Курс лекцій

Бендюг В.І.,
Комариста Б.М.

[Основи комп’ютерно – інтегрованого управління та комп’ютерні мережі]

Метою вивчення цієї дисципліни є забезпечення студентів необхідними базовими навичками в галузі комп’ютерних мереж, серед яких функціонування, експлуатація та адміністрування мережі, які вони зможуть використовувати в подальшому процесі навчання.

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Хіміко-технологічний факультет

Основи комп'ютерно – інтегрованого управління та комп'ютерні мережі

Курс лекцій

для студентів напряму підготовки
6.050202 – «Автоматизація та комп'ютерно-інтегровані технології»

Затверджено методичною радою
хіміко-технологічного факультету НТУУ «КПІ»

Київ – 2014

Основи комп'ютерно – інтегрованого управління та комп'ютерні мережі. Курс лекцій *для студентів напряму підготовки 6.050202 – «Автоматизація та комп'ютерно-інтегровані технології»* [Електронний ресурс] / [уклад. Бендюг В.І., Комариста Б.М.]. – К: 2014. – 90 с. Систем. вимоги: MS Windows; Adobe Acrobat Reader — Назва з екрану.

Гриф надано методичною радою ХТФ НТУУ "КПІ", протокол № 00 від 00.00.2014 р.

Електронне навчальне видання

Основи комп'ютерно – інтегрованого управління та комп'ютерні мережі

Курс лекцій

для студентів напряму підготовки
6.050202 – «Автоматизація та комп'ютерно-інтегровані технології»

Укладачі: Бендюг Владислав Іванович, , канд. техн. наук, доцент
Комариста Богдана Миколаївна

Відповідальний редактор Д. М. Складаний, канд. техн. наук, доцент

Рецензент О. В. Косогін, канд. техн. наук, доцент.

За редакцією укладачів

ЗМІСТ

ЗМІСТ 3

ВСТУП 5

Розділ 1 Знайомство з комп'ютерними МЕРЕЖАМИ 6

Тема 1.1. Поняття локальних комп'ютерних мереж 6

1.1.1. Для чого потрібна мережа 6
1.1.2. Варіанти використання мережі 6
1.1.2.1. Мережа для роботи 6
1.1.2.2. Мережа для навчання 7
1.1.2.3. Мережа для бізнесу 7
1.1.3. Передумови для організації мережі 7
1.1.4. Загальні відомості про ЛОМ 8
1.1.4.1. Багаторівнева модель мережі 8
1.1.4.2. Проблеми перетворення даних при передачі 10
1.1.4.3. Середовище передачі даних 10
1.1.4.4. Протоколи та стандарти 12
1.1.4.5. Робота в режимі клієнт-сервер 18
1.1.4.6. Типові топології ЛОМ 19
1.1.4.7. Локальна мережа Ethernet 22
1.1.4.8. Локальна мережа Token Ring 22
1.1.4.9. Локальна мережа Arknet 22
1.1.5. Вибір оптимального середовища передачі даних 23
1.1.6. Вибір топології локальної мережі 24

Тема 1.2. Високошвидкісні технології локальних обчислювальних мереж 25

1.2.1. Технологія Fast Ethernet (IEEE 802.3u) 25
1.2.1.1. Fast Ethernet як розвиток класичного Ethernet'a 25
1.2.1.2. Створення стандартові Fast Ethernet 27
1.2.1.3. Підрівень Logical Link Control (LLC) 28
1.2.1.4. Підрівень керування доступом до середовища Media Access Control (MAC) 29
1.2.1.5. Формати кадрів 30
1.2.1.6. У яких випадках рекомендується використовувати Fast Ethernet 32
1.2.2. Технологія FDDI 34
1.2.2.1. Історія створення стандартові FDDI 34
1.2.2.2. Основи технології FDDI 34
1.2.2.3. У яких випадках рекомендовано використовувати технологію FDDI 39
1.2.3. Технологія 100VG-AnyLAN 39
1.2.3.1. Загальна характеристика технології 100VG-AnyLAN 39
1.2.3.2. Структура мережі 100VG-AnyLAN 40
1.2.3.3. Стек протоколів технології 100VG-AnyLAN 43
1.2.4. Перспективи високошвидкісних технологій – перехід на гігабітні швидкості 43

Розділ 2 Протоколи tcp/ip 45

Тема 2.1. Стек протоколів TCP/IP 45

2.2.1. Історія та перспективи стеку TCP/IP 45
2.1.2. Структура стеку TCP/IP 46
2.1.3. Адресація в IP-мережах 49
2.1.3.1. Типи адреса: фізична (MAC-адреси), мережева (IP-адреси) та символьна (DNS-ім'я) 49
2.1.3.2. Три основні класи IP-адреси 50
2.1.3.3. Особливі IP-адреси 51
2.1.3.4. Використання масок у IP-адресації 52
2.1.3.5. Порядок розподілення IP-адреса 53
2.1.3.6. Автоматизація процесу призначення IP-адреса 54
2.1.3.7. Перетворення IP-адреса в локальні адреси 55
2.1.3.8. Перетворення доменних імен у IP-адреси 57
Резюме 61
2.1.4. Протокол IP 62

2.1.4.1. Формат пакетові IP 62
2.1.4.2. Керування фрагментацією 63
2.1.4.3. Маршрутизація з допомогою IP-адреса 65
2.1.4.4. Приклад взаємодії вузлів з використанням протоколові IP 68
2.1.4.5. Структуризація мереж IP з допомогою масок 71
2.1.5. Протокол надійної доставки повідомлень TCP 72
2.1.5.1. Сегменти TCP 72
2.1.5.2. Порти та встановлення TCP-з'єднань 72
2.1.5.3.Концепція квітирування 73
2.1.5.4. Реалізація методові вікна в протоколі TCP 75
2.1.5.5. Вибір тайм-ауту 75
2.1.5.6. Реакція на перевантаження мережі 75
2.1.5.7. Формат повідомлення TCP 76
2.1.6. Протокол доставки дейтаграм користувача UDP 76
2.1.6.1 Зарезервовані та доступні порти UDP 77
2.1.6.2. Мультиплексування та демультиплексування прикладних протоколів за допомогою протоколові UDP 77
2.1.6.3. Формат повідомлень UDP 78
2.1.7. Протоколи прикладного рівня 78
2.1.6.1. Протокол TELNET 79
2.1.6.2. Протокол FTP 79
2.1.6.3. Протокол SMTP 79
2.1.6.4. NFS 79
2.1.6.5. Протокол SNMP 80

Тема 2.2. Internet 80
2.2.1.Необхідність Інтернету 80
2.2.2. Інтернет TCP/IP 81
2.2.2.3. Засобу Інтернету 81
2.2.2.3.1 Засобу Інтернету прикладного рівня. 82
2.2.2.3.2 Засобу Інтернету мережевого рівня. 83
2.2.2.4. Історія створення Інтернету 84
2.2.2.5. Група Активності Інтернету(IAB). 86
2.2.2.6. Нова організація IAB 86
2.2.2.7 Технічні звіти Інтернету 87
2.2.2.8. Протоколи Інтернету і стандартизація. 88
2.2.2.9. Майбутні ріст і технологія 88
2.2.2.10 FNC і NREN 89
2.2.2.11. Підсумки. 89

Література 90

Основна література 90

Додаткова література 90

ВСТУП

Дисципліна “Основи комп’ютерно – інтегрованого управління та комп’ютерні мережі” викладається згідно з учбовим планом бакалаврської підготовки хіміко-технологічного факультету й призначена ознайомити майбутніх фахівців хімічної промисловості з функціонуванням, керуванням комп’ютерними мережами зв’язку та роботою в них.

Дисципліна “Основи комп’ютерно – інтегрованого управління та комп’ютерні мережі” базується на знаннях студентів про принципи роботи ПЕОМ, вмінні працювати в операційних середовищах Microsoft Windows (викладається в дисципліні “Комп’ютерна техніка та організація обчислювальних робіт”), та на їх досвіді програмування, набутому на основі курсу “Програмування та алгоритмічні мови”.

Даний курс вивчається в 3-му семестрі: всього 144 години, в тому числі лекцій – 18 години, лабораторних занять 36 години, самостійна робота студентів 90 годин, включає проведення модульної контрольної роботи і закінчується екзаменом.

Метою вивчення цієї дисципліни є забезпечення студентів необхідними базовими навичками в галузі комп’ютерних мереж, серед яких функціонування, експлуатація та адміністрування мережі, які вони зможуть використовувати в подальшому процесі навчання.

В результаті вивчення дисципліни студент повинен знати:

- основні принципи роботи комп’ютерних мереж;
- призначення апаратних компонентів, які забезпечують функціонування мережі;
- основи компонування мережі;
- мережні архітектури;
- принципи експлуатації мережі;
- основні мережні протоколи.

Крім того студент повинен вміти:

- встановлювати мережеву операційну систему;
- проводити моніторинг мережі;
- захищати інформацію в мережі;
- працювати з всесвітньою мережею Internet.

Знання та навички, одержані при вивченні цього курсу, у подальшому використовуються в усіх дисциплінах, які потребують використання додаткової інформації, що можна отримати з мережі з використанням ПЕОМ, і в першу чергу в курсовому та дипломному проектуванні де потребується аналіз та обробка великої кількості новітніх даних та робіт проведених останнім часом.

РОЗДІЛ 1 ЗНАЙОМСТВО З КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

Тема 1.1. Поняття локальних комп'ютерних мереж

1.1.1. Для чого потрібна мережа

Використання мережі надає користувачам наступні додаткові можливості:

- оперативного обміну інформацією між користувачами;
- одержання і передачі повідомлень у виді електронної пошти, факсів, голосової пошти й інших видів повідомлень;
- миттєвого одержання інформації з будь-якої крапки земної кулі;
- вилученого керування виробничими процесами і вилученим адмініструванням;
- обміну інформацією між комп'ютерами, що працюють на різних платформах.

Розглянемо більш детально основні переваги, що надає користувачам об'єднання комп'ютерів у мережу:

1) Поділ ресурсів, що припускає спільне використання периферійних пристроїв, таких як принтери, а також дискового простори вилучених комп'ютерів, що дозволяє більш раціонально використовувати наявну дискову пам'ять і принтери.
2) Поділ даних — надання доступу і можливості керування базами даних з вилучених робочих місць, що мають у цьому необхідність.
3) Спільне застосування програмних засобів.
4) Використання обчислювальної потужності вилученого процесора, що дозволяє істотно знизити витрати на модернізацію устаткування, відновлення парку комп'ютерів, оскільки з'являється можливість одержати термінальний доступ, коли комп'ютер з невеликими можливостями підключається до більш могутнього комп'ютера і використовується як вилучений термінал — клавіатура з дисплеєм і засіб зв'язку з вилученою робочою станцією.
5) Можливість багатокористувацького режиму роботи з програмами і документами.

Навіть з'єднання всього двох комп'ютерів між собою може принести істотні вигоди і зручності.

1.1.2. Варіанти використання мережі

Користувачі можуть використовувати надані мережею додаткові можливості цілком або частково, постійно або тимчасово. Це залежить від конкретної задачі, заради якої застосовується дана мережа, тобто від її призначення. Розглянемо кілька варіантів застосування мережі для різних цілей.

1.1.2.1. Мережа для роботи

Тут мається на увазі робота, зв'язана з обробкою текстових і графічних матеріалів, обчисленнями, звертанням до бази даних, тобто та робота, що виконується колективно, але розподілена в просторі і часі таким чином, що тільки зв'язок між комп'ютерами дозволяє оперативно використовувати результати роботи колеги або результати своєї роботи при продовженні її на іншому комп'ютері. У цьому випадку комп'ютери в мережі мають рівноправне положення, і кожен користувач може, при наявності прав доступу, одержувати інформацію або використовувати ресурси іншого комп'ютера.

Можливо, що один комп'ютер виділений особливо. Його ресурси можуть використовуватися всіма користувачами й у його пам'яті зберігаються результати праці всієї групи, оскільки надійність збереження інформації в цій виділеній машині може бути

вище, ніж в інших. Такий комп'ютер називається файл-сервер. Підвищена надійність може бути забезпечена особливим пристроєм дискової підсистеми комп'ютера, що, безсумнівно, відіб'ється на його ціні. У невеликих мережах витрати на устаткування не повинні бути дуже високими, а надійність збереження інформації можна забезпечити регулярним збереженням даних в архівах, дублюванням збережених даних, чим, власне, і займаються вищезгадані дорогі дискові підсистеми, але в автоматичному режимі.

1.1.2.2. Мережа для навчання

Це може бути комп'ютеризований клас, у якому один комп'ютер виділений для викладача, а інші — для учнів, причому з виділеного комп'ютера повинний бути доступ до кожного комп'ютера класу з можливістю втручання в його роботу і роботу учня. Зворотний доступ від учня до викладача може бути передбачений тільки в обмеженому виді, для одержання завдань і пересилання відповідей. Такий клас зовсім не обов'язково повинний розташовуватися в одному приміщенні. Він цілком може бути розподіленим по території організації для навчання співробітників на робочих місцях. У цьому випадку підвищені вимоги пред'являються до комп'ютера викладача, а інші комп'ютери можуть бути самими звичайними. Саме собою зрозуміло, що така організація мережі може застосовуватися і зовсім в інших цілях. Можливо, необхідний постійний контакт із групою співробітників для своєчасного втручання в який-небудь колективний процес розрахунку. Це може бути і просто сеанс одночасної шахової гри з декількома супротивниками.

1.1.2.3. Мережа для бізнесу

Мережа, що відповідає такій розпливчастій вимозі, конкретно визначити важко, оскільки і два попередні варіанти можуть бути варіантами бізнесу. Але все-таки деякі особливості такої мережі можна виділити. Кілька комп'ютерів даної мережі можуть мати спеціалізоване призначення, при цьому доступ до кожного з них обмежений для більшості користувачів. Вільний доступ передбачений тільки до частини інформації, що можуть використовувати фахівці. Так, можливий розподіл співробітників на кадрову службу, бухгалтерію, відділ продажів і інші відділи. Ви, як керівник і мережевий адміністратор, одержуєте доступ до всіх ресурсів для можливості контролю й одержання різних звітів і довідок. Обмеження доступу до інформації не завжди спрямовано на збереження якої-небудь таємниці. Часто це зв'язано з прагненням відгородити важливі файли від впливу випадкових факторів, що руйнує.

1.1.3. Передумови для організації мережі

Передумовами для організації мережі можуть бути наступні умови:

- деяка кількість окремо працюючих комп'ютерів, не спроможних гнучко обмінюватися інформацією між собою і з іншими територіально вилученими комп'ютерами;
- необхідність створення загальнодоступної бази даних для нагромадження і збереження інформації в необхідних обсягах і з необхідною оперативністю доступу;
- накопичене програмне й інформаційне забезпечення, не використовуване в повному обсязі і не має загального стандарту збереження;
- можливість підключення до глобальної обчислювальної мережі (наприклад, Internet) обмежена підключенням окремих користувачів, що не має зв'язки з іншими комп'ютерами, що знижує ефективність даного підключення і вимагає додаткових витрат для розширення доступу до глобальної мережі у виді організації додаткових підключень.

Вас таке положення не влаштовує, і змінити ситуацію може тільки організація

обчислювальної мережі у відповідним вашим умовам масштабах, що поєднує весь парк комп'ютерів (усіх користувачів) у єдиний інформаційний простір (ЕИП), що володіє наступними властивостями:

- система збереження й обробки даних, створених у різний час і різних користувачів, доступна всім користувачам мережі в будь-який момент часу, що дозволяє підвищити оперативність і ефективність рішення багатьох задач за рахунок колективного використання даних і результатів роботи кожного. При цьому можливий оперативний контроль над ходом роботи, узгодження й об'єднання її результатів з метою одержання максимально ефективного готового рішення;
- вірогідність і надійність збереження інформації підвищені за рахунок високої перешкодостійкості й відмовостійкості системи, забезпечуваної завдяки ефективному резервуванню й організації архівного збереження даних;
- спрощений пошук необхідної інформації за рахунок використання об'єднаного архіву;
- стандартизація документообігу відповідно до загальних вимог;
- забезпечення доступу до інформації авторизованому користувачеві відповідно до даними йому правами доступу і привілеями.

1.1.4. Загальні відомості про ЛОМ

Під локальною обчислювальною мережею розуміють спільне підключення декількох окремих комп'ютерних робочих місць (робітників станцій) до єдиного каналу передачі даних, при якому користувачі одержують можливість одночасного використання програм і баз даних, знаходячись на своїх робочих місцях.

У сучасній технічній літературі часто застосовується інше скорочення для цього поняття — англомовне LAN (Local Area Network).

За допомогою ЛВС користувачі персональних комп'ютерів, розташованих на вилучених робочих місцях, можуть спільно використовувати устаткування, програмне забезпечення й інформацію. Ліквідуються обмеження, накладені географічним, просторовим поділом робочих місць.

1.1.4.1. Багаторівнева модель мережі

Для забезпечення однакового представлення даних при передачі інформації в лініях зв'язку була сформована Міжнародна організація по стандартизації (ISO — International Standards Organization). Ця організація призначена для розробки моделі міжнародного комунікаційного протоколу, у рамках якої повинні створюватися міжнародні стандарти систем передачі даних.

ISO (International Organization for Standardization - Міжнародна організація по стандартизації, часто також називана **International Standards Organization).** Асоціація національних організацій по стандартизації, що забезпечує розробку і підтримку глобальних стандартів у сфері комунікацій і обміну інформацією. Добре відома семирівнева модель OSI/ISO, що визначає стандарти взаємодії комп'ютерів у мережах.

ISO розробила базову модель взаємодії відкритих систем (OSI — Open Systems Interconnection). Ця модель стала міжнародним стандартом для розробки систем передачі даних. Модель містить сімох рівнів:

1) Фізичний — бітові протоколи передачі даних.
2) Канальний — формування кадрів, керування доступом до середовища.
3) Мережевий — маршрутизація, керування потоками даних.
4) Транспортний — забезпечення взаємодії вилучених процесів.
5) Сеансовий — підтримка діалогу між вилученими процесами.

6) Представницький — інтерпретація переданих даних.
7) Прикладний — користувальницьке керування даними.

OSI model (Open Systems Interconnection model - Модель взаємодії відкритих систем). Семирівнева ієрархічна модель, розроблена Міжнародним комітетом зі стандартизації (ISO) для визначення, специфікації і зв'язку мережних протоколів.

Основна ідея цієї моделі полягає в тім, що кожному рівневі приділяється конкретна роль. Завдяки цьому загальна задача передачі даних розчленовується на окремі, легко доступні для огляду задачі. Необхідні угоди для зв'язку одного з рівнів з вищестоящими і нижчестоящими рівнями називаються *протоколом*.

Протокол (protocol). Формат опису переданих повідомлень і правила, по яких відбувається обмін інформацією між двома або декількома системами.

Процес взаємодії користувача з мережним середовищем полягає в послідовному перетворенні переданих користувальницьких даних на передавальній стороні від сьомого рівня до першого з наступним зворотним перетворенням на прийомній стороні.

- На першому, фізичному рівні, визначаються електричні, механічні, функціональні і процедурні параметри для фізичного зв'язку в системах. Фізичний зв'язок і нерозривна з нею експлуатаційна готовність є основною функцією 1-го рівня. Стандарти фізичного рівня включають рекомендації V.24 МККТТ (CCITT), EIA RS232, X.21 і інші. Усе більше значення для функції передачі даних здобуває стандарт ISDN (Integrated Services Digital Network, Цифрової мережі з інтеграцією послуг). Як середовище передачі даних використовують мідний кабель (екранована кручена пари), коаксіальний кабель, оптоволоконний кабель і радіорелейну лінію.

CCITT (International Consultative Committee for Telegraphy and Telephony – Міжнародний Консультативний Комітет з Телефонії і Телеграфії, МККТТ). Підрозділ Міжнародного Телекомунікаційного Союзу (ITU) ООН. CCITT розробляє технічні стандарти, відомі як "Recommendations" (рекомендації) по всіх міжнародних аспектах цифрових і аналогових комунікацій.

EIA (Electronic Industries Association - Асоціація електронної промисловості). Об'єднуючих виробників електронного устаткування організація зі штаб-квартирою у Вашингтоні. Основна задача асоціації - розробка електричний і функціональні специфікації інтерфейсного устаткування. Однієї з найбільш відомих розробок асоціації є інтерфейс RS-232C.

RS-232C. Стандартний інтерфейс послідовної передачі даних.

ISDN (Integrated Services Digital Network - Цифрова мережа з інтеграцією послуг). Технологія, запропонована споконвічно для міжнародного телефонного зв'язку. ISDN поєднує голосові і цифрові мережі в єдиному середовищі, даючи користувачеві можливість передачі по мережі голосу і даних. Стандарти, що керують ISDN, створюються CCITT.

- Канальний рівень перетворить дані, отримані від 1-го рівня, у так називані кадри і послідовності кадрів. На цьому рівні здійснюється керування доступом до передавального середовища, використовуваної декількома ЕОМ, синхронізація, виявлення і виправлення помилок. У свою чергу канальний рівень розділяється на два підрівня, що часто називають також рівнями. Канальний рівень (Data Link Layer) поділяється в локальних мережах на два підрівня:
  - логічної передачі даних (Logical Link Control, LLC);
  - керування доступом до середовища (Media Access Control, MAC).
- Мережевий рівень встановлює в обчислювальній мережі зв'язок між двома абонентами. З'єднання відбувається завдяки функціям маршрутизації, що вимагають наявності мережевої адреси в пакеті. До функцій мережевого рівня також відноситься обробка помилок, мультиплексування, керування потоками даних. Приклад стандарту цього рівня — рекомендація X.25 МККТТ (для мереж

загального користування з комутацією пакетів).

X.25. Рекомендації ITU - TSS (раніше CCITT - МККТТ), що визначають стандарти для комунікаційних протоколів доступу до мереж з комутацією пакетів (packet data networks - PDN).

- Транспортний рівень підтримує безперервну передачу даних між двома взаємодіючими один з одним користувальницькими процесами. Надійність і безперервність передачі даних забезпечуються завдяки можливості виявлення і виправлення помилок і апаратно-незалежної реалізації сервісу транспортування.
- Сеансовий рівень забезпечує керування діалогом, тобто координує прийом, передачу і підтримку одного сеансу зв'язку. Для координації необхідний контроль робочих параметрів, керування потоками даних проміжних нагромаджувачів і діалоговий контроль, що гарантує передачу наявних у розпорядженні даних. Крім того, сеансовий рівень додатково містить функції керування паролями, підрахунку оплати за використання ресурсів мережі, синхронізації і скасування зв'язку в сеансі передачі після збою внаслідок помилок у нижчерозташованих рівнях.
- Представницький рівень забезпечує форму представлення переданих по мережі даних; а також їхню підготовку для користувальницького прикладного рівня. На цьому рівні відбувається перетворення даних з кадрів, використовуваних для передачі даних, в екранний формат або формат для друкувальних пристроїв кінцевої системи.
- На прикладному рівні необхідно надати в розпорядження користувачів уже перероблену інформацію. З цим може справитися системне і користувальницьке прикладне програмне забезпечення.

1.1.4.2. Проблеми перетворення даних при передачі

Для передачі інформації з комунікаційних ліній вона перетвориться в ланцюжок наступний друг за другом бітів (двійкове кодування за допомогою двох станів: “0” і “1”).

Передані алфавітно-цифрові знаки представляються за допомогою бітових комбінацій. Бітові комбінації розташовуються у визначеній кодовій таблиці, що містить 4-, 5-, 6-, 7- або 8-бітові коди.

Кількість представлених знаків у коді залежить від кількості використовуваних у ньому бітів. Чотирибітовий код дозволяє передати максимум 16 значень, 5-бітовий код — 32 значення, 6-бітовий код — 64 значення, 7-бітовий — 128 значень і 8-бітовий код — 256 алфавітно-цифрових знаків.

1.1.4.3. Середовище передачі даних

У будь-якій мережі інформація від одного комп'ютера до іншого передається через деяке середовище передачі даних. Предметом нашого розгляду стануть кабельні мережі. У таких мережах інформація у формі електричного сигналу передається по кабелі. На сьогоднішній день для побудови мереж застосовуються три види кабелів:

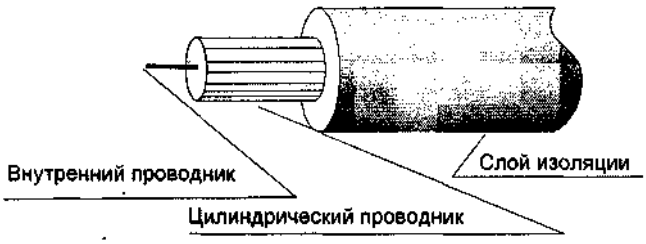
- коаксіальний;
- кручена пари;
- волоконнооптичний.

Від якості і характеристик кабелю багато в чому залежить якість роботи мережі. Тому не зайвим буде ознайомитися з застосовуваними кабелями більш докладно. Для передачі електричного сигналу потрібно, як мінімум, два провідники. По суті, і кабель являє собою два провідники, але конструктивно вони виконані таким чином, що переданий по них сигнал перетерплює менше перекручувань, менше загасає (втрачає в потужності), може мати більш широку смугу частот, чим сигнал, переданий по звичайних проводах.

Коаксіальний кабель (coaxial). Являє собою гнучкий, ізольований зовні циліндричний

провідник, усередині якого строго по його осі розташований другий провідник, а простір між провідниками заповнений діелектриком.

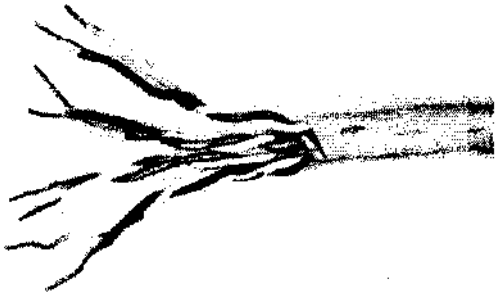
Існує кілька типів коаксіального кабелю, що відрізняються характеристиками й областями застосування – для локальних мереж, для глобальних мереж, для кабельного телебачення і т.п. (див. мал. 1.1.1).



Малюнок 1.1.1 - Пристрій коаксіального кабелю

Кручена пари (twisted pair). Скручена пара проводів. Кручена пара існує в екранованому варіанті **(Shielded Twisted Pair, STP)**, коли пари мідних проводів обертається в ізоляційний екран, і неекранованому **(Unshielded Twisted Pair, UTP)**, коли ізоляційна обгортка відсутня.

Неекранована кручена пари (мал. 1.1.2) або кабель UTP являє собою кабель, що складається з двох або більш пар, скручених між собою провідників, покритих ізоляцією й ув'язнених у загальну захисну полімерну "сорочку". Кожен провідник у такому кабелі має своє унікальне розцвічення і номер. Маркірування кабелю звичайно містить зведення про його категорії "CATEGORY 5 UTP". Зведення про застосування різних категорій кабелю приведені в табл. 1.1.1.



Малюнок 1.1.2 - Кабель на основі кручений пари

Таблиця 1.1.1 - Застосування різних категорій кабелю типу "кручена пари"

Категорія	*Область застосування*
1	Використовується для телефонних комунікацій і не підходить для передачі даних у комп'ютерних мережах
2	Використовується для передачі даних зі швидкість до 4 Мбіт/с включно
3	Використовується для передачі даних зі швидкість до 10 Мбіт/с включно. Застосовується в мережах
4	Використовується для передачі даних зі швидкість до 16 Мбіт/с включно. Застосовується в мережах Token Ring
5	Використовується для передачі даних зі швидкістю до 100 Мбіт/с включно. Застосовується в сучасних мережах

Волоконнооптичний кабель (optical fiber). Складається з тонких (5-6- мікрон) волокон, по яких поширюються світлові сигнали.

Волоконнооптичний кабель є найбільш якісним – він забезпечує передачу даних з дуже високою швидкістю (до 10 Гбіт/с і вище) і до того ж краще інших типів передавального середовища забезпечує захист даних від зовнішніх перешкод.

1.1.4.4. Протоколи та стандарти

При передачі інформації між однаковими обчислювальними системами і типами комп'ютерів, що розрізняються, застосовують різні коди. Для правильної і, отже, повної і безпомилкової передачі даних необхідно дотримувати погоджених і встановлених правил. Усі ці правила обговорені в протоколі передачі даних.

Протокол передачі даних описує складові і властивості процесу передачі даних.

- Синхронізація — механізм розпізнавання початку блоку даних і його кінця.
- Ініціалізація — установлення з'єднання між взаємодіючими партнерами.
- Блокування — розбивка переданої інформації на блоки даних строго визначеної максимальної довжини (включаючи пізнавальні знаки початку блоку і його кінця).
- Адресація — забезпечення ідентифікації різного використовуваного устаткування, що обмінюється один з одним інформацією під час взаємодії.
- Виявлення помилок — установка бітів парності й обчислення контрольних бітів.
- Нумерація блоків — присвоєння кожному блокові ідентифікаційного номера дозволяє виявити помилково передану або інформацію, що втратилася.
- Керування потоком даних — процес розподілу і синхронізації інформаційних потоків. Так, наприклад, якщо не вистачає місця в буфері пристрою або дані недостатньо швидко обробляються в периферійних пристроях (наприклад, принтерах), те це може привести до нагромадження повідомлень і/або запитів.
- Методи відновлення процесу передачі даних після його переривання, що дозволяють повернутися до визначеного положення для повторної передачі інформації.
- Дозвіл доступу — розподіл, контроль і керування обмеженнями доступу до даних ставляться в обов'язок пункту дозволу доступу (наприклад, “тільки передача” або “тільки прийом”).
- Мережні пристрої і засоби комунікацій. Під засобом комунікації розуміється середовище передачі.

Для забезпечення роботи мережі все її устаткування повинне працювати за визначеними стандартами і правилам, що дозволяють здійснювати неспотворену передачу інформації від одного комп'ютера мережі до іншого, а також домогтися сумісності комп'ютерів і мережних програм і устаткування різних виробників. Протоколів існує багато, оскільки кожний описує визначену сторону роботи мережі. Розглянемо одну з найважливіших груп протоколів, що застосовується в мережі, — TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol - протокол керування передачею/протокол Internet). Відомий також як стек протоколів Internet (Internet Protocol Suite). Даний стік протоколів використовується в сімействі мереж Internet і для об'єднання гетерогенних мереж.

Задумано ці протоколи для роботи в мережі Internet, що відбито й у їхній назві, але вони виявилися корисні і для локальних мереж. Багато програм для роботи в мережах використовують IP-протокол.

IP (Internet Protocol). Протокол мережевого рівня з набору протоколів Internet.

TCP/IP-протоколи відповідають за передачу і прийом минаючої по мережі інформації. Протокол TCP поділяє всю інформацію, що підлягає передачі, на окремі блоки — пакети.

TCP (Transmission Control Protocol). Основний транспортний протокол у наборі протоколів Internet, що забезпечує надійні, орієнтовані на з'єднання, повнодуплексні потоки. Протокол використовується для доставки даних.

Протокол IP ці пакети нумерує і розсилає по заздалегідь визначеній цифровій адресі у виді кадру інформації — пакета, у який вкладений пакет, створений на основі TCP-

протоколу. На прийомному кінці процедура виконується в зворотному порядку. Пакети приймаються, сортуються і збираються у вихідному сполученні. Цифровий, а вірніше IP-адреса, являє собою четирибайтову послідовність чисел, записуваних звичайно в десятковому виді, наприклад, так: 192.168.55.3. Мережі умовно поділяються на три класи. Кожному класові відповідає свій діапазон адрес (табл. 1.1.2).

Таблиця 1.1.2 - Діапазони адрес для класів мереж

Клас	*Маска підмережі*	*Діапазон*	*Зарезервовані адреси мережі*
A	255.0.0.0	01.0.0.0 - 126.0.0.0	10.0.0.0 - 127.0.0.0
B	255.255.0.0	128.0.0.0 - 191.255.0.0	169.254.X.X, 172.16.0.0 - 172.31.0.0
C	255.255.255.0	192.0.0.0 -222.0.0.0	192.168.0.0 - 192.168.255.0

Маска підмережі вказує на біти, призначені для вказівки адреси мережі, в інших полях адреси повинний розташовуватися адреса комп'ютера. Кожному класові мережі відповідає свій діапазон застосовуваних і незастосовуваних у Internet (зарезервованих) адрес.

Структура адреси стає більш зрозумілої при представленні в двійковому коді. Наприклад, маска 255.255.255.0 у двійковому коді виглядає так: 11111111.11111111.11111111.0. Усі поля адреси мережі зайняті одиницями. Адреса 198.168.55.1 у двійковому коді виглядає так: 11000110.10101000.110111.1. По таблиці можна визначити, що це адреса мережі класу "З", а адреса комп'ютера (вузла) виражений молодшою одиницею. Чим нижче клас мережі, тим більше адрес мережі може існувати, і тем менше комп'ютерів може знаходитися в такій мережі. Кожен комп'ютер у мережі має свою унікальну адресу, призначена адміністратором мережі або отриманий автоматично. Саме з такими адресами і працює протокол IP.

Навіть у самій складній мережі, що допускає передачу інформації з найбільш короткому або найменш завантаженому в даний момент шляху, пакети на прийомному кінці сортуються відповідно до послідовності їхньої передачі, тоді як реальна послідовність прийому може істотно відрізнятися від вихідної. Проте, перекручувань інформації не відбувається.

Крім TCP/IP-протоколів, нам буде потрібно інтерфейс NetBEUI. Така назва протоколу ми побачимо, набудовуючи комп'ютер для роботи в мережі.

NetBEUI (NetBIOS Extended User Interface - Протокол розширеного користувальницького інтерфейсу мережевої базової системи введення-висновку). Транспортний протокол, використовуваний Microsoft LAN Manager, Windows for Workgroups, Windows NT і іншими мережними ОС.

NetBIOS (Network Basic Input/Output System - Мережева базова система введення/висновку). Стандартний мережевий інтерфейс, запропонований для IBM PC і сумісних систем.

NetBIOS — це протокол, що доповнює специфікацію інтерфейсу NetBIOS, використовувану мережною операційною системою. NetBEUI формалізує кадр транспортного рівня, не стандартизований у NetBIOS. Даний інтерфейс відповідає не якомусь конкретному рівневі моделі OSI, а охоплює транспортний рівень, мережевий рівень і підрівень LLC канального рівня. NetBEUI взаємодіє прямо з NDIS рівня MAC. Таким чином, це не маршрутизований протокол. Цей протокол працює зі звичайними буквено-цифровими іменами і відповідає за сеанси передачі даних між вузлами мережі, у нашому випадку — між комп'ютерами. Він застосовується тільки в локальних мережах, і спрощує роботу з мережними адресами, дозволяючи використовувати зрозумілі імена комп'ютерів, що можуть бути зв'язані з ім'ям користувача або призначенням комп'ютера в мережі. Це істотно полегшує навігацію в мережі, пошук необхідної адреси і зв'язок з ним.

MAC (Media Access Control - керування доступом до середовища). Протокол, використовуваний для визначення способу одержання доступу робочих станцій до

середовища передачі, найбільше часто використовуваний у локальних мережах. Для ЛВС, що відповідають стандартам IEEE, MAC-рівень є нижнім підрівнем каналу передачі даних (data link layer).

IEEE(Institute of Electricaland Electronic Engineers - Інститут інженерів по електротехніці і радіоелектроніці). Професійне об'єднання, що випускають свої власні стандарти. Членами IEEE є ANSI і ISO.

ANSI (American National Standards Institute - Американський інститут стандартів). Організація, відповідальна за стандарти в США.

Різні фірми пропонували різні варіанти структури локальних мереж. Ці варіанти відбиті в різних стандартах, що описують правила з'єднання комп'ютерів у мережу, типи мережевого устаткування, застосовувані кабелі, рознімання та інші тонкості будівлі мережі. Ми будемо розглядати переважно стандарт Ethernet, широко використовуваний у нас і підходящий для роботи з розповсюдженими операційними системами і мережним устаткуванням.

Ethernet. Стандарт організації локальних мереж (ЛВС), описаний у специфікаціях IEEE і інших організацій. IEEE 802.3 Ethernet використовує смугу 10 Mbps і метод доступу до середовища CSMA/CD. Найбільш популярною реалізацією Ethernet є 10Base-T. Розвитком технології Ethernet є Fast Ethernet (100 Мбіт/сек).

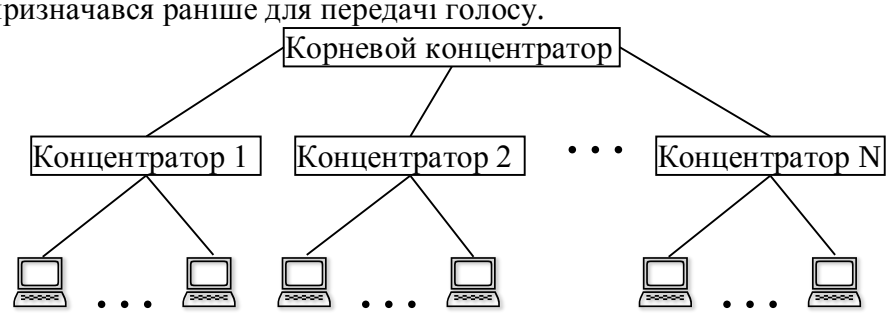
Після появи експериментальної мережі Ethernet Network фірми Xerox у 1975 році цей стандарт неодноразово модернізувався, з'явилося трохи його модифікацій. В даний час стандарт Ethernet застосовується більш ніж у п'ятьох мільйонах мереж, у яких задіяно понад п'ятдесят мільйонів комп'ютерів.

Застосування стандарту Ethernet дозволяє відносно простими засобами домогтися стабільної роботи мережі. Розглянемо ці засоби докладніше. Інформація в комп'ютерних мережах звичайно передається в двійковому коді, у тім виді, у якому неї можуть використовувати комп'ютери. Якщо кілька комп'ютерів одночасно передадуть якісь дані в мережу, то, незважаючи на наявність адреси, жоден комп'ютер цю інформацію прийняти не зможе. "Мішанина" з нулів і одиниць не буде розпізнане як осмислене повідомлення з визначеною адресою, і інформація буде загублена. Для того щоб не втрачати інформацію, включені в мережу комп'ютери повинні "поділити" цю мережу, а точніше середовище передачі даних, між собою. Можливі різні способи роздягнула цього середовища. За аналогією з радіо, можна було б передавати інформацію у виді високочастотного сигналу з частотною, фазовою або амплітудною модуляцією, розділивши застосовуваний у мережі частотний діапазон між комп'ютерами і використовуючи як адресу вузла значення довжини хвилі або частоти несущого цього сигналу. Недолік такого методу поділу середовища передачі даних очевидний. Щоб у такій мережі побачити всі підключені комп'ютери, потрібне сканування по всьому частотному діапазоні, а передача інформації, призначеної для декількох або навіть усіх комп'ютерів мережі, перетворюється в досить складну задачу. В усіх мережах типу Ethernet застосовується більш простий метод поділу середовища передачі даних — це метод CSMA/CD (Carrier-sense-multiply-access with collision detection, множинний доступ з контролем несущої і виявленням конфліктів). Іншими словами цей метод можна назвати так: "Метод колективного доступу з упізнанням несущої і виявленням колізій". Цей метод не вимагає розподілу частотного діапазону між комп'ютерами, що, крім спрощення всього процесу, підвищує швидкодію каналів зв'язку.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection - множинний доступ до середовища з виявленням конфліктів і детектуванням несущої). Метод доступу до середовища передачі (кабелеві), визначений у специфікації IEEE802.3 для локальних мереж Ethernet. CSMA/CD вимагає, щоб кожен вузол, почавши передачу, продовжував "прослухувати" мережа на предмет виявлення спроби одночасної передачі іншим пристроєм - колізії. При виникненні конфлікту, передача повинна бути негайно перервана і може бути відновлена після закінчення випадкового проміжку часу. У мережі Ethernet із

завантаженням 35-40% колізії виникають досить часто і можуть істотно сповільнити роботу. При невеликому числі станцій імовірність колізій істотно знижується.

Суть цього методу полягає в наступному: сформований TCP/IP пакет інформації міститься в окремий кадр даних, а комп'ютер чекає моменту, коли в мережі не буде несущою — фізичного носія інформації, що представляє собою електромагнітні коливання визначених частот. Комп'ютер чекає повної тиші. У тиші, що наступила, він передає свій кадр інформації. Інші комп'ютери виявляють факт передачі й аналізують наявність у переданому коді їхньої адреси. Знайшовши свою адресу, комп'ютер приймає інформацію і посилає відповідь про вдале завершення передачі кадру. Одночасна передача кадрів двома комп'ютерами приводить до ситуації, що називається колізія. Виявлення колізії — застава правильної передачі інформації. Передавальні комп'ютери порівняли те, що відправляли з тим, що виявилося в мережі, і при наступному зручному випадку знову постелють цей кадр. І так до одержання позитивної відповіді про прийом кадру. Таким чином, у кожен момент часу "говорити" дозволено одному комп'ютерові. Інші повинні "слухати". Ясно, що до одного кабелю неможливо підключити нескінченно велике число комп'ютерів. Частоти, на яких передається інформація в мережах Ethernet, досить високі. У нашому випадку вони досягають 16 Мгц. Але існують мережі, у яких ці частоти доходять до сотень мегагерц. Незважаючи на високі частоти несущої, тривалість самого кадру виявляється досить помітною. Крім того, після передачі або прийому інформації кожен комп'ютер повинний витримати паузу в 9,6 мкс, а після виявлення колізії тривалість паузи визначається по випадковому законі, і може приймати значення, що досягають 52,4 мс. За одиницю часу по мережі може передаватися деяка обмежена кількість інформації. Крім того, за технологією CSMA/CD, сигнал про виникнення колізії комп'ютер повинний одержати до закінчення передачі свого кадру. Отже, довжина кабелю в мережі теж обмежена. Як бачимо, на параметри мережі по об'єктивних причинах накладається цілий ряд обмежень. Певні обмеження накладаються і на тип використовуваного кабелю і мережевого устаткування стандартом 10Base-T. Цей стандарт припускає використання так називаної кручений пари — кабелю, що призначався раніше для передачі голосу.



Малюнок 1.1.3 - Можливий варіант побудови мережі

Застосування якісного телефонного кабелю для передачі інформації в комп'ютерних мережах виявилося надзвичайно плідним. У стандарті визначені також концентратори або хаби (hub). Ці пристрої призначені для підключення до однієї крапки кабелю декількох комп'ютерів. Для надійної роботи мережі кількість концентраторів між будь-якими двома робочими станціями не повинне бути більше чотирьох (правило чотирьох хабів). У результаті обліку всіх обмежень стандарт 10Base-T дозволяє створити мережу з наступними параметрами:

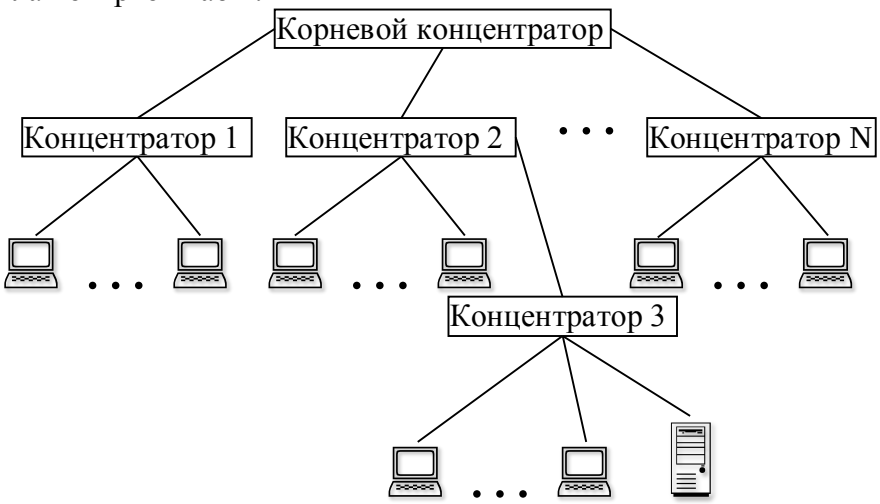
- максимальна кількість станцій у мережі — не більш 1024;
- максимальна відстань між двома вузлами мережі (двома точками підключення станцій або концентраторів) — не більш 500 м;
- максимальна довжина сегмента — не більш 100 м;
- максимальна пропускна здатність мережі — 10 Мбіт/с.

Такими параметрами буде володіти мережа, схема якої приведена на мал. 1.1.3.

Звичайно, реальна мережа може мати схему, що трохи відрізняється від ідеальної,

але усі відомі обмеження повинні бути дотримані. Від цього буде залежати надійність роботи мережі. Не буде суперечити стандартам і такий варіант, як зображений на мал. 1.1.4.

У той же час, варіант, показаний на мал. 1.1.5, уже не відповідає вимогам стандарту. У цьому варіанті між комп'ютерами, підключеними до концентраторів 3 і 4, виявилося більш чотирьох концентраторів, що може привести до збоїв у роботі мережі через порушення правила чотирьох хабів.



Малюнок 1.1.4 - Ще один варіант побудови мережі

Параметри кабельних мереж сімейства стандартів Ethernet приведені в табл. 1.1.3.

Таблиця 1.1.3 - Параметри специфікацій фізичного рівня для стандарту Ethernet

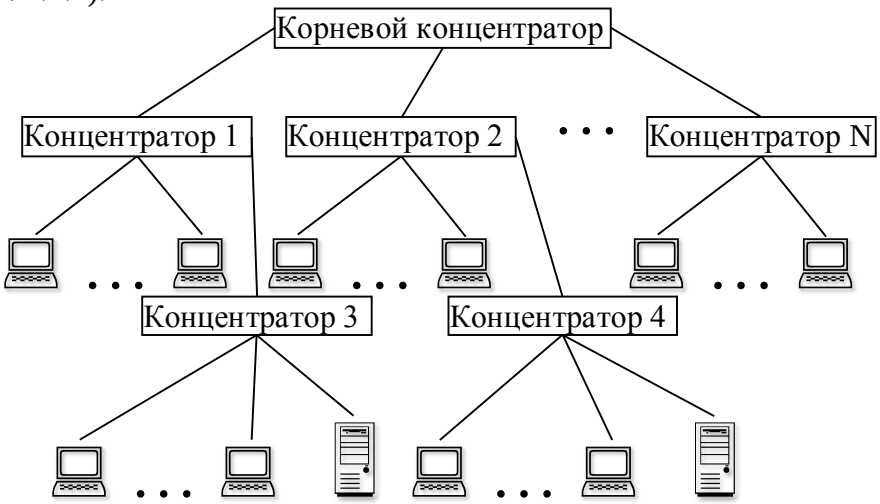
Характеристика	***10Base-5***	***10Base-2***	***10Base-T***	***10Base-F***
Кабель	Товстий коаксіальний кабель RG-8 або RG-11	Тонкий коаксіальний кабель RG-58	Неекранована кручена пара категорії 3, 4, 5	Багатомодовий волоконнооптичний кабель
Максимальна довжина сегмента, м	500	185	100	2000
Максимальна відстань між вузлами мережі (при використанні повторювачів), м	2500	925	500	2500
Максимальне число станцій у сегменті	100	30	1024	1024
Максимальне число повторювачів між будь-якими станціями мережі	4	4	4	4

Скориставшись приведеною таблицею, можна досить точно уявити собі параметри проектованої мережі. Докладно розроблені протоколи і стандарти дозволяють проектувати мережі будь-якої мислимої конфігурації без серйозних проблем у розрахунках.

Якщо, наприклад, ми хочемо організувати мережу, розташовану на декількох поверхах або навіть у різних будинках, то цілком виправдане застосування коаксіального кабелю для з'єднання поверхів або будинків. Коаксіальний кабель, володіючи більшою механічною міцністю і стійкістю до кліматичного впливу, буде служити довше кручений

пари, а відстань, що коаксіальний кабель може перекрити без додаткових пристроїв, досягає п'ятисот метрів (для товстого кабелю), що дозволить з'єднати між собою досить вилучені друг від друга приміщення.

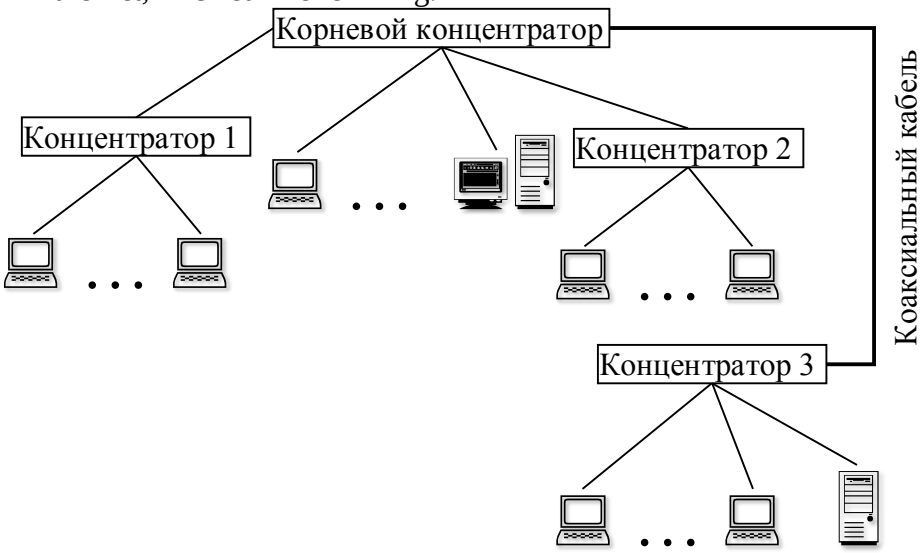
На мал. 1.1.6 показаний варіант побудови мережі з застосуванням коаксіального кабелю для з'єднання поверхів або вилучених приміщень. Один із простих, хоча і не самих надійних варіантів побудови мережі, — це мережа 10Base-2. Вона побудована з застосуванням тонкого коаксіального кабелю, що підключається до мережних адаптерів комп'ютерів (мал. 1.1.7).



Малюнок 1.1.5 - Неправильний варіант побудови мережі

Існують і інші протоколи і стандарти для побудови мереж.

У 1980 році в IEEE був організований комітет 802 по стандартизації локальних мереж. Результати роботи цього комітету лягли в основу комплексу міжнародних стандартів ISO 8802-1...5. Ці стандарти були створені на основі розповсюджених фірмових стандартів мереж Ethernet, ArcNet і Token Ring.



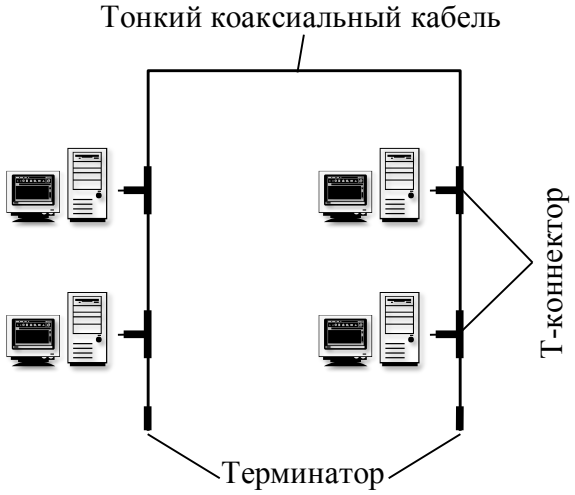
Малюнок 1.1.6 - Варіант побудови мережі з застосуванням коаксіального кабелю (деякі подробиці опущені)

Відповідно до нових стандартів можуть бути спроектовані мережі з пропускною здатністю, що досягає 1 Гбайт/с. В останні роки в локальних мережах усі частіше застосовуються так називані активні комутатори.

Вони дозволяють ускладнити топологію мережі, використовувати резервні шляхи для інформаційного потоку, чим досягається підвищення надійності і швидкодії мережі.

Незважаючи на швидкий розвиток нових технологій і поява нових стандартів, традиційні стандарти ніхто не скасовує, і вони як і раніше застосовуються настільки

широко, що важко очікувати їхній відхід зі сцени, принаймні, протягом декількох років.



Малюнок 1.1.7 - Мережа 10Base-2

1.1.4.5. Робота в режимі клієнт-сервер

Об'єднані в мережу комп'ютери являють собою організовану систему, де кожному комп'ютерові буде постійно або тимчасово приділятися визначена роль. Незалежно від призначення мережі і типів застосовуваних протоколів, два взаємодіючих у даний момент комп'ютера знаходяться в нерівному положенні. Один посилає деякий запит, іншої повинний певним чином відреагувати на цей запит. Прохач виступає в ролі клієнта, а що проситься — у ролі сервера. У ряді випадків комп'ютери можуть мінятися ролями в процесі спілкування, але в кожен момент часу один клієнт, інший сервер. Як і в сфері послуг, клієнт завжди правий. Сервер повинний забезпечити клієнта визначеним сервісом — набором послуг. Файловий сервер повинний забезпечити доступ до файлів відповідно до прав клієнта, сервер додатків повинний забезпечити клієнта необхідними додатками. У різних мережах сервер може виконувати самі різноманітні задачі. Це і поштовий сервер, і сервер бази даних, сервер доступу до глобальної мережі Internet, сервер печатки, що забезпечує клієнтів доступом до принтерів мережі. Словом, якщо потрібно зробити послугу, то сервер зробить її клієнтові. У деяких випадках сервер є як би центром мережі, а іноді, навпаки, один клієнт збирає навколо себе кілька серверів. Можливий варіант мережі з виділеним сервером. Це значить, що один комп'ютер приділяється винятково для роботи як сервер. Це особливо важливо у великих мережах, де сервер працює з великим навантаженням і потрібна високою стабільністю його роботи. Існують операційні системи, спеціально призначені для сервера мережі. Так, Unix широко застосовується для серверів у великих мережах, NetWare фірми Novell — для мереж масштабу підприємства, Windows NT або Windows 2000 Server — для мереж різного призначення. В останні роки безліч додатків розрахована для роботи в режимі клієнт-сервер. Це дозволяє декільком користувачам звертатися до тим самим файлів без ризику зруйнувати або зіпсувати інформацію. Розповсюджений в усім світі комплект MS Office 97/2000/XP саме підтримує роботу в такому режимі, що може бути особливо корисно для додатків Excel і Access, що дозволяють створювати зручні спеціалізовані додатки як для організацій, так і для особистого застосування і працювати з базами даних. Можливе застосування декількох операційних систем в одній мережі і декількох серверів. Це дозволяє використовувати особливості кожної операційної системи і більш ефективно застосовувати мережа, якщо коло розв'язуваних задач широка й одна операційна система не надає досить зручних засобів для їхнього рішення. Необхідно відзначити, що саме по собі поняття сервера і клієнта зовсім необов'язково нерозривно зв'язано з мережею. Технологія клієнт-сервер може з успіхом застосовуватися і на локальному комп'ютері, що буде і клієнтом, і сервером одночасно. Як клієнта і сервера можна розглядати частини додатка, що призначено для роботи в режимі

клієнт-сервер. Підключення комп'ютера-сервера до мережі нічим не відрізняється від підключення звичайного комп'ютера.

Сервер великої мережі, використовуваної великим підприємством або цілою корпорацією (у такій мережі сервер не один), працює цілодобово, виконуючи безліч специфічних серверних задач, без рішення яких мережа такого масштабу не зможе нормально функціонувати. Для мереж невеликого розміру немає необхідності тримати комп'ютери включеними цілодобово і можливо реалізувати всі потреби в плані мережевого сервісу на основі розповсюджених Windows 95/98. Ці операційні системи мають безліч позитивних якостей, але не призначені для безперервної роботи протягом декількох днів. Якщо така необхідність з'явиться, варто подбати про виділення декількох хвилин у добу для перезавантаження комп'ютера. Ця міра дозволить істотно знизити ризик зависання системи і втрати даних. Windows 2000 менш піддана різного роду збоям. Отже, на сервері вона повинна працювати більш стійко. Для виділеного сервера звичайно виділяється окреме приміщення.

1.1.4.6. Типові топології ЛОМ

При побудові мережі спочатку необхідно вибрати спосіб організації фізичних зв'язків, тобто топологію. Під топологією розуміється конфігурація графа, вершинами (або вузлами) якого є комп'ютери мережі або інше мережне устаткування (наприклад, концентратори), а ребрами — фізичні зв'язки між ними.

Шинна топологія

При шинній топології середовище передачі інформації представляється у формі комунікаційного шляху, доступного для всіх робочих станцій, до якого вони усі повинні бути підключені (мал. 1.1.8). Усі робочі станції можуть безпосередньо вступати в контакт із будь-якою робочою станцією, що мається в мережі.

Малюнок 1.1.8 – Топологія загальна шина

Робочі станції в будь-який час, без переривання роботи всієї обчислювальної мережі, можуть бути підключені до неї або відключені. Функціонування обчислювальної мережі не залежить від стану окремої робочої станції.

У стандартній ситуації для шинної мережі Ethernet часто використовують тонкий кабель або Cheapernet-кабель із трійниковим з'єднувачем. Вимикання й особливе підключення до такої мережі вимагають розриву шини, що викликає порушення циркулюючого потоку інформації і зависання системи.

Існують пасивні штепсельні коробки, через які можна відключати і/або включати робочі станції під час роботи обчислювальної мережі.

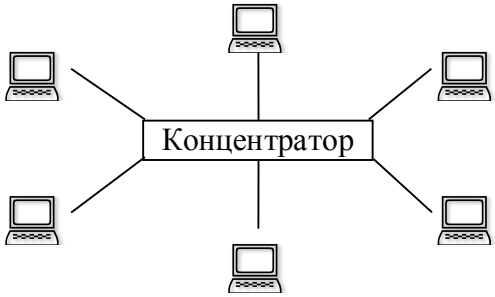
Завдяки тому, що робочі станції можна включати без переривання мережних процесів і комунікаційного середовища, дуже легко прослухувати інформацію, тобто відгалужувати неї з комунікаційного середовища. У ЛВС із прямою (немодульованою) передачею інформації завжди може існувати тільки одна передавальна інформацію станція. Для запобігання колізій (зіткнень даних) у більшості випадків застосовується часовий метод поділу, відповідно до якого для кожної підключеної робочої станції у визначені моменти часу надається виключне право на використання каналу передачі даних. Тому вимоги до пропускної здатності обчислювальної мережі при підвищеному навантаженні знижуються, наприклад, при введенні нових робочих станцій.

Колізія, конфлікт (Collision). Спроба двох (або більш) станцій одночасно почати передачу пакета в мережі CSMA/CD. При виявленні конфлікту обидві станції припиняють передачу і намагаються відновити неї після закінчення обумовленого випадковим образом інтервалу часу. Використання випадкової затримки дозволяє вирішити проблему виникнення повторного конфлікту.

Робочі станції приєднуються до шини за допомогою пристроїв TAP (Terminal Access Point, точка підключення термінала). TAP являє собою спеціальний тип приєднання до коаксіального кабелю. Зонд голчастої форми впроваджується через зовнішню оболонку зовнішнього провідника і шар діелектрика до внутрішнього провідника і приєднується до нього. TAP має "народне" назва — "Зуб вампіра". У ЛОМ із модульованою широкосмуговою передачею інформації різні робочі станції одержують, у міру потреби, частоту, на якій вони можуть відправляти й одержувати інформацію. Дані, що пересилаються, модулюються на відповідних несущих частотах, тобто між середовищем передачі інформації і робітниками станціями знаходяться, відповідно, модеми для модуляції і демодуляції. Техніка широкосмугових повідомлень дозволяє одночасно транспортувати в комунікаційному середовищі досить великий обсяг інформації. Для подальшого розвитку дискретного транспортування даних не грає ролі, яка первісна інформація подана в модем (аналогова або цифрова), тому що надалі вона все рівно буде перетворена.

Топологія типу зірка

Концепція топології мережі у виді зірки прийшла з області великих ЕОМ, у якій головний комп'ютер одержує й обробляє всі дані з периферійних пристроїв як активний вузол обробки даних. Цей принцип застосовується в системах передачі даних, наприклад, в електронній пошті. Вся інформація між двома периферійними робітниками місцями проходить через центральний вузол обчислювальної мережі. Пропускна здатність мережі визначається обчислювальною потужністю вузла і гарантується для кожної робочої станції. Колізій не виникає. Кабельне з'єднання задоволене простої, тому що кожна робоча станція зв'язана з вузлом. Витрати на прокладку кабелів високі, особливо коли центральний вузол географічно розташований не в центрі топології. При розширенні обчислювальних мереж не можна використовувати раніше виконані кабельні зв'язки: до нового робочого місця необхідно прокладати окремий кабель з центра мережі (мал. 1.1.9).



Малюнок 1.1.9– Топологія зірка

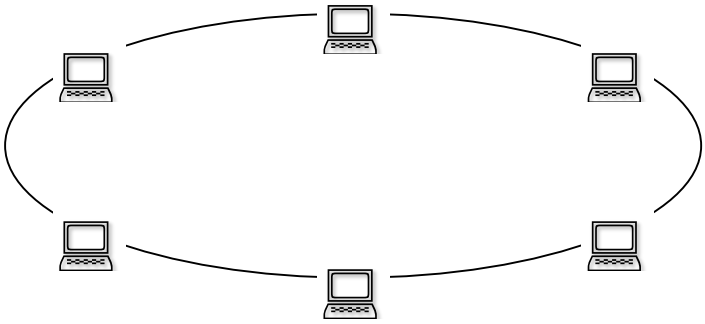
Топологія у виді зірки є найбільш швидкодіючою з усіх топологій обчислювальних мереж, оскільки передача даних між робочими станціями проходить через центральний вузол по окремих лініях, використовуваним тільки цими робітниками станціями. Дана топологія мережі характеризується порівняно невисокою частотою запитів на передачу інформації від однієї станції до іншої.

Продуктивність обчислювальної мережі з топологією типу зірка визначається потужністю її центрального вузла, що виконує функції сервера. Він може бути вузьким місцем обчислювальної мережі. У випадку виходу з ладу центрального вузла порушується робота всієї мережі.

Перевагою такої топології мережі є можливість реалізувати оптимальний механізм захисту інформації, що зберігається на сервері, від несанкціонованого доступу. Вся обчислювальна мережа може керуватися з її центра.

Кільцева топологія

При кільцевій топології мережі робочі станції зв'язані одна з іншої по колу, тобто робоча станція 1 з робочою станцією 2, робоча станція 3 з робочою станцією 4 і т.д. Остання робоча станція зв'язана з першої. Комунікаційний зв'язок замикається в кільце (мал. 1.1.10).



Малюнок 1.1.10– Кільцева топологія

Прокладка кабелів від однієї робочої станції до іншої може бути досить складні і дорогої, особливо якщо географічно робочі станції розташовані далеко від кільця (наприклад, у лінію).

Повідомлення циркулюють регулярно по колу. Робоча станція посилає по визначеній кінцевій адресі інформацію, попередньо одержавши з кільця запит. Пересилання повідомлень є дуже ефективної, тому що більшість повідомлень можна відправляти по кабельній системі одне за іншим. Дуже просто можна організувати кільцевий запит на всі станції. Тривалість передачі інформації збільшується пропорційно кількості робочих станцій, що входять в обчислювальну мережу.

Основна проблема при кільцевій топології полягає в тім, що кожна робоча станція повинна активно брати участь у пересиланні інформації, і у випадку виходу з ладу хоча б однієї з них уся мережа паралізується. Несправності в кабельних з'єднаннях локалізуються легко.

Підключення нової робочої станції вимагає короткострокового вимикання мережі, тому що під час установки кільце повинне бути розімкнуте. Обмеження на довжину обчислювальної мережі не існує, тому що воно, у кінцевому рахунку, визначається винятково відстанню між двома робочими станціями.

Спеціальною формою кільцевої топології є логічна кільцева мережа. Фізично вона монтується як з'єднання зоряних топологій. Окремі зірки включаються за допомогою спеціальних комутаторів (англ. Hub — концентратор), що по-російському також іноді називають "хаб". У залежності від числа робочих станцій і довжини кабелю між робочими станціями, застосовують активні або пасивні концентратори. Активні концентратори додатково містять підсилювач для підключення від 4 до 32 робочих станцій. Пасивний концентратор виконує винятково функції розгалужувача (максимум на 3 робочі станції). Керування окремою робочою станцією в логічній кільцевій мережі відбувається так само, як і в звичайній кільцевій мережі. Кожної робочої станції привласнюється відповідний їй адреса, по якому передається керування (від старшого до молодшого і від самого молодшого до самого старшого). Розрив з'єднання відбувається тільки для нижче розташованого (найближчого) вузла обчислювальної мережі, так що лише в рідких випадках може порушуватися робота всієї мережі.

Змішані топології

Поряд з відомими топологіями обчислювальних мереж кільце, зірка і шина, на практиці застосовується і комбінована, наприклад, деревоподібна структура. Вона утвориться в основному у виді комбінацій вищезгаданих топологій обчислювальних мереж. Підстава дерева обчислювальної мережі розташовується в крапці (корінь), у якій збираються комунікаційні лінії інформації (галузі дерева).

Обчислювальні мережі з деревоподібною структурою використовуються там, де неможливо безпосереднє застосування базових мережних структур у чистому виді. Для

підключення великого числа робочих станцій потрібні мережні підсилювачі і/або комутатори. Комутатор, що володіє одночасно і функціями підсилювача, називають активним концентратором.

На практиці застосовують їхні різновиди, що забезпечують підключення від 8 або 32 ліній.

Пристрій, до якого можна приєднати максимум три станції, називають пасивним концентратором. Пасивний концентратор звичайно використовують як розгалужувач. Він не має потреби в підсилювачі. Передумовою для підключення пасивного концентратора є те, що максимально можлива відстань до робочої станції не повинна перевищувати декількох десятків метрів.

1.1.4.7. Локальна мережа Ethernet

Специфікацію Ethernet наприкінці сімдесятих років запропонувала компанія Xerox Corporation. Пізніше до цього проекту приєдналися компанії Digital Equipment Corporation (DEC) і Intel Corporation. У 1982 році була опублікована специфікація на Ethernet версії 2,0. На базі Ethernet інститутом IEEE був розроблений стандарт IEEE 802.3. Розходження між ними незначні.

Основні принципи роботи такі.

- На логічному рівні в Ethernet застосовується топологія шина.
- Усі пристрої, підключені до мережі, рівноправні, тобто будь-яка станція може почати передачу в будь-який момент часу (якщо передавальне середовище вільне).
- Дані, переданою одною станцією, доступні всім станціям мережі.

1.1.4.8. Локальна мережа Token Ring

Цей стандарт розроблений фірмою IBM. Як передавальне середовище застосовується неекранованої або екранована кручена пари (UTP або STP) або оптоволокно. Швидкість передачі даних 4 або 16 Мбіт/с. Як метод керування доступом станцій до передавального середовища використовується метод — маркерне кільце (Token Ring).

Основні положення цього методу:

- пристрої підключаються до мережі по топології кільце;
- усі пристрої, підключені до мережі, можуть передавати дані, тільки одержавши дозвіл на передачу (маркер);
- у будь-який момент часу тільки одна станція в мережі має таке право.

Типи пакетів

У IBM Token Ring використовуються три основних типи пакетів.

- ***Пакет керування/дані*** (Data/Command Frame). З його допомогою виконується передача даних або команд керування роботою мережі.
- ***Маркер*** (Token). Станція може почати передачу даних тільки після одержання такого пакета. В одному кільці може бути тільки один маркер і, відповідно, тільки одна станція з правом передачі даних.
- ***Пакет скидання*** (Abort). Посилка такого пакета викликає припинення будь-яких передач.

1.1.4.9. Локальна мережа Arknet

Arknet (Attached Resource Computer NETWork) — проста, недорога, надійна і досить гнучка архітектура локальної мережі. Розроблена корпорацією DataPoint у 1977 році. Згодом ліцензію на Arknet придбала корпорація SMC (Standard Microsistem Corporation), що стала основним розроблювачем і виробником устаткування для мереж. Як передавальне середовище використовуються кручена пара, коаксіальний кабель (RG-62) із хвильовим

опором 93 Ом і оптоволоконний кабель. Швидкість передачі даних — 2,5 Мбіт/с. При підключенні пристроїв у Arknet застосовують топології шина і зірка. Метод керування доступом станцій до передавального середовища — маркерна шина (Token Bus). Цей метод передбачає наступні правила:

- усі пристрої, підключені до мережі, можуть передавати дані, тільки одержавши дозвіл на передачу (маркер);
- у будь-який момент часу тільки одна станція в мережі має таке право;
- дані, переданою одною станцією, доступні всім станціям мережі.

Основні принципи роботи такі.

Передача кожного байта в Arknet виконується спеціальною посилкою ISU (Information Symbol Unit, одиниця передачі інформації), що складає з трьох службових старт/стопових бітів і восьми бітів даних. На початку кожного пакета передається початковий роздільник AB (Alert Burst), що складається із шести службових бітів. Початковий роздільник виконує функції преамбули пакета.

У Arknet визначені 5 типів пакетів.

- Пакет ITT (Information To Transmit) — запрошення до передачі. Ця посилка передає керування від одного вузла мережі іншому. Станція, що прийняла цей пакет, одержує право на передачу даних.
- Пакет FBE (Free Buffer Enquiries) — запит про готовність до прийому даних. Цим пакетом перевіряється готовність вузла до прийому даних.
- Пакет даних. За допомогою цієї посилки виробляється передача даних.
- Пакет ACK (ACKnowledgments) — підтвердження прийому. Підтвердження готовності до прийому даних або підтвердження прийому пакета даних без помилок, тобто у відповідь на FBE і пакет даних.
- Пакет NAK (Negative AcKnowledgments) — неготовність до прийому. Неготовність вузла до прийому даних (відповідь на FBE) або прийнятий пакет з помилкою.

1.1.5. Вибір оптимального середовища передачі даних

Як середовище передачі найбільше часто використовуються кручена пара, коаксіальний кабель або оптоволокняні лінії. При виборі типу кабелю враховують наступні показники:

- вартість монтажу й обслуговування;
- швидкість передачі інформації;
- обмеження на величину відстані передачі інформації (без додаткових підсилювачів-повторювачів);
- безпека передачі даних.

Головна проблема полягає в одночасному забезпеченні цих показників, наприклад, найвища швидкість передачі даних обмежена максимально можливою відстанню передачі даних, при якому ще забезпечується необхідний рівень їхнього захисту. Простота нарощування і розширення кабельної системи впливають на її вартість.

Кручена пари (twisted pair) є найбільш дешевим кабельним з'єднанням. Вона дозволяє передавати інформацію зі швидкістю до 100 Мбіт/з, легко нарощується, однак має недостатню перешкодозахищеність в умовах високого рівня перешкод на лінії зв'язку. Перевагами є низька ціна і відсутність проблем при монтажі. Для підвищення перешкодозахищеності інформації часто використовують екрановану кручену пару, тобто кручену пару, поміщену в оболонку, що екранує, подібно екранові коаксіального кабелю. Це збільшує вартість кручений пари і наближає неї за ціною до коаксіального кабелю.

Коаксіальний кабель — добре перешкодозахищений і застосовується для зв'язку на

великі відстані (кілька кілометрів). Швидкість передачі інформації — від 1 до 500 Мбіт/с, у залежності від типу кабелю й умов застосування.

У залежності від діаметра кабелю, передбаченого визначеним стандартом, розрізняють "товстий" і "тонкий", коаксіальний кабель.

Оптоволокняні лінії найбільш дорогі. Швидкість поширення інформації з них досягає декількох Гбіт у секунду. Припустиме видалення — більш 50 км. Зовнішній вплив перешкод практично відсутній. На даний момент це найбільш дороге з'єднання для ЛОМ. Застосовуються там, де виникають перешкоди у виді електромагнітних полів або потрібна передача інформації на дуже великі відстані без використання повторювачів.

На базі різних стандартів можуть бути організовані мережі різної структури, з різними методами передачі інформації.

На сьогоднішній день фізичні специфікації технології Ethernet включають наступні середовища передачі даних:

- ***10Base-5*** — коаксіальний кабель діаметром 0,5 дюйма, називаний "товстим" коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента — 500 м (без повторювачів);
- ***10Base-2*** — коаксіальний кабель діаметром 0,25 дюйма, називаний "тонким" коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента — 185 м (без повторювачів);
- ***10Base-T*** — кабель на основі неекранованої кручений пари (Unshielded Twisted Pair, UTP). Утворить зіркоподібну топологію на основі концентратора. Відстань між концентратором і кінцевим вузлом — не більш 100 м;
- ***10Base-F*** — волоконнооптичний кабель. Топологія аналогічна топології стандарту 10Base-T. Мається кілька варіантів цієї специфікації — FOIRL (відстань до 1000 м), 10Base-FL (відстань до 2000 м), 10Base-FB (відстань до 2000 м).

1.1.6. Вибір топології локальної мережі

Топологія — розділ математики, що вивчає властивості фігур, що не змінюються при будь-яких переміщеннях і деформаціях. Цей термін є скороченням від словосполучення "топологічний простір", що означає — безліч елементів будь-якої природи, у якому визначені граничні співвідношення. Таким чином, топологія мережі — це безліч її елементів, у якому визначені граничні співвідношення. І справді, ЛОМ будується на основі деяких граничних співвідношень, отриманих розрахунковим шляхом, виходячи з властивостей електричних сигналів, використовуваних у мережі і параметрів середовища поширення цих сигналів (звичайно це кабель). Незважаючи на те, що в нашій мережі може бути зовсім не багато комп'ютерів, визначені для ЛОМ граничні співвідношення не дозволяють будувати мережа так, як нам захочеться. Для кожної з приведених нижче типових топологій існує ряд обмежень, що приводять до наступних можливих варіантів:

- ***шина*** (bus) — комп'ютери підключені уздовж одного кабелю (сегмента) (мал. 1.1.8);
- ***зірка*** (star) — комп'ютери підключені до сегментів кабелю, що виходить з однієї крапки, або концентратора (hub) (мал. 1.1.9);
- ***кільце*** (ring) — комп'ютери підключені до кабелю, замкнутому в кільце (мал. 1.1.10).

Перше обмеження полягає в тому, що конфігурація *кільце* не застосовується в мережах Ethernet. Для конфігурації *шина* обмежена число комп'ютерів, які можна підключити до сегмента мережі (на малюнку показаний саме сегмент мережі), воно не може перевищувати 30 одиниць, а довжина сегмента не повинна перевищувати 185 м. Застосовуючи репітери (повторювачі), якими можна з'єднувати сегменти мережі, можна

збільшити її довжина до 925 м. Кількість сегментів при цьому не повинно бути більше 5, кількість репітерів між будь-якими двома комп'ютерами не більш 4, а самі комп'ютери можуть знаходитися тільки в 3 з 5 сегментів. Коротко це правило записується як 5-4-3. Як середовище передачі даних у такій мережі використовується тонкий коаксіальний кабель. У конфігурації *зірка* також діють обмеження. Насправді в чистому виді такі схеми застосовуються рідко. Частіше мережа має комбіновану топологію. Кожен варіант має свої переваги і недоліки. Комбінуючи, можна компенсувати недоліки однієї схеми перевагами іншої. Хоча при цьому можливо як посилення переваг, так і збільшення недоліків.

Тема 1.2. Високошвидкісні технології локальних обчислювальних мереж

1.2.1. Технологія Fast Ethernet (IEEE 802.3u)

Технологія Fast Ethernet є еволюційним розвитком класичної технології Ethernet. Її основними достоїнствами є:

- збільшення пропускної здатності сегментів мережі до 100 Мб/с;
- збереження методу випадкового доступу Ethernet;
- збереження зіркоподібної топології мереж і підтримка традиційних середовищ передачі даних - кручений пари й оптоволоконного кабелю.

Зазначені властивості дозволяють здійснювати поступовий перехід від мереж 10Base-T - найбільш популярного на сьогоднішній день варіанта Ethernet - до швидкісних мереж, що зберігають значну наступність з добре знайомою технологією: Fast Ethernet не вимагає корінного перенавчання персоналу і заміни устаткування у всіх вузлах мережі. Офіційний стандарт 100Base-T (802.3u) установив три різних специфікації для фізичного рівня (у термінах семирівневої моделі OSI) для підтримки наступних типів кабельних систем:

- 100Base-TX для двопарного кабелю на неекранованій кручений парі UTP Category 5, або екранованої кручений парі STP Type 1;
- 100Base-T4 для чотирипарного кабелю на неекранованій кручений парі UTP Category 3, 4 або 5;
- 100Base-FX для багатомодового оптоволокняного кабелю.

1.2.1.1. Fast Ethernet як розвиток класичного Ethernet'а

Ріст вимог до пропускної здатності локальних мереж

Сьогодні все частіше й частіше виникають підвищені вимоги до пропускної здатності каналів між клієнтами мережі і серверами. Це відбувається по різних причинах:

- підвищення продуктивності клієнтських комп'ютерів;
- збільшення числа користувачів у мережі;
- поява додатків, що працюють з мультимедійною інформацією, що зберігається у файлах дуже великих розмірів;
- збільшення числа сервісів, що працюють у реальному масштабі часу.

Отже, мається потреба в економічному рішенні, що надає потрібну пропускну здатність у всіх перерахованих випадках. Ситуація ускладнюється ще і тим, що потрібні різні технологічні рішення - для організації магістралей мережі і підключення серверів одні, а для підключення настільних клієнтів - інші.

10-мегабитный Ethernet улаштовував більшість користувачів протягом близько 15 років. Однак на початку 90-х років початку відчуватися його недостатня пропускна здатність. Якщо для комп'ютерів на процесорах Intel 80286 або 80386 із шинами ISA (8 Мбайт/с) або EISA (32 Мбайт/с) пропускна здатність сегмента Ethernet складала 1/8 або 1/32

каналу "пам'ять – диск", то це добре узгоджувалася зі співвідношенням обсягів локальних даних і зовнішніх даних для комп'ютера. Тепер же в могутніх клієнтських станцій із процесорами Pentium або Pentium PRO і шиною PCI (133 Мбайт/с) ця частка упала до 1/133, що явно недостатньо. Тому багато сегментів 10-Мегабитного Ethernet'а стали перевантаженими, реакція серверів у них значно упала, а частота виникнення колізій істотно зросла, ще більш знижуючи номінальну пропускну здатність.

Засоби підвищення пропускної здатності мережі

Для підвищення пропускної здатності мережі можна застосувати кілька способів: сегментація мережі за допомогою мостів і маршрутизаторів, сегментація мережі за допомогою комутаторів і підвищення пропускної здатності самого протоколу.

Маршрутизатор (Router). Система, що відповідає за прийняття рішень про вибір одного з декількох шляхів передачі мережевого трафіку. Для виконання цієї задачі використовуються маршрутизовані протоколи, що містять інформацію про мережі й алгоритми вибору найкращого шляху на основі декількох критеріїв, називаних метрикою маршрутизації ("routing metrics"). У термінах OSI маршрутизатор є проміжною системою Мережевого рівня.

Сегментація мережі за допомогою мостів або маршрутизаторів може підвищити пропускну здатність сегментів мережі за рахунок їхнього розвантаження від трафіку інших сегментів тільки в тому випадку, коли міжсегментний трафік складає незначну частку від внутрішньосегментного, оскільки і мости, і маршрутизатори не мають високу внутрішню пропускну здатність.

На початку 90-х років відбулося дві значних події, що дали можливість підвищити пропускну здатність сегментів локальних мереж, і в першу чергу сегментів технології Ethernet.

Міст (Bridge). Пристрій, що з'єднує дві або кілька фізичних мереж і передавального пакетів з однієї мережі в іншу. Мости можуть фільтрувати пакети, тобто передавати в інші сегменти або мережі тільки частина трафіку, на основі інформації канального рівня (MAC-адреса). Якщо адреса одержувача присутній у таблиці адрес моста, кадр передається тільки в той сегмент або мережу, де знаходиться одержувач. Схожими пристроями є повторювачі (repeater),які просто передають електричні сигнали з одного кабелю в іншій і маршрутизатори (router),які приймають рішення про передачу пакетів на основі різних критеріїв, заснованих на інформації мережевого рівня. У термінології OSI міст є проміжною системою на рівні каналу передачі даних (Data Link Layer).

Перша подія складалася в появі мостів нового покоління - комутаторів, що на відміну від традиційного моста мали велика кількість портів і забезпечували передачу кадрів між портами одночасно. Це дозволило тепер ефективно застосовувати комутатори і для тих мереж, у яких міжсегментний трафік не дуже відрізнявся від внутрішньосегментного. Майбутнє технології Ethernet після появи комутаторів стало більш стійким, тому що з'явилася можливість з'єднати низьку вартість технології Ethernet з високою продуктивністю мереж, побудованих на основі комутаторів.

Повторювач (Repeater). Пристрій, що передає електричні сигнали з одного кабелю в іншій без маршрутизації або фільтрації пакетів. У термінах OSI репітер являє собою проміжний пристрій Фізичного рівня.

Друга подія полягала в появі експериментальних мереж, у яких використовувався протокол Ethernet з більш високою бітовою швидкістю передачі даних, а саме 100 Мб/с. До цього тільки технологія *Fiber Distributed Data Interface (FDDI)* забезпечувала таку бітову швидкість, але вона була спеціально розроблена для побудови магістралей мереж і була занадто дорогою для підключення до мережі окремих робочих станцій або серверів.

Комутатор (Switch, Switching hub). За принципом обробки кадрів нічим не відрізняється від моста. Основна його відмінність від моста полягає в тому, що він є свого роду комунікаційним мультипроцесором, що обробляє кадри по алгоритму моста незалежно від процесорів інших портів. За рахунок цього загальна продуктивність комутатора звичайно

набагато вище продуктивності традиційного моста, що має один процесорний блок. Можна сказати, що комутатори – це мости нового покоління, що обробляють кадри в рівнобіжному режимі.

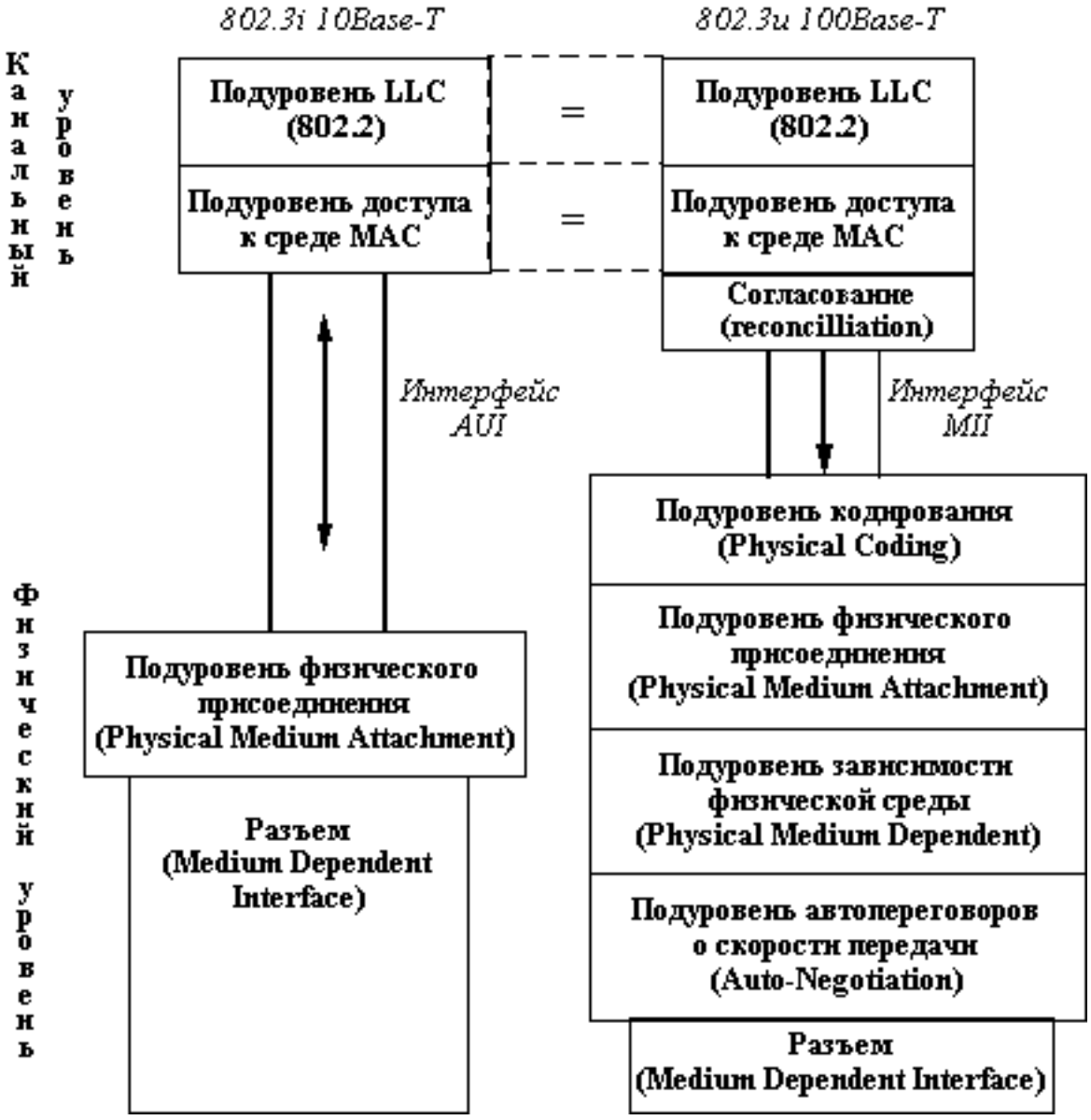
1.2.1.2. Створення стандартові Fast Ethernet

У 1992 році група виробників мережевого устаткування, включаючи таких лідерів технології Ethernet як SynOptics, 3Com і ряд інших, утворили некомерційне об'єднання *Fast Ethernet Alliance* для розробки стандарту на нову технологію, що узагальнила б досягнення окремих компаній в області Ethernet-спадкоємного високошвидкісного стандарту. Нова технологія одержала назву Fast Ethernet.

Одночасно були початі роботи в інституті IEEE по стандартизації нової технології - там була сформована дослідницька група для вивчення технічного потенціалу високошвидкісних технологій. За період з кінця 1992 року і по кінець 1993 року група IEEE вивчила 100-Мегабитные рішення, запропоновані різними виробниками. Поряд із пропозиціями Fast Ethernet Alliance група розглянула також і іншу високошвидкісну технологію, запропоновану компаніями *Hewlett-Packard* і *AT&T*.

У центрі дискусій була проблема збереження змагальницького методу доступу CSMA/CD. Пропозиція по Fast Ethernet'у зберігало цей метод і тим самим забезпечувало наступність і погодженість мереж 10Base-T і 100Base-T. Коаліція HP і AT&T, що мала підтримку набагато меншого числа виробників у мережній індустрії, чим Fast Ethernet Alliance, запропонувала зовсім новий метод доступу, називаний *Demand Priority*. Він істотно змінював картину поводження вузлів у мережі, тому не зміг вписатися в технологію Ethernet і стандарт 802.3, і для його стандартизації був організований новий комітет IEEE 802.12.

У травні 1995 року комітет IEEE прийняв специфікацію Fast Ethernet як стандарт 802.3u, що не є самостійним стандартом, а являє собою доповнення до існуючого стандарту 802.3 у виді глав з 21 по 30. Відмінності Fast Ethernet від Ethernet зосереджені на фізичному рівні (малюнок 1.2.1).



Малюнок 1.2.1- Відмінності стека протоколів 100Base-T від стека протоколів 10Base-T

Більш складна структура фізичного рівня технології Fast Ethernet викликана тим, що в ній використовується три варіанти кабельних систем - оптоволокно, 2-х парна кручена пари категорії 5 і 4-х парна кручена пари категорії 3, причому в порівнянні з варіантами фізичної реалізації Ethernet (а них нараховується шість), тут відмінності кожного варіанта від інших глибше - міняється і кількість провідників, і методи кодування. А тому що фізичні варіанти Fast Ethernet створювалися одночасно, а не еволюційно, як для мереж Ethernet, те малася можливість детально визначити ті підрівні фізичного рівня, що не змінюються від варіанта до варіанта, і інші підрівні, специфічні для кожного варіанта.

Підрівні LLC і MAC у стандарті Fast Ethernet не перетерпіли змін і будуть розглянуті нижче.

1.2.1.3. Підрівень Logical Link Control (LLC)

Підрівень LLC забезпечує інтерфейс протоколу Ethernet із протоколами вищих рівнів, наприклад, з IP або IPX. Кадр LLC, зображений на малюнку 1.2.2, вкладається в кадр MAC, і дозволяє за рахунок полів DSAP і SSAP ідентифікувати адреса сервісів призначення і джерела відповідно. Наприклад, при вкладенні в кадр LLC пакета IPX, значення як DSAP (Destination Service Access Point – Точка Доступу до Сервісу Призначення), так і SSAP

(Source Service Access Point – Точка Доступу до Сервісу Відправника) повинні бути рівні E0. Поле керування кадру LLC дозволяє реалізувати процедури обміну даними трьох типів.

- Процедура типу 1 визначає обмін даними без попереднього встановлення з'єднання і без повторної передачі кадрів у випадку виявлення помилкової ситуації, тобто є процедурою дейтаграмного типу. Саме цей тип процедури і використовується у всіх практичних реалізаціях Ethernet. Поле керування для цього типу процедур має значення 03, що визначає всі кадри як ненумеровані.
- Процедура типу 2 визначає режим обміну з установленням з'єднань, нумерацією кадрів, керуванням потоком кадрів і повторною передачею помилкових кадрів. У цьому режимі протокол LLC аналогічний протоколові HDLC. У локальних мережах Ethernet цей режим використовується рідко.

HDLC (High-level Data Link Control - Високорівневий Протокол Керування Каналом). Міжнародний комунікаційний протокол, розроблений ISO.

- Процедура типу 3 визначає режим передачі даних без установлення з'єднання, але з одержанням підтвердження про доставку інформаційного кадру адресатові. Тільки після цього може бути відправлений наступний інформаційний кадр.

1.2.1.4. Підрівень керування доступом до середовища Media Access Control (MAC)

Підрівень MAC відповідальний за формування кадру Ethernet, одержання доступу до поділюваного середовища передачі даних і за відправлення за допомогою фізичного рівня кадру по фізичному середовищу вузлові призначення.

Поділюване середовище Ethernet, незалежно від її фізичної реалізації (коаксіальний кабель, кручене пари або оптоволокно з повторювачами), у будь-який момент часу знаходиться в одному з трьох станів - вільна, зайнята, колізія. Стан зайнятості відповідає нормальній передачі кадру одним з вузлів мережі. Стан колізії виникає при одночасній передачі кадрів більш, ніж одним вузлом мережі.

MAC-підрівень кожного вузла мережі одержує від фізичного рівня інформацію про стан поділюваного середовища. Якщо вона вільна, і в MAC-підрівня мається кадр для передачі, то він передає його через фізичний рівень у мережу. Фізичний рівень одночасно з побітною передачею кадру стежить за станом середовища. Якщо за час передачі кадру колізія не виник, то кадр вважається переданим. Якщо ж за цей час колізія був зафіксований, то передача кадру припиняється, і в мережу видається спеціальна послідовність з 32 біт (так називана jam-послідовність), що повинна допомогти однозначно розпізнати колізію усіма вузлами мережі.

Після фіксації колізії MAC-підрівень робить випадкову паузу, а потім знову намагається передати даний кадр. Випадковий характер паузи зменшує імовірність одночасної спроби захоплення поділюваного середовища декількома вузлами при наступній спробі. Інтервал, з якого вибирається випадкова величина паузи, зростає з кожною спробою (до 10-ої), так що при великому завантаженні мережі і частому виникненні колізій відбувається пригальмовування вузлів. Максимальне число спроб передачі одного кадру - 16, після чого MAC-підрівень залишає даний кадр і починає передачу наступного кадру, що надійшов з LLC-підрівня.

MAC-підрівень вузла приймача, що одержує біти кадру від свого фізичного рівня, перевіряє поле адреси кадру, і якщо адреса збігається з його власним, то він копіює кадр у свій буфер. Потім він перевіряє, чи не містить кадр специфічні помилки: по контрольній сумі (FCS error), по максимально припустимому розмірі кадру (jabber error), по мінімально припустимому розмірі кадру (runts), по невірно знайдених границях байт (alignment error). Якщо кадр коректний, то його поле даних передається на LLC-підрівень, якщо немає - те відкидається.

1.2.1.5. Формати кадрів

Формати кадрів технології Fast Ethernet не відрізняються від форматів кадрів технологій 10-Мегабитного Ethernet'а.

Кадр 802.3/LLC

6 байт	6 байт	2 байти	1 байт	1 байт	1(2) байта	46-1497 (1496) байт	4 байти
DA	SA	L	DSAP	SSAP	Control	Data	FCS
			Заголовок LLC				

Кадр Raw 802.3/Novell 802.3

6 байт	6 байт	2 байти	46-1500 байт	4 байти
DA	SA	L	Data	FCS

Кадр Ethernet Dix (II)

6 байт	6 байт	2 байти	46-1500 байт	4 байти
DA	SA	T	Data	FCS

Кадр Ethernet SNAP

6 байт	6 байт	2 байти	1 байт	1 байт	1 байт	3 байти	2 байти	46-1497 (1496) байт	4 байти
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AA	AA	03	000000			
			Заголовок LLC			Заголовок SNAP			

Малюнок 1.2.2 – Формати кадрів Ethernet

Нижче перераховані всі чотири типи кадрів Ethernet (тут під кадром розуміється весь набір полів, що відносяться до канального рівня, тобто поля MAC і LLC рівнів). Той самий тип кадру може мати різні назви, тому нижче для кожного типу кадру приведене по нескольку найбільш уживаних назв:

- кадр 802.3/LLC (кадр 802.3/802.2 або кадр Novell 802.2);
- кадр Raw 802.3 (або кадр Novell 802.3);
- кадр Ethernet DIX (або кадр Ethernet II);
- кадр Ethernet SNAP.

Формати всіх цих чотирьох типів кадрів Ethernet приведені на мал. 1.2.2.

Кадр 802.3/LLC

Заголовок кадру 802.3/LLC є результатом об'єднання полів заголовків кадрів, визначених у стандартах IEEE 802.3 і 802.2.

Стандарт 802.3 визначає вісьмох полів заголовка (мал. 1.2.2; поле преамбули і початковий обмежник кадру на малюнку не показані).

- ***Поле преамбули*** (Preamble) складається із семи синхронізуючий байт 10101010. При манчестерском кодуванні ця комбінація представляється у фізичному середовищі періодичним хвильовим сигналом з частотою 5 Мгц.
- ***Початковий обмежник кадру*** (Start-of-frame-delimiter, SFD) складається з одного байта 10101011. Поява цієї комбінації біт є вказівкою на те, що наступний байт — це перший байт заголовка кадру.
- ***Адреса призначення*** (Destination Address, DA) може бути довжиною 2 або 6 байт. На практиці завжди використовуються адреси з 6 байт. Перший біт старшого байта адреси призначення є ознакою того, є адреса індивідуальним або груповим. Якщо він дорівнює 0, то адреса є *індивідуальним (unicast)*, а якщо 1, те це *групова адреса (multicast)*. Групова адреса може призначатися усім вузлам мережі або ж визначеній групі вузлів мережі. Якщо адреса складається з всіх одиниць, тобто має шестнадцатеричное представлення OxFFFFFFFFFFFF, те він призначається

усім вузлам мережі і називається *широкомовною адресою (broadcast)*. В інших випадках групова адреса зв'язана тільки з тими вузлами, що сконфигурированы (наприклад, вручну) як члени групи, номер якої зазначений у груповій адресі. Другий біт старшого байта адреси визначає спосіб призначення адреси — централізований або локальний. Якщо цей біт дорівнює 0 (що буває майже завжди в стандартній апаратурі Ethernet), то адреса призначена централізовано, за допомогою комітету IEEE. Комітет IEEE розподіляє між виробниками устаткування так називані організаційно унікальні ідентифікатори (Organizationally Unique Identifier, OUI). Цей ідентифікатор міститься в 3 старших байти адреси (наприклад, ідентифікатор 000081 визначає компанію Bay Networks). За унікальність молодших 3-х байт адреси відповідає виробник устаткування. Двадцять чотири біти, що відводяться виробникові для адресації інтерфейсів його продукції, дозволяють випустити 16 мільйонів інтерфейсів під одним ідентифікатором організації. Унікальність адрес, що централізовано розподіляються, поширюється на всі основні технології локальних мереж - Ethernet, Token Ring, FDDI і т.д.

- ***Адреса джерела*** (Source Address, SA) — це 2- або 6-байтовое поле, що містить адресу вузла — відправника кадру. Перший біт адреси завжди має значення 0.
- ***Довжина*** (Length, L) — 2-байтовое поле, що визначає довжину полючи даних у кадрі.
- ***Поле даних*** (Data) може містити від 0 до 1500 байт. Але якщо довжина полючи менше 46 байт, то використовується наступне поле — поле заповнення, — щоб доповнити кадр до мінімально припустимого значення в 46 байт.
- ***Поле заповнення*** (Padding) складається з такої кількості байт заповнювачів, що забезпечує мінімальну довжину полючи даних у 46 байт. Це забезпечує коректну роботу механізму виявлення колізій. Якщо довжина полючи даних достатня, то поле заповнення в кадрі не з'являється.
- ***Поле контрольної суми*** (Frame Check Sequence, FCS) складається з 4 байт, що містять контрольну суму. Це значення обчислюється по алгоритму CRC-32. Після одержання кадру робоча станція виконує власне обчислення контрольної суми для цього кадру, порівнює отримане значення зі значенням полючи контрольної суми і, таким чином, визначає, чи не перекручений отриманий кадр.

Кадр 802.3 є кадром MAC-подуровня, тому у відповідності зі стандартом 802.2 у його поле даних вкладається кадр подуровня LLC з вилученими прапорами початку і кінця кадру. Формат кадру LLC був описаний вище. Тому що кадр LLC має заголовок довжиною 3 (у режимі LLC1) або 4 байт (у режимі LLC2), те максимальний розмір полючи даних зменшується до 1497 або 1496 байт.

Кадр Ethernet SNAP

Для усунення різнобою в кодуваннях типів протоколів, повідомлення яких вкладені в поле даних кадрів Ethernet, комітетом 802.2 були проведені робота з подальшої стандартизації кадрів Ethernet. У результаті з'явився кадр Ethernet SNAP (SNAP — SubNetwork Access Protocol, протокол доступу до подсетям). Кадр Ethernet SNAP (див. мал. 1.2.2) являє собою розширення кадру 802.3/LLC за рахунок уведення додаткового заголовка протоколу SNAP, що складає з двох полів: OUI і Type. Поле Type складається з 2-х байт і повторює по форматі і призначенню поле Type кадру Ethernet II (тобто в ньому використовуються ті ж значення кодів протоколів). Поле OUI (Organizationally Unique Identifier) визначає ідентифікатор організації, що контролює коди протоколів у поле Type. За допомогою заголовка SNAP досягнута сумісність з кодами протоколів у кадрах Ethernet II, а також створена універсальна схема кодування протоколів. Коди протоколів для технологій 802 контролює IEEE, що має OUI, рівний 000000. Якщо в майбутньому будуть потрібні інші коди протоколів для якої-небудь нової технології, для цього досить вказати інший ідентифікатор організації, що призначає ці коди, а старі значення кодів залишаться в силі (у сполученні з іншим ідентифікатором OUI).

Тому що SNAP являє собою протокол, вкладений до протоколу LLC, те в полях DSAP і SSAP записується код Oxaa, відведений для протоколу SNAP. Поле Control заголовка LLC встановлюється в 0x03, що відповідає використанню ненумерованих кадрів.

Заголовок SNAP є доповненням до заголовка LLC, тому він припустимий не тільки в кадрах Ethernet, але й у кадрах протоколів інших технологій 802. Наприклад, протокол IP завжди використовує структуру заголовків LLC/SNAP при інкапсуляції в кадри всіх протоколів локальних мереж: FDDI, Token Ring, 100VG-AnyLAN, Ethernet, Fast Ethernet, Gigabit Ethernet.

Правда, при передачі пакетів IP через мережі Ethernet, Fast Ethernet і Gigabit Ethernet протокол IP використовує кадри Ethernet DIX.

У кадрах стандарту Ethernet-II (або Ethernet DIX), опублікованого компаніями Xerox, Intel і Digital ще до появи стандарту IEEE 802.3, замість двухбайтового полючи L (довжина полючи даних) використовується двухбайтовое поле T (тип кадру). Значення полючи типу кадру завжди більше 1518 байт, що дозволяє легко розрізнити ці два різних формати кадрів Ethernet DIX і IEEE 802.3.

Час передачі кадрів Fast Ethernet у 10 разів менше соответствуюего часу технології 10-Мегабитного Ethernet'a: бітовий інтервал складає 10 нс замість 100 нс, а межкадровый інтервал – 0,96 мкс замість 9,6 мкс відповідно.

1.2.1.6. У яких випадках рекомендується використовувати Fast Ethernet

У технології Fast Ethernet є кілька ключових властивостей, що визначають області і ситуації її ефективного застосування. До цих властивостей відносяться:

- Великий ступінь наступності стосовно класичного 10-мегабитному Ethernet'y;
- Висока швидкість передачі даних - 100 Мб/с;
- Можливість працювати на всіх основних типах сучасної кабельної проводки - UTP Category 5, UTP Category 3, STP Type 1, многомодовом оптоволокне.

Наявність багатьох загальних рис у технологій Fast Ethernet і Ethernet дає просту загальну рекомендацію - Fast Ethernet варто застосовувати в тих організаціях і в тих частинах мереж, де до цього широко застосовувався 10-мегабитный Ethernet, але сьогоднішні умови або ж найближчі перспективи вимагають у цих частинах мереж більш високої пропускної здатності. При цьому зберігається весь досвід обслуговуючого персоналу, що звик до особливостей і типових несправностей мереж Ethernet. Крім того, можна по колишньому використовувати засобу аналізу протоколів, що працюють з агентами MIB-II, RMON MIB і звичними форматами кадрів.

Організацій, що широко застосовують Ethernet досить багато, тому що Ethernet був і залишається найбільше ефективною технологією по відношенню ціна/продуктивність серед низкоскоростных (4 - 20 Мб/с) технологій. Ця властивість відноситься тепер і до Fast Ethernet, але стосовно до технологій зі швидкістю 100 Мб/с. Однак, Fast Ethernet крім позитивних властивостей, успадкував і недоліки технології Ethernet - великі затримки доступу до середовища при коефіцієнті використання середовища вище 30-40%, що є наслідком застосування алгоритму доступу CSMA/CD, невеликі відстані між вузлами навіть при використання оптоволокна - наслідок методу виявлення колізій, відсутність визначення резервних зв'язків у стандарті і відсутність підтримки пріоритетного трафика додатків реального часу.

Fast Ethernet у мережах робочіх груп

До моменту появи стандарту Fast Ethernet у побудові локальних мереж масштабу будинку або кампуса склався наступний підхід - магістраль великої мережі будувалася на технології FDDI - високошвидкісний і отказоустойчивой, але досить дорогою, а мережі робочих груп і відділів використовували Ethernet або Token Ring.

Тому основна область використання Fast Ethernet сьогодні - це настільні застосування, мережі робочих груп і відділів. При цьому доцільно робити перехід до Fast Ethernet поступово, залишаючи Ethernet там, де він добре справляється зі своєю роботою. Одним з очевидних випадків, коли Ethernet не слід заміняти Fast Ethernet'ом, є підключення до мережі старих персональних комп'ютерів із шиною ISA - їхня пропускна здатність каналу "мережа – диск" не дозволить користувачеві відчути вигоди від підвищення в 10 разів швидкості мережевої технології. Для усунення вузьких місць для мереж, що складаються з таких комп'ютерів, більше підходить використання комутаторів з портами 10 Мб/з, тому що в цьому випадку вузлам гарантированно надається по 10 Мб/з - саме стільки, скількох їм потрібно при їхній архітектурі і параметрах продуктивності.

Нові клієнтські комп'ютери з процесором Pentium Pro і шиною PCI - очевидні претенденти на використання швидкості 100 Мб/с. Тому навіть при досить невизначених вимогах їхніх користувачів до пропускної здатності мережі має сенс купувати для них мережні адаптери Fast Ethernet, що можуть працювати на швидкості 10 Мб/с, поки в організації не з'являться концентратори або комутатори з портами Fast Ethernet. Перехід до швидкості 100Мб/с буде для користувачів практично безболісним, тому що більшість мережних адаптерів не потрібно конфигурировать для переходу на Fast Ethernet (це не відноситься до полнодуплексному варіанта Fast Ethernet, тому що через відсутність стандарту ручне конфигурирование може знадобитися).

Fast Ethernet у магістралях будинків і кампусов

Створення достатнє великих мереж, до яких відносяться мережі будинків і кампусов з кількістю вузлів у кілька сотень, також можливо з використанням технології Fast Ethernet. Ця технологія може використовуватися в таких мережах як у "чистому" виді, так і в сполученні з іншими технологіями, наприклад, FDDI або ATM.

Мережі будинків і навіть великих поверхів зараз практично не будуються без використання комутаторів, тому обмеження на максимальний діаметр мережі в 250 - 272 метра легко переборюються, тому що з'єднання комутатор-комутатор дозволяє подовжити мережа до 412 м при напівдуплексному зв'язку на оптоволокне, і до 2 км при аналогічної полнодуплексной зв'язку.

Полнодуплексный (Full Duplex). Канал або пристрій, що виконує одночасно прийом і передачу даних.

Напівдуплексний (Half Duplex). Пристрій або канал, здатний у кожен момент тільки передавати або приймати інформацію. Прийом і передача, таким чином, повинні виконуватися по черзі.

Відсутність стандартного резервування на рівні повторювачів також мало обмежує побудова отказоустойчивых магістралей - підтримка комутаторами алгоритму Spanning Tree дозволяє автоматично переходити з основного зв'язку, що відмовило, на резервну.

Основними двома факторами, що стримують застосування технології Fast Ethernet на магістралях, є:

- широке використання в даний час для цієї мети технології FDDI;
- відсутність у технології Fast Ethernet засобів підтримки трафика реального часу.

Тому, якщо ці фактори не відносяться до вашої мережі, те її магістраль можна успішно будувати і на технології, що комутирується, Fast Ethernet, особливо на її полнодуплексной версії. Правда в останньому випадку настійно рекомендується використовувати комутатори того самого виробника.

1.2.2. Технологія FDDI

1.2.2.1. Історія створення стандартові FDDI

Технологія *Fiber Distributed Data Interface* - перша технологія локальних мереж, що використовувала як середовище передачі даних оптоволоконный кабель.

Спроби застосування світла як середовище, що несе інформацію, починалися давно - ще в 1880 році Олександр Белл запатентував пристрій, що передавало мову на відстань до 200 метрів за допомогою дзеркала, що вібрувало синхронно зі звуковими хвилями і відбитим світлом, що модулювало.

Роботи з використання світла для передачі інформації активізувалися в 1960-і роки в зв'язку з винаходом лазера, що міг забезпечити модуляцію світла на дуже високих частотах, тобто створити широкополосный канал для передачі великої кількості інформації з високою швидкістю. Приблизно в той же час з'явилися оптичні волокна, що могли передавати світло в кабельних системах, подібно тому як мідні проводи передають електричні сигнали в традиційних кабелях. Однак утрати світла в цих волокнах були занадто великі, щоб вони могли бути використані як альтернатива мідним жилам. Недорогі оптичні волокна, що забезпечують низькі втрати потужності світлового сигналу і широку смугу пропущення (до декількох Ггц) з'явилися тільки в 1970-і роки. На початку 1980-х років почалася промислова установка й експлуатація оптоволоконных каналів зв'язку для територіальних телекомунікаційних систем.

У 1980-і роки почалися також роботи зі створення стандартних технологій і пристроїв для використання оптоволокнных каналів у локальних мережах. Роботи з узагальнення досвіду і розробці першого оптоволоконного стандарту для локальних мереж були зосереджені в Американському Національному Інституті по Стандартизації - ANSI, у рамках створеного для цієї мети комітету X3T9.5.

Початкові версії різних складових частин стандарту FDDI були розроблені комітетом X3T9.5 у 1986 - 1988 роках, і тоді ж з'явилося перше устаткування - мережні адаптери, концентратори, мости і маршрутизатори, що підтримують цей стандарт.

В даний час більшість мережних технологій підтримують оптоволоконные кабелі в якості одного з варіантів фізичного рівня, але FDDI залишається найбільш відпрацьованою високошвидкісною технологією, стандарти на яку пройшли перевірку часом і устоялися, так що устаткування різних виробників показує гарний ступінь сумісності.

1.2.2.2. Основи технології FDDI

Технологія FDDI багато в чому ґрунтується на технології Token Ring, розвиваючи й удосконалюючи її основні ідеї. Розроблювачі технології FDDI ставили перед собою в якості найбільш пріоритетні наступні цілі:

- підвищити бітову швидкість передачі даних до 100 Мб/з;
- підвищити отказоустойчивость мережі за рахунок стандартних процедур відновлення її після відмовлень різного роду - ушкодження кабелю, некоректної роботи вузла, концентратора, виникнення високого рівня перешкод на лінії і т.п.;
- максимально ефективно використовувати потенційну пропускну здатність мережі як для асинхронного, так і для синхронного трафиков.

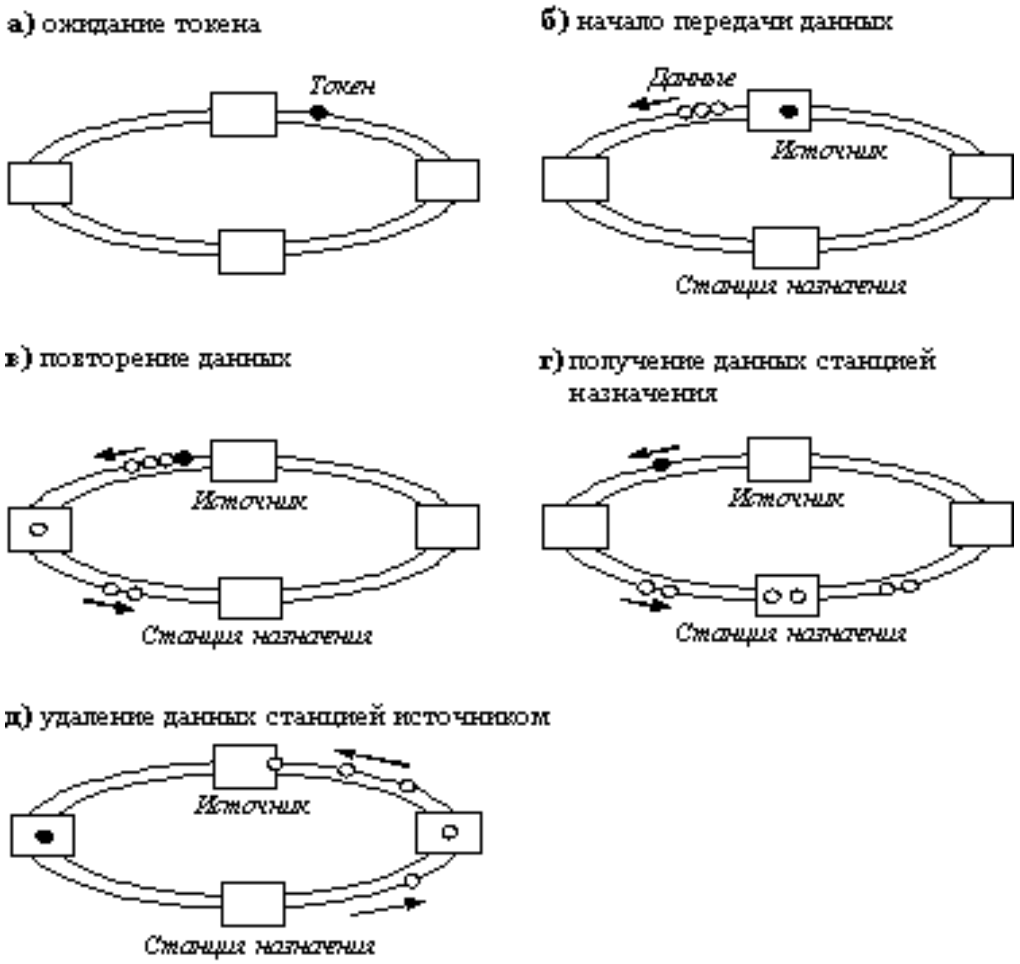
Мережа FDDI будується на основі двох оптоволоконних кілець, що утворять основний і резервний шляхи передачі даних між вузлами мережі. Використання двох кілець - це основний спосіб підвищення отказоустойчивости в мережі FDDI, і вузли, що хочуть їм скористатися, повинні бути підключені до обох кілець. У нормальному режимі роботи мережі дані проходять через усі вузли і всі ділянки кабелю *первинного* (Primary) кільця, тому цей режим названий режимом *Thru* – "*наскрізним*" або "*транзитним*". *Вторинне кільце* (Secondary) у цьому режимі не використовується.

Малюнок 1.2.3 - Реконфигурация кілець FDDI при відмовленні

У випадку якого-небудь виду відмовлення, коли частина первинного кільця не може передавати дані (наприклад, обрыв кабелю або відмовлення вузла), первинне кільце поєднується з вторинним (мал. 1.2.3), утворити знову єдине кільце. Цей режим роботи мережі називається *Wrap*, тобто "*згортання*" або "*згортання*" кілець. Операція згортання виробляється силами концентраторів і/або мережних адаптерів FDDI. Для спрощення цієї процедури дані по первинному кільцю завжди передаються проти вартовий стрілки, а по вторинному - по вартовий. Тому при утворенні загального кільця з двох кілець передавачі станцій як і раніше залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати і приймати інформацію сусідніми станціями.

У стандартах FDDI приділяється багато уваги різним процедурам, що дозволяють визначити наявність відмовлення в мережі, а потім зробити необхідну реконфигурацию. Мережа FDDI може цілком відновлювати свою працездатність у випадку одиничних відмовлень її елементів. При множинних відмовленнях мережа розпадається на трохи не зв'язаних мереж.

Кільця в мережах FDDI розглядаються як загальне поділюване середовище передачі даних, тому для неї визначений спеціальний метод доступу. Цей метод дуже близький до методу доступу мереж Token Ring і також називається методом маркерного (або токенного) кільця - token ring (мал. 1.2.4, а).

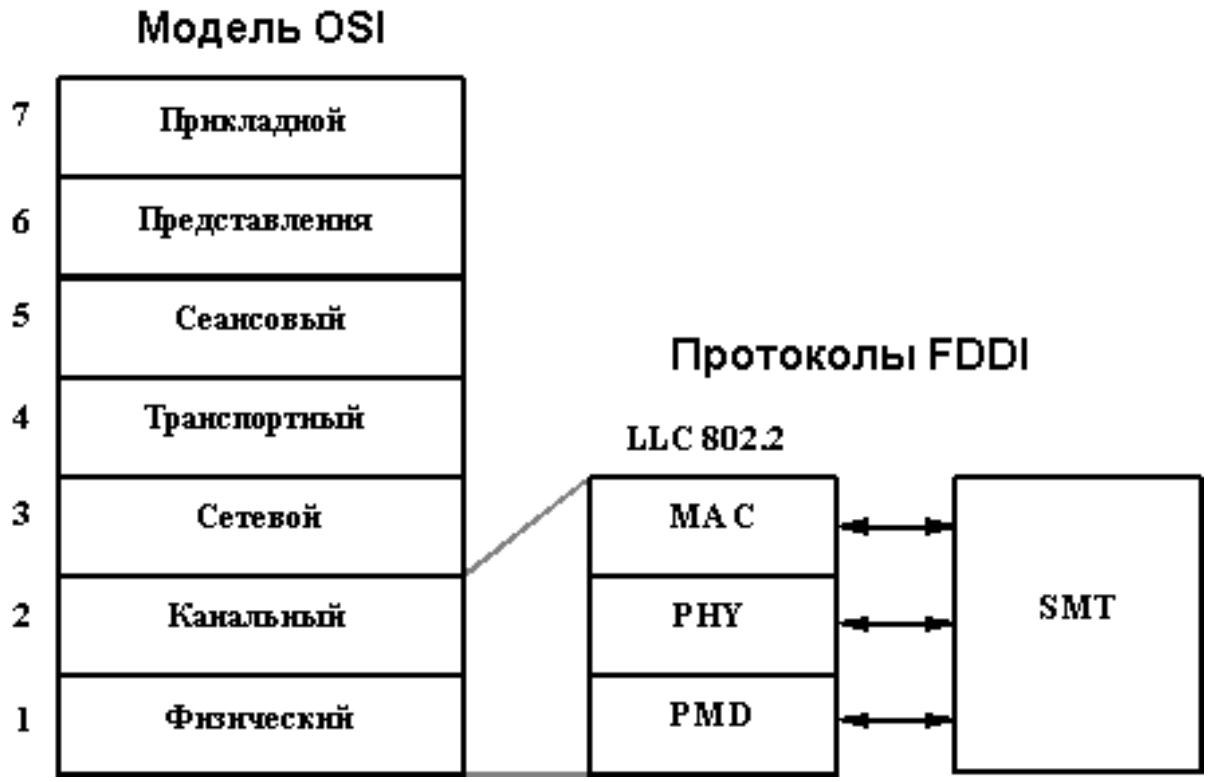


Малюнок 1.2.4 - Обробка кадрів станціями кільця FDDI

Станція може почати передачу своїх власних кадрів даних тільки в тому випадку, якщо вона одержала від попередньої станції спеціальний кадр - токен доступу (мал. 1.2.4, б). Після цього вона може передавати свої кадри, якщо вони в неї маються, протягом часу, називаного часом утримання токена - *Token Holding Time (THT).* Після витікання часу THT станція зобов'язана завершити передачу свого чергового кадру і передати токен доступу наступної станції. Якщо ж у момент прийняття токена в станції немає кадрів для передачі по мережі, то вона негайно транслює токен наступної станції. У мережі FDDI у кожної станції є попередній сусід (upstream neighbor) і наступний сусід (downstream neighbor), обумовлені її фізичними зв'язками і напрямком передачі інформації.

Кожна станція в мережі постійно приймає передані їй попереднім сусідом кадри й аналізує їхню адресу призначення. Якщо адреса призначення не збігається з її власним, то вона транслює кадр своєму наступному сусідові. Цей випадок приведений на малюнку (мал. 1.2.4, в). Потрібно відзначити, що, якщо станція захопила токен і передає свої власні кадри, то протягом цього періоду часу вона не транслює прихожі кадри, а видаляє них з мережі.

Якщо ж адреса кадру збігається з адресою станції, то вона копіює кадр у свій внутрішній буфер, перевіряє його коректність (в основному по контрольній сумі), передає його поле даних для наступної обробки протоколові лежачому вище над FDDI рівнем (наприклад, IP), а потім передає вихідний кадр по мережі наступної станції (мал. 1.2.4, г). У переданому в мережу кадрі станція призначення відзначає три ознаки: розпізнавання адреси, копіювання кадру і відсутності або наявності в ньому помилок.



Малюнок 1.2.5 - Структура протоколів технології FDDI

Після цього кадр продовжує подорожувати по мережі, транслюючи кожним вузлом. Станція, що є джерелом кадру для мережі, відповідальна за те, щоб видалити кадр із мережі, після того, як він, зробивши повний оборот, знову дійде до неї (мал. 1.2.4, д). При цьому вихідна станція перевіряє ознаки кадру, чи дійшов він до станції призначення і чи не був при цьому ушкоджений. Процес відновлення інформаційних кадрів не входить в обов'язку протоколу FDDI, цим повинні займатися протоколи більш високих рівнів.

На малюнку 1.2.5 приведена структура протоколів технології FDDI у порівнянні із семиуровневой моделлю OSI. FDDI визначає протокол фізичного рівня і протокол подуровня доступу до середовища (MAC) канального рівня. Як і багато інших технологій локальних мереж, технологія FDDI використовує протокол 802.2 подуровня керування каналом даних (LLC), визначений у стандартах IEEE 802.2 і ISO 8802.2. FDDI використовує перший тип процедур LLC, при якому вузли працюють у дейтаграммном режимі - без установлення з'єднань і без відновлення загублених або ушкоджених кадрів.

Фізичний рівень розділений на два подуровня: незалежний від середовища подуровень *PHY (Physical)*, і залежний від середовища подуровень *PMD (Physical Media Dependent)*. Роботу всіх рівнів контролює протокол керування станцією *SMT (Station Management)*.

Рівень PMD забезпечує необхідні засоби для передачі даних від однієї станції до іншої по оптоволокну. У його специфікації визначаються:

- вимоги до потужності оптичних сигналів і до многомодовому оптоволоконному кабелю 62,5/125 мкм;
- вимоги до оптичних обхідних перемикачів (optical bypass switches) і оптичним приемопередатчикам;
- параметри оптичних рознімань MIC (Media Interface Connector), їхнє маркірування;
- довжина хвилі в 1300 нанометрів, на якій працюють приемопередатчики;
- представлення сигналів в оптичних волокнах відповідно до методу NRZI.

Специфікація TP-PMD визначає можливість передачі даних між станціями по кручений парі відповідно до методу MLT-3.

Рівень PHY виконує кодування і декодування даних, що циркулюють між MAC-рівнем і рівнем PMD, а також забезпечує тактирование інформаційних сигналів. У його специфікації визначаються:

- кодування інформації у відповідності зі схемою 4B/5B;
- правила тактирования сигналів;
- вимоги до стабільності тактової частоти 125 МГц;
- правила перетворення інформації з рівнобіжної форми в послідовну.

Рівень MAC відповідальний за керування доступом до мережі, а також за прийом і обробку кадрів даних. У ньому визначені наступні параметри:

- протокол передачі токена;
- правила захоплення і ретрансляції токена;
- формування кадру;
- правила генерації і розпізнавання адрес;
- правила обчислення і перевірки 32-розрядної контрольної суми.

Рівень SMT виконує усі функції по керуванню і моніторингові всіх інших рівнів стека протоколів FDDI. У керуванні кільцем бере участь кожен вузол мережі FDDI. Тому усі вузли обмінюються спеціальними кадрами SMT для керування мережею. У специфікації SMT визначене наступне:

- алгоритми виявлення помилок і відновлення після збоїв;
- правила моніторингу роботи кільця і станцій;
- керування кільцем;
- процедури ініціалізації кільця.

Отказоустойчивость мереж FDDI забезпечується за рахунок керування рівнем SMT іншими рівнями: за допомогою рівня PHY усуваються відмовлення мережі по фізичних причинах, наприклад, через обрив кабелю, а за допомогою рівня MAC - логічні відмовлення мережі, наприклад, утрата потрібного внутрішнього шляху передачі токена і кадрів даних між портами концентратора.

У наступній таблиці представлені результати порівняння технології FDDI з технологіями Ethernet і Token Ring.

Таблиця 1.2.1 - Порівняння технології FDDI з технологіями Ethernet і Token Ring

Характеристика	***FDDI***	***Ethernet***	***Token Ring***
Бітова швидкість	100 Мб/з	10 Мб/з	16 Мб/с
Топологія	Подвійне кільце дерев	Шина/зірка	Зірка/кільце
Метод доступу	Частка від часу обороту токена	CSMA/CD	Пріоритетна система резервування
Середовище передачі даних	Многомодовое оптоволокно, неекранована кручена пари	Товстий коаксиал, тонкий коаксиал, кручена пари, оптоволокно	Екранованої і неекранована кручена пари, оптоволокно
Максимальна довжина мережі (без мостів)	200 км (100 км на кільце)	2500 м	1000 м
Максимальна відстань між вузлами	2 км (-11 d утрат між вузлами)	2500 м	100 м
Максимальна кількість вузлів	500 (1000 з'єднань)	1024	260 для екранованої кручений пари, 72

Характеристика	*FDDI*	*Ethernet*	*Token Ring*
			для неекранованої кручений пари
Тактирование і відновлення після відмовлень	Розподілена реалізація тактирования і відновлення після відмовлень	Не визначені	Активний монітор

1.2.2.3. У яких випадках рекомендовано використовувати технологію FDDI

Особливістю технології FDDI є сполучення декількох дуже важливих для локальних мереж властивостей:

- високий ступінь отказоустойчивости;
- здатність покривати значні території, аж до територій великих міст;
- висока швидкість обміну даними;
- можливість підтримки синхронного мультимедийного трафика;
- гнучкий механізм розподілу пропускної здатності кільця між станціями;
- можливість роботи при коефіцієнті завантаження кільця близькому до одиниці;
- можливість легкої трансляції трафика FDDI у трафики таких популярних протоколів як Ethernet і Token Ring за рахунок сумісності форматів адрес станцій і використання загального подуровня LLC.

Поки FDDI - це єдина технологія, який удалося об'єднати всі перераховані властивості. В інших технологіях ці властивості також зустрічаються, але не в сукупності. Так, технологія Fast Ethernet також має швидкість передачі даних 100 Мб/з, але вона не дозволяє відновлювати роботу мережі після однократного обриву кабелю і не дає можливості працювати при великому коефіцієнті завантаження мережі.

За унікальне сочетание властивостей приходиться платити - технологія FDDI є сьогодні самою дорогою 100 Мб технологією. Тому її основні області застосування - це магістралі кампусов і будинків, а також підключення корпоративних серверів. У цих випадках витрати виявляються обґрунтованими - магістраль мережі повинна бути отказоустойчивой і швидкої, то ж відноситься до сервера, побудованому на базі дорогою мультипроцессорной платформи й обслуговуюча сотні користувачів.

Багато сучасних корпоративних мереж побудовані з використанням технології FDDI на магістралі в сполученні з технологіями Ethernet, Fast Ethernet і Token Ring у мережах поверхів і відділів. Група центральних серверів також звичайно підключається до магістрального кільця FDDI прямо, за допомогою мережних адаптерів FDDI.

У зв'язку з появою більш дешевих, чим FDDI 100 Мб технологій, таких як Fast Ethernet і 100VG-AnyLAN, технологія FDDI, мабуть, не знайде широкого застосування при підключенні робочих станцій і створенні невеликих локальних мереж, навіть при збільшенні швидкодії цих станцій і наявності в мережах мультимедийной інформації.

1.2.3. Технологія 100VG-AnyLAN

1.2.3.1. Загальна характеристика технології 100VG-AnyLAN

Як альтернативу технології Fast Ethernet, фірми AT&T і HP висунули проект нової технології зі швидкістю передачі даних 100 Мб/з - *100Base-VG*. У цьому проекті було запропоновано удосконалити метод доступу з урахуванням потреби мультимедийных додатків, при цьому зберегти сумісність формату пакета з форматом пакета мереж 802.3. У вересні 1993 року з ініціативи фірм IBM і HP був утворений комітет IEEE 802.12, що зайнявся стандартизацією нової технології. Проект був розширений за рахунок підтримки

в одній мережі кадрів не тільки формату Ethernet, але і формату Token Ring. У результаті нова технологія одержала назву *100VG-AnyLAN*, тобто технологія для будь-яких мереж (Any LAN - будь-які мережі), маючи у виді, що в локальних мережах технології Ethernet і Token Ring використовуються в гнітючій кількості вузлів.

Улітку 1995 року технологія 100VG-AnyLAN одержала статус стандарту IEEE 802.12.

У технології 100VG-AnyLAN визначений новий метод доступу *Demand Priority* і нова схема квартетного кодування *Quartet Coding*, що використовує надлишковий код 5B/6B.

Метод доступу *Demand Priority* заснований на передачі концентраторові функцій арбітра, що вирішує проблему доступу до поділюваного середовища. Метод Demand Priority підвищує коефіцієнт використання пропускної здатності мережі за рахунок уведення простого, детерминированного методу поділу загального середовища, що використовує два рівні пріоритетів: низький - для звичайних додатків і високий - для мультимедийных.

Технологія 100VG-AnyLAN має меншу популярність серед виробників комунікаційного устаткування, чим конкуруюча пропозиція - технологія Fast Ethernet. Компанії, що не підтримують технологію 100VG-AnyLAN, пояснюють це тим, що для більшості сьогоднішніх додатків і мереж досить можливостей технології Fast Ethernet, що не так помітно відрізняється від звичної більшості користувачів технології Ethernet. У більш далекій перспективі ці виробники пропонують використовувати для мультимедийных додатків технологію ATM, а не 100VG-AnyLAN.

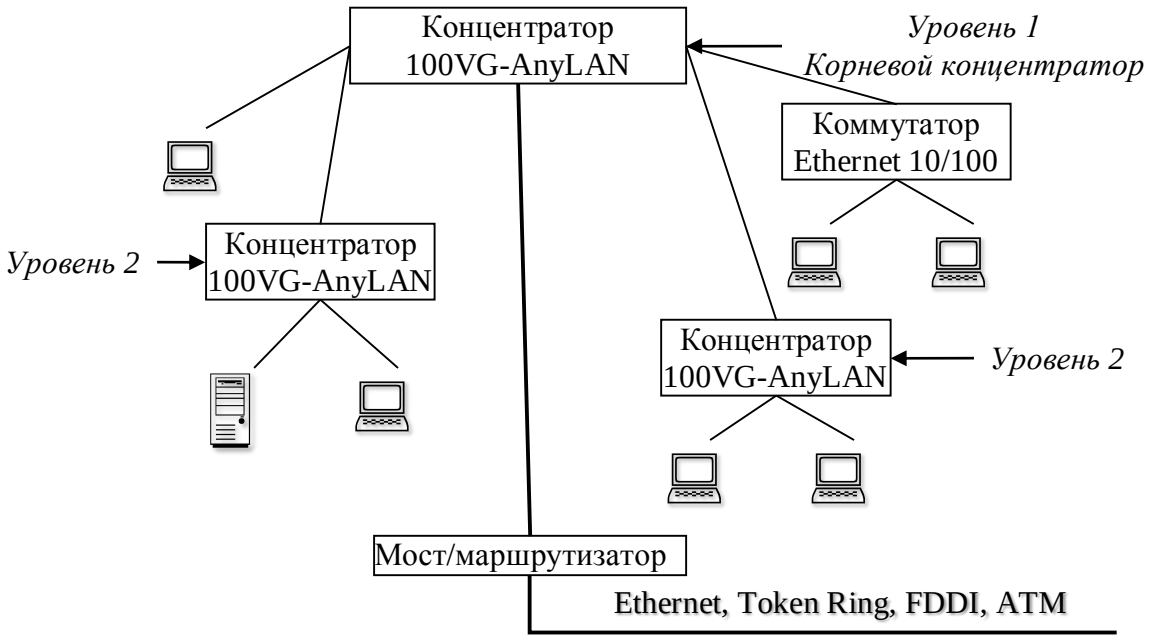
ATM (Asynchronous Transfer Mode - Асинхронний Режим Передачі). Стандартизована ITU технологія комутації пакетів фіксованої довжини - осередків (cell). Режим ATM є асинхронним у тім змісті, що осередку від окремих користувачів передаються аперіодично. Ця технологія призначена для передачі даних зі швидкістю від 1.5 Мбит/сек до 2 Гбит/сек і забезпечує ефективну передачу різних типів даних (голос, відео, multimedia, трафик ЛВС) на значні відстані. Специфікації ATM розробляються Форумом ATM (ATM Forum) незалежною асоціацією виробників і користувачів.

Проте, число прихильників технології 100VG-AnyLAN росте і нараховує близько 30 компаній. Серед них знаходяться не тільки копанні Hewlett-Packard і IBM, але і такі лідери як Cisco Systems, Cabletron, D-Link і інші. Усі ці компанії підтримують обидві конкуруючі технології у своїх продуктах, випускаючи модулі з портами як Fast Ethernet, так і 100VG-AnyLAN.

1.2.3.2. Структура мережі 100VG-AnyLAN

Мережа 100VG-AnyLAN завжди включає центральний концентратор, називаний концентратором рівня 1 або кореневим концентратором (мал. 1.2.6).

Корнєвій концентратор має зв'язку з кожним вузлом мережі, утворити топологію типу зірка. Цей концентратор являє собою інтелектуальний центральний контролер, що керує доступом до мережі, постійно виконуючи цикл "кругового" сканування своїх портів і перевіряючи наявність запитів на передачу кадрів від приєднаних до них вузлів. Концентратор приймає кадр від вузла, що видав запит, і передає його тільки через той порт, до якого приєднаний вузол с адресою, що збігається з адресою призначення, зазначеним у кадрі.



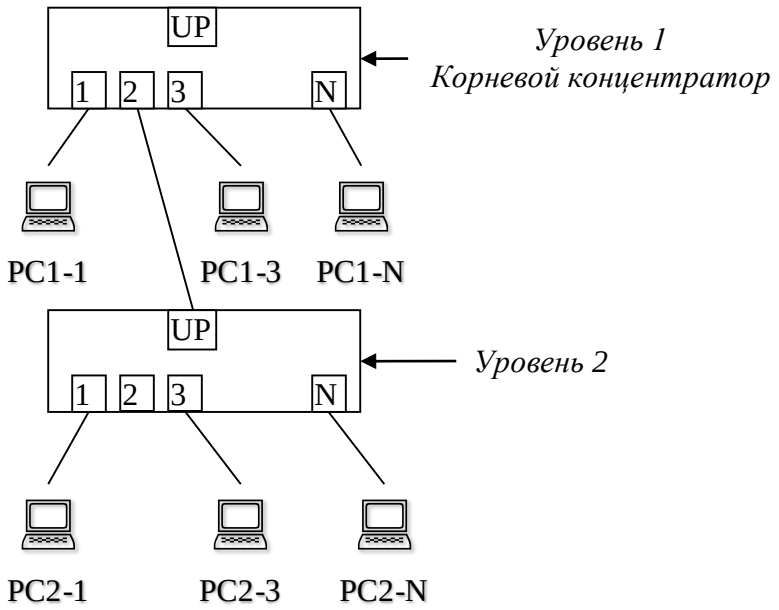
Малюнок 1.2.6 - Структура мережі 100VG-AnyLAN

Кожен концентратор може бути сконфигурирован на підтримку або кадрів 802.3 Ethernet, або кадрів 802.5 Token Ring. Усі концентратори, розташовані в тому самому логічному сегменті (не розділеному мостами, комутаторами або маршрутизаторами), повинні бути сконфигурированы на підтримку кадрів одного типу. Для з'єднання мереж 100VG-AnyLAN, що використовують різні формати кадрів 802.3, потрібний міст, комутатор або маршрутизатор. Аналогічний пристрій потрібно й у тому випадку, коли мережа 100VG-AnyLAN повинна бути з'єднана з мережею FDDI або ATM.

Кожен концентратор має один "висхідний" (up-link) порт і N "спадних" портів (down-link), як це показано на малюнку 1.2.7.

Висхідний порт працює як порт вузла, але він зарезервований для приєднання як вузол до концентратора більш високого рівня. Спадні порти служать для приєднання вузлів, у тому числі і концентраторів нижнього рівня. Кожен порт концентратора може бути сконфигурирован для роботи в нормальному режимі або в режимі монітора. Порт, сконфигурированный для роботи в нормальному режимі, передає тільки ті кадри, що призначені вузлові, підключеному до даного порту. Порт, сконфигурированный для роботи в режимі монітора, передає всі кадри, оброблювані концентратором. Такий порт може використовуватися для підключення аналізатора протоколів.

Вузол являє собою комп'ютер або комунікаційний пристрій технології 100VG-AnyLAN - міст, комутатор, маршрутизатор або концентратор. Концентратори, що підключаються як вузли, називаються концентраторами 2-го і 3-го рівнів. Усього дозволяється утворювати до трьох рівнів ієрархії концентраторів.



Малюнок 1.2.7 - Кругове опитування портів концентраторами мережі 100VG-AnyLAN

Зв'язок, що з'єднує концентратор і вузол, може бути утворена або 4 парами неекранованої кручений пари категорій 3, 4 або 5 (4-UTP Category 3, 4, 5), або 2 парами неекранованої кручений пари категорії 5 (2-UTP Category 5), або 2 парами екранованої кручений пари типу 1 (2-STP Type 1), або 2 парами многомодового оптоволоконного кабелю.

Варіанти кабельної системи можуть використовуватися будь-які, але нижче буде розглянутий варіант 4-UTP, що був розроблений першим і одержав найбільше поширення.

На закінчення роздягнула приведемо таблицю, складену компанією Hewlett-Packard, у якій приводяться результати порівняння цієї технології з технологіями 10Base-T і 100Base-T.

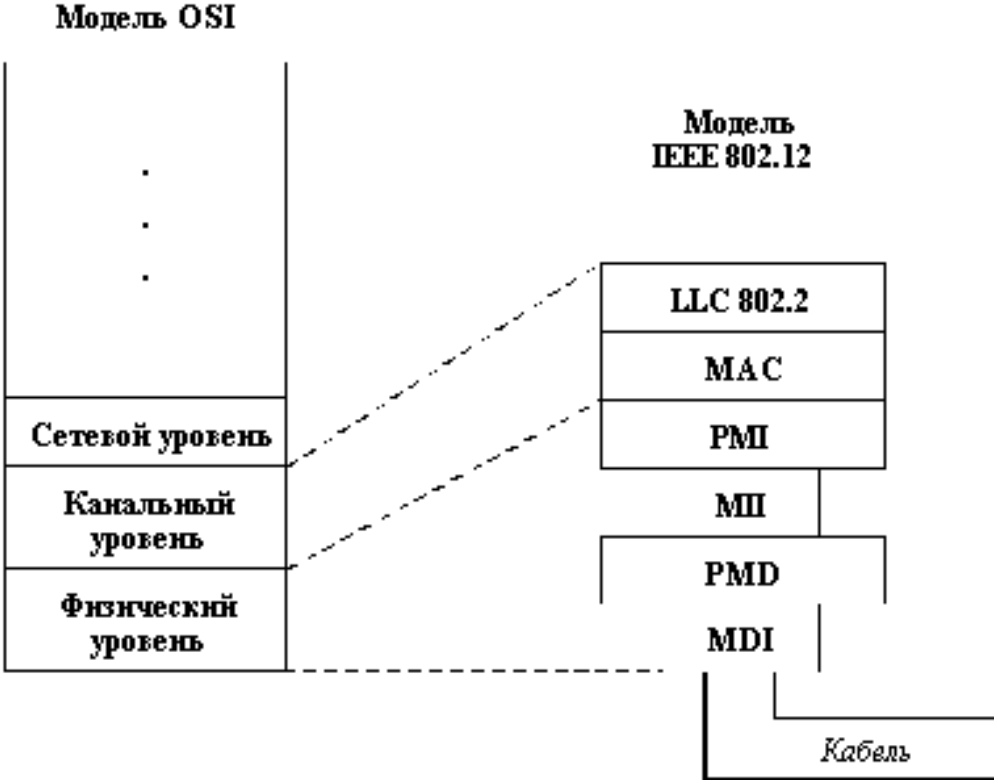
Таблиця 1.2.2 - Порівняння технології ***100VG-AnyLAN*** з технологіями 10Base-T Ethernet і 100Base-T Fast Ethernet

Характеристика	***10Base-T***	***100VG-AnyLAN***	***100Base-T***
		Топологія	
Максимальний діаметр мережі	2500 м	8000 м	412 м
Каскадирование концентраторів	Так; 3 рівні	Так; 5 рівнів	Два концентратори максимум
		Кабельна система	
UTP Category 3,4	100 м	100 м	100 м
UTP Category 5	150 м	200 м	100 м
STP Type 1	100 м	100 м	100 м
Оптоволокно	2000 м	2000 м	412 м
		Продуктивність	
При довжині мережі 100 м	80% (теоретична)	95% (продемонстрована)	80% (теоретична)
При довжині мережі 2500 м	80% (теоретична)	80% (продемонстрована)	Не підтримується
		Технологія	
Кадри IEEE 802.3	Так	Так	Так
Кадри 802.5	Немає	Так	Немає
Метод доступу	CSMA/CD	Demand Priority	CSMA/CD + подуровень

Характеристика	*10Base-T*	*100VG-AnyLAN*	*100Base-T*
			узгодження (Reconciliation sublayer)

1.2.3.3. Стек протоколів технології 100VG-AnyLAN

Структура стека протоколів технології 100VG-AnyLAN погодиться з архітектурними моделями OSI/ISO і IEEE, у яких канальний рівень розділений на подуровни. Як видно з малюнка 1.2.8, стік протоколів технології 100VG-AnyLAN складається з подуровня доступу до середовища *(Media Access Control, MAC)*, подуровня, що незалежить від фізичного середовища *(Physical Media Independent, PMI)* і подуровня, що залежить від фізичного середовища *(Physical Media Dependent, PMD)*.



Малюнок 1.2.8 - Структура стека протоколів технології 100VG-AnyLAN

1.2.4. Перспективи високошвидкісних технологій – перехід на гігабітні швидкості

Хоча перехід на нові високошвидкісні технології, такі як Fast Ethernet і 100VG-AnyLAN, почався не дуже давно, уже знаходяться в розробці два нових проекти - технологія Gigabit Ethernet і Gigabit VG, запропоновані відповідно Gigabit Ethernet Alliance і комітетом IEEE 802.12.

Інтерес до технологій для локальних мереж з гигабитными швидкостями підвищився в зв'язку з двома обставинами - по-перше, успіхом порівняно недорогих (у порівнянні з FDDI) технологій Fast Ethernet і 100VG-AnyLAN, по-друге, із занадто великими труднощями, випробовуваними технологією ATM на шляху до кінцевого користувача.

Технологія ATM має багатьма приваблив властивостями - масштабируемой швидкістю передачі даних, що доходить до 10 Гб/з, відмінною підтримкою мультимедийного трафика і можливістю роботи як у локальних, так і в глобальних мережах. Однак, вартість технології ATM і її складність не завжди виправдані. От для таких застосувань, у яких потрібна в першу чергу висока швидкість обміну, а без інших можливостей, пропонованих ATM, можна прожити, і призначені активно розроблювальні сьогодні гигабитные варіанти Ethernet і VG.

За комітетом 802.12 коштує, природно, компанія Hewlett-Packard. До ентузіастів перекладу технології VG на гигабитные швидкості відносяться також компанії Compaq Computer, Texas Instrument і Motorola.

У Gigabit Ethernet Alliance входять поряд з іншими компанії Bay Networks, Cisco Systems і 3Com.

Обидві групи мають намір широко використовувати досягнення технології Fibre Channel, що вже працює з гигабитными швидкостями. У всякому разі, Fibre Channel зі своїм методом кодування 8B/10B фігурує як один з варіантів фізичного рівня для оптоволоконного кабелю.

Розроблювальні пропозиції залишають метод доступу в незмінному виді: CSMA/CD для технології Gigabit Ethernet і Demand Priority для Gigabit VG.

У зв'язку з обмеженнями, що накладаються методом CSMA/CD на довжину кабелю, версія Gigabit Ethernet для поділюваного середовища буде допускати довжину зв'язків до 25 метрів на кручений парі. У зв'язку з такими серйозними обмеженнями більш популярні будуть, мабуть, полнодуплексные версії гигабитного Ethernet'a, що працюють тільки з комутаторами і допускають відстанню між вузлом і комутатором у 500 метрів для многомодового кабелю і до 2 км для одномодового кабелю.

Для технології Gigabit VG пропонується реалізувати швидкість 500 Мб/із для кручений пари і 1 Гб/із для оптоволокна. Граничні відстані між вузлами очікуються наступні: для кручений пари - 100 м, для многомодового оптоволокна - 500 м і для одномодового оптоволокна - 2 км.

РОЗДІЛ 2 ПРОТОКОЛИ TCP/IP

Тема 2.1. Стек протоколів TCP/IP

2.2.1. Історія та перспективи стеку TCP/IP

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

Стік TCP/IP був розроблений з ініціативи Міністерства оборони США більш 20 років тому для зв'язку експериментальної мережі ARPAnet з іншими мережами як набір загальних протоколів для різнорідного обчислювального середовища. Великий внесок у розвиток стека TCP/IP, що одержав свою назву по популярних протоколах IP і TCP, вніс університет Беркли, реалізувавши протоколи стека у своїй версії ОС UNIX, Популярність цієї операційної системи привела до широкого поширення протоколів TCP, IP і інших протоколів стека. Сьогодні цей стік використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Internet, а також у величезному числі корпоративних мереж.

Стік TCP/IP на нижньому рівні підтримує всі популярні стандарти фізичного і канального рівнів: для локальних мереж — це Ethernet, Token Ring, FDDI, для глобальних — протоколи роботи на аналогових що комутируються і виділених лініях SLIP, PPP, протоколи територіальних мереж X.25 і ISDN.

SLIP (Serial Line IP). Протокол Internet, використовуваний для реалізації IP при з'єднанні двох систем послідовними лініями (телефонними або RS-232). В даний час замість SLIP в основному використовується протокол PPP.

PPP(Point-to-PointProtocol). Будучи спадкоємцем SLIP, PPP забезпечує з'єднання маршрутизатор-маршрутизатор і хост-сеть як для синхронних, так і для асинхронних пристроїв.

Основними протоколами стека, що дали йому назва, є протоколи IP і TCP. Ці протоколи в термінології моделі OSI відносяться до мережевого і транспортного рівнів відповідно. IP забезпечує просування пакета по складеній мережі, а TCP гарантує надійність його доставки.

FTP (File Transfer Protocol). Використовуваний у Internet протокол (і програма) передачі файлів між хост-компьютерами.

Telnet. Протокол віртуального термінала в наборі протоколів Internet. Дозволяє користувачам одного хоста підключатися до іншого вилученому хосту і працювати з ним як через звичайний термінал.

За довгі роки використання в мережах різних країн і організацій стік TCP/IP увібрав у себе велика кількість протоколів прикладного рівня. До них відносяться такі популярні протоколи, як протокол пересилання файлів FTP, протокол эмуляции термінала telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Internet, гіпертекстові сервисы служби WWW і багато хто інші.

SMTP (Simple Mail Transfer Protocol). Протокол електронної пошти Internet. Визначений у RFC 821, а формати повідомлень описані в RFC 822.

Сьогодні стік TCP/IP являє собою один з найпоширеніших стеков транспортних протоколів обчислювальних мереж. Дійсно, тільки в мережі Internet об'єднано близько 10 мільйонів комп'ютерів по усім світі, що взаємодіють один з одним за допомогою стека протоколів TCP/IP.

Стрімке зростання популярності Internet привів і до змін у розміщенні сил у світі комунікаційних протоколів — протоколи TCP/IP, на яких побудований Internet, стали швидко тіснити безперечного лідера минулих років — стік IPX/SPX компанії Novell. Сьогодні у світі загальна кількість комп'ютерів, на яких установлений стек TCP/IP, зрівнялося з загальною кількістю комп'ютерів, на яких працює стек IPX/SPX, і це говорить про різкий перелом у відношенні адміністраторів локальних мереж до протоколів, використовуваним на настільних комп'ютерах, тому що саме вони складають гнітюче число світового комп'ютерного парку і саме на них раніш майже скрізь працювали протоколи

компанії Novell, необхідні для доступу до файлових серверів NetWare. Процес становлення стека TCP/IP у якості стека номер один у будь-яких типах мереж продовжується, і зараз будь-яка промислова операційна система обов'язково включає програмну реалізацію цього стека у своєму комплекті постачання.

IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange). IPX використовується як основний протокол у мережах Novell NetWare для обміну даними між вузлами мережі і додатками, що працюють на різних вузлах. Протокол SPX містить розширений у порівнянні з IPX набір команд, що дозволяє забезпечити більш широкі можливості на транспортному рівні. SPX забезпечує гарантовану доставку пакетів.

Хоча протоколи TCP/IP нерозривно зв'язані з Internet і кожний з багатомільйонної армади комп'ютерів Internet працює на основі цього стека, існує велика кількість локальних, корпоративних і територіальних мереж, що безпосередньо не є частинами Internet, у яких також використовують протоколи TCP/IP. Щоб відрізняти них від Internet, ці мережі називають мережами TCP/IP або просто IP-мережами.

Оскільки стік TCP/IP споконвічно створювався для глобальної мережі Internet, він має багато особливостей, що дають йому перевага перед іншими протоколами, коли мова заходить про побудову мереж, що включають глобальні зв'язки. Зокрема, дуже корисною властивістю, що робить можливим застосування цього протоколу у великих мережах, є його здатність фрагментировать пакети. Дійсно, велика складена мережа часто складається з мереж, побудованих на зовсім різних принципах. У кожній з цих мереж може бути установлена власна величина максимальної довжини одиниці переданих даних (кадру). У такому випадку при переході з однієї мережі, що має велику максимальну довжину, у мережу з меншою максимальною довжиною може виникнути необхідність розподілу переданого кадру на кілька частин. Протокол IP стека TCP/IP ефективно вирішує цю задачу.

Іншою особливістю технології TCP/IP є гнучка система адресації, що дозволяє більш просто в порівнянні з іншими протоколами аналогічного призначення включати в інтермережу мережі інших технологій. Це властивість також сприяє застосуванню стека TCP/IP для побудови великих гетерогенних мереж.

У стеці TCP/IP дуже ощадливо використовуються можливості широкомовних розсилань. Це властивість досконала необхідно при роботі на повільних каналах зв'язку, характерних для територіальних мереж.

DNS (Domain Name System - Система Імен Доменов). Розподілений механізм імен/адрес, використовуваних у мережі Internet. Використовується для дозволу логічних імен у IP-адреси. DNS використовується в мережі Internet, забезпечуючи можливість роботи зі зрозумілими і легко запам'ятовуються іменами замість чисел IP-адреси.

Однак, як і завжди, за одержувані переваги треба платити, і платою тут виявляються високі вимоги до ресурсів і складність адміністрування IP-мереж. Могутні функціональні можливості протоколів стека TCP/IP вимагають для своєї реалізації високих обчислювальних витрат. Гнучка система адресації і відмовлення від широкомовних розсилань приводять до наявності в IP-мережі різних централізованих служб типу DNS, DHCP і т.п. Кожна з цих служб спрямована на полегшення адміністрування мережі, у тому числі і на полегшення конфигурирования устаткування, але в той же час сама вимагає пильної уваги з боку адміністраторів.

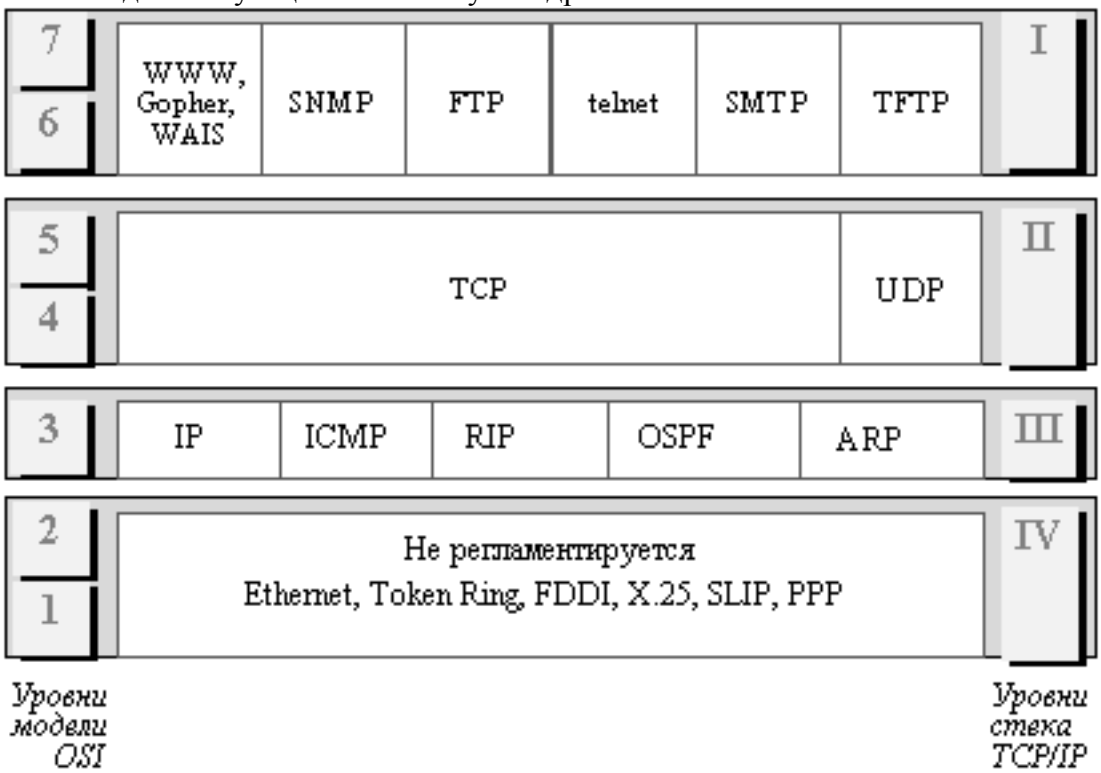
Можна приводити й інші доводи за і проти стека протоколів Internet, однак факт залишається фактом — сьогодні це самий популярний стік протоколів, широко використовуваний як у глобальних, так і локальних мережах.

2.1.2. Структура стеку TCP/IP

Тому що стік TCP/IP був розроблений до появи моделі взаємодії відкритих систем ISO/OSI, те, хоча він також має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделі OSI досить умовно.

Структура протоколів TCP/IP приведена на малюнку 2.2.1. Протоколи TCP/IP поділяються на 4 рівні.

Самий нижній (***рівень IV***) відповідає фізичному і канальному рівням моделі OSI. Цей рівень у протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного і канального рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальних мереж - протоколи з'єднань "точка-крапка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay. Розроблена також спеціальна специфікація, що визначає використання технології ATM як транспорт канального рівня. Звичайно з появою нової технології локальних або глобальних мереж вона швидко включається в стек TCP/IP за рахунок розробки відповідного RFC, що визначає метод інкапсуляції пакетів IP у її кадри.



Малюнок 2.1.1 - Стік TCP/IP

RFC (Request For Comments). Серія документів, почата в 1969 році й утримуючого опису набору протоколів Internet і зв'язану з ними інформацію. Не всі (фактично, далеко не всі) RFC описують стандарти Internet, але всі стандарти Internet описані в RFC. Документи RFC можна знайти на сервері InterNIC

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

Frame Relay. Високошвидкісна технологія, заснована на комутації пакетів, для передачі даних між інтелектуальними окінечними пристроями типу маршрутизаторів або FRAD, що працюють зі швидкістю від 56Kbps до 1.544Mbps. Дані поділяються на кадри перемінної довжини передавальним пристроєм, а кожен кадр містить заголовок з адресою одержувача. Кадри передаються цифровим пристроєм і збираються на прийомному кінці. Технологія Frame relay забезпечує меншу кількість помилок і велику (приблизно втроє) швидкість доставки в порівнянні з X.25, на основі якої вона була розроблена. Великою перевагою мереж frame relay загального користування є зоряна топологія на логічному рівні.

Як основний протокол мережевого рівня (у термінах моделі OSI) у стеці використовується протокол IP, що споконвічно проектувався як протокол передачі пакетів у складених мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і ощадливо витрачаючи пропускну здатність низькошвидкісних ліній зв'язку. Протокол IP є

дейтаграмним протоколом, тобто він не гарантує доставку пакетів до вузла призначення, але намагається це зробити.

До рівня міжмережевої взаємодії відносяться і всі протоколи, зв'язані зі складанням 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 для обміну інформацією про помилки між маршрутизаторами мережі і вузлом - джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи і т.п.

Наступний рівень (***рівень II***) називається основним. На цьому рівні функціонують протокол керування передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача *UDP (User Datagram Protocol)*. Протокол TCP забезпечує надійну передачу повідомлень між вилученими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і IP, і виконує тільки функції сполучної ланки між мережним протоколом і численними прикладними процесами.

Верхній рівень (***рівень I***) називається прикладним. За довгі роки використання в мережах різних країн і організацій стік TCP/IP нагромадив велику кількість протоколів і сервісів прикладного рівня. До них відносяться такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Internet, гіпертекстові сервіси доступу до вилученої інформації, такі як WWW і багато хто інші. Зупинимося трохи докладніше на деякі з них.

Протокол пересилання файлів *FTP (File Transfer Protocol)* реалізує вилучений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує як транспорт протокол із установленням з'єднань - TCP. Крім пересилання файлів протокол FTP пропонує й інші послуги. Так, користувачеві надається можливість інтерактивної роботи з вилученою машиною, наприклад, він може 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 парольна аутентифікація не потрібно, і неї обходять за рахунок використання для такого доступу визначеного імені користувача Anonymous.

У стеці TCP/IP протокол FTP пропонує найбільш широкий набір послуг для роботи з файлами, однак він є і самого складним для програмування. Додатка, яким не потрібні всі можливості FTP, можуть використовувати іншої, більш економічний протокол - найпростіший протокол пересилання файлів *TFTP (Trivial File Transfer Protocol)*. Цей протокол реалізує тільки передачу файлів, причому як транспорт використовується більш простій, чим TCP, протокол без установлення з'єднання - UDP.

Протокол *telnet* забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найбільше часто цей протокол використовується для эмуляции термінала вилученого комп'ютера. При використанні сервісу telnet користувач фактично керує вилученим комп'ютером так само, як і локальний користувач, тому такий вид доступу вимагає гарного захисту. Тому сервери telnet завжди використовують як мінімум аутентифікацію по паролі, а іноді і більш могутні засоби захисту, наприклад, систему Kerberos.

Протокол *SNMP (Simple Network Management Protocol)* використовується для організації мережевого керування. Споконвічно протокол SNMP був розроблений для вилученого контролю і керування маршрутизаторами Internet, що традиційно часто називають також шлюзами. З ростом популярності протокол SNMP стали застосовувати і

для керування будь-яким комунікаційним устаткуванням - концентраторами, мостами, мережними адаптерами і т.д. і т.п. Проблема керування в протоколі SNMP розділяється на двох задач.

Перша задача зв'язана з передачею інформації. Протоколи передачі керуючої інформації визначають процедуру взаємодії SNMP-агента, що працює в керованому устаткуванні, і SNMP-монітора, що працює на комп'ютері адміністратора, що часто називають також консоллю керування. Протоколи передачі визначають формати повідомлень, якими обмінюються агенти і монітор.

Друга задача зв'язана з контрольованими перемінними, що 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 дані керування мережею. Ця специфікація, відома як база даних *MIB (Management Information Base)*, визначає ті елементи даних, що керований пристрій повинний зберігати, і припустимі операції над ними.

2.1.3. Адресація в IP-мережах

2.1.3.1. Типи адреса: фізична (MAC-адреси), мережева (IP-адреси) та символьна (DNS-ім'я)

Кожен комп'ютер у мережі TCP/IP має адреси трьох рівнів:

- ***Локальна адреса вузла***, обумовлена технологією, за допомогою якої побудована окрема мережа, у яку входить даний вузол. Для вузлів, що входять у локальні мережі - це Mac-адрес мережевого адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками устаткування і є унікальними адресами, тому що керуються централізовано. Для всіх існуючих технологій локальних мереж MAC-адрес має формат 6 байтів: старші 3 байти - ідентифікатор фірми виробника, а молодші 3 байти призначаються унікальним образом самим виробником. Для вузлів, що входять у глобальні мережі, такі як X.25 або frame relay, локальна адреса призначається адміністратором глобальної мережі.
- ***IP-адреса***, що складається з 4 байт, наприклад, 109.26.17.100. Ця адреса використовується на мережному рівні. Він призначається адміністратором під час конфигурирования комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі і номери вузла. Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Network Information Center, NIC), якщо мережа повинна працювати як складова частина Internet. Звичайно провайдери послуг Internet одержують діапазони адрес у підрозділів NIC, а потім розподіляють них між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Розподіл IP-адреси на поле номера мережі і номери вузла - гнучке, і границя між цими полями може встановлюватися досить довільно. Вузол може входити в кілька IP-мереж. У цьому випадку вузол повинний мати кілька IP-адрес, по числу мережних зв'язків. У такий спосіб IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережне з'єднання.
- ***Символьний ідентифікатор-ім'я***, наприклад, SERV1.IBM.COM. Ця адреса призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домена. Така адреса, називана також DNS-ім'ям, використовується на прикладному рівні, наприклад, у протоколах FTP або telnet.

2.1.3.2. Три основні класи IP-адреси

IP-адреса має довжину 4 байти і звичайно записується у виді чотирьох чисел, що представляють значення кожного байта в десятковій формі, і розділених крапками, наприклад:

- 128.10.2.30 - традиційна десяткова форма представлення адреси,
- 10000000 00001010 00000010 00011110 - двоичная форма представлення цієї ж адреси.

На малюнку 2.1.2 показана структура IP-адреси.

Клас А

0	N мережі	N вузла

Клас У

1	0	N мережі	N вузла

Клас З

1	1	0	N мережі	N вузла

Клас D

1	1	1	0	адреса групи multicast

Клас E

1	1	1	1	0	зарезервований

Малюнок 2.1.2 - Структура IP-адреса

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

- Якщо адреса починається з 0, то мережу відносять до ***класу А***, і номер мережі займає один байт, інші 3 байти інтерпретуються як номер вузла в мережі. Мережі класу А мають номера в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей.) Мереж класу А небагато, зате кількість вузлів у них може досягати 2^{24}, тобто 16 777 216 вузлів.
- Якщо перші два біти адреси рівні 10, то мережа відноситься до ***класу В*** и є мережею середніх розмірів з максимальним числом вузлів 2^{16}, що складає 65536 вузлів. У мережах класу В під адресу мережі і під адресу вузла приділяється по 16 битов, тобто по 2 байти.
- Якщо адреса починається з послідовності 110, то це мережа ***класу С*** с числом вузлів не більше 2^8, тобто 256 вузлів. Під адресу мережі приділяється 24 битка, а під адресу вузла - 8 битов.
- Якщо адреса починається з послідовності 1110, то він є адресою ***класу D*** і позначає особливу, групову адресу - multicast. Якщо в пакеті як адресу призначення зазначена адреса класу D, то такий пакет повинні одержати усі вузли, яким привласнений дана адреса.
- Якщо адреса починається з послідовності 11110, то це адреса ***класу Е***, вона зарезервований для майбутніх застосувань.

У таблиці приведені діапазони номерів мереж, що відповідають кожному класові мереж.

Таблиця 2.1.1 – Характеристики адрес різного класу

Клас	*Перші біти*	*Найменший номер мережі*	*Найбільший номер мережі*	*Максимальне число вузлів у мережі*
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0.	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	Multicast

Клас	*Перші біти*	*Найменший номер мережі*	*Найбільший номер мережі*	*Максимальне число вузлів у мережі*
E	11110	240.0.0.0	247.255.255.255	Зарезервований

2.1.3.3. Особливі IP-адреси

У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес.

- Якщо вся IP-адреса складається тільки з двоичных нулів, то він позначає адресу того вузла, що згенерував цей пакет; цей режим використовується тільки в деяких повідомленнях ICMP.
- Якщо в поле номера мережі коштують только нулі, то за замовчуванням вважається, що вузол призначення належить тієї ж самої мережі, що і вузол, що відправив пакет.
- Якщо всі двоичные розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинний розсилатися усім вузлам, що знаходяться в тій же мережі, що і джерело цього пакета. Таке розсилання називається *обмеженим широкомовним повідомленням (limited broadcast)*.
- Якщо в поле номера вузла призначення коштують только одиниці, то пакет, що має така адреса, розсилається усім вузлам мережі з заданим номером мережі. Наприклад, пакет з адресою 192.190.21.255 доставляється усім вузлам мережі 192.190.21.0. Таке розсилання називається *широкомовним повідомленням (broadcast)*.

При адресації необхідно враховувати ті обмеження, що вносяться особливим призначенням деяких IP-адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двоичных одиниць або тільки з одних двоичных нулів. Звідси випливає, що максимальна кількість вузлів, приведена в таблиці для мереж кожного класу, на практиці повинне бути зменшене на 2. Наприклад, у мережах класу З під номер вузла приділяється 8 біт, що дозволяють задавати 256 номерів: від 0 до 255. Однак на практиці максимальне число вузлів у мережі класу З не може перевищувати 254, тому що адреси 0 і 255 мають спеціальне призначення. З цих же розумінь випливає, що кінцевий вузол не може мати адресу типу 98.255.255.255, оскільки номер вузла в цій адресі класу А складається з одних двоичных одиниць.

Особливий зміст має IP-адресу, перший октет якого дорівнює 127. Він використовується для тестування програм і взаємодії процесів у межах однієї машини. Коли програма посилає дані по IP-адресі 127.0.0.1, то утвориться як би “петля”. Дані не передаються по мережі, а повертаються модулям верхнього рівня як тільки що прийняті. Тому в IP-мережі забороняється привласнювати машинам IP-адреси, що починаються з 127. Ця адреса має назва *loopback*. Можна віднести адреса 127.0.0.0 до внутрішньої мережі модуля маршрутизації вузла, а адреса 127.0.0.1 — до адреси цього модуля на внутрішній мережі. Насправді будь-яка адреса мережі 127.0.0.0 служить для позначення свого модуля маршрутизації, а не тільки 127.0.0.1, наприклад 127.0.0.3.

У протоколі IP немає поняття широковещательности в тім змісті, у якому воно використовується в протоколах канального рівня локальних мереж, коли дані повинні бути доставлені абсолютно усім вузлам. Як обмежена широкомовна IP-адреса, так і широкомовну IP-адресу мають межі поширення в інтермережі — вони обмежені або мережею, до якої належить вузол-джерело пакета, або мережею, номер якої зазначений в адресі призначення. Тому розподіл мережі за допомогою маршрутизаторів на частині локалізує широкомовний шторм межами однієї зі складову загальну мережу частин просто тому, що немає способу адресувати пакет одночасно усім вузлам усіх мереж складеної мережі.

Уже згадувана форма групової IP-адреси — *multicast* — означає, що даний пакет

повинний бути доставлений відразу декільком вузлам, що утворять групу з номером, зазначеним у поле адреси. Вузли самі ідентифікують себе, тобто визначають, до якій із груп вони відносяться. Той самий вузол може входити в кілька груп. Члени якої-небудь групи multicast не обов'язково повинні належати однієї мережі. Щоб передати повідомлення від відправника, що знаходиться в одній мережі, одержувачеві, що знаходиться в іншій мережі, потрібно зробити деяку кількість *транзитних передач між* мережами, або *хопов* (від *hop* - стрибок), щораз вибираючи підходящий маршрут. У загальному випадку члени групи multicast можуть розподілятися по зовсім різних мережах, що знаходиться друг від друга на довільній кількості хопов. Групова адреса не поділяється на поля номера мережі і вузла й обробляється маршрутизатором особливим образом.

Маршрут. Послідовність маршрутизаторів, через які проходить пакет.
Маршрутизація. Вибір найкращого шляху проходження пакета.

Основне призначення multicast-адрес — поширення інформації зі схеми “один-ко-многим”. Хост, що хоче передавати ту саму інформацію багатьом абонентам, за допомогою спеціального протоколу IGMP (Internet Group Management Protocol) повідомляє про створення в мережі нової мультивещательной групи з визначеною адресою. Машрутизаторы, що підтримують мультивещательность, поширюють інформацію про створення нової групи в мережах, підключених до портів цього маршрутизатора. Хосты, що хочуть приєднатися до знову створюваного мультивещательной групі, сповіщають про це своїм локальним маршрутизаторам і ті передають цю інформацію хосту, ініціаторові створення нової групи.

Щоб маршрутизатори могли автоматично поширювати пакети з адресою multicast по складеній мережі, необхідно використовувати в кінцевих маршрутизаторах модифіковані протоколи обміну маршрутною інформацією, такі як, наприклад, MOSPF (Multicast OSPF, аналог OSPF).

Групова адресація призначена для економічного поширення в Internet або великої корпоративної мережі аудио- або відеопрограм, призначених відразу великий аудиторії слухачів або глядачів. Якщо такі засоби знайдуть широке застосування (зараз вони представляють в основному невеликі експериментальні острівці в загальному Internet), то Internet зможе створити серйозну конкуренцію радіо і телебаченню.

2.1.3.4. Використання масок у IP-адресації

Традиційна схема розподілу IP-адреси на номер мережі і номер вузла заснований на понятті класу, що визначається значеннями декількох перших біт адреси. Саме тому, що перший байт адреси 185.23.44.206 попадає в діапазон 128-191, ми можемо сказати, що ця адреса відноситься до класу B, а виходить, номером мережі є перші два байти, доповнені двома нульовими байтами — 185.23.0.0, а номером вузла — 0.0.44.206.

А що якщо використовувати яку-небудь іншу ознаку, за допомогою якого можна було б більш гнучко встановлювати границю між номером мережі і номером вузла? Як таку ознаку зараз одержали широке поширення маски. *Маска* — це число, що використовується в парі з IP-адресою; двоичная запис маски містить одиниці в тих розрядах, що повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі є цільною частиною адреси, одиниці в масці також повинні представляти безперервну послідовність.

Для стандартних класів мереж маски мають наступні значення:

- клас А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- клас У - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
- клас З - 11111111. 11111111. 11111111. 00000000 (255.255.255.0).

Постачаючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і зробити більш гнучкої систему адресації. Наприклад, якщо розглянутий вище адреса 185.23.44.206 асоціювати з маскою 255.255.255.0, те номером мережі буде 185.23.44.0, а не 185.23.0.0, як це визначено системою класів.

У масках кількість одиниць у послідовності, що визначає границю номера мережі,

не обов'язково повинне бути кратним 8, щоб повторювати розподіл адреси на байти. Нехай, наприклад, для IP-адреси 129.64.134.5 зазначено маску 255.255.128.0, тобто в двоичном виді:

- IP-адреса 129.64.134.5 - 10000001. 01000000. 10000110. 00000101
- Маска 255.255.128.0- 11111111.11111111.10000000.00000000

Якщо ігнорувати маску, то відповідно до системи класів адреса 129.64.134.5 відноситься до класу B, а виходить, номером мережі є перші 2 байти — 129.64.0.0, а номером вузла — 0.0.134.5.

Якщо ж використовувати для визначення границі номера мережі маску, то 17 послідовних одиниць у масці, "накладені" на IP-адресу, визначають як номер мережі в двоичном вираженні число:

10000001. 01000000. 10000000. 00000000 або в десятковій формі запису — номер мережі 129.64.128.0, а номер вузла 0.0.6.5.

Механізм масок широко розповсюджений у IP-маршрутизації, причому маски можуть використовуватися для самих різних цілей. З їхньою допомогою адміністратор може структурировать свою мережу, не вимагаючи від постачальника послуг додаткових номерів мереж. На основі цього ж механізму постачальники послуг можуть поєднувати адресні простори декількох мереж шляхом уведення так званих "префіксів" з метою зменшення обсягу таблиць маршрутизації і підвищення за рахунок цього продуктивності маршрутизаторів.

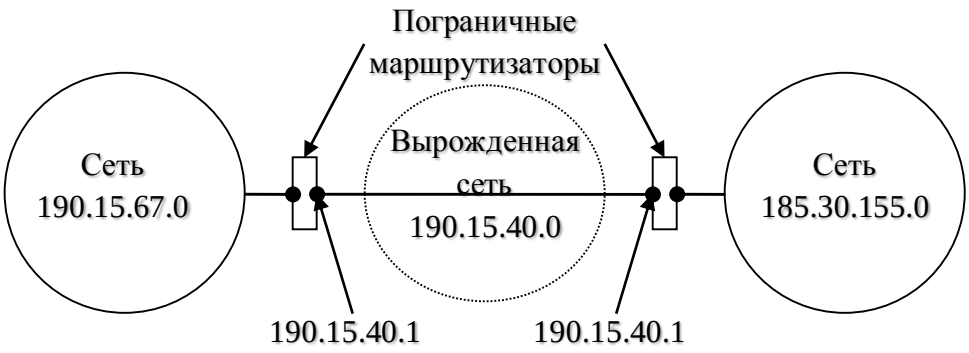
2.1.3.5. Порядок розподілення IP-адреса

Номера мереж призначаються або централізовано, якщо мережа є частиною Internet, або довільно, якщо мережа працює автономно. Номера вузлів і в тім і в іншому випадку адміністратор вільний призначати за своїм розсудом, не виходячи, зрозуміло, з дозволеного для цього класу мережі діапазону.

Координуючу роль у централізованому розподілі IP-адрес до деякого часу грала організація InterNIC, однак з ростом мережі задача розподілу адрес став занадто складної, і InterNIC делегувала частина своїх функцій іншим організаціям і великим постачальникам послуг Internet.

Уже порівняно давно спостерігається дефіцит IP-адрес. Дуже важко одержати адреса класу B и практично неможливо стати власником адреси класу A. При цьому треба відзначити, що дефіцит обумовлений не тільки ростом мереж, але і тим, що наявна безліч IP-адрес використовується нераціонально. Дуже часто власники мережі класу З витрачають лише невелику частину з наявних у них 254 адрес. Розглянемо приклад, коли дві мережі необхідно з'єднати глобальним зв'язком. У таких випадках як канал зв'язку використовують два маршрутизатори, з'єднаних за схемою "точка-крапка" (мал. 2.1.3). Для вырожденной мережі, утвореної каналом, що зв'язує порти двох суміжних маршрутизаторів, приходиться виділяти окремий номер мережі, хоча в цій мережі маються всего 2 вузли.

Якщо ж деяка IP-мережа створен для роботи в "автономному режимі", без зв'язку з Internet, тоді адміністратор цієї мережі вільний призначити їй довільно обраний номер. Але й у цій ситуації для того, щоб уникнути яких-небудь колізій, у стандартах Internet визначено кілька діапазонів адрес, що рекомендуються для локального використання. Ці адреси не обробляються маршрутизаторами Internet ні при яких умовах. Адреси, зарезервовані для локальних цілей, обрані з різних класів: у класі A — це мережа 10.0.0.0, у класі B — це діапазон з 16 номерів мереж 172.16.0.0-172.31.0.0, у класі З — це діапазон з 255 мереж - 192.168.0.0-192.168.255.0.



Малюнок 2.1.3 – Нераціональне використання простору IP-адрес

Для зм'якшення проблеми дефіциту адрес розроблювачі стека TCP/IP пропонують різні підходи. Принциповим рішенням є перехід на нову версію IPv6, у якій різко розширюється адресний простір за рахунок використання 16-байтных адрес. Однак і поточна версія IPv4 підтримує деякі технології, спрямовані на більш ощадливу витрату IP-адрес. Однієї з таких технологій є технологія масок і її розвиток — технологія *безкласової міждоменной маршрутизації (Classless Inter-Domain Routing, CIDR)*. Технологія CIDR відмовляється від традиційної концепції поділу адрес протоколу IP на класи, що дозволяє одержувати в користування стільки адрес, скільки реально необхідно. Завдяки CIDR постачальник послуг одержує можливість “нарізати” блоки з виділеного йому адресного простору в точній відповідності з вимогами кожного клієнта, при цьому в нього залишається простір для маневру на випадок його майбутнього росту.

Інша технологія, що може бути використана для зняття дефіциту адрес, це *трансляція адрес (Network Address Translator, NAT)*. Вузлам внутрішньої мережі адреси призначаються довільно (природно, відповідно до загальних правил, визначеними в стандарті), так, начебто ця мережа працює автономно. Внутрішня мережа з'єднується з Internet через деякий проміжний пристрій (маршрутизатор, межсетевой екран). Цей проміжний пристрій одержує у своє розпорядження деяка кількість зовнішніх “нормальних” IP-адрес, погоджених з постачальником послуг або іншою організацією, що розподіляє IP-адреси. Проміжний пристрій здатний перетворювати внутрішні адреси в зовнішні, використовуючи для цього якісь таблиці відповідності. Для зовнішніх користувачів усі численні вузли внутрішньої мережі виступають під декількома зовнішніми IP-адресами. При одержанні зовнішнього запиту цей пристрій аналізує його вміст і при необхідності пересилає його у внутрішню мережу, заміняючи IP-адресу на внутрішню адресу цього вузла. Процедура трансляції адрес визначена в RFC 1631.

2.1.3.6. Автоматизація процесу призначення IP-адреса

Призначення IP-адрес вузлам мережі навіть при не дуже великому розмірі мережі може представляти для адміністратора стомлюючу процедуру. Протокол *Dynamic Host Configuration Protocol (DHCP)* звільняє адміністратора від цих проблем, автоматизуючи процес призначення IP-адрес.

DHCP може підтримувати спосіб автоматичного динамічного розподілу адрес, а також більш прості способи ручного й автоматичного статичного призначення адрес. Протокол DHCP працює відповідно до моделі клієнт-сервер. Під час старту системи комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на одержання IP-адреси. DHCP-сервер відгукується і посилає повідомлення-відповідь, що містить IP-адресу. Передбачається, що DHCP-клієнт і DHCP-сервер знаходяться в одній IP-мережі.

При динамічному розподілі адрес DHCP-сервер видає адреса клієнтові на обмежений час, називаний *часом оренди (lease duration)*, що дає можливість згодом повторно використовувати цю IP-адресу для призначення іншому комп'ютерові. Основна перевага DHCP — автоматизація рутинної роботи адміністратора по конфігуруванню стека TCP/IP на кожнім комп'ютері. Іноді динамічний поділ адрес дозволяє будувати IP-мережу, кількість вузлів у якій перевищує кількість наявних у розпорядженні адміністратора IP-

адрес.

У ручній процедурі призначення статичних адрес активна участь приймає адміністратор, що надає DHCP-серверові інформацію про відповідність IP-адрес фізичним адресам або іншим ідентифікаторам клієнтів. DHCP-сервер, користуючись цією інформацією, завжди видає визначеному клієнтові призначений адміністратором адреса.

При автоматичному статичному способі DHCP-сервер привласнює IP-адреса з пула наявних IP-адрес без втручання оператора. Границі пула призначуваних адрес задає адміністратор при конфігурованні DHCP-сервера. Адреса дається клієнтові з пула в постійне користування, тобто з необмеженим терміном оренди. Між ідентифікатором клієнта і його IP-адресою як і раніше, як і при ручному призначенні, існує постійна відповідність. Воно встановлюється в момент першого призначення DHCP-сервером IP-адреси клієнтові. При всіх наступних запитах сервер повертає та ж сама IP-адреса.

DHCP забезпечує надійний і простий спосіб конфігурації мережі TCP/IP, гарантуючи відсутність дублювання адрес за рахунок централізованого керування їхнім розподілом. Адміністратор керує процесом призначення адрес за допомогою параметра “тривалість оренди”, що визначає, як довго комп'ютер може використовувати призначену IP-адресу, перед тим як знову запросити його від DHCP-сервера в оренду.

Прикладом роботи протоколу DHCP може служити ситуація, коли комп'ютер, що є DHCP-клієнтом, віддаляється з підмережі. При цьому призначений йому IP-адреса автоматично звільняється. Коли комп'ютер підключається до інший підмережі, те йому автоматично призначається нова адреса. Ні користувач, ні мережевий адміністратор не втручаються в цей процес. Це властивість дуже важлива для мобільних користувачів.

DHCP-сервер може призначити клієнтові не тільки IP-адреса клієнта, але й інші параметри стека TCP/IP, необхідні для його ефективної роботи, наприклад, маску, IP-адресу маршрутизатора за замовчуванням, IP-адреса сервера DNS, доменне ім'я комп'ютера і т.п.

2.1.3.7. Перетворення IP-адреса в локальні адреси

Однієї з головних задач, що ставилася при створенні протоколу IP, було забезпечення спільної погодженої роботи в мережі, що складається з подсетей, у загальному випадку різні мережні технології, що використовують. Безпосередньо з рішенням цієї задачі зв'язаний рівень межсетевых інтерфейсів стека TCP/IP. На цьому рівні визначаються вже розглянуті вище специфікації упакування (інкапсуляції) IP-пакетів у кадри локальних технологій. Крім цього, рівень межсетевых інтерфейсів повинний займатися також украй важливою задачею відображення IP-адрес у локальні адреси.

Для визначення локальної адреси по IP-адресі використовується *протокол дозволу адреси (Address Resolution Protocol, ARP)*. Протокол ARP працює різним образом у залежності від того, який протокол канального рівня працює в даній мережі — протокол локальної мережі (Ethernet, Token Ring, FDDI) з можливістю широкомовного доступу одночасно до усіх вузлів мережі або ж протокол глобальної мережі (X.25, frame relay), як правило не підтримуючий широкомовний доступ. Існує також протокол, що вирішує зворотну задачу — перебування IP-адреси по відомій локальній адресі. Він називається *реверсивним ARP (Reverse Address Resolution Protocol, RARP)* і використовується при старті бездискових станцій, що не знають у початковий момент своєї IP-адреси, але знаючу адресу свого мережевого адаптера.

Необхідність у звертанні до протоколу ARP виникає щораз, коли модуль IP передає пакет на рівень мережних інтерфейсів, наприклад драйверові Ethernet. IP-адреса вузла призначення відомий модулеві IP. Потрібно на його основі знайти Mac-адрес вузла призначення.

Робота протоколу ARP починається з перегляду так називаної ARP-таблиці (табл. 2.1.2). Кожен рядок таблиці установлює відповідність між IP-адресою і Mac-адресом. Для кожної мережі, підключеної до мережевого адаптера комп'ютера або до порту маршрутизатора, будується окрема ARP-таблиця.

Таблиця 2.1.2 - Приклад ARP-таблиці

IP-адреса	*MAC-адрес*	*Тип запису*
194.85.135.75	008048EB7E60	Динамічний
194.85.135.70	08005A21A722	Динамічний
194.85.60.21	008048EB7567	Статичний

Поле “Тип запису” може містити одне з двох значень — “Динамічний” або “Статичний”. Статичні записи створюються вручну за допомогою утиліти агр і не мають терміну старіння, точніше, вони існують доти, поки комп'ютер або маршрутизатор не будуть виключені. Динамічні ж записи створюються модулем протоколу ARP, що використовує широкомовні можливості локальних мережних технологій. Динамічні записи повинні періодично обновлятися. Якщо запис не обновлявся протягом визначеного часу (порядку декількох хвилин), то вона виключається з таблиці. Таким чином, у ARP-таблиці утримуються записи не про усі вузли мережі, а тільки про тих, котрі активно беруть участь у мережних операціях. Оскільки такий спосіб збереження інформації називають кэшированием, ARP-таблиці іноді називають ARP-кэш.

У глобальних мережах адміністраторові мережі найчастіше приходиться вручну формувати ARP-таблиці, у яких він задає, наприклад, відповідність IP-адреси адресі вузла мережі X.25, що має для протоколу IP зміст локальної адреси. Останнім часом намітилася тенденція автоматизації роботи протоколу ARP і в глобальних мережах. Для цієї мети серед усіх маршрутизаторів, підключених до якої-небудь глобальної мережі, виділяється спеціальний маршрутизатор, що веде ARP-таблицю для всіх інших вузлів і маршрутизаторів цієї мережі. При такому централізованому підході для усіх вузлів і маршрутизаторів вручну потрібно задати тільки IP-адресу і локальну адресу виділеного маршрутизатора. Потім кожен вузол і маршрутизатор реєструє свої адреси у виділеному маршрутизаторі, а при необхідності установлення відповідності між IP-адресою і локальною адресою вузол звертається до виділеного маршрутизатора з запитом і автоматично одержує відповідь без участі адміністратора. Працюючий у такий спосіб маршрутизатор називають ARP-сервером.

Отже, після того як модуль IP звернувся до модуля ARP із запитом на дозвіл адреси, відбувається пошук у ARP-таблиці зазначеного в запиті IP-адреси. Якщо така адреса в ARP-таблиці відсутній, то вихідний IP-пакет, для якого потрібно було визначити локальну адресу, ставиться в чергу. Далі протокол ARP формує свій запит (ARP-запит), вкладає його в кадр протоколу канального рівня і розсилає запит широкомовно.

Усі вузли локальної мережі одержують ARP-запит і порівнюють зазначений там IP-адреса з власним. У випадку їхнього збігу вузол формує ARP-відповідь, у якому указує своя IP-адреса і своя локальна адреса, а потім відправляє його вже спрямовано, тому що в ARP-запиті відправник указує свою локальну адресу. ARP-запити і відповіді використовують той самий формат пакета. У табл. 2.1.3 приведені значення полів приклада ARP-запиту для передачі по мережі Ethernet.

Таблиця 2.1.3 - Приклад ARP-запиту

Тип мережі	1 (0x1)
Тип протоколу	2048 (0x800)
Довжина локальної адреси	6 (Ox6)
Довжина мережевої адреси	4 (0x4)
Опція	1 (0x1)
Локальна адреса відправника	008048EB7E60
Мережева адреса відправника	194.85.135.75
Локальний (шуканий) адреса одержувача	000000000000
Мережева адреса одержувача	194.85.135.65

У поле “Тип мережі” для мереж Ethernet указується значення 1.

Поле “Тип протоколу” дозволяє використовувати протокол ARP не тільки для протоколу IP, але і для інших мережних протоколів. Для IP значення цього полючи

дорівнює $O8OO_{16}$.

Довжина локальної адреси для протоколу Ethernet дорівнює 6 байт, а довжина IP-адреси — 4 байт. У поле операції для ARP-запитів указується значення 1, якщо це запит, і 2, якщо це відповідь.

З цього запиту видно, що в мережі Ethernet вузол з IP-адресою 194.85.135.75 намагається визначити, який Mac-адрес має інший вузол тієї ж мережі, мережева адреса якого 194.85.135.65. Поле шуканої локальної адреси заповнено нулями.

Відповідь надсилає вузол, що пізнав свою IP-адресу. Якщо в мережі немає машини із шуканою IP-адресою, то ARP-відповіді не буде. Протокол IP знищує IP-пакети, що направляються по цій адресі. (Помітимо, що протоколи верхнього рівня не можуть відрізнити випадок ушкодження мережі Ethernet від випадку відсутності машини із шуканою IP-адресою.) У табл. 2.1.4 поміщені значення полів ARP-відповіді, що міг би надійти на приведений вище приклад ARP-запиту.

Таблиця 2.1.4 - Приклад ARP-відповіді

Тип мережі	1 (0x1)
Тип протоколу	2048 (0x800)
Довжина локальної адреси	6 (Ox6)
Довжина мережевої адреси	4 (0x4)
Опція	2 (0x2)
Локальна адреса відправника	00E0F77F1920
Мережева адреса відправника	194.85.135.65
Локальний (шуканий) адреса одержувача	008048EB7E60
Мережева адреса одержувача	194.85.135.75

Ця відповідь одержує машина, що зробила ARP-запит. Модуль ARP аналізує ARP-відповідь і додає запис у свою ARP-таблицю (табл. 2.1.5). У результаті обміну цими двома ARP-повідомленнями модуль IP-вузла 194.85.135.75 визначив, що IP-адресі 194.85.135.65 відповідає MAC-адрес 00E0F77F1920. Новий запис у ARP-таблиці з'являється автоматично, після декількох милісекунд після того, як вона потрібна була.

Таблиця 2.1.5 - Обновлена ARP-таблиця

IP-адреса	*MAC-адреса*	*Тип запису*
194.85.135.75	008048EB7E60	Динамічний
194.85.135.70	08005A21A722	Динамічний
194.85.60.21	008048EB7567	Статичний
194.85.135.65	00E0F77F1920	Динамічний

2.1.3.8. Перетворення доменних імен у IP-адреси

Організація доменів та доменних імен

Для ідентифікації комп'ютерів апаратне і програмне забезпечення в мережах TCP/IP покладається на IP-адреси, тому для доступу до мережевого ресурсу в параметрах програми цілком достатньо вказати IP-адреса, щоб програма правильно зрозуміла, д якому хосту неї потрібно звернутися. Наприклад, команда ftp://192.45.66.17 буде встановлювати сеанс зв'язку з потрібним ftp-сервером, а команда http://203.23.106.33 відкриє початкову сторінку на корпоративному Web-сервері. Однак користувачі звичайно воліють працювати із символьними іменами комп'ютерів, і операційні системи локальних мереж привчили них до цього зручного способу. Отже, у мережах TCP/IP повинні існувати символьні імена хостов і механізм для установлення відповідності між символьними іменами і IP-адресами.

В операційних системах, що спочатку розроблялися для роботи в локальних мережах, таких як Novell NetWare, Microsoft Windows або IBM OS/2, користувачі завжди працювали із символьними іменами комп'ютерів. Тому що локальні мережі складалися з невеликого числа комп'ютерів, то використовувалися так називані плоскі імена, що складаються з послідовності символів, не розділених на частині. Прикладами таких імен є: NW1_1, mail2, MOSCOW_SALES_2. Для установлення відповідності між символьними

іменами і Mac-адресами в цих операційних системах застосовувався механізм широкомовних запитів, подібний до механізму запитів протоколу ARP. Так, широкомовний спосіб дозволу імен реалізований у протоколі NetBIOS, на якому були побудовані багато локальні ОС. Так називані NetBIOS-імена сталі на довгі роки одним з основних типів плоских імен у локальних мережах.

Для стека TCP/IP, розрахованого в загальному випадку на роботу у великих територіально розподілених мережах, подібний підхід виявляється неефективним з кількох причин.

Плоскі імена не дають можливості розробити єдиний алгоритм забезпечення унікальності імен у межах великої мережі. У невеликих мережах унікальність імен комп'ютерів забезпечує адміністратор мережі, записуючи кілька десятків імен у журналі або файлі. При росту мережі задачу вирішують уже трохи адміністраторів, погоджуючи імена між собою неформальним способом. Однак якщо мережа розташована в різних містах або країнах, то адміністраторам кожної частини мережі потрібно придумати спосіб іменування, що дозволив би їм давати імена новим комп'ютерам незалежно від інших адміністраторів, забезпечуючи в той же час унікальність імен для всієї мережі. Самий надійний спосіб рішення цієї задачі — відмовлення від плоских імен у принципі.

Широкомовний спосіб установлення відповідності між символьними іменами і локальними адресами добре працює тільки в невеликій локальній мережі, не розділеної на підмережі. У великих мережах, де загальна широкомовність не підтримується, потрібний інший спосіб дозволу символьних імен. Звичайно гарною альтернативою широкомовності є застосування централізованої служби, що підтримує відповідність між різними типами адрес усіх комп'ютерів мережі. Компанія Microsoft для своєї корпоративної операційної системи Windows NT розробила централізовану службу WINS, що підтримує базу даних NetBIOS-імен і відповідних їм IP-адрес.

Для ефективної організації іменування комп'ютерів у великих мережах природним є застосування ієрархічних складених імен.

У стеці TCP/IP застосовується доменна система імен, що має ієрархічну деревоподібну структуру, що допускає використання в імені довільної кількості складових частин.

Ієрархія доменних імен аналогічна ієрархії імен файлів, прийнятої в багатьох популярних файлових системах. Дерево імен починається з кореня, що позначається тут крапкою “.”. Потім випливає старша символьна частина імені, друга по старшинству символьна частина імені і т.д. Молодша частина імені відповідає кінцевому вузлові мережі. На відміну від імен файлів, при записі яких спочатку вказується сама старша складова, що потім складає більш низького рівня і т.д., запис доменного імені починається із самої молодшої складової, а закінчується самої старшої. Складові частини доменного імені відокремлюється друг від друга крапкою. Наприклад, в імені partnering.microsoft.com складова partnering є ім'ям одного з комп'ютерів у домені microsoft.com.

Поділ імені на частині дозволяє розділити адміністративну відповідальність за призначення унікальних імен між різними людьми або організаціями в межах свого рівня ієрархії. Так, наприклад, одна людина може нести відповідальність за те, щоб усі імена, що мають закінчення “ru”, мали унікальну наступну вниз по ієрархії частина. Якщо ця людина справляється зі своїми обов'язками, то усі імена типу www.ru, mail.mmt.ru або m2.zil.mmt.ru будуть відрізнятися другий по старшинству частиною.

Поділ адміністративної відповідальності дозволяє вирішити проблему утворення унікальних імен без взаємних консультацій між організаціями, що відповідають за імена одного рівня ієрархії. Очевидно, що повинна існувати одна організація, що відповідає за призначення імен верхнього рівня ієрархії.

Сукупність імен, у яких кілька старших складових частин збігаються, утворять *домен* імен (*domain*). Наприклад, імена wwwl.zil.mmt.ru, ftp.zil.mmt.ru, yandex.ru і s1.mgu.ru входять у домен ru, тому що всі ці імена мають одну загальну старшу частину — ім'я ru.

Іншим прикладом являються імена s1.mgu.ru, s2.mgu.ru і rn.mgu.ru, що входять у домен mgu.ru. Цей домен утворять імена, у яких дві старші частини завжди рівні mgu.ru. Ім'я www.mmt.ru у домен mgu.ru не входить, тому що має відмінну складову mmt.

Якщо один домен входить в інший домен як його складова частина, то такий домен можуть називати *піддоменом (subdomain)*, хоча назва домен за ним також залишається. Звичайно піддомен називають по імені тієї його старшої складової, котра відрізняє його від інших піддоменів. Наприклад, піддомен mmt.ru звичайно називають піддоменом (або доменом) mmt. Ім'я піддомену призначає адміністратор вище розташованого домену. Гарною аналогією домену є каталог файлової системи.

Якщо в кожнім домені і піддомені забезпечується унікальність імен наступного рівня ієрархії, то і всій системі імен буде складатися з унікальних імен.

За аналогією з файловою системою, у доменній системі імен розрізняють короткі імена, відносні імена і повні доменні імена. Коротке ім'я — це ім'я кінцевого вузла мережі: хосту або порту маршрутизатора. Коротке ім'я — це лист дерева імен. Відносне ім'я — це складене ім'я, що починається з деякого рівня ієрархії, але не самого верхнього. Наприклад, www1.zil — це відносне ім'я. *Повне доменне ім'я (fully qualified domain name, FQDN)* включає складових усіх рівнів ієрархії, починаючи від короткого імені і кінчаючи кореневою крапкою: wwwl.zil.mmt.ru.

Необхідно підкреслити, що комп'ютери входять у домен у відповідності зі своїми складеними іменами, при цьому вони можуть мати зовсім різні IP-адреси, що належать до різних мереж і підмереж. Наприклад, у домен mgu.ru можуть входити хости з адресами 132.13.34.15, 201.22.100.33, 14.0.0.6. Доменна система імен реалізована в мережі Internet, але вона може працювати і як автономна система імен у великій корпоративній мережі, що використовує стік TCP/IP, але не зв'язаної з Internet.

У Internet кореневий домен керується центром InterNIC. Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Імена цих доменів повинні додержуватися міжнародного стандарту ISO 3166. Для позначення країн використовуються трибуквені і двобуквені абревіатури, а для різних типів організацій — наступні позначення:

- ***com*** — комерційні організації (наприклад, microsoft.com);
- ***edu*** — освітні (наприклад, mit.edu);
- ***gov*** — урядові організації (наприклад, nsf.gov);
- ***org*** — некомерційні організації (наприклад, fidonet.org);
- ***net*** — організації, що підтримують мережі (наприклад, nsf.net).

Кожен домен адмініструється окремою організацією, що звичайно розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Щоб одержати доменне ім'я, необхідно зареєструватися в якій-небудь організації, який InterNIC делегували свої повноваження з розподілу імен доменів.

Система доменних імен DNS

Відповідність між доменними іменами і IP-адресами може встановлюватися як засобами локального хосту, так і засобами централізованої служби. На ранньому етапі розвитку Internet на кожнім хості вручну створювався текстовий файл із відомим ім'ям hosts. Цей файл складався з деякої кількості рядків, кожна з яких містила одну пару “IP-адреса — доменне ім'я”, наприклад 102.54.94.97 — rhino.acme.com.

В міру росту Internet файли hosts також росли, і створення масштабовуваного рішення для дозволу імен стало необхідністю.

Таким рішенням стала спеціальна служба — *система доменних імен (Domain Name System, DNS)*. DNS — це централізована служба, заснована на розподіленій базі відображень “доменне ім'я — IP-адреса”. Служба DNS використовує у своїй роботі протокол типу “сервер^-сервер-клієнт-сервер”. У ньому визначені DNS-сервери і DNS-клієнти. DNS-сервери підтримують розподілену базу відображень, а DNS-клієнти

звертаються до серверів із запитами про дозвіл доменного імені в IP-адресу.

Служба DNS використовує текстові файли майже такого формату, як і файл hosts, і ці файли адміністратор також підготовляє вручну. Однак служба DNS спирається на ієрархію доменів, і кожен сервер служби DNS зберігає тільки частина імен мережі, а не усі імена, як це відбувається при використанні файлів hosts. При зростанні кількості вузлів у мережі проблема масштабування вирішується створенням нових доменів і піддоменів імен і додаванням у службу DNS нових серверів.

Для кожного домену імен створюється свій DNS-сервер. Цей сервер може зберігати відображення “доменне ім'я — IP-адреса” для усього домену, включаючи всі його піддомени. Однак при цьому рішення виявляється погано масштабовуваним, тому що при додаванні нових піддоменів навантаження на цей сервер може перевищити його можливості. Частіше сервер домену зберігає тільки імена, що закінчуються на наступному нижче розташованому рівні ієрархії в порівнянні з ім'ям домену. (Аналогічно каталогові файлової системи, що містить запису про файли і підкаталоги, безпосередньо в нього “вхідних”.) Саме при такій організації служби DNS навантаження з дозволу імен розподіляється більш-менш рівномірно між усіма DNS-серверами мережі. Наприклад, у першому випадку DNS-сервер домену mmt.ru буде зберігати відображення для всіх імен, що закінчуються на mmt.ru: www1.zil.mmt.ru, ftp.zil.mmt.ru, mail.mmt.ru і т.д. У другому випадку цей сервер зберігає відображення тільки імен типу mail.mmt.ru, www.mmt.ru, а всі інші відображення повинні зберігатися на DNS-сервері піддомену zil.

Кожен DNS-сервер крім таблиці відображень імен містить посилання на DNS-сервери своїх піддоменів. Ці посилання зв'язують окремі DNS-сервери в єдину службу DNS. Посилання являють собою IP-адреси відповідних серверів. Для обслуговування кореневого домену виділено трохи дублюючих один одного DNS-серверів, IP-адреси яких є широко відомими (їхній можна довідатися, наприклад, у InterNIC).

Процедура дозволу DNS-імені багато в чому аналогічна процедурі пошуку файловою системою адреси файлу по його символьному імені. Дійсно, в обох випадках складене ім'я відбиває ієрархічну структуру організації відповідних довідників — каталогів файлів або таблиць DNS. Тут домен і доменний DNS-сервер є аналогом каталогу файлової системи. Для доменних імен, так само як і для символьних імен файлів, характерна незалежність іменування від фізичного місця розташування.

Процедура пошуку адреси файлу по символьному імені полягає в послідовному перегляді каталогів, починаючи з кореневого. При цьому попередньо перевіряється кеш і поточний каталог. Для визначення IP-адреси по доменному імені також необхідно переглянути всі DNS-сервери, що обслуговують ланцюжок піддоменів, що входять в ім'я хосту, починаючи з кореневого домена. Істотною же відмінністю є те, що файлова система розташована на одному комп'ютері, а служба DNS по своїй природі є розподіленою.

Існують дві основні схеми дозволу DNS-імен. У першому варіанті роботу з пошуку IP-адреси координує DNS-клієнт:

1) DNS-клієнт звертається до кореневого DNS-сервера з указівкою повного доменного імені;
2) DNS-сервер відповідає, вказуючи адресу наступного DNS-сервера, що обслуговує домен верхнього рівня, задана в старшій частині запитаного імені;
3) DNS-клієнт робить запит наступного DNS-сервера, що відсилає його до DNS-сервера потрібного піддомену, і т.д., поки не буде знайдений DNS-сервер, у якому зберігається відповідність запитаного імені IP-адресі. Цей сервер дає остаточна відповідь клієнтові.

Така схема взаємодії називається нерекурсивною або ітеративної, коли клієнт сам ітеративно виконує послідовність запитів до різних серверів імен. Тому що ця схема завантажує клієнта досить складною роботою, то вона застосовується рідко.

В другому варіанті реалізується рекурсивна процедура:

1) DNS-клієнт запитує локальний DNS-сервер, тобто той сервер, що обслуговує

піддомен, до якого належить ім'я клієнта;

2) якщо локальний DNS-сервер знає відповідь, то він відразу ж повертає його клієнтові; це може відповідати випадкові, коли запитане ім'я входить у той же піддомен, що й ім'я клієнта, а також може відповідати випадкові, коли сервер уже дізнавався дану відповідність для іншого клієнта і зберіг його у своєму кеші;

3) якщо ж локальний сервер не знає відповідь, то він виконує ітеративні запити до кореневого сервера і т.д. точно так само, як це робив клієнт у першому варіанті; одержавши відповідь, вона передає його клієнтові, що усе це час простий чекав його від свого локального DNS-сервера.

У цій схемі клієнт передоручає роботу своєму серверові, тому схема називається непрямої або рекурсивної. Практично всі DNS-клієнти використовують рекурсивну процедуру.

Для прискорення пошуку IP-адрес DNS-сервери широко застосовують процедуру кешування минаючих через них відповідей. Щоб служба DNS могла оперативно відпрацьовувати зміни, що відбуваються в мережі, відповіді кешуються на визначений час — звичайно від декількох годин до декількох днів.

Резюме

- У стеці TCP/IP використовуються три типи адрес: локальні (називані також апаратними), IP-адреси і символьні доменні імена. Усі ці типи адрес привласнюються вузлам складеної мережі незалежно друг від друга.
- IP-адреса має довжину 4 байти і складається з номера мережі і номера вузла. Для визначення границі, що відокремлює номер мережі від номера вузла, реалізуються два підходи. Перший заснований на понятті класу адреси, другий — на використанні масок.
- Клас адреси визначається значеннями декількох перших біт адреси. В адресах класу А під номер мережі приділяється один байт, а інші три байти — під номер вузла, тому вони використовуються в найбільших мережах. Для невеликих мереж більше підходять адреси класу З, у які номер мережі займає три байти, а для нумерації вузлів може бути використаний тільки один байт. Проміжне положення займають адреси класу В.
- Інший спосіб визначення, яка частина адреси є номером мережі, а яка номером вузла, заснований на використанні маски. Маска — це число, що використовується в парі з IP-адресою; двійковий запис маски містить одиниці в тих розрядах, що у IP-адресі повинні інтерпретуватися як номер мережі.
- Номера мереж призначаються або централізовано, якщо мережа є частиною Internet, або довільно, якщо мережа працює автономно.
- Процес розподілу IP-адрес по вузлах мережі може бути автоматизований за допомогою протоколу DHCP.
- Установлення відповідності між IP-адресою й апаратною адресою (найчастіше Mac-адресом) здійснюється протоколом дозволу адрес ARP, що для цієї мети переглядає ARP-таблиці. Якщо потрібна адреса відсутній, то виконується широкомовний ARP-запит.
- У стеці TCP/IP застосовується доменна система символьних імен, що має ієрархічну деревоподібну структуру, що допускає використання в імені довільної кількості складових частин. Сукупність імен, у яких кілька старших складових частин збігаються, утворять домен імен. Доменні імена призначаються централізовано, якщо мережа є частиною Internet, у противному випадку —

локально.

- Відповідність між доменними іменами і IP-адресами може встановлюватися як засобами локального хосту з використанням файлу hosts, так і за допомогою централізованої служби DNS, заснованої на розподіленій базі відображень “доменне ім'я — IP-адреса”.

2.1.4. Протокол IP

Основу транспортних засобів стека протоколів TCP/IP складає протокол міжмережевої взаємодії - Internet Protocol (IP). До основних функцій протоколу IP відносяться:

- перенос між мережами різних типів адресної інформації в уніфікованій формі;
- зборка і розбирання пакетів при передачі їх між мережами з різним максимальним значенням довжини пакета.

2.1.4.1. Формат пакетові IP

Пакет IP складається з заголовка і полючи даних. Заголовок пакета має наступні поля:

- Поле ***Номер версії (Version)*** указує версію протоколу IP. Зараз повсюдно використовується версія 4 і готується перехід на версію 6, називану також IPv6.
- Поле ***Довжина заголовка (IHL)*** пакета IP займає 4 біти і вказує значення довжини заголовка, обмірюване в 32-бітових словах. Звичайно заголовок має довжину в 20 байт (п'ять 32-бітових слів), але при збільшенні обсягу службової інформації ця довжина може бути збільшена за рахунок використання додаткових байт у поле *Опції (IP Options)*.
- Поле ***Тип сервісу (Type of Service)*** займає 1 байт і задає пріоритетність пакета і вид критерію вибору маршруту. Перші три біти цього поля утворять підполе *пріоритету* пакета *(Precedence)*. Пріоритет може мати значення від 0 (нормальний пакет) до 7 (пакет керуючої інформації). Маршрутизатори і комп'ютери можуть брати до уваги пріоритет пакета й обробляти більш важливі пакети в першу чергу. Поле *Тип сервісу* містить також три біти, що визначають критерій вибору маршруту. Установлений біт D (delay) говорить про те, що маршрут повинний вибиратися для мінімізації затримки доставки даного пакета, біт T - для максимізації пропускної здатності, а біт R - для максимізації надійності доставки.
- Поле ***Загальна довжина (Total Length)*** займає 2 байти і вказує загальну довжину пакета з урахуванням заголовка і полючи даних.
- Поле ***Ідентифікатор пакета (Identification)*** займає 2 байти і використовується для розпізнавання пакетів, що утворилися шляхом фрагментації вихідного пакета. Усі фрагменти повинні мати однакове значення цього полючи.
- Поле ***Прапори (Flags)*** займає 3 біти, воно вказує на можливість фрагментації пакета (установлений біт Do not Fragment - DF - забороняє маршрутизаторові фрагментувати даний пакет), а також на те, чи є даний пакет проміжним або останнім фрагментом вихідного пакета (установлений біт More Fragments - MF - говорить про тім пакет переносить проміжний фрагмент).
- Поле ***Зсув фрагмента (Fragment Offset)*** займає 13 біт, він використовується для вказівки в байтах зсуву полючи даних цього пакета від початку загального поля даних вихідного пакета, підданого фрагментації. Використовується при зборці/розбиранню фрагментів пакетів при передачах їх між мережами з різними величинами максимальної довжини пакета.

- Поле ***Час життя (Time to Live)*** займає 1 байт і вказує граничний термін, протягом якого пакет може переміщатися по мережі. Час життя даного пакета виміряється в секундах і задається джерелом передачі засобами протоколу IP. На шлюзах і в інших вузлах мережі після закінчення кожної секунди з поточного часу життя віднімається одиниця; одиниця віднімається також при кожній транзитній передачі (навіть якщо не пройшла секунда). При витіканні часу життя пакет анулюється.
- Ідентифікатор ***Протоколу верхнього рівня (Protocol)*** займає 1 байт і вказує, якому протоколові верхнього рівня належить пакет (наприклад, це можуть бути протоколи TCP, UDP або RIP).
- ***Контрольна сума (Header Checksum)*** займає 2 байти, вона розраховується по всьому заголовку.
- Поля ***IP-адреса джерела (Source IP Address)*** і ***IP-адреса призначення (Destenation IP Address)*** мають однакову довжину - 32 біта, і однакову структуру.
- Поле ***Опції (IP Options)*** є необов'язковим і використовується звичайно тільки при налагодженні мережі. Це поле складається з декількох підполів, кожне з яких може бути одного з восьми визначених типів. У цих підполях можна вказувати точний маршрут проходження маршрутизаторів, реєструвати прохідні пакетом маршрутизатори, поміщати дані системи безпеки, а також тимчасові оцінки. Тому що число підполів може бути довільним, то наприкінці полючи Опції повинна бути додана трохи байт для вирівнювання заголовка пакета по 32-бітній границі.
- Поле ***Вирівнювання (Padding)*** використовується для того, щоб переконається в тім, що IP-заголовок закінчується на 32-бітній границі. Вирівнювання здійснюється нулями.

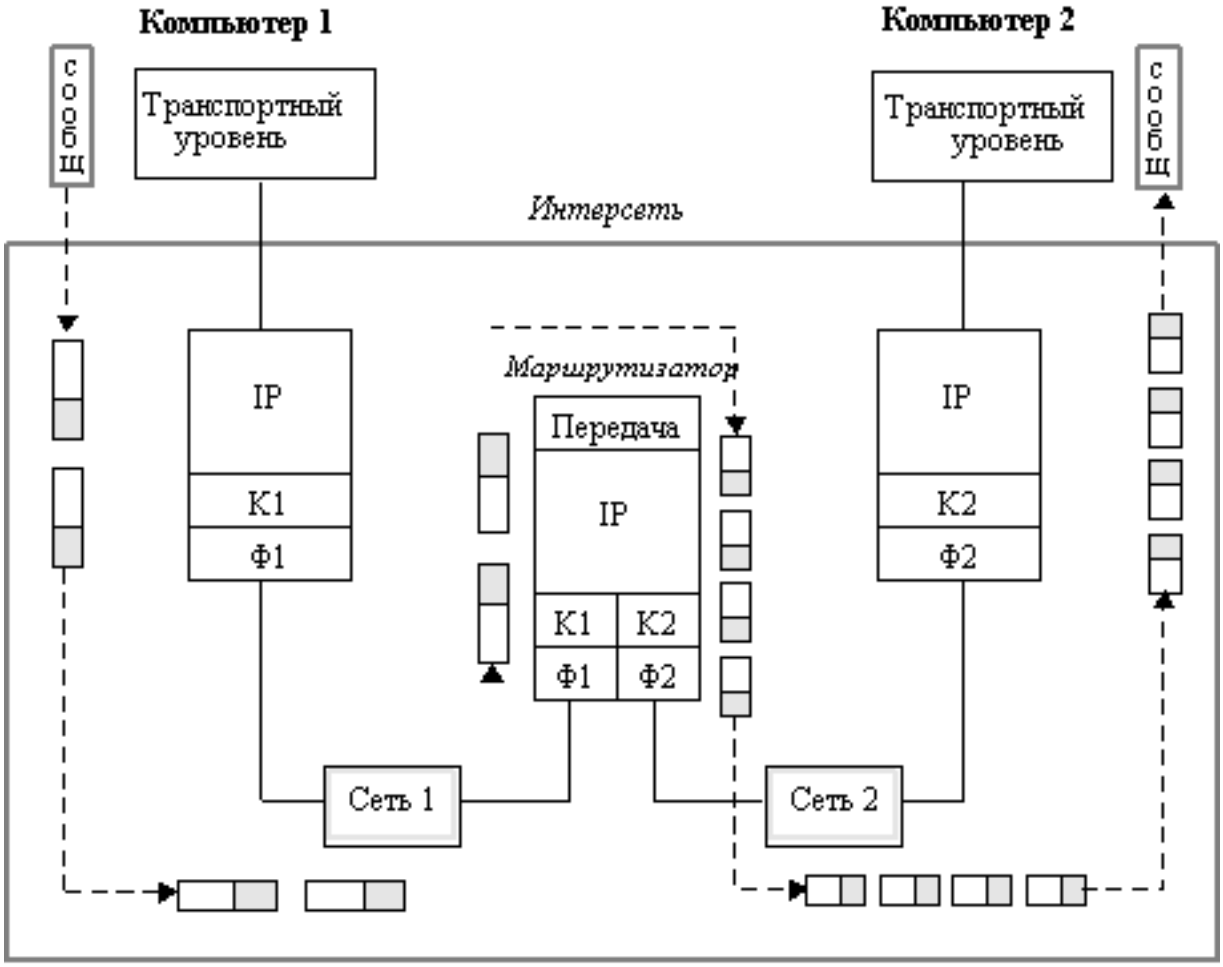
Максимальна довжина полючи даних пакета обмежена розрядністю полючи, що визначає цю величину, і складає 65535 байтів, однак при передачі по мережах різного типу довжина пакета вибирається з урахуванням максимальної довжини пакета протоколу нижнього рівня, що несе IP-пакети. Якщо це кадри Ethernet, то вибираються пакети з максимальною довжиною в 1500 байтів, що уміщаються в поле даних кадру Ethernet.

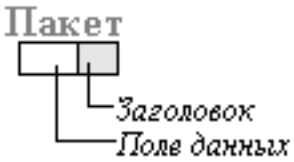
2.1.4.2. Керування фрагментацією

Протоколи транспортного рівня (протоколи TCP або UDP), що користуються мережним рівнем для відправлення пакетів, вважають, що максимальний розмір полючи даних IP-пакета дорівнює 65535, і тому можуть передати йому повідомлення такої довжини для транспортування через інтермережу. У функції рівня IP входить розбивка занадто довгого для конкретного типу складової мережі повідомлення на більш короткі пакети зі створенням відповідних службових полів, потрібних для наступної зборки фрагментів у вихідне повідомлення.

У більшості типів локальних і глобальних мереж визначається таке поняття як максимальний розмір полючи даних кадру або пакета, у які повинний інкапсулювати свій пакет протокол IP. Цю величину звичайно називають *максимальною одиницею транспортування - Maximum Transfer Unit, MTU*. Мережі Ethernet мають значення MTU, рівний 1500 байт, мережі FDDI - 4096 байт, а мережі X.25 найчастіше працюють з MTU у 128 байт.

Робота протоколу IP по фрагментації пакетів у хостах і маршрутизаторах ілюструється малюнком 2.1.4.





Малюнок 2.1.4 - Фрагментація IP-пакетів при передачі між мережами з різними максимальними розмірами пакетів. ДО1 і Ф1 канальний і фізичний рівень мережі 1, ДО2 і Ф2 канальний і фізичний рівень мережі 2

Нехай комп'ютер 1 зв'язаний з мережею, що має значення MTU у 4096 байтів, наприклад, з мережею FDDI. При надходженні на IP-рівень комп'ютера 1 повідомлення від транспортного рівня розміром у 5600 байтів, протокол IP поділяє його на два IP-пакети, встановлюючи в першому пакеті ознака фрагментації і привласнюючи пакетові унікальний ідентифікатор, наприклад, 486. У першому пакеті величина полючи зсуву дорівнює 0, а в другому - 2800. Ознака фрагментації в другому пакеті дорівнює нулеві, що показує, що це останній фрагмент пакета. Загальна величина IP-пакета складає 2800+20 (розмір заголовка IP), тобто 2820 байтів, що уміщається в поле даних кадру FDDI.

Далі комп'ютер 1 передає ці пакети на канальний рівень ДО1, а потім і на фізичний рівень Ф1, що відправляє їх маршрутизаторові, зв'язаному з даною мережею.

Маршрутизатор бачить по мережній адресі, що прибулі два пакети потрібно передати в мережу 2, що має менше значення MTU, рівне 1500. Імовірно, це мережа Ethernet. Маршрутизатор витягає фрагмент транспортного повідомлення з кожного пакета FDDI і поділяє його ще навпіл, щоб кожна частина умістилася в поле даних кадру Ethernet. Потім він формує нові пакети IP, кожний з яких має довжину 1400 + 20 = 1420 байтів, що менше 1500 байтів, тому вони нормально містяться в поле даних кадрів Ethernet.

У результаті в комп'ютер 2 по мережі Ethernet приходить чотири IP-пакети з загальним ідентифікатором 486, що дозволяє протоколові IP, що працює в комп'ютері 2, правильно зібрати вихідне повідомлення. Якщо пакети прийшли не в тім порядку, у якому були послані, то зсув укаже правильний порядок їхнього об'єднання.

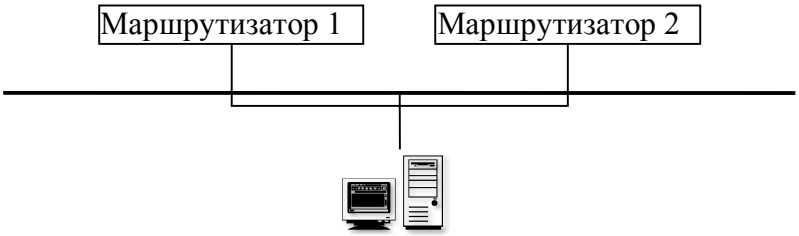
Відзначимо, що IP-маршрутизатори не збирають фрагменти пакетів у більш великі пакети, навіть якщо на шляху зустрічається мережа, що допускає таке укрупнення. Це зв'язано з тим, що окремі фрагменти повідомлення можуть переміщатися по інтермережі по різних маршрутах, тому немає гарантії, що усі фрагменти проходять через який-небудь проміжний маршрутизатор на їхньому шляху.

При приході першого фрагмента пакета вузол призначення запускає таймер, що визначає максимально припустимий час чекання приходу інших фрагментів цього пакета. Якщо таймер минає раніш прибуття останнього фрагмента, то всі отримані до цього моменту фрагменти пакета відкидаються, а у вузол, що послав вихідний пакет, направляється повідомлення про помилку за допомогою протоколу ICMP.

2.1.4.3. Маршрутизація з допомогою IP-адреса

Розглянемо тепер принципи, на підставі яких у мережах IP відбувається вибір маршруту передачі пакета між мережами.

Спочатку необхідно звернути увагу на той факт, що не тільки маршрутизатори, але і кінцеві вузли - комп'ютери - повинні брати участь у виборі маршруту. Приклад, приведений на малюнку 2.1.5, демонструє цю необхідність. Тут у локальній мережі мається кілька маршрутизаторів, і комп'ютер повинний вибирати, якому з них варто відправити пакет.



Малюнок 2.1.5 - Вибір маршрутизатора кінцевим вузлом

Довжина маршруту може істотно змінитися в залежності від того, який маршрутизатор вибере комп'ютер для передачі свого пакета на сервер, розташований, наприклад, у Німеччині, якщо маршрутизатор 1 з'єднаний виділеною лінією з маршрутизатором у Копенгагені, а маршрутизатор 2 має супутниковий канал, що з'єднує його з Токіо.

У стеці TCP/IP маршрутизатори і кінцеві вузли приймають рішення про те, кому передавати пакет для його успішної доставки вузлові призначення, на підставі так званих *таблиць маршрутизації (routing tables)*.

Наступна таблиця являє собою типовий приклад таблиці маршрутів, що використовує IP-адреси мереж.

Таблиця 2.1.6 - Таблиця маршрутів, що використовує IP-адреси мереж

Адреса мережі призначення	*Адреса наступного маршрутизатора*	*Номер порту мережі призначення*	*Відстань до мережі призначення*
56.0.0.0	198.21.17.7	1	20
56.0.0.0	213.34.12.4	2	130
116.0.0.0	213.34.12.4	2	1450
129.13.0.0	198.21.17.6	1	50
198.21.17.0	-	2	0
213.34.12.0	-	1	0
default	198.21.17.7	1	-

У цій таблиці в стовпці “Адреса мережі призначення” вказуються адреси всіх мереж, яким даний маршрутизатор може передавати пакети. У стеці TCP/IP прийнятий так називаний *однокроковий підхід* до оптимізації маршруту просування пакета *(next-hop routing)* - кожен маршрутизатор і кінцевий вузол бере участь у виборі тільки одного кроку передачі пакета. Тому в кожнім рядку таблиці маршрутизації вказується не весь маршрут у виді послідовності IP-адрес маршрутизаторів, через які повинний пройти пакет, а тільки одна IP-адреса - адреса наступного маршрутизатора, якому потрібно передати пакет. Разом з пакетом наступному маршрутизаторові передається відповідальність за вибір наступного кроку маршрутизації. Однокроковий підхід до маршрутизації означає розподілене рішення задачі вибору маршруту. Це знімає обмеження на максимальну кількість транзитних маршрутизаторів на шляху пакета.

Альтернативою однокроковому підходові є вказівка в пакеті всієї послідовності маршрутизаторів, що пакет повинний пройти на своєму шляху. Такий підхід називається *маршрутизацією від джерела - Source Routing*. У цьому випадку вибір маршруту виробляється кінцевим вузлом або першим маршрутизатором на шляху пакета, а всі інші маршрутизатори тільки відпрацьовують обраний маршрут, здійснюючи комутацію пакетів, тобто передачу їх з одного порту на іншій. Алгоритм Source Routing застосовується в мережах IP тільки для налагодження, коли маршрут задається в поле *Опції (IP Options)* пакета.

У випадку, якщо в таблиці маршрутів мається більш одного рядка, що відповідає тому самому адресі мережі призначення, то при ухваленні рішення про передачу пакета використовується той рядок, у якій зазначене найменше значення в поле “Відстань до мережі призначення”.

При цьому під відстанню розуміється будь-яка метрика, використовувана відповідно до заданого в мережному пакеті класом сервісу. Це може бути кількість транзитних маршрутизаторів у даному маршруті (кількість хопів від hop - стрибок), час проходження пакета по лініях зв'язку, надійність ліній зв'язку, або інша величина, що відбиває якість даного маршруту стосовно конкретного класу сервісу. Якщо маршрутизатор підтримує кілька класів сервісу пакетів, то таблиця маршрутів складається і застосовується окремо для кожного виду сервісу (критерію вибору маршруту).

Для відправлення пакета наступному маршрутизаторові потрібне знання його локальної адреси, але в стеці TCP/IP у таблицях маршрутизації прийняте використання тільки IP-адрес для збереження їхнього універсального формату, що не залежить від типу мереж, що входять в інтермережу. Для перебування локальної адреси по відомій IP-адресі необхідно скористатися протоколом ARP.

Кінцевий вузол, як і маршрутизатор, має у своєму розпорядженні таблицю маршрутів уніфікованого формату і на підставі її даних приймає рішення, якому маршрутизаторові потрібно передавати пакет для мережі N. Рішення про те, що цей пакет потрібно взагалі маршрутизовати, комп'ютер приймає в тому випадку, коли він бачить, що адреса мережі призначення пакета відрізняється від адреси його власної мережі (кожному комп'ютерові при конфігуруванні адміністратор привласнює його IP-адресу або кілька IP-адрес, якщо комп'ютер одночасно підключений до декількох мереж). Коли комп'ютер вибрав наступний маршрутизатор, то він переглядають кеш-таблицю адрес свого протоколу ARP і, може бути, знаходить там відповідність IP-адреси наступного маршрутизатора його MAC-адресі. Якщо ж ні, то по локальній мережі передається широкомовний ARP-запит і локальна адреса витягається з ARP-відповіді.

Після цього комп'ютер формує кадр протоколу, використовуваного на обраному порту, наприклад, кадр Ethernet, у який поміщає MAC-адрес маршрутизатора. Маршрутизатор приймає кадр Ethernet, витягає з нього пакет IP і переглядає свою таблицю маршрутизації для перебування наступного маршрутизатора. При цьому він виконує ті ж дії, що і кінцевий вузол.

Однокрокова маршрутизація володіє ще одною перевагою - вона дозволяє скоротити обсяг таблиць маршрутизації в кінцевих вузлах і маршрутизаторах за рахунок використання як номер мережі призначення так називаного *маршруту за замовчуванням - default*, що звичайно займає в таблиці маршрутизації останній рядок. Якщо в таблиці маршрутизації є такий запис, то всі пакети з номерами мереж, що відсутні в таблиці маршрутизації, передаються маршрутизаторові, зазначеному в рядку *default*. Тому маршрутизатори часто зберігають у своїх таблицях обмежену інформацію про мережі інтермережі, пересилаючи пакети для інших мереж у порт і маршрутизатор, використовувані за замовчуванням. Мається на увазі, що маршрутизатор, використовуваний за замовчуванням, передасть пакет на магістральну мережу, а маршрутизатори, підключені до магістралі, мають повну інформацію про склад інтермережі.

Особливо часто прийомом маршрутизації за замовчуванням користуються кінцеві вузли. Хоча вони також у загальному випадку мають у своєму розпорядженні таблицю маршрутизації, її обсяг звичайно незначний, тому що маршрутизація для комп'ютера - не основне заняття. Головна роль у маршрутизації пакетів у концепції протоколу IP приділяється, природно, маршрутизаторам, що повинні володіти набагато більш повними таблицями маршрутизації, чим кінцеві вузли. Кінцевий вузол часто взагалі працює без таблиці маршрутизації, маючи тільки зведення про IP-адресу маршрутизатора за замовчуванням. При наявності одного маршрутизатора в локальній мережі цей варіант - єдино можливий для всіх кінцевих вузлів. Але навіть при наявності декількох маршрутизаторів у локальній мережі, коли проблема їхнього вибору коштує перед кінцевим вузлом, завдання маршруту за замовчуванням часто використовується в комп'ютерах для скорочення обсягу їхньої маршрутної таблиці.

Іншим способом розвантаження комп'ютера від необхідності ведення великих таблиць маршрутизації є одержання від маршрутизатора зведень про раціональний маршрут для якої-небудь конкретної мережі за допомогою протоколу ICMP.

Крім маршруту default, у таблиці маршрутизації можуть зустрітися два типи спеціальних записів - запис про специфічний для вузла маршруті і запис про адреси мереж, безпосередньо підключених до портів маршрутизатора.

Специфічний для вузла маршрут містить замість номера мережі повна IP-адреса, тобто адреса, що має ненульову інформацію не тільки в поле номера мережі, але й у поле номера вузла. Передбачається, що для такого кінцевого вузла маршрут повинний вибиратися не так, як для всіх інших вузлів мережі, до якої він відноситься. У випадку, коли в таблиці є різні записи про просування пакетів для всієї мережі N і її окремого вузла, що має адресу N_m, при надходженні пакета, адресованого вузлові N_m, маршрутизатор віддасть перевагу запису для N_m.

Запису в таблиці маршрутизації, що відносяться до мереж, безпосередньо підключеним до маршрутизатора, у поле “Відстань до мережі призначення” містять нулі.

Ще одною відмінністю роботи маршрутизатора і кінцевого вузла при виборі маршруту є спосіб побудови таблиці маршрутизації. Якщо маршрутизатори звичайно автоматично створюють таблиці маршрутизації, обмінюючи службовою інформацією, то для кінцевих вузлів таблиці маршрутизації створюються, як правило, вручну адміністраторами, і зберігаються у виді постійних файлів на дисках.

Існують різні алгоритми побудови таблиць для однокрокової маршрутизації. Їх можна розділити на три класи:

- алгоритми фіксованої маршрутизації;
- алгоритми простої маршрутизації;
- алгоритми адаптивної маршрутизації.

Незалежно від алгоритму, використовуваного для побудови таблиці маршрутизації, результат їхньої роботи має єдиний формат. За рахунок цього в одній і тій же мережі різні вузли можуть будувати таблиці маршрутизації по своїх алгоритмах, а потім обмінюватися між собою відсутніми даними, тому що формати цих таблиць фіксовані. Тому

маршрутизатор, що працює по алгоритму адаптивної маршрутизації, може постачити кінцевий вузол, що застосовує алгоритм фіксованої маршрутизації, зведеннями про шляху до мережі, про яку кінцевий вузол нічого не знає.

Фіксована маршрутизація

Цей алгоритм застосовується в мережах із простою топологією зв'язків і заснований на ручному складанні таблиці маршрутизації адміністратором мережі. Алгоритм часто ефективно працює також для магістралей великих мереж, тому що сама магістраль може мати просту структуру з очевидними найкращими шляхами проходження пакетів у підмережі, приєднані до магістралі.

Розрізняють *одномаршрутні таблиці*, у яких для кожного адресата заданий один шлях, і *багатомаршрутні таблиці*, що визначають кілька альтернативних шляхів для кожного адресата. При використанні багатомаршрутних таблиць повинне бути задане правило вибору одного з них. Найчастіше один шлях є основним, а інші - резервними.

Проста маршрутизація

Алгоритми простої маршрутизації підрозділяються на три підкласи:

- ***Випадкова маршрутизація*** - пакети передаються в будь-якому, випадковому напрямку, крім вихідного.
- ***Лавинна маршрутизація*** - пакети передаються у всіх напрямках, крім вихідного (застосовується в мостах для пакетів з невідомою адресою доставки).
- ***Маршрутизація по попередньому досвіді*** - таблиці маршрутів складаються на підставі даних, що утримуються в минаючим через маршрутизатор пакетах. Саме так працюють прозорі мости, збираючи зведення про адреси вузлів, що входять у сегменти мережі. Такий спосіб маршрутизації володіє повільної адаптованістю до змін топології мережі.

Адаптивна маршрутизація

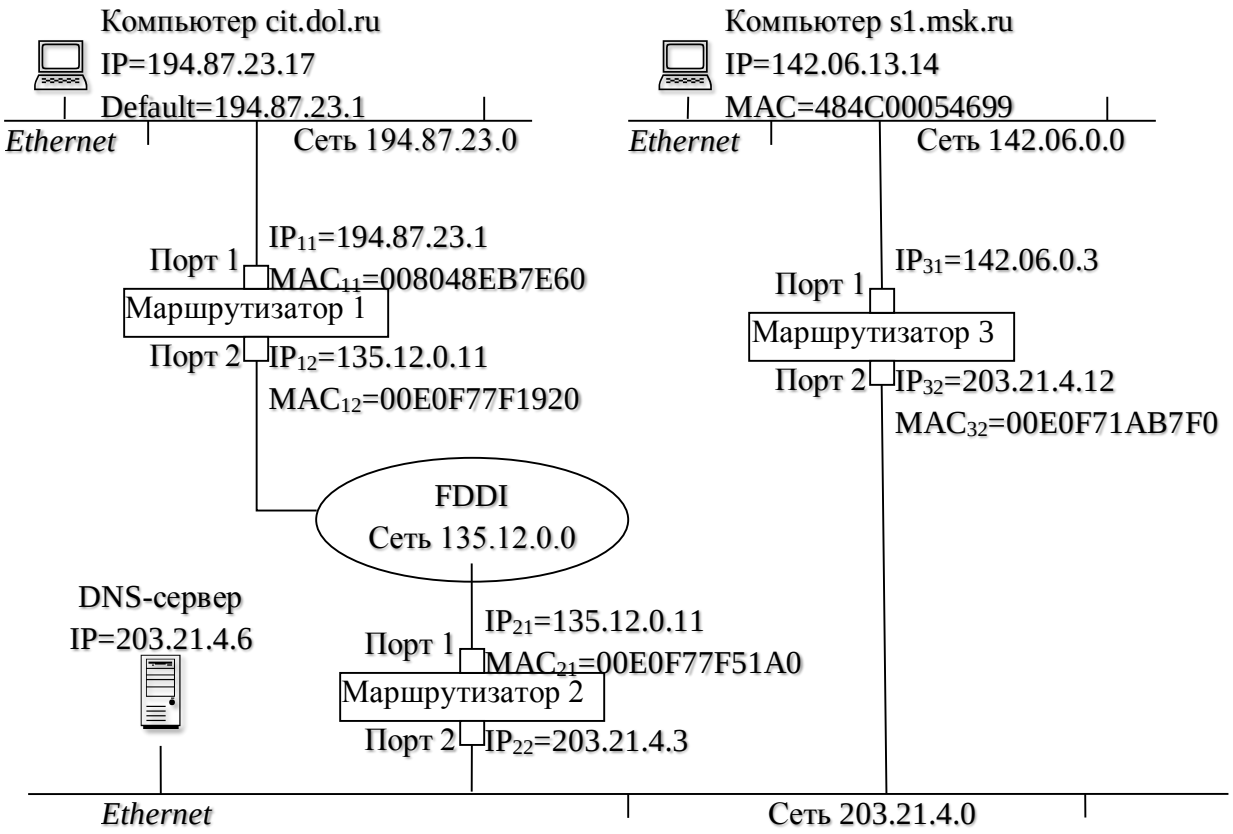
Це основний вид алгоритмів маршрутизації, що застосовуються маршрутизаторами в сучасних мережах зі складною топологією. Адаптивна маршрутизація заснована на тім, що маршрутизатори періодично обмінюються спеціальною топологічною інформацією про наявним в інтермережі мережах, а також про зв'язки між маршрутизаторами. Звичайно враховується не тільки топологія зв'язків, але і їхня пропускна здатність і стан.

Адаптивні протоколи дозволяють усім маршрутизаторам збирати інформацію про топологію зв'язків у мережі, оперативно відпрацьовуючи всі зміни конфігурації зв'язків. Ці протоколи мають розподілений характер, що виражається в тім, що в мережі відсутні які-небудь виділені маршрутизатори, які б збирали й узагальнювали топологічну інформацію: ця робота розподілена між усіма маршрутизаторами.

2.1.4.4. Приклад взаємодії вузлів з використанням протоколові IP

Розглянемо на прикладі інтермережі, приведеної на малюнку 2.1.6, яким образом відбувається взаємодія комп'ютерів через маршрутизатори і доставка пакетів комп'ютерові призначення.

Нехай у приведеному прикладі користувач комп'ютера cit.dol.ru, що знаходиться в мережі Ethernet з IP-адресою 194.87.23.0 (адреса класу 3), хоче взаємодіяти по протоколі FTP з комп'ютером s1.msk.ru, що належить мережі Ethernet з IP-адресою 142.06.0.0 (адреса класу B). Комп'ютер cit.dol.ru має IP-адреса 194.87.23.17, а комп'ютер s1.msk.ru - IP-адреса 142.06.13.14.



Малюнок 2.1.6 - Приклад взаємодії комп'ютерів через інтермережу

1) Користувач комп'ютера cit.dol.ru знає символьне ім'я комп'ютера s1.msk.ru, але не знає його IP-адреси, тому для організації ftp-сеансу він набирає команду
   > ftp s1.msk.ru
   У комп'ютері cit.dol.ru повинні бути задані деякі параметри для стека TCP/IP, щоб він міг виконати поставлену перед ним задачу.
   У число цих параметрів повинні входити власна IP-адреса, IP-адреса DNS-сервера і IP-адреса маршрутизатора за замовчуванням. Тому що до мережі Ethernet, до якої відноситься комп'ютер cit.dol.ru, підключений тільки один маршрутизатор, то таблиця маршрутизації кінцевим вузлам цієї мережі не потрібна, досить знати IP-адресу маршрутизатора за замовчуванням. У даному прикладі він дорівнює 194.87.23.1.
   Тому що користувач у команді ftp не задав IP-адресу вузла, з яким він хоче взаємодіяти, те стік TCP/IP повинний визначити його самостійно. Він може зробити запит до сервера DNS по наявний у нього IP-адресі, але звичайно кожен комп'ютер спочатку переглядає свою власну таблицю відповідності символьних імен і IP-адрес. Така таблиця зберігається найчастіше у виді текстового файлу простої структури - кожен його рядок містить запис про одне символьне ім'я і його IP-адресу. В ОС Unix такий файл традиційно має ім'я hosts.
2) Будемо вважати, що комп'ютер cit.dol.ru має файл HOSTS, а в ньому є рядок
   142.06.13.14 s1.msk.ru
   Тому дозвіл імені виконується локально, так що протокол IP може тепер формувати IP-пакети з адресою призначення 142.06.13.14 для взаємодії з комп'ютером s1.msk.ru.
3) Протокол IP комп'ютера cit.dol.ru перевіряє, чи потрібно маршрутизовати пакети для адреси 142.06.13.14. Тому що адреса мережі призначення дорівнює 142.06.0.0, а адреса мережі, до якого належить комп'ютер, дорівнює 194.87.23.0, то маршрутизація необхідна.

4) Комп'ютер cit.dol.ru починає формувати кадр Ethernet для відправлення IP-пакета маршрутизаторові за замовчуванням з IP-адресою 194.87.23.1. Для цього йому потрібний MAC-адрес порту маршрутизатора, підключеного до його мережі. Ця адреса швидше за усе вже знаходиться в кеш-таблиці протоколу ARP комп'ютера, якщо він хоча б раз за останнє включення обмінювався даними з комп'ютерами інших мереж. Нехай ця адреса в нашому прикладі був знайдений саме в кеш-пам'яті. Позначимо його MAC_{11}, відповідно до номера маршрутизатора і його порту.
5) У результаті комп'ютер cit.dol.ru відправляє по локальній мережі кадр Ethernet, що має наступні поля:

MAC_{11}=008048EB7E60		**142.06.13.14** IP-адреса призначення	
Заголовок кадру Ethernet		Заголовок пакета IP	Поле даних пакета IP

6) Кадр приймається портом 1 маршрутизатора 1 відповідно до протоколу Ethernet, тому що MAC-вузол цього порту розпізнає своя адреса MAC_{11}. Протокол Ethernet витягає з цього кадру IP-пакет і передає його програмному забезпеченню маршрутизатора, що реалізує протокол IP. Протокол IP витягає з пакета адреса призначення і переглядає запису своєї таблиці маршрутизації. Нехай маршрутизатор 1 має у своїй таблиці маршрутизації запис
142.06.0.0 135.12.0.11 2,
яка говорить про те, що пакети для мережі 142.06.0.0 потрібно передавати маршрутизаторові 135.12.0.11, підключеному до тієї ж мережі, що і порт 2 маршрутизатори 1.
7) Маршрутизатор 1 переглядає параметри порту 2 і знаходить, що він підключений до мережі FDDI. Тому що мережа FDDI має значення максимального блоку, що транспортується, MTU більше, ніж мережа Ethernet, те фрагментація полючи даних IP-пакета не потрібно. Тому маршрутизатор 1 формує кадр формату FDDI, у якому вказує MAC-адреса порту маршрутизатора 2, що він знаходить у своїй кеш-таблиці протоколу ARP:

MAC_{21}=00E0F77F51A0		**142.06.13.14** IP-адреса призначення	
Заголовок кадру FDDI		Заголовок пакета IP	Поле даних пакета IP

8) Аналогічно діє маршрутизатор 2, формуючи кадр Ethernet для передачі пакета маршрутизаторові 3 по мережі Ethernet с IP-адресою 203.21.4.12:

MAC_{32}=00E0F71AB7F0		**142.06.13.14** IP-адреса призначення	
Заголовок кадру Ethernet		Заголовок пакета IP	Поле даних пакета IP

9) Нарешті, після того, як пакет надійшов у маршрутизатор мережі призначення - маршрутизатор 3, з'являється можливість передачі цього пакета комп'ютерові призначення. Маршрутизатор 3 бачить, що пакет потрібно передати в мережу 142.06.0.0, що безпосередньо підключена до його першого порту. Тому він посилає ARP-запит по мережі Ethernet с IP-адресою комп'ютера s1.msk.ru (вважаємо, що цієї інформації в його кеші немає), одержує відповідь, що містить адресу MAC кінцевого вузла, і формує кадр Ethernet, що доставляє IP-пакет по локальній мережі адресатові.

MAC-адреса кінцевого вузла 484C00054699		**142.06.13.14** IP-адреса призначення	Сегмент TCP
Заголовок кадру Ethernet		Заголовок пакета IP	Поле даних пакета IP

2.1.4.5. Структуризація мереж IP з допомогою масок

Часто адміністратори мереж випробують незручності, через те, що кількість централізована виділених їм номерів мереж недостатньо для того, щоб структурувати мережу належним чином, наприклад, розмістити всі слабко взаємодіючі комп'ютери по різних мережах.

У такій ситуації можливі два шляхи. Перший з них зв'язаний з одержанням від InterNIC додаткових номерів мереж. Другий спосіб, що вживається більш часто, зв'язаний з використанням так званих *масок*, що дозволяють розділяти одну мережу на кілька мереж.

Маска - це число, двійковий запис якого містить одиниці в тих розрядах, що повинні інтерпретуватися як номер мережі.

Наприклад, для стандартних класів мереж маски мають наступні значення:

- 255.0.0.0 - маска для мережі класу А;
- 255.255.0.0 - маска для мережі класу В;
- 255.255.255.0 - маска для мережі класу С.

У масках, що використовує адміністратор для збільшення числа мереж, кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково повинне бути кратним 8, щоб повторювати розподіл адреси на байти.

Нехай, наприклад, маска має значення 255.255.192.0 (11111111 11111111 11000000 00000000). І нехай мережа має номер 129.44.0.0 (10000001 00101100 00000000 00000000), з якого видно, що вона відноситься до класу В. Після накладення маски на цю адресу число розрядів, що інтерпритуються як номер мережі, збільшилося з 16 до 18, тобто адміністратор одержав можливість використовувати замість одного, централізовано заданого йому номера мережі, чотири:

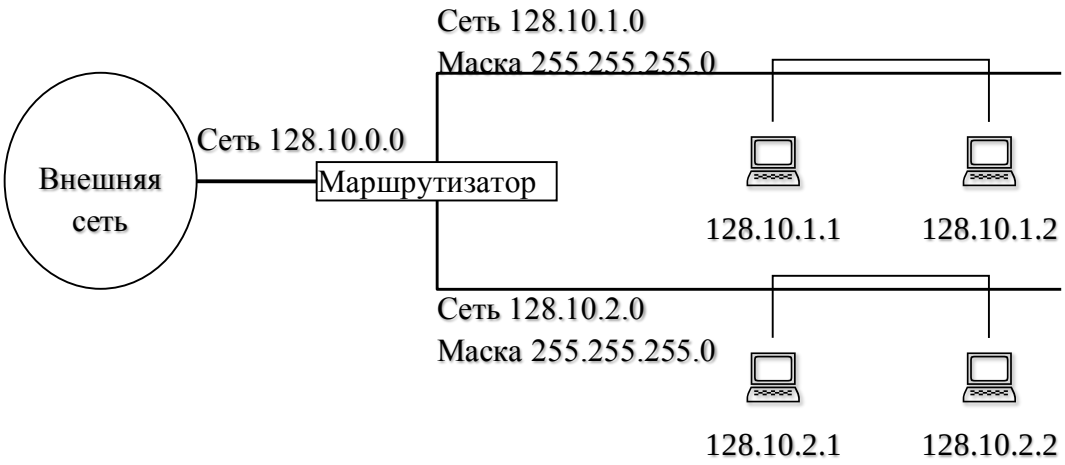
129.44.0.0	(10000001	00101100	00000000	00000000)
129.44.64.0	(10000001	00101100	01000000	00000000)
129.44.128.0	(10000001	00101100	10000000	00000000)
129.44.192.0	(10000001	00101100	11000000	00000000)

Наприклад, IP-адреса 129.44.141.15 (10000001 00101100 10001101 00001111), що по стандартах IP задає номер мережі 129.44.0.0 і номер вузла 0.0.141.15, тепер, при використанні маски, буде інтерпретуватися як пари:

- 129.44.128.0 - номер мережі,
- 0.0.13.15 - номер вузла.

Таким чином, установивши нове значення маски, можна змусити маршрутизатор по-іншому інтерпретувати IP-адреса. При цьому два додаткових останніх біти номера мережі часто інтерпретуються як номери підмереж.

Ще один приклад. Нехай деяка мережа відноситься до класу В и має адресу 128.10.0.0 (малюнок 2.1.7). Ця адреса використовується маршрутизатором, що з'єднує мережа з іншою частиною інтермережі. І нехай серед усіх станцій мережі є станції, слабко взаємодіючі між собою. Їх бажано було б ізолювати в різних мережах. Для цього мережа можна розділити на двох мереж, підключивши них до відповідних портів маршрутизатора, і задати для цих портів як маску, наприклад, число 255.255.255.0, тобто організувати усередині вихідної мережі з централізовано заданим номером дві підмережі класу С (можна було б вибрати й інший розмір для поля адреси підмережі). Ззовні мережа як і раніше буде виглядати, як єдина мережа класу В, а на місцевому рівні це будуть дві окремі мережі класу С. Прихожий загальний трафік буде розділятися місцевим маршрутизатором між підмережами.



Малюнок 2.1.7 - Приклад використання масок для структурування мережі

Необхідно помітити, що, якщо приймається рішення про використання механізму масок, те відповідним чином повинні бути сконфігуровані і маршрутизатори, і комп'ютери мережі.

2.1.5. Протокол надійної доставки повідомлень TCP

У стеці протоколів TCP/IP протокол *TCP (Transmission Control Protocol)* працює так само, як і протокол UDP, на транспортному рівні. Він забезпечує надійне транспортування даних між прикладними процесами шляхом установлення логічного з'єднання.

2.1.5.1. Сегменти TCP

Одиницею даних протоколу TCP є сегмент. Інформація, що надходить до протоколу TCP у рамках логічного з'єднання від протоколів більш високого рівня, розглядається протоколом TCP як неструктурований потік байт. Дані, що надходять, буферизуються засобами TCP. Для передачі на мережевий рівень з буфера “вирізує” деяка безперервна частина даних, називана сегментом.

У протоколі TCP передбачений випадок, коли додаток звертається з запитом про термінову передачу даних (біт PSH у запиті встановлений у 1). У цьому випадку протокол TCP, не очікуючи заповнення буфера до рівня розміру сегмента, негайно передає зазначені дані в мережу. Про такі дані говорять, що вони передаються поза потоком - *out of band.*

Не всі сегменти, послані через з'єднання, будуть того самого розміру, однак обоє учасника з'єднання повинні домовитися про максимальний розмір сегмента, що вони будуть використовувати. Цей розмір вибирається таким чином, щоб при упакуванні сегмента в IP-пакет він містився туди цілком, тобто максимальний розмір сегмента не повинний перевершувати максимального розміру полючи даних IP-пакета. У противному випадку довелося б виконувати фрагментацію, тобто поділяти сегмент на кілька частин, для того, щоб він вмістився в IP-пакет.

Аналогічні проблеми вирішуються і на мережному рівні. Для того, щоб уникнути фрагментації, повинний бути обраний відповідний максимальний розмір IP-пакета. Однак при цьому повинні бути прийняті в увагу максимальні розміри полючи даних кадрів (MTU) усіх протоколів канального рівня, використовуваних у мережі. Максимальний розмір сегмента не повинний перевищувати мінімальне значення на безлічі всіх MTU складеної мережі.

2.1.5.2. Порти та встановлення TCP-з’єднань

У протоколі TCP також, як і в UDP, для зв'язку з прикладними процесами використовуються порти. Номера портам привласнюються аналогічним образом: маються стандартні, зарезервовані номери (наприклад, номер 21 закріплений за сервісом FTP, 23 - за telnet), а менш відомі додатки користуються довільно обраними локальними номерами.

Однак у протоколі TCP порти використовуються трохи іншим способом. Для організації надійної передачі даних передбачається встановлення *логічного з'єднання* між двома прикладними процесами. У рамках з'єднання здійснюється обов'язкове підтвердження правильності прийому для всіх переданих повідомлень, і при необхідності виконується повторна передача. З'єднання в TCP дозволяє вести передачу даних одночасно в обидва боки, тобто повнодуплексну передачу.

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 декількох з'єднаннях.

Установлення з'єднання виконується в наступній послідовності:

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

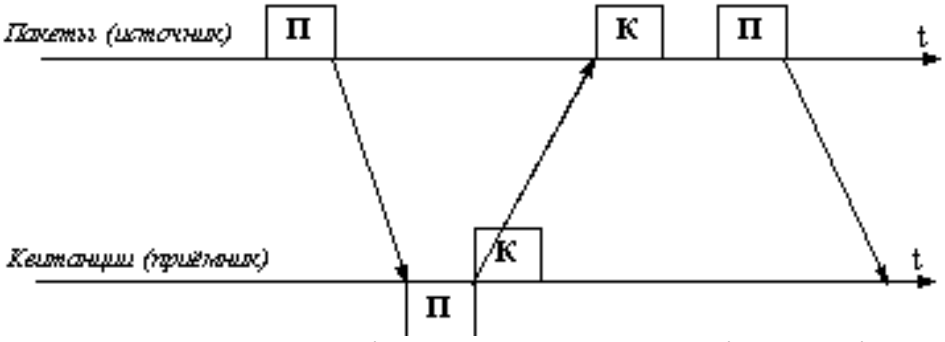
2.1.5.3. Концепція підтвердження

У рамках з'єднання правильність передачі кожного сегмента повинна підтверджуватися квитанцією одержувача. *Підтвердження* - це один із традиційних методів забезпечення надійного зв'язку. Ідея підтвердження полягає в наступному.

Для того, щоб можна було організувати повторну передачу перекручених даних відправник нумерує одиниці, що відправляються, переданих даних (далі для простоти називані кадрами). Для кожного кадру відправник очікує від приймача так називану позитивну квитанцію - службове повідомлення, що сповіщає про те, що вихідний кадр був отриманий і дані в ньому виявилися коректними. Час цього чекання обмежено - при відправленні кожного кадру передавач запускає таймер, і якщо по його витіканню позитивна квитанція на отримана, то кадр вважається загубленим. У деяких протоколах приймач, у випадку одержання кадру з перекрученими даними повинний відправити негативну квитанцію - явна вказівка того, що даний кадр потрібно передати повторно.

Існують два підходи до організації процесу обміну позитивними і негативними квитанціями:

- с простоями;
- с організацією “вікна”.

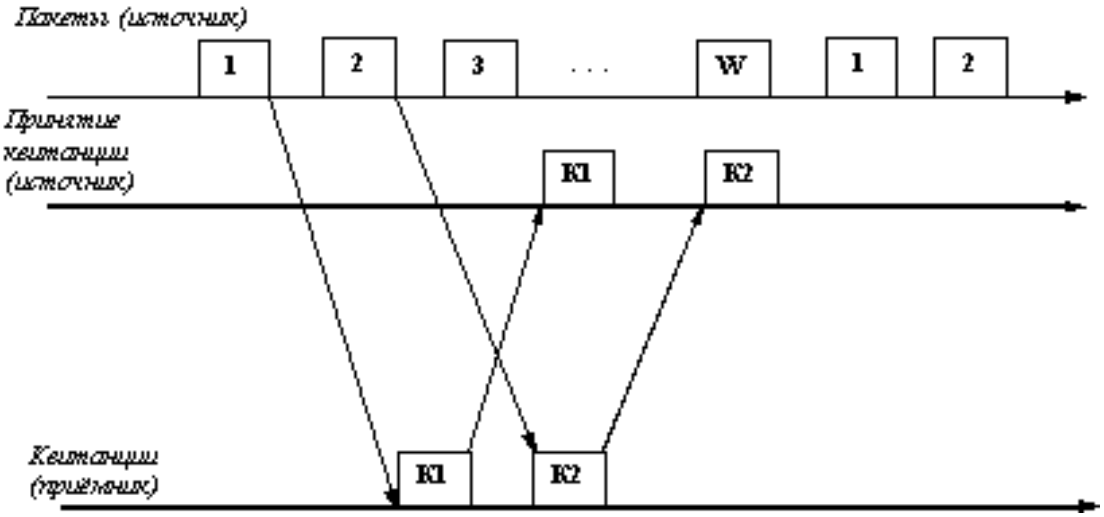


Малюнок 2.1.8 - Метод підтвердження коректності передачі кадрів із простоєм джерела

Метод *із простоями* вимагає, щоб джерело, що послало кадр, очікував одержання квитанції (позитивного або негативної) від приймача і тільки після цього посилав наступний кадр (або повторював перекручений). З малюнка 2.1.8 видно, що в цьому випадку продуктивність обміну даними істотно знижується - хоча передавач і міг би послати наступний кадр відразу ж після відправлення попереднього, він зобов'язаний чекати приходу квитанції. Зниження продуктивності для цього методу корекції особливо помітно на низькошвидкісних каналах зв'язку, тобто в територіальних мережах.

В другому методі для підвищення коефіцієнта використання лінії джерелу дозволяється передати деяка кількість кадрів у безперервному режимі, тобто в максимально можливому для джерела темпі, без одержання на ці кадри відповідних квитанцій. Кількість кадрів, що дозволяється передавати таким чином, називається *розміром вікна*. Малюнок 2.1.9 ілюструє даний метод для розміру вікна в W кадрів. Звичайно кадри при обміні нумеруються циклічно, від 1 до W. При відправленні кадру з номером 1 джерелу дозволяється передати ще W-1 кадрів до одержання квитанції на кадр 1. Якщо ж за цей час квитанція на кадр 1 так і не прийшла, то процес передачі припиняється, і по витіканню деякого тайм-ауту кадр 1 вважається загубленим (або квитанція на нього загублена) і він передається знову.

Якщо ж потік квитанцій надходить більш-менш регулярно, у межах допуску в W кадрів, то швидкість обміну досягає максимально можливої величини для даного каналу і прийнятого протоколу.



Малюнок 2.1.9 - Метод “ковзного вікна” - безперервне відправлення пакетів

Цей алгоритм називають алгоритмом ковзного вікна. Дійсно, при кожнім одержанні квитанції вікно переміщається (сковзає), захоплюючи нові дані, що дозволяється передавати без підтвердження.

2.1.5.4. Реалізація методові вікна в протоколі TCP

У протоколі TCP реалізований різновид алгоритму підтвердження з використанням вікна. Особливість цього алгоритму полягає в тому, що, хоча одиницею переданих даних є сегмент, вікно визначене на безлічі нумерованих байт неструктурованого потоку даних, що надходять з верхнього рівня і буферизованого протоколу TCP.

Квитанція посилається тільки у випадку правильного прийому даних, негативні квитанції не посилаються. Таким чином, відсутність квитанції означає або прийом перекрученого сегмента, або втрату сегмента, або втрату квитанції.

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

2.1.5.5. Вибір тайм-ауту

Вибір часу чекання (тайм-ауту) чергової квитанції є важливою задачею, результат рішення якої впливає на продуктивність протоколу TCP.

Тайм-аут не повинен бути занадто коротким, щоб по можливості виключити надлишкові повторні передачі, що знижують корисну пропускну здатність системи. Але він не повинний бути і занадто великим, щоб уникнути тривалих простоїв, зв'язаних з чеканням неіснуючої або “заблудлої” квитанції.

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

2.1.5.6. Реакція на перевантаження мережі

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

Після прийому квитанції з нульовим значенням вікна протокол-відправник час від часу робить контрольні спроби продовжити обмін даними. Якщо протокол-приймач уже готов приймати інформацію, то у відповідь на контрольний запит він посилає квитанцію з указівкою ненульового розміру вікна.

Іншим проявом перевантаження мережі є переповнення буферів у маршрутизаторах. У таких випадках вони можуть централізовано змінити розмір вікна, посилаючи керуючі

повідомлення деяким кінцевим вузлам, що дозволяє їм диференційоване керувати інтенсивністю потоку даних у різних частинах мережі.

2.1.5.7. Формат повідомлення TCP

Повідомлення протоколу TCP називаються сегментами і складаються з заголовка і блоку даних. Заголовок сегмента має наступні поля:

- ***Порт джерела (Sours Port)*** займає 2 байти, ідентифікує процес-відправник;
- ***Порт призначення (Destination Port)*** займає 2 байти, ідентифікує процес-одержувач;
- ***Послідовний номер (Sequence Number)*** займає 4 байти, указує номер байта, що визначає зсув сегмента щодо потоку даних, що відправляється;
- ***Підтверджений номер (Acknowledgement Number)*** займає 4 байти, містить максимальний номер байта в отриманому сегменті, збільшений на одиницю; саме це значення використовується як квитанцію;
- ***Довжина заголовка (HLEN)*** займає 4 біти, указує довжину заголовка сегмента TCP, обмірювану в 32-бітових словах. Довжина заголовка не фіксована і може змінюватися в залежності від значень, встановлюваних у поле Опції;
- ***Резерв (Reserved)*** займає 6 бітів, поле зарезервоване для наступного використання;
- ***Кодові біти (Code Bits)*** займають 6 бітів, містять службову інформацію про тип даного сегмента, що задається установкою в одиницю відповідний біт цього полючи:
  - URG - термінове повідомлення;
  - ACK - квитанція на прийнятий сегмент;
  - PSH - запит на відправлення повідомлення без чекання заповнення буфера;
  - RST - запит на відновлення з'єднання;
  - SYN - повідомлення використовуване для синхронізації лічильників переданих даних при встановленні з'єднання;
  - FIN - ознака досягнення передавальною стороною останнього байта в потоці переданих даних.
- ***Вікно (Window)*** займає 2 байти, містить значення розміру, що повідомляється, вікна в байтах;
- ***Контрольна сума (Checksum)*** займає 2 байти, розраховується по сегменті;
- ***Покажчик терміновості (Urgent Pointer)*** займає 2 байти, використовується разом з кодовим битому URG, указує на кінець даних, які необхідно терміново прийняти, незважаючи на переповнення буфера;
- ***Опції (Options)*** - це поле має перемінну довжину і може взагалі бути відсутнє, максимальна величина полючи 3 байти; використовується для рішення допоміжних задач, наприклад, при виборі максимального розміру сегмента;
- ***Заповнювач (Padding)*** може мати перемінну довжину, являє собою фіктивне поле, використовуване для доведення розміру заголовка до цілого числа 32-бітових слів.

2.1.6. Протокол доставки дейтаграм користувача UDP

Задачею протоколу транспортного рівня *UDP (User Datagram Protocol)* є передача даних між прикладними процесами без гарантій доставки, тому його пакети можуть бути загублені, продубльовані або прийти не в тім порядку, у якому вони були відправлені.

2.1.6.1 Зарезервовані та доступні порти UDP

У той час, як задачею мережевого рівня є передача даних між довільними вузлами мережі, задача транспортного рівня полягає в передачі даних між будь-якими *прикладними процесами*, що виконуються на будь-яких вузлах мережі. Дійсно, після того, як пакет засобами протоколу IP доставлений у комп'ютер-одержувач, дані необхідно направити конкретному процесові-одержувачеві. Кожен комп'ютер може виконувати кілька процесів, більш того, прикладний процес теж може мати кілька крапок входу, що виступають як адресу призначення для пакетів даних.

Пакети, що надходять на транспортний рівень, зорганізуються операційною системою у виді безлічі черг до крапок входу різних прикладних процесів. У термінології TCP/IP такі системні черги називаються *портами*. Таким чином, адресою призначення, що використовується на транспортному рівні, є ідентифікатор (номер) порту прикладного сервісу. Номер порту, що задається транспортним рівнем, у сукупності з номером мережі і номером комп'ютера, що задаються мережним рівнем, однозначно визначають прикладний процес у мережі.

Призначення номерів портів прикладним процесам здійснюється або централізовано, якщо ці процеси являють собою популярні загальнодоступні сервіси, типу сервісу вилученого доступу до файлів TFTP (Trivial FTP) або сервісу вилученого керування telnet, або локально для тих сервісів, що ще не стали настільки розповсюдженими, щоб за ними закріплювати стандартні (зарезервовані) номера.

TFTP (Trivial File Transfer Protocol). Найпростіший протокол передачі даних, що є значно спрощеним варіантом протоколу FTP. TFTP підтримує просту передачу даних між двома системами без аутентифікації. На відміну від протоколу FTP для використання TFTP потрібен протокол USD.

USD(UserdatagramProtocol). Протокол користувальницьких дейтаграм.

Централізоване присвоєння сервісам номерів портів виконується організацією *Internet Assigned Numbers Authority*. Ці номери потім закріплюються й опубліковуються в стандартах Internet. Наприклад, згаданому вище сервісові вилученого доступу до файлів TFTP привласнений стандартний номер порту 69.

Локальне присвоєння номера порту полягає в тім, що розроблювач деякого додатка просто зв'язує з ним будь-який доступний, довільно обраний числовий ідентифікатор, звертаючи увагу на те, щоб він не входив у число зарезервованих номерів портів. Надалі усі вилучені запити до даного додатка від інших додатків повинні адресуватися з указівкою призначеного йому номера порту.

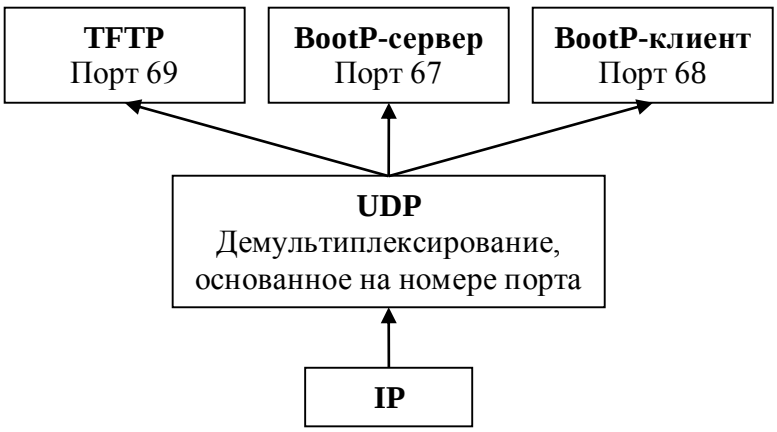
2.1.6.2. Мультиплексування та демультиплексування прикладних протоколів за допомогою протоколові UDP

Протокол UDP веде для кожного порту дві черги: черга пакетів, що надходять у даний порт із мережі, і черга пакетів, що відправляються даним портом у мережу.

Процедура обслуговування протоколом UDP запитів, що надходять від декількох різних прикладних сервісів, називається *мультиплексуванням*.

Boot (Bootstrap Protocol). Протокол, використовуваний для вилученого завантаження бездискових робочих станцій. Станція в результаті одержує IP-адресу. Для завантаження використовується протокол TFTP.

Розподіл протоколом UDP пакетів, що надходять від мережевого рівня, між набором високорівневих сервісів, ідентифікованих *номерами* портів, називається демультиплексуванням (малюнок 2.1.10).



Малюнок 2.1.10 – Демультиплексування пакетів протоколом UDP

Хоча до послуг протоколу UDP може звернутися будь-як додаток, багато хто з них воліють мати справу з іншим, більш складним протоколом транспортного рівня TCP. Справа в тім, що протокол UDP виступає простим посередником між мережним рівнем і прикладними сервісами, і, на відміну від TCP, не бере на себе ніяких функцій по забезпеченню надійності передачі. UDP є *дейтаграмним* протоколом, тобто він не встановлює логічного з'єднання, не нумерує і не упорядковує пакети даних.

З іншого боку, функціональна простота протоколу UDP обумовлює простоту його алгоритму, компактність і висока швидкодія. Тому ті додатки, у яких реалізований власний, досить надійний, механізм обміну повідомленнями, заснований на встановленні з'єднання, воліють для безпосередньої передачі даних по мережі використовувати менш надійні, але більш швидкі засоби транспортування, у якості яких стосовно протоколу TCP і виступає протокол UDP. Протокол UDP може бути використаний і в тому випадку, коли гарна якість каналів зв'язку забезпечує достатній рівень надійності і без застосування додаткових прийомів типу встановлення логічного з'єднання і підтвердження переданих пакетів.

2.1.6.3. Формат повідомлень UDP

Одиниця даних протоколу UDP називається *UDP-пакетом* або *користувальницькою дейтаграмою (user datagram)*. UDP-пакет складається з заголовка і полючи даних, у якому розміщається пакет прикладного рівня. Заголовок має простий формат і складається з чотирьох двобайтових полів:

- ***UDP source port*** - номер порту відправник^-відправника-процесу-відправника;
- ***UDP destination port*** - номер порту одержувач^-одержувача-процесу-одержувача;
- ***UDP message length*** - довжина UDP-пакета в байтах;
- ***UDP checksum*** - контрольна сума UDP-пакета.

Не всі поля UDP-пакета обов'язково повинні бути заповнені. Якщо дейтаграма що посилається не припускає відповіді, то на місці адреси відправника можуть міститися нулі. Можна відмовитися і від підрахунку контрольної суми, однак варто врахувати, що протокол IP підраховує контрольну суму тільки для заголовка IP-пакета, ігноруючи поле даних.

2.1.7. Протоколи прикладного рівня

Чому існують два транспортних протоколи TCP і UDP, а не один з них? Справа в тім, що вони надають різні послуги прикладним процесам. Більшість прикладних програм користуються тільки одним з них. Ви, як програміст, вибираєте той протокол, що щонайкраще відповідає вашим потребам. Якщо вам потрібна надійна доставка, то кращим може бути TCP. Якщо вам потрібна доставка дейтаграм, то краще може бути UDP. Якщо вам потрібна ефективна доставка по довгому і ненадійному каналі передачі даних, то краще може підійти протокол TCP. Якщо потрібна ефективність на швидких мережах з короткими з'єднаннями, то кращим може бути протокол UDP. Якщо ваші потреби не попадають у

жодну з цих категорій, то вибір транспортного протоколу не ясний. Однак прикладні програми можуть усувати недоліки обраного протоколу. Наприклад, якщо ви вибрали UDP, а вам необхідна надійність, те прикладна програма повинна забезпечити надійність. Якщо ви вибрали TCP, а вам потрібно передавати запису, то прикладна програма повинна вставляти маркери в потік байтів так, щоб можна було розрізнити запису.

Які ж прикладні програми доступні в мережах з TCP/IP?

Загальна їхня кількість велика і продовжує постійно збільшуватися. Деякі додатки існують із самого початку розвитку Internet. Наприклад, TELNET і FTP. Інші з'явилися недавно: X-Window, SNMP.

Протоколи прикладного рівня орієнтовані на конкретні прикладні задачі. Вони визначають як процедури по організації взаємодії визначеного типу між прикладними процесами, так і форму представлення інформації при такій взаємодії. У цьому розділі ми коротко опишемо деякі з прикладних протоколів.

2.1.6.1. Протокол TELNET

Протокол TELNET дозволяє обслуговуючій машині розглядати усі вилучені термінали як стандартні “мережні віртуальні термінали” рядкового типу, що працюють у коді ASCII, а також забезпечує можливість узгодження більш складних функцій (наприклад, локальний або вилучений контроль^-контроль-луна-контроль, сторінковий режим, висота і ширина екрана і т.д.) TELNET працює на базі протоколу TCP. На прикладному рівні над TELNET знаходиться або програма підтримки реального термінала (на стороні користувача), або прикладний процес в обслуговуючій машині, до якого здійснюється доступ з термінала.

Робота з TELNET походить на набір телефонного номера. Користувач набирає на клавіатурі щось начебто

telnet delta

і одержує на екрані запрошення на вхід у машину delta.

Протокол TELNET існує вже давно. Він добре випробуваний і широко розповсюджений. Створено безліч реалізацій для самих різних операційних систем. Цілком припустимо, щоб процес-клієнт працював, скажемо, під керуванням ОС VAX/VMS, а сервер^-сервер-процес-сервер під ОС UNIX System V.

2.1.6.2. Протокол FTP

Протокол FTP (File Transfer Protocol - протокол передачі файлів) розповсюджений також широко як TELNET. Він є одним з найстарших протоколів сімейства TCP/IP. Також як TELNET він користується транспортними послугами TCP. Існує безліч реалізацій для різних операційних систем, що добре взаємодіють між собою. Користувач FTP може викликати кілька команд, що дозволяють йому подивитися каталог вилученої машини, перейти з одного каталогу в інший, а також скопіювати один або кілька файлів.

2.1.6.3. Протокол SMTP

Протокол SMTP (Simple Mail Transfer Protocol - простий протокол передачі пошти) підтримує передачу повідомлень (електронної пошти) між довільними вузлами мережі Internet. Маючи механізми проміжного збереження пошти і механізми підвищення надійності доставки, протокол SMTP допускає використання різних транспортних служб. Він може працювати навіть у мережах, що не використовує протоколи сімейства TCP/IP. Протокол SMTP забезпечує як групування повідомлень на адресу одного одержувача, так і розмноження декількох копій повідомлення для передачі в різні адреси. Над модулем SMTP розташовується поштова служба конкретних обчислювальних систем.

2.1.6.4. NFS

Мережева файлова система NFS (Network File System) уперше була розроблена компанією Sun Microsystems Inc. NFS використовує транспортні послуги UDP і дозволяє

монтувати в єдине ціле файлові системи декількох машин з ОС UNIX. Бездискові робочі станції одержують доступ до дисків файлу-сервера так, начебто це їхні локальні диски.

NFS значно збільшує навантаження на мережу. Якщо в мережі використовуються повільні лінії зв'язку, то від NFS мало користі. Однак, якщо пропускна здатність мережі дозволяє NFS нормально працювати, те користувачі одержують великі переваги. Оскільки сервер і клієнт NFS реалізуються в ядрі ОС, усі звичайні немережеві програми одержують можливість працювати з вилученими файлами, розташованими на підмонтованих NFS-дисках, точно також як з локальними файлами.

2.1.6.5. Протокол SNMP

Протокол SNMP (Simple Network Management Protocol - простий протокол керування мережею) працює на базі UDP і призначений для використання мережними керуючими станціями. Він дозволяє керуючим станціям збирати інформацію про положення справ у мережі Internet. Протокол визначає формат даних, їхня обробка й інтерпретація залишаються на розсуд керуючих станцій або менеджера мережі.

Тема 2.2. Internet

2.2.1.Необхідність Інтернету

Передача даних стала фундаментальною частиною обчислень. Мережі, розкидані по усім світі, збирають дані про такі різні предмети, як атмосферні умови, виробництво продуктів і повітряних перевезень. Групи створюють електронні довідкові списки, що дозволяють їм одержувати інформацію, цікаву усім. Аматори обмінюються програмами для їхніх домашніх комп'ютерів. У науковому світі мережі даних стали необхідні, тому що вони дозволяють ученим посилати програми і дані на вилучені суперкомп'ютери для обробки, одержувати результати й обмінюватися науковою інформацією з колегами.

На жаль, більшість мереж є незалежними сутностями, створеними для задоволення потреб однієї групи людей. Користувачі вибирають апаратну технологію, що підходить для їхніх комунікаційних проблем. Більш важливо те, що не можна створити універсальну мережу на основі однієї апаратної технології, тому що немає такої мережі, що задовольнила б усі потреби. Деяким користувачам потрібна високошвидкісна мережа, що з'єднує їхньої машини, але такі мережі не можуть бути розширені на великі відстані. Іншим потрібна більш повільна мережа, що буде з'єднувати машини, що знаходяться на відстані тисяч кілометрів друг від друга.

Недавно, проте, з'явилася нова технологія, що уможливила взаємне з'єднання великого числа розділених фізичних мереж і змусила них працювати як одне єдине ціле. Ця нова технологія, що називається *міжмережевим обміном (internetworking)*, пристосовує друг до друга різні апаратні технології, що лежать в основі фізичних мереж, за допомогою додавання як фізичних з'єднань мереж, так і нового набору угод. Технологія міжмережевого обміну ховає деталі мережевого устаткування і дозволяє комп'ютерам взаємодіяти поза залежністю від типу їхніх фізичних з'єднань.

Технологія міжмережевого обміну, описана в книзі, являє приклад Взаємодії *Відкритих Систем*. Вони називаються відкритими тому, що на відміну від конкретних комунікаційних систем, продаваних тим або іншому виробникові, її специфікації доступні усім. Тому кожної може створити програмне забезпечення, необхідне для взаємодії в об'єднаній мережі. Більш того, уся ця технологія була розроблена для того, щоб спростити взаємодія між машинами з різними апаратними архітектурами, щоб використовувати майже будь-яке устаткування мережі з комутацією пакетів, і щоб дозволити взаємодія різних операційних систем.

Щоб оцінити значення міжмережевої технології, подумайте, як вона вплинула на дослідження. Представте на хвилину ефект взаємного з'єднання всіх комп'ютерів, використовуваних ученими. Любою вчений може обмінятися результатами експерименту з будь-яким іншим ученим. Можна створити національні центри даних, що збирають дані про природні явища і роблять їх доступними для усіх учених. Комп'ютерні засоби і

програми, доступні в одному місці, можуть використовуватися вченими в інших місцях. У результаті швидкість, з яким здійснюються наукові дослідження, може різко зрости.

2.2.2. Інтернет TCP/IP

Урядові агентства усвідомили важливість і потенціал міжмережевої технології в майбутньому і стали фінансувати дослідження, що зробили б можливим створення національної об'єднаної мережі. Ця книга розглядає принципи й ідеї, що лежать в основі ведучої міжмережевої технології, що з'явилася в результаті проведення розробок, що фінансувалися агентством DARPA(Defense Advanced Research Projects Agency). Технологія DARPA включає набір мережних стандартів, що описують детально процес взаємодії комп'ютерів, а також ряд угод при взаємодії мереж і маршрутизації трафіку. Офіційно називаний Зв'язуванням Міжмережевих Протоколів TCP/IP (а в повсякденній мові - TCP/IP по іменах двох основних стандартів), він може використовуватися для взаємодії комп'ютерів за допомогою необмеженого числа мереж. Наприклад, деякі корпорації використовують TCP/IP для зв'язку мереж усередині їхньої корпорації, навіть якщо корпорація не має зв'язки з зовнішніми мережами. Інші групи використовують TCP/IP для зв'язку вилучених друг від друга місць.

Хоча технологія TCP/IP цікава сама по собі, вона особливо гарна через свою життєздатність, що вона продемонструвала. Вона стала базовою технологією для великого співтовариства мереж, що зв'язують більшість дослідницьких інститутів, включаючи університетські, об'єднані або урядові лабораторії. Національний Науковий Фонд(NSF), Міністерство Енергетики(DOE), Міністерство Оборони(DOD), Агентство по охороні здоров'я(HHS) і NASA взаємодіють один з одним, використовуючи TCP/IP для з'єднання великого числа їхніх дослідницьких центрів з центрами DARPA. Сутність, що вийшла, відома як об'єднаний Інтернет, Інтернет DARPA/NSF, Інтернет TCP/IP, або просто Інтернет, дозволяє дослідникам усіх зв'язаних інститутів розділяти інформацію з колегами по всій країні так само легко, як якби вони були в сусідній кімнаті. Таким чином, Інтернет продемонстрував життєздатність технології TCP/IP і показав, як можна об'єднати велику кількість різноманітних базових мережних технологій.

Більшість матеріалів описаних вище стосується будь-якого Інтернету, що використовує TCP/IP, але деякі розділи присвячені спеціально об'єднаному Інтернету. Читачі, що цікавляться тільки технологією, повинні чітко розрізняти реальну існуючу архітектуру Інтернету і гіпотетичний Інтернет TCP/IP, що міг би існувати. Проте, буде помилкою ігнорувати секції, що описують об'єднаний Інтернет цілком - мережі багатьох корпорацій уже наздогнали по складності Інтернет десятилітньої давнини, і багато проблем, з якими вони зіштовхуються зараз, уже давно вирішені в об'єднаному Інтернету.

2.2.2.3. Засобу Інтернету

Не можна говорити про технічні деталі, що лежать в основі Інтернету, не розуміючи засобів, що він забезпечує. Ця глава коротко розглядає засоби Інтернету, більш докладно зупиняючи на тих засобах, якими користується більшість користувачів, і відкладаючи до наступних глав розгляд питання про те, як комп'ютери приєднуються до Інтернету і як реалізуються ці засоби.

Велика частина опису засобів буде присвячена стандартам, називаним протоколами. Протоколи, такі як TCP і IP, дають формули для передачі повідомлень, описують деталі форматів повідомлень і вказують, як обробляти помилки. Найважливіше те, що вони дозволяють нам розглядати стандарти взаємодії поза залежністю від того, на устаткуванні якого виробника, вони реалізуються. Власне кажучи, протоколи є для комунікації тим, чим є мови програмування для обчислень. Мова програмування дозволяє описати або зрозуміти обчислення, не знаючи системи команд конкретного ЦП. Аналогічно, комунікаційний протокол дозволяє нам описати або зрозуміти процес передачі даних, не знаючи на якому устаткуванні цей процес виконується.

Приховання низькорівневих деталей взаємодії допомагає поліпшити продуктивність. По-перше, програмістам, що працюють з високорівневими протокольними абстракціями, не потрібно знати або пам'ятати безліч деталей про конкретні параметри устаткування. Вони можуть швидко створювати нові програми. По-друге, тому що програми, розроблені, використовуючи високорівневі абстракції, не обмежені архітектурою конкретної машини або конкретного мережевого устаткування, їх не треба змінювати при заміні машини або зміні конфігурації. По-третє, тому що прикладні програми, побудовані, використовуючи високорівневі протоколи, незалежні від використовуваного устаткування, вони можуть забезпечувати пряму взаємодію різних машин. Програмістам не потрібно писати спеціальні версії прикладних програм для переміщення і трансляції даних для всіх можливих пар типів машин. Ми побачимо, що всі мережні засоби описуються протоколами.

Наступні секції розглянуть протоколи, використовувані для опису засобів прикладного рівня, а також протоколи, використовувані при визначенні мережних засобів. Наступні глави опишуть кожний з цих протоколів більш детально.

2.2.2.3.1 Засобу Інтернету прикладного рівня.

З погляду користувача, Інтернет TCP/IP є набором прикладних програм, що використовують мережу для виконання корисних комунікаційних задач. Ми будемо використовувати термін взаємна працездатність(interoperability) для опису здатності різних обчислювальних систем взаємодіяти при рішенні обчислювальних задач. Ми затверджуємо, що прикладні програми Інтернету показують високий ступінь взаємної працездатності. Більшість користувачів, що користуються Інтернетом, роблять це, просто запускаючи прикладні програми , не розуміючи при цьому технології TCP/IP, структури Інтернету, і навіть не знаючи шляхи, що проходять дані до призначення; вони покладаються на те, що прикладні програми самі розберуться з цими деталями. Тільки програмісти, що пишуть такі прикладні програми, дивляться на Інтернет як на мережу і розуміють деталі цієї технології.

Самі популярні і широко розповсюджені прикладні засоби Інтернету включають:

- ЕЛЕКТРОННУ ПОШТУ. Електронна пошта дозволяє користувачеві створити лист і послати його людині або групі людей. Інша частина цього додатка дозволяє користувачеві читати листа, що він одержав. Електронна пошта була так успішна, що багато користувачів Інтернету використовують неї для звичайної комерційної переписки. Хоча існує багато систем електронної пошти, важливо розуміти, що використання TCP/IP робить доставку листа більш надійної. Замість того, щоб покладатися на проміжні машини при передачі листа, система надання листа в TCP/IP працює, прямо з'єднуючи машину відправника з машиною одержувача. Тому відправник знає, що як тільки лист залишив його машину, воно успішно досягло місця призначення.
- ПЕРЕДАЧУ ФАЙЛІВ. Хоча користувачі іноді і передають файли, використовуючи електронну пошту, лист призначено для коротких, текстових файлів. Протоколи TCP/IP включають прикладну програму передачі файлів, що дозволяє користувачам передавати або приймати досить великі файли програм або даних. Наприклад, використовуючи програму передачі файлів, можна скопіювати з однієї машини на іншу великі об'єми даних, що містять зображення із супутника, програми, написані на Фортрані або Паскалі, або англійський словник. Ця система забезпечує спосіб перевірки особистості користувача або навіть заборона доступу. Як і лист, передача файлів по Інтернету TCP/IP надійний, тому що дві взаємодіючі машини роблять це прямо, не покладаючись на проміжні машини для створення копій файлу.
- ВИЛУЧЕНИЙ ДОСТУП. Будучи самим цікавим додатком Інтернету, вилучений доступ дозволяє користувачеві, що знаходиться на одному комп'ютері, взаємодіяти з вилученою машиною і виконувати на ній інтерактивний сеанс роботи. Вилучений доступ дозволяє створити враження, що термінал користувача або його робоча станція приєднані прямо до вилученої машини, посилаючи кожен символ, натиснутий на клавіатурі користувача на вилучену машину і відображаючи кожен символ, повернутий з

вилученої машини, на екрані термінала користувача. Коли сеанс із вилученою машиною завершується, додаток повертає користувача в локальну систему.

Ми повернемося до кожного з цих додатків пізніше, щоб розглянути його більш детально. Ми побачимо, як вони використовують базові протоколи TCP/IP і чому наявність стандартів прикладних протоколів допомогла упевнитися, що вони широко поширені.

2.2.2.3.2 Засобу Інтернету мережевого рівня.

Програміст, що пише прикладні програми, що використовують протоколи TCP/IP, має зовсім інше представлення про Інтернет, чим користувач, що просто запускає прикладні програми, такі як електронна пошта. На мережному рівні Інтернет надає два основних типи сервісу, що використовують прикладні програми. І хоча на даному етапі несуттєве розуміння деталей цих засобів, їх не можна опустити при будь-якому огляді TCP/IP:

- ДЕЙТАГРАММНОЕ ЗАСІБ ДОСТАВКИ ПАКЕТІВ. Це засіб, що буде згодом детально пояснено, утворить основу всіх інших засобів Інтернету. Доставка без з'єднання (дейтаграмна доставка) є абстракцією сервісу, що надає більшість мереж з комутацією пакетів. Це просто означає, що Інтернет TCP/IP визначає маршрут передачі невеликого повідомлення від однієї машини до інший, ґрунтуючись тільки на адресній інформації, що знаходиться в повідомленні. Тому що дейтаграмний засіб маршрутизує кожен пакет окремо, воно не гарантує надійної доставки пакетів у тім порядку, у якому вони були послані. Тому що цей засіб звичайно прямо відображається на лежаче в його основі устаткування, засіб без з'єднання дуже ефективно. Більш того, використання доставки пакетів без з'єднання як основу всіх засобів Інтернету робить протоколи TCP/IP адаптовуваним до широкого діапазону мережевого устаткування.
- НАДІЙНИЙ ПОТОКОВИЙ ТРАНСПОРТНИЙ ЗАСІБ. Більшості додатків потрібно щось більше, ніж проста доставка пакетів, тому що вони жадають від комунікаційного програмного забезпечення автоматичного відновлення при помилках передачі, утраті пакетів або збоях проміжних маршрутизаторів на шляху між відправником до одержувачем. Надійний транспортний засіб обробляє ці ситуації. Воно дозволяє додаткові на одному комп'ютері встановлювати "з'єднання" з додатком на іншому комп'ютері, а потім посилати великі об'єми даних по з'єднанню, так якби це було пряме апаратне з'єднання. Насправді, звичайно, протоколи взаємодії поділяють потік даних на маленькі повідомлення і посилають їхній потім по одному, очікуючи від одержувача підтвердження прийому.

Багато мереж забезпечує базові засоби, аналогічні описаним вище, тому дехто може здивуватися:"Чим же відрізняються засоби TCP/IP від інших?". Основними відмінностями є:

- НЕЗАЛЕЖНІСТЬ ВІД МЕРЕЖЕВОЇ ТЕХНОЛОГІЇ. Хоча TCP/IP і ґрунтується на зручній пакетній технології, він незалежний від устаткування конкретного виробника. Об'єднаний Інтернет включає велике число мережних технологій від мереж, призначених для роботи в одному будинку, до мереж, що працюють на великих відстанях. Протоколи TCP/IP визначають елемент передачі даних, називаний дейтаграмою, і описують, як передавати дейтаграми по конкретній мережі.
- ЗАГАЛЬНА СВЯЗНОСТЬ. Інтернет TCP/IP дозволяє будь-якій парі комп'ютерів, приєднаних до нього, взаємодіяти один з одним. Кожному комп'ютерові призначається адреса, що відома по всьому Інтернету. Кожна дейтаграма містить адреси відправника й одержувача. Проміжні маршрутизатори використовують адреса одержувача для того, щоб приймати рішення про подальший маршрут дейтаграми.
- МЕЖКОНЦЕВЫЕ ПІДТВЕРДЖЕННЯ. Протоколи TCP/IP Інтернету забезпечують підтвердження між відправником і одержувачем, а не між відправником і проміжними машинами на шляху, навіть коли дві машини не зв'язані загальною фізичною мережею.
- СТАНДАРТНІ ПРИКЛАДНІ ПРОТОКОЛИ. Крім базових засобів транспортного рівня(таких, як надійні потокові з'єднання), протоколи TCP/IP включають

стандарти для найбільше часто використовуваних додатків, таких як електронна пошта, передача файлів і вилучений доступ. Тому при розробці прикладних програм, що використовують TCP/IP, програмісти часто можуть знайти, що існуюче програмне забезпечення вже забезпечує комунікаційні засоби, що їм потрібні.

Наступні глави розглянуть у деталях засобу, що пропонуються програмістові, а також більшість стандартів прикладних протоколів.

2.2.2.4. Історія створення Інтернету

Частиною того, що робить Інтернет настільки чудовим, є майже повсюдне його використання, а також його розміри і темпи росту об'єднаного Інтернету. DARPA початку роботи в напрямку розробки міжмережевої технології в середині 70-х, але архітектура і протоколи прийняли форму, у якій вони відомі зараз, лише в 1977-1979 роках. У цей час DARPA була відома як основне агентство, що фінансує дослідження в області мереж з комутацією пакетів, і впровадила безліч нововведень у цій області в добре відому ARPANET. ARPANET використовувала звичайні виділені лінії точка-крапка для з'єднання комп'ютерів, але DARPA також фінансувала використання комутації пакетів у радіомережах і супутникових лініях зв'язку. Власне кажучи зростаючу розмаїтість апаратних мережних технологій змусило DARPA вивчити міжмережеву взаємодію і просунутися в напрямку до об'єднаної мережі.

Приступність результатів досліджень, що фінансувалися DARPA, привернула увагу декількох дослідницьких груп, особливо тих дослідників, хто вже мав досвід використання пакетної комутації в ARPANET. DARPA збирало неформальні зустрічі дослідників для обміну ідеями й обговорення результатів експериментів. З 1979 року в проект TCP/IP уключилося так багато дослідників, що DARPA утворило неформальний комітет для координації і керування розробкою протоколів і архітектур що розвивається об’єднаного Інтернету. Названа Група по Конфігурації і Керуванню Інтернетом(ICCB), ця група регулярно збиралася до 1983 року, коли вона була реорганізована.

Об’єднаний Інтернет почав існувати з 1980 року, коли DARPA початку встановлювати на машинах, приєднаних до її дослідницької мережі, новий протоколи TCP/IP. ARPANET незабаром після створення став магістральною мережею нового Інтернету і був використаний для більшості з ранніх експериментів з TCP/IP. Перехід до технології Інтернету був довершений у січні 1983 року, коли секретаріат МО США установив, що всі комп'ютери, приєднані до глобальних мереж, використовують TCP/IP. У цей же самий час Оборонне Комунікаційне Агентство(DCA) розділило ARPANET на дві окремі мережі, одна для подальших досліджень і одна для військового зв'язку. За дослідницькою мережею залишилося ім'я ARPANET, а військова частина, що була трохи більше, одержала назву MILNET.

Для того щоб змусити дослідників в університетах використовувати нові протоколи, DARPA стала продавати їхню реалізацію за низькою ціною. У цей час більшість університетських факультетів комп'ютерних наук використовували версію операційної системи UNIX, розроблену в програмному відділенні Університету Берклі в Каліфорнії, частіше називану Berkeley UNIX або BSD UNIX. Фінансуючи створення фірмою Bolt Beranek and NewMan, Inc. (BBN) реалізації протоколів TCP/IP для UNIX і фінансуючи інтеграцію цих протоколів у програмні продукти, вироблені відділенням у Berkeley, DARPA змогла організувати взаємодію з 90% усіх комп'ютерних факультетів університетів. Нове програмне забезпечення з протоколами з'явилося вчасно, тому що багато факультетів відразу ж здобували ще комп'ютери і з'єднували їхній як локальні мережі. Факультетам були потрібні протоколи взаємодії, а інших протоколів у той час не було в загальному користуванні.

Програмне відділення Берклі стало популярним, тому що воно пропонувало не тільки базові протоколи TCP/IP. Крім стандартних прикладних програм TCP/IP, Берклі пропонувало набір утиліт для роботи з мережею, що нагадували засобу UNIX, використовувані на одній машині. Головна перевага утиліт Берклі полягало в їхній

подібності зі стандартним UNIxом. Наприклад, досвідчений користувач UNIX може швидко навчитися користуватися утилітою копіювання вилучених файлів Берклі, тому що він поводиться точно так, як утиліта копіювання файлів у UNIX, за винятком того, що вона дозволяє користувачам копіювати файли на вилучену машину або з неї.

Крім набору службових програм UNIX Берклі забезпечує нову абстракцію операційної системи відому як порт(socket), що дозволяє прикладним програмам одержувати доступ до комунікаційних протоколів. Будучи узагальненням механізму UNIX для введення-висновку, порт має опції для декількох типів мережних протоколів крім TCP/IP. Її принципи стали обговорюватися з часу її розробки, і багато розроблювачів операційних систем запропонували альтернативні варіанти. Незалежно від своїх достоїнств, введення абстракції порту було важливим, тому що дозволяло програмістам використовувати протоколи TCP/IP з мінімумом витрат. Тому, це стимулювало розроблювачів експериментувати з TCP/IP.

Успіх технології TCP/IP і Інтернету в університетському середовищі змусив інші групи теж використовувати його. З огляду на, що мережева взаємодія незабаром стане важливою частиною наукових досліджень, NSF взяв активну участь у розширенні Інтернету TCP/IP серед учених. Починаючи з 1985 року, він почав запроваджувати в життя програму створення мереж на основі його шести суперкомп'ютерних центрів. У 1986 він розширив діяльність у цьому напрямку, почавши фінансувати нову глобальну магістральну мережу, названу NSFNET, що згодом зв'язала всі суперкомп'ютерні центри між собою і ARPANET. Нарешті, у 1986 NSF почав частково фінансувати багато регіональних мереж, кожна з яких зараз з'єднує основні науково-дослідні центри в цьому районі. Усі мережі, що фінансувалися NSF, використовують протоколи TCP/IP, і усі є частиною об’єднаного Інтернету.

За сімох років після свого створення Інтернет об'єднав сотні індивідуальних мереж, розміщених у США і Європі. Він з'єднав майже 20000 комп'ютерів в університетах, урядових і часток дослідницьких лабораторіях. Як розмір, так і використання Інтернету продовжують рости швидше, ніж передбачалося. До кінця 1987 року було встановлено, що його ріст досяг 15% на місяць і залишався таким останні два роки. У 1990 році об'єднаний Інтернет уключав більш 3000 активних мереж і більш ніж 200000 комп'ютерів.

Використання протоколів TCP/IP і ріст Інтернету не обмежувалися проектами, що фінансуються урядом. Основні комп'ютерні корпорації приєдналося до Інтернету, так само як і безліч інших великих корпорацій, включаючи: нафтові компанії, автомобільні концерни, електронні фірми і телефонні компанії. До того ж, багато компаній використовують протоколи TCP/IP у своїх внутрішніх мережах, навіть якщо вони і не приєднані до об'єднаного Інтернету.

Швидке розширення привело до проблем діапазонів, непередбаченим у вихідному проекті, і змусило розроблювачів знайти технології для керування великими, розподіленими ресурсами. У вихідному проекті, наприклад, імена й адреси всіх комп'ютерів, приєднаних до Інтернету, зберігалися в одному файлі, що редагувався вручну і потім поширювався по всьому Інтернету. Але в середині 1980 року стало ясно, що центральна база даних неефективна. По-перше, запити на відновлення файлу незабаром повинні були перевищити можливості людей, що обробляли них. По-друге, навіть якщо існував коректний центральний файл, не вистачало пропускної здатності мережі, щоб дозволити або частий розподіл його по всіх місцях, або оперативний доступ до нього з кожного місця.

Були розроблені нові протоколи і стала використовуватися система імен по всьому об'єднаному Інтернету, що дозволяла будь-якому користувачеві автоматично визначати адресу вилученої машини по її імені. Відомий як Доменна Система Імен, цей механізм ґрунтується на машинах, називаних серверами імен, що відповідають на запити про імена. Немає однієї машини, що містить усю базу даних про імена. Замість цього, дані розподілені

по декількох машинах, що використовують протоколи TCP/IP для зв'язку між собою при відповіді на запити.

2.2.2.5. Група Активності Інтернету(IAB).

Тому що зв'язування протоколів TCP/IP не були розроблені яким-небудь виробником або відомим професійним суспільством, природно поставити запитання:"хто визначає напрямки розвитку і вирішують, коли протоколи стають стандартами?". Відповіддю є група, відома як Група Активності Інтернету(IAB). IAB визначає головний напрямок розробок на основі протоколів TCP/IP , координує більшість їхній і керує еволюцією об'єднаного Інтернету. Вона вирішує, які протоколи є необхідною частиною зв'язування TCP/IP і визначає офіційну політику.

Утворена в 1983 році, коли DARPA реорганізувало ICCB, IAB успадкувала багато від своїх попередників. Її початковими цілями було стимулювати обмін ідеями між людьми, задіяними в дослідженнях, пов'язаних з TCP/IP і Інтернетом, і тримати дослідників у курсі загальних цілей. Після перших шести років існування IAB з дослідницької групи DARPA перетворився в незалежну організацію. За ці роки кожен член IAB побував головою Цільових Сил Інтернету(ITF), відповідаючи за дослідження проблеми або ряду питань, що представляють інтерес. IAB складалося з приблизно десяти цільових сил із задачами від дослідження, як трафік різних додатків впливає на Інтернет, до поточних інженерних проблем Інтернету. IAB збиралася кілька разів у рік для заслуховування звітів усіх цільових сил, короткого огляду і перегляду технічних напрямків, обговорення політики й обміну інформацією з представниками інших агентств, таких як DARPA і NSF, що фінансували роботу Інтернету і дослідження для нього.

Голова IAB мав звання Архітектор Інтернету і відповідав за пропозицію напрямків технічного розвитку і координацію роботи різних цільових сил. Голова IAB створював нові цільові сили за порадою IAB і також представляв IAB перед іншими організаціями.

Новачки в TCP/IP іноді дивуються, довідавшись, що IAB не мав великого бюджету; хоча він і визначав напрямку, він не фінансував велику частину досліджень і інженерних розробок. Замість цього, добровольці самі виконували велику частину роботи. Члени IAB відповідали за прийом добровольців для роботи їхній у підлеглих їм цільових силах, за скликання зустрічей цільових сил, і за звіти про роботу перед IAB. Звичайно, добровольці з'являлися з дослідницького співтовариства або комерційних організацій, що використовували TCP/IP. Активні дослідники брали участь у цільових силах Інтернету по двох причинах. По-перше, робота в цільових силах забезпечувала можливість довідатися нове про дослідницькі проблеми. По-друге, тому що нові ідеї і рішення проблем висунуті і перевірені цільовими силами, часто ставали частиною технології Інтернету, члени розуміли, що їхня робота прямо впливає на цю область.

2.2.2.6. Нова організація IAB

Починаючи з літа 1989 року, як технологія TCP/IP, так і об'єднаний Інтернет з дослідницького проекту виросли в засоби виробництва, якими користувалися тисячі людей у своїх щоденних справах. Більше не можна було реалізувати нові ідеї, установивши вночі нове програмне забезпечення на декількох машинах. Тепер уже сотні комерційних компаній, що поширювала продукти TCP/IP, визначали, чи будуть їхні продукти взаємно працездатні, вирішуючи питання про внесення змін у їхні програми.

Дослідники, що розробляли початкові специфікації і тестували нові ідеї в лабораторіях, більше не могли розраховувати на швидке впровадження і використання своїх ідей. По іронії долі дослідники, що проектували TCP/IP і спостерігали за його розвитком, виявилися переможені комерційним успіхом їхнього дітища. Коротко говорячи, TCP/IP став успішною, продуктивною технологією і тепер уже ринок став керувати його розвитком.

Тому IAB був реорганізований улітку 1989 року для приведення у відповідність з новою політичною і комерційною реальністю TCP/IP і об'єднаного Інтернету. Головування

змінилося. Дослідники були переведені з IAB у допоміжну групу, і був створений новий IAB, для того щоб включати представників більш широкого співтовариства.

Крім самої IAB організація включає дві основні групи: Дослідницькі Цільові сили Інтернету(IRTF) і Інженерні Цільові Сили Інтернету(IETF).

Як це випливає з її імені, IETF концентрується на оперативній і тактичній інженерній проблемах. IETF існувала й у старій структурі IAB, і її успіх з'явився однієї з причин реорганізації. На відміну від більшості цільових сил IAB, що були обмежені кількома людьми, що концентрувалися на одній конкретній проблемі, IETF розрісся і став включати сотні активних членів, що працювали над багатьма проблемами паралельно. До реорганізації IETF був розділений на 20 робочих груп, кожна з яких працювала над конкретною проблемою. Робочі групи збиралися на свої зустрічі для вироблення рішень проблем. Крім того, весь IETF збирався регулярно, щоб заслуховувати звіти робочих груп і обговорювати пропоновані зміни або додавання до технології TCP/IP. Проведені звичайно три рази в рік, зустрічі всієї IETF збирали сотні учасників і глядачів. IETF став занадто великим, щоб їм керував один голова.

IETF зберігся в реорганізованій структурі IAB, але був розділений на вісьмох областей, кожна з яких мала свого власного керуючого. Голова IETF і вісім керуючих областями складають Керівну Інженерну Групу Інтернету (IESG), члени якої відповідальні за координацію всіх проектів робочих груп IETF.

Тому що IETF був широко відомий по всьому Інтернету, і тому що його зустрічі одержали широке схвалення, ім'я IETF було збережено при реорганізації й усе ще позначає цю групу цілком, включаючи голови, керуючих областями, і всіх членів робочих груп. По аналогічних причинах було залишене ім'я "робоча група IETF".

Створені при реорганізації, Дослідницькі Цільові Сили Інтернету одержали таке ім'я як дослідницьке доповнення до IETF. IRTF координує роботи дослідників, зв'язані з протоколами TCP/IP і архітектурою Інтернету в цілому. Як і IETF, IRTF має невелику групу, називану Керівною Дослідницькою Групою Інтернету або IRSG, що встановлює пріоритети і координує роботи дослідників. На відміну від IETF, IRTF, проте, у даний час набагато менше по розмірах. Кожен член IRSG набирає добровольців у Дослідницькі Групи Інтернету, аналогічні робочим групам IETF; IRTF не поділений на області.

2.2.2.7 Технічні звіти Інтернету

Ми вже говорили, що немає ні виробників, ні професійних суспільств, що володіють технологією TCP/IP. Тому, документацію на протоколи, стандарти, і політикові не можна одержати від виробника. Замість цього, DCA фінансує групу в SRI International, що одержує і поширює інформацію про TCP/IP і об'єднаний Інтернет. Відома, як Мережевий Інформаційний Центр або просто NIC, ця група керує багатьма адміністративними питаннями Інтернету крім поширення документації.

Уся документація про роботи в Інтернету, пропозиціях про нові або перероблені протоколи, і стандартах протоколів TCP/IP з'являється у виді серії технічних звітів, називаних Request For Comments або RFC(буквальний переклад приблизно такий - Потрібні Коментарі).(Ранні версії RFC були відомі як чорнові проекти Інтернету). RFC можуть бути маленькі або великими, можуть описувати фундаментальні концепції або деталі приватного питання, і можуть бути стандартами або просто пропозиціями нових протоколів. Редактор RFC називається Делегованим Архітектором Інтернету, і є членом IAB.

Поки RFC редагуються, на них не посилаються так, як це робиться з дослідницькими академічними статтями. Також, деякі звіти, що мають відношення до Інтернету, уже публікувалися в більш ранніх, рівнобіжних серіях звітів, названих Інженерними Замітками про Інтернет або IEN. Хоча серії IEN більш не використовуються, не всі IEN були опубліковані в RFC. Посилання на IEN і RFC розкидані по всій книзі.

Обидві серії RFC і IEN нумерувалися послідовно в хронологічному порядку написання. Кожен новий або переробленому RFC призначався новий номер, тому читачам

потрібно бути упевненим у тім, що вони одержали версію документа з найбільшим номером; індекс допоможе знайти потрібну версію.

NIC поширює RFC і IEN по всьому співтовариству. Ви можете одержати RFC від NIC, пославши лист по звичайній пошті,електронній пошті або прямо зв'язавши з ним по Інтернету, використовуючи програму передачі файлів. Запитаєте експерта по локальних мережах, як одержати RFC з вашого місця або подивитеся додаток 1для подальших інструкцій про те, як одержати них.

2.2.2.8. Протоколи Інтернету і стандартизація.

Читачі, знайомі з мережами передачі даних, розуміють, що існує безліч стандартів протоколів комунікації. Багато хто з них передували Інтернету, тому виникає питання:"Чому розроблювачі Інтернету придумали нові протоколи, коли вже існує так багато міжнародних стандартів?". Відповідь складна, але нижче приведена проста максима:

Використовуйте існуючі стандартні протоколи доти, поки ці стандарти застосовні; придумуйте нові протоколи тільки тоді, коли існуючі стандарти неефективні, але приготуйтеся перейти на міжнародні стандарти, коли вони стануть доступні і забезпечать такої ж можливості.

Тому, зв'язування протоколів TCP/IP не ігнорували міжнародних стандартів. Вона з'явилася просто тому, що існуючі стандарти не задовольняли потреби. Філософія використання стандартів, коли вони з'являються, також означає, що коли з'являться міжнародні стандарти і забезпечать ту ж саму взаємну працездатність, що і TCP/IP, Інтернет перейде з TCP/IP на ці нові стандарти. Ці ідеї погодяться з політикою федерального уряду, що прийняло Профіль Відкритих Систем, що описує використання міжмережевої технології МОС скрізь, де ця технологія забезпечує можливості, еквівалентні TCP/IP.

2.2.2.9. Майбутні ріст і технологія

Як технологія TCP/IP, так і Інтернет продовжують розвиватися. Розробляються нові протоколи; переглядаються старі. NSF значно ускладнила систему, увівши свою магістральну мережу, кілька регіональних мереж, і сотні університетських мереж. Інші групи також продовжують приєднуватися до Інтернету. Сама значна зміна відбулася не через приєднання додаткових мереж, а через додатковий трафіку. Фізики, хіміки, і астрономи працюють і обмінюються об'ємами даних набагато більшими, ніж дослідники в комп'ютерних науках, що складають велику частину користувачів трафіку раннього Інтернету. Ці нові вчені привели до значного збільшення завантаження Інтернету, коли вони почали використовувати його, і завантаження постійно збільшувалося в міру того, як вони усе активніше використовували його.

Щоб пристосуватися до росту трафіку, пропускна здатність магістральної мережі NSFNET була збільшена вдвічі, привівши до того, що поточна пропускна здатність приблизно в 28 разів більше, ніж первісна; планується ще одне збільшення, щоб довести цей коефіцієнт до 30, наприкінці 1990 року. На дійсний момент важко пророчити, коли зникне необхідність додаткового підвищення пропускної здатності.

Ріст потреб у мережному обміні не був несподіваним. Комп'ютерна індустрія одержала велике задоволення від постійних вимог на збільшення обчислювальної потужності і більшого об'єму пам'яті для даних протягом довгого років. Користувачі тільки почали розуміти, як використовувати мережі. У майбутньому ми можемо очікувати постійне збільшення потреб у взаємодії. Тому будуть потрібні технології взаємодії з більшою пропускною здатністю, щоб пристосуватися до цього росту.

Малюнок 1.2 узагальнює розширення Інтернету й ілюструє важливу складового росту: зміна в складності, що виникла через те, що кілька автономних груп є частинами об’єднаного Інтернету. Вихідні проекти для багатьох підсистем припускали централізоване керування. Треба було багато зусиль, щоб доробити ці проекти для роботи при децентралізованому керуванні.

	Число мереж	Число комп'ютерів	Число керуючих

1980	10	10**2	1
1990	10**3	10**5	10
1995	10**5	10**10	100

Малюнок 1.2 Ріст об'єднаного Інтернету. Крім збільшення трафіку через збільшення розміру, Інтернет зштовхнувся зі складністю, що з'явилася результатом децентралізованого керування як при розробці, так і при роботі.

2.2.2.10 FNC і NREN

Федеральна Мережева Рада(FNC) служить для координації діяльності федеральних агентств, що фінансують дослідження або розробки в області TCP/IP і Інтернету. FNC складається з представників DARPA, NSF, NASA, DOE, DOD і HHS. Члени FNC беруть участь у зустрічах IAB і допомагають визначати пріоритети в дослідницьких і інженерних проектах Інтернету.

З огляду на потреби своїх агентств, що збільшилися, і загальнонаціональну зацікавленість у високошвидкісній обчислювальній мережі, FNC разом з лідерами цього технічного співтовариства виробив план перетворення Інтернету в Національну Дослідницьку й Освітню Мережу(NREN). Відповідно до цього плану, NREN буде розширюватися таким чином, щоб у кінцевому рахунку з'єднати всі освітні інститути і дослідницькі лабораторії. Для цього будуть потрібні більш високошвидкісні комунікаційні технології, а також перехід від фінансованих федеральним урядом магістральних мереж до засобів, що працюють на комерційній основі. FNC буде використовувати федеральні дослідницькі фонди для стимуляції досліджень і розробки необхідних технологій.

2.2.2.11. Підсумки.

Об'єднана мережа складається з набору зв'язаних мереж, що взаємодіють як єдине ціле. Головною перевагою Інтернету є те, що він забезпечує універсальне взаємне з'єднання, дозволяючи в цей же час окремим групам використовувати будь-як мережне устаткування, що найкраще підходить для їхніх цілей. Ми розглянемо принципи, що лежать в основі міжмережевої взаємодії в загальному і деталі міжмережевого зв'язування протоколів зокрема. Ми також розглянули, як міжмережеві протоколи використовуються в Інтернету. Наша демонстраційна технологія, названа TCP/IP по імені двох основних протоколів, була розроблена DARPA. Вона забезпечує основу об'єднаного Інтернету, великої, працюючої об'єднаної мережі, що з'єднує більшість науково-дослідних інститутів, включаючи багато університетських, урядових лабораторій. Об'єднаний Інтернет швидко розширюється і продовжує підтримуватися DARPA, NSF, DOE, NASA і іншими урядовими агентствами.

Література

Основна література

1) Компьютерные сети. 4-е изд. / Э. Таненбаум. — СПб.: Питер, 2003. — 992 с: ил. — (Серия Классика computer science).
2) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е издание – СПб.: Питер, 2010. – 944 с.: ил.
3) Кузин А.В. Компьютерные сети: учебное пособие. – 3-е изд. перераб. и доп. – М.: Форум: Инфра-М, 2011. – 192 с.: ил. –(Профессиональное образование).
4) Ноэл Майкл, Спенс Колин Microsoft SharePoint 2010. Полное руководство.: Пер. с англ. – М.: ООО «И.Д.Вильямс», 2011. – 880 с.: ил.- Паралел. тит. англ.
5) Джон Росс. Wi-Fi. Беспроводная сеть / Джон Росс: пер. с англ. В.А. Ветлужских. – М.: НТ Пресс, 2007. – 320 с.: ил. – (Возьми меня с собой).
6) Глушаков С.В., Хачиров Т.С. Настраиваем сеть своими руками.- М.: Изд. Act: Харьков: Фолио, 2001. – 96 с.
7) Дибров М.В. Маршрутизаторы. Учебное пособие. – Красноярск, 2008. – 389 с.

Додаткова література

8) П. Храмцов. Компьютерные сети. М.: Электроника, 1996.- 678 с.
9) М. Гук. Аппаратные средства локальных сетей (энциклопедия) Сб: Питер 2000, 576 с.
10) Буров Є. Комп'ютерні мережі – Л.: БаК, 1999.
11) Кульгин М. Технологии корпоративных сетей – СПб.: Питер, 2000.
12) Создание internet. Официальное руководство Microsoft. М: BHV. 2000, 672 с.
13) С. Золотов. Протоколы работы в Internet. Сб: BHV. 1999, 304 с.
14) Л. Куин. Fast Ethernet. М: BHV. 2000, 448 с.
15) Й. Штеффен. Internet: сотни полезных рецептов. М.: BHV. 2000, 304 с.