Юрий Ревич. Как СССР создал первую в мире  
вычислительную сеть глобального масштаба.  
[http://slon.ru/future/rossiya\\_rodina\\_setey-430638.xhtml](http://slon.ru/future/rossiya_rodina_setey-430638.xhtml)
41. rfc990 (Адресна схема протоколу IP)
42. rfc997 (Адресна схема протоколу IP)
43. rfc1003 (VLSM)
44. rfc1517 (CIDR)
45. rfc1518 (CIDR)
46. rfc1519 (CIDR)
47. rfc1520 (CIDR)

## ЗМІСТ

	стор.
ВСТУП	3
1. АРХІТЕКТУРА РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ	4
1.1 Виникнення комп'ютерних мереж	4
1.2 Класифікація мереж	12
1.3. Організація передачі повідомлень в мережах. Методи передавання даних	14
1.4..Теоретичні основи передачі даних	15
1.5. Мережа з маршрутизацією пакетів	16
1.6. Мережа із селекцією пакетів	17
1.7. Стандарти інформаційно-обчислювальних мереж	19
2. АРХІТЕКТУРА ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ	36
2.1. Основні поняття. Топологія мереж	36
2.2 Основні типи ЛКМ, їх характеристики	45
а. мережа Ethernet	45
б. Token Ring (маркерне (естафетне) кільце)	48
в. Token Bus (Маркерна (естафетна) шина)	51
г. Опти-волоконний розподільчий інтерфейс	53
д. мережа Apple Talk	55
е.Мережа ARCnet	56
ж. Мережа Fast Ethernet	57
з. Мережа Gigabit Ethernet	58
і. Мережа Gigabit Ethernet	60
2.3.Компоненти та устаткування ЛКМ. Вибір типу файл-сервера, інтерфейси	61
2.4 Поняття про корпоративні мережі	65
2.5. Безпроводові мережі	74
2.6. Оптичні мережі	
3. ОПЕРАЦІЙНІ СЕРЕДОВИЩА ЛКМ	78
3.1. Архітектура програмних засобів	78
3.2. Основні характеристики ОС	91
3.3. Мережні обчислення	98
4. СІМ'Я ОС Netware	99
4.1. Загальні відомості	99
4.2 Програмне забезпечення файл-сервера та робочих станцій. Багатосерверні мережі	100
4.3.Адресація в мережі. Маршрутизація	104
4.4 Можливості Netware (основні)	105

5. ОДНОРАНГОВІ ЛКМ	112
6. ПРОТОКОЛИ ГЛОБАЛЬНИХ ТА ЛОКАЛЬНИХ МЕРЕЖ	119
6.1. Стек протоколів ТСП/ІР. Історія та перспективи стека ТСП/ІР	119
6.2. Маршрутизація. Протокол ІР	134
Список літератури	153

Навчальне видання

Роман Євстахович Рикалюк

## КОМП'ЮТЕРНІ МЕРЕЖІ

Редактор М.М.Мартиняк-Жовтанецька

Підписано до друку . Формат 60х84/16. Папір друк.№2.  
Різогр.друк. Умовн.друк.арк. 3.2. Умовн.фарбовідб. 3.2.  
Обл.-вид.арк. 3.5. Тираж 200 прим. Зам. 1.

---

Видавничий центр Львівського національного університету  
імені Івана Франка  
79602, Львів-центр, вул.Дорошенка, 37