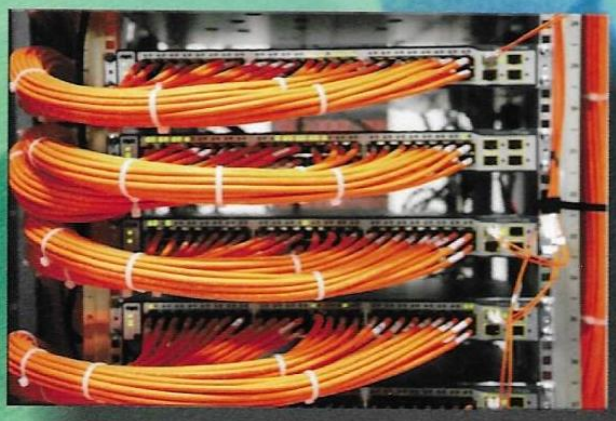
Національна Академія статистики,
обліку та аудиту
Н А С О А

В. М. Ахрамович

КОМП'ЮТЕРНІ МЕРЕЖІ

Навчальний посібник



Київ - 2010

Національна Академія статистики, обліку та аудиту

НАСОА

В.М. Ахрамович

Комп'ютерні мережі

Навчальний посібник

Київ 2010

УДК 681.324(075)

ББК 32.988.02я7

М59

Рецензенти:
д.т.н., проф. Хорошко В. О.
д.е.н, проф. Устенко С. В
д.ф.-м.н., проф. Ткач Б.П.

Схвалено Вченою радою Національної Академії статистики обліку та аудиту. (протокол № 4 від 26 листопада 2009 р.).

Ахрамович В.М. Комп'ютерні мережі: навчю посіб. /В.М.Ахрамович;

Націон. Акад. статистики, обліку та аудиту.-К.: ДП «Інформ.-аналіт.

Агентство», 2010.- 245 с. іл. – Бібліограф.: 242.

ISBN 5-94723-478-5

У навчальному посібнику викладені теоретичні та практичні аспекти комп'ютерних локальних, корпоративних та глобальних мереж. Наведена історична довідка розвитку мереж. Розкриті моделі, класифікація, концепції побудови, топологія, архітектура, складові мереж, структура, вказані основні характеристики. Розглянуті кабельні системи, мережеві адаптери, засоби об'єднання мереж, операційні системи та програмне забезпечення, протоколи, методи доступу до мереж, доступ до мережевих ресурсів, обмін даними та методики розрахунку мереж, технології їх створення й функціонування, адміністрування, підходи на основі віртуальних та безпровідних мереж. Зазначено, що розвиток корпоративних мереж безпосередньо зв’язаний з технологіями Intranet. Розглянуті аспекти перспектив розвитку мереж.

Показані можливості сучасних технологій мереж, в тому числі безпровідних, налагодження параметрів мереж і захисту інформації в мережах, керуванням доступом до ресурсів, парольний захист та використання мережевих екранів, спрощена методика теоретично-статистичного обрахунку затрат на експлуатацію мереж та розрахунку мереж на можливість появи колізій.

Для студентів різних спеціальностей, які вивчають курс «Комп'ютерні мережі», «Комп'ютерні мережі та телекомунікації», «Інформаційні мережі» і т.п.

УДК 681.324(075)

ББК 32.988.02я7

ISBN 5-94723-478-5

Вступ

Разом зі здешевленням електронно-обчислювальних машин на початку 60-х років з'явилися нові способи організації обчислювального процесу, які дозволили врахувати інтереси користувачів. Почали розвиватися інтерактивні багатотермінальні системи. У таких системах комп'ютер віддавався в розпорядження відразу декільком користувачам. Кожен користувач отримував у своє розпорядження термінал, за допомогою якого він міг вести діалог із комп'ютером. При цьому користувачеві була помітна паралельна робота з комп'ютером інших користувачів. Розділяючи, таким чином, комп'ютер, користувачі дістали можливість за порівняно невелику плату користуватися перевагами комп'ютеризації.

Термінали, вийшовши за межі обчислювального центру, розповсюдились на території підприємства. І хоча обчислювальна потужність залишалася повністю централізованою, деякі функції - такі як введення й виведення даних - стали розподіленими. Такі багатотермінальні централізовані системи зовні вже були дуже схожі на локальні обчислювальні мережі. Дійсно, рядовий користувач роботу за терміналом мейнфрейма сприймав приблизно так само, як зараз він сприймає роботу за підключеним до мережі персональним комп'ютером. Користувач міг дістати доступ до спільних файлів і периферійних пристроїв, при цьому в нього підтримувалася повна ілюзія одноосібного володіння комп'ютером, оскільки він міг запустити потрібну йому програму в будь-який момент, і майже відразу ж отримати результат.

Навіть у результаті достатнього поверхневого розгляду роботи в мережі стає ясно, що обчислювальна мережа — це складний комплекс взаємозв'язаних і погоджено функціонуючих програмних і апаратних компонентів. Вивчення мережі в цілому вимагає знання принципів роботи її окремих елементів:

- комп'ютерів;
- операційних систем;
- спеціального мережевого та комунікаційного обладнання;
- мережевих систем програм.

Увесь комплекс програмно-апаратних засобів мережі може бути описаний багатошаровою моделлю. В основі будь-якої мережі лежить апаратний шар стандартних комп'ютерних платформ. У даний час в мережах широко і успішно застосовуються комп'ютери різних класів — від персональних комп'ютерів до мейнфреймів і СуперЕОМ. Набір комп'ютерів у мережі повинен відповідати набору різноманітних завдань, що вирішуються мережею.

Другий шар — це комунікаційне устаткування. Хоча комп'ютери і є центральними елементами обробки даних у мережах, останнім часом не менш важливу роль почали грати комунікаційні пристрої. Кабельні системи, повторювачі, мости, комутатори, маршрутизатори й модульні концентратори з допоміжних компонентів мережі перетворилися на основних разом із комп'ютерами й системним програмним забезпеченням як за впливом на характеристики мережі, так і за вартістю. Сьогодні комунікаційний пристрій може бути складним спеціалізованим мультипроцесором, який потрібно конфігурувати, оптимізувати й адмініструвати. Вивчення принципів роботи комунікаційного устаткування вимагає знайомства з великою кількістю протоколів, які використовуються як у локальних, так і глобальних мережах.

Третій шар, який створює програмну платформу мережі, – операційні системи (ОС). Від того, які концепції управління локальними й розподіленими ресурсами покладені в основу мережевої ОС, залежить ефективність роботи всієї мережі. При проектуванні мережі важливо враховувати, наскільки просто дана операційна система може взаємодіяти з іншими ОС мережі, наскільки вона гарантує безпеку й захищеність даних, наскільки вона дозволяє нарощувати число користувачів, чи можна перенести її на комп'ютер іншого типу й багато інших міркувань.

Найвищий шар мережевих засобів – різні мережеві системи програм, такі як мережеві бази даних, поштові системи, засоби архівації даних, системи автоматизації колективної роботи й ін. Дуже важливо представляти діапазон можливостей, що надаються додатками для різних сфер застосування, а також знати, наскільки вони сумісні з іншими мережевими додатками й операційними системами.

Вивчення дисципліни «Комп'ютерні мережі» сприяє формуванню у студентів системи знань у галузі теорії та практики застосування і проектування сучасних мереж різних рівнів, програмних продуктів, технічних засобів у сфері управлінської діяльності.

До початку вивчення навчальної дисципліни «Комп’ютерні мережі» для спеціалістів спеціальності 7.050102 «Економічна кібернетика» студенти повинні пройти вивчення наступ-

них навчальних дисциплін, які формують відповідну базову підготовку: «Інформатика та комп'ютерна техніка» , «Захист інформації та інформаційних продуктів», «Математичне програмування», «Економіка і організація інформаційного бізнесу», «Математичні основи кібернетики», «Теорія масового обслуговування», «Системи обробки економічної інформації», «Організація інформаційного керівництва». В свою чергу вивчення дисципліни дозволить більш детально опанувати матеріал при вивченні навчальних дисциплін: «Електронна комерція», «Корпоративні інформаційні системи», «Ефективність інформаційних систем», «Управління проектами інформатизації», «Управління потенціалом підприємства»

До початку вивчення навчальної дисципліни «Комп'ютерні мережі та телекомунікації» для бакалаврів спеціальності 6.030601 «Менеджмент зовнішньоекономічної діяльності» студенти повинні пройти вивчення наступних навчальних дисциплін, які формують відповідну базову підготовку: «Інформатика та комп'ютерна техніка», «Основи менеджменту», «Системи технологій». В свою чергу вивчення дисципліни дозволить більш детально опанувати матеріал при вивченні навчальних дисциплін:«Управління персоналом», «Інформаційні системи в менеджменті», «Організація праці менеджера», «Основи зовнішньоекономічної діяльності», «Організація зовнішньоторгових операцій».

В результі вивчення дисципліни студенти повинні знати: архітектуру комп'ютерних мереж, мережеві операційні системи та спеціальне програмне забезпечення.

Студенти повинні оволодіти навичками роботи в локальних та глобальних комп'ютерних мережах з метою використання їх можливостей для отримання вихідних даних для розв'язання фахових задач, аналізу, володіти методами проектування, побудови та використання комп'ютерних мереж і захисту інформації в них .

РОЗДІЛ 1
ЛОКАЛЬНІ МЕРЕЖІ

Призначення комп'ютерної мережі

До появи комп'ютерних мереж люди обмінювалися інформацією приблизно так:

- передавали інформацію усно (усне мовлення);
- писали записки або листи (письмове спілкування);
- роздруковували кожний документ на комп'ютері ;
- записували інформацію на дискету, несли дискету до іншого комп'ютеру й копіювали в нього дані.

Комп'ютерні мережі спрощують цей процес, надаючи користувачам доступ майже до будь-яких типів даних і пристроїв. **Основне призначення комп'ютерних мереж - спільне використання ресурсів і здійснення зв'язку як усередині одного підрозділу, організації, так і за її межами.** Ресурси (resources) - це програми, дані, додатки, периферійні пристрої, такі як дисководи, принтери, модеми й т.п.

До появи комп'ютерних мереж кожний користувач повинен був мати свій принтер, сканер і інші периферійні устрої. Щоб спільно використовувати, наприклад, принтер, існував єдиний засіб - пересісти за комп'ютер, підключений до цього принтера.

Локальні обчислювальні мережі (ЛОМ) - це сукупність комп'ютерів, кабелів, мережевих адаптерів, що працюють під управлінням мережевої операційної системи й прикладного програмного забезпечення, розташовані на обмеженій території офісу чи будівлі. Для мережевої комп'ютерної системи часто використовується абревіатура NOS (Network Operating System).

У локальних мережах поняття ***інтерактивного зв'язку*** комп'ютерів - це обмін повідомленнями в реальному режимі часу; мережі дозволяють цілому ряду користувачів одночасно «володіти» програмами, базами даних, периферійними пристроями й т.п. Наприклад, якщо декільком користувачам треба роздрукувати документ, усі вони можуть звернутися до мережевого принтера.

У даний час більшість організацій береже і спільно використовує в мережевому середовищі величезні обсяги життєво важливих даних і спеціальних програм, створених для спільного використання в умовах локальних мереж, наприклад, ряд спеціальних банківських програм, програм бухобліку. От чому мережі зараз так само необхідні, як ще зовсім нещодавно були необхідні друкарські машинки й картотеки.

Концепції побудови мережі

Найпростіша мережа (network) складається як мінімум із двох комп'ютерів, сполучених один з одним кабелем. Як правило, для такого з'єднання використовували послідовні порти, один із комп'ютерів призначався **майстром,** а інший **– підлеглим.** Користувач комп'ютера-майстра мав значну перевагу в правах (міг копіювати файли та каталоги з комп'ютера-майстра на підлеглий комп'ютер і навпаки, установлювати програми на підлеглому комп'ютері, видаляти, зберігати інформацію й т.п.). Тобто таке з'єднання дозволяло їм використовувати дані спільно. Усі мережі (незалежно від складності) засновуються саме на цьому простому принципі. Комп'ютер, або сервер, або робоча станція, підключається до мережі за допомогою внутрішньої плати - мережевого адаптеру (хоча бувають і зовнішні мережеві адаптери, що підключаються до комп'ютера через паралельний порт). Мережеві адаптери перетворюють коди, які використовуються всередині комп'ютера, у послідовний потік потужних сигналів для передавання у мережі. Мережеві адаптери повинні бути сумісні з кабельною системою мережі, внутрішньою інформаційною шиною ПК (персонального комп'ютера) і мережевою операційною системою.

У мережі розрізняють: "**client**" - комп'ютер, що під'єднаний до мережі, але який не надає свої власні ресурси іншим мережевим машинам**;** "**server**"-- комп'ютер, що під'єднаний до мережі, який має ресурси, призначені для спільного використання**; "client/server**"- термін, що означає, виконання мережевої задачі розбивається на дві частини: одна виконується на робочій станції, інша - на сервері**; "file server**"- мережевий диск (диски), доступний користувачам інших комп'ютерів; "**print server"**- комп'ютер, відповідальний за мережевий друк; "**local**

resources" - (локальні ресурси) - диски, принтери й інші пристрої, пов'язані безпосередньо з робочою станцією; "**network resources** " - диск, принтер або інший пристрій, розташований на сервері, який надає ресурси іншим користувачам, на відміну від локальних ресурсів**;** "**mail server"**- серверний комп'ютер, на якому зберігаються повідомлення, які надійшли електронною поштою; **"coaxial cable"** - кабель, що складається з двох провідників: центральний провідник покритий ізоляційним прошарком і одягнений у металевий чохол другого провідника; **"repeater"** (підсилювач) - пристрій, що збільшує потужність сигналу таким чином, щоб він без перекручувань міг передаватися далі мережею; **"shielded twisted pair"** - кабель типу «скручена пара», що складається з однієї й більше пар проводів, скручених із метою поліпшення їхніх електричних характеристик; **волокнисто-оптичний кабель** (двох типів): **багатомодовий кабель (fiber optic cable multimode)** і **одномодовий кабель (fiber optic cable single mode).** "**computer name**" - ім'я, яке призначається кожному комп'ютеру мережі; "**modem**" - пристрій, що перекладає комп'ютерні сигнали в сигнали, які можна передавати лініями до такого модему, що перетворить їх у початкову форму; **"network drive"** - диск, який використовується комп'ютером, але не під'єднаний до нього безпосередньо; **"off- line"** - недоступний компонент у мережі; **"on-line"** - доступний компонент у мережі; **"operator"** - користувач, що може контролювати роботу мережі, але не має повноважень для призначення або зміни прав користувача, адміністрування; "**packets**"- дані, що передаються мережею, розбиті на порції, названі пакетами, розмір і структура пакета визначаються протоколом; **"print queue"** - черга на друк в мережі; "**protocol**" **–** це правила і технічні процедури, що дозволяють декільком комп'ютерам при об'єднанні в мережу спілкуватися один з одним. Протоколи передають дані, керуючись стандартизованими форматами, виявляють і виправляють помилки і т.д.

Відзначимо основні моменти, що стосуються протоколів:

Існує безліч протоколів. І хоча всі вони беруть участь у реалізації зв'язку, кожен протокол має:

- різні цілі;
- виконує певні завдання;
- має свої переваги й обмеження.

Функції протоколу визначаються рівнем, на якому він працює. Якщо, наприклад, якийсь протокол працює на фізичному рівні, то це означає, що він забезпечує проходження пакетів через мережеву плату та їх надходження в мережевий кабель.

Протокол передавання даних вимагає:

Синхронізацію. Під синхронізацією розуміють механізм розпізнавання початку блоку даних і його кінця.

Ініціалізацію. Під ініціалізацією розуміють установлення з'єднання між взаємодіючими партнерами. За умови, що приймач і передавач використовують однаковий протокол, синхронізація встановлюється автоматично.

Блокування. Під блокуванням розуміють розбивку інформації, яка передається, на блоки даних певної максимальної довжини (включаючи розпізнавальні знаки початку блоку і його кінця).

Адресацію. Адресація забезпечує ідентифікацію різного використовуваного устаткування, що обмінюється одне з одним інформацією під час взаємодії.

Виявлення помилок. Під виявленням помилок розуміють установку й перевірку контрольних бітів.

Нумерацію блоків. Поточна нумерація блоків дозволяє встановити втрачену або помилково передану інформацію.

Керування потоком даних. Керування потоком даних служить для розподілу й синхронізації інформаційних потоків, наприклад, якщо не вистачає місця в буфері пристрою даних, дані недостатньо швидко обробляються в периферійних пристроях, повідомлення чи запити накопичуються.

Методи відновлення. Після переривання процесу передавання даних використовують методи відновлення, щоб повернутися до певного положення для повторної передавання інформації.

Дозвіл доступу. Розподіл, контроль і керування обмеженнями доступу до даних ставляться в обов'язок пункту дозволу доступу (наприклад, "тільки передавання" або "тільки приймання").

Розподіл файлів означає, що мережа дозволяє користуватися файлами декільком користувачам. Є два способи представлення файлів: передача файлів із комп'ютера на комп'ютер та відправка файлів на проміжний пункт, де вони будуть знаходитись до того часу, поки їх не забере інший користувач.

Розподіл ресурсів - це встановлення певних пристроїв, наприклад, диску чи принтеру, таким чином, щоб усі комп'ютери мережі могли ними користуватися.

Розподіл програм - використання програми, що знаходиться на спільному диску мережі.

Спочатку комп'ютерні мережі були невеличкими й об'єднували до десяти комп'ютерів і один-два принтери. Технологія обмежувала розміри мережі, у тому числі кількість комп'ютерів у мережі і її фізичну довжину. Наприклад, на початку 1980-х років найпопулярніший тип мереж складався не більше, ніж з 30 комп'ютерів, а довжина її кабелю не перевищувала 185 м.

Одночасне опрацювання документа декількома користувачами на зорі створення локальних мереж виключалося. Подібна схема роботи називається роботою в автономному середовищі. Такі мережі легко розташовувалися в межах одного поверху будинку або невеличкої організації. Для маленьких фірм подібна конфігурація підходить і сьогодні. Ці мережі називаються **локальними обчислювальними мережами** [ЛОМ (LAN)].

При *симплексному з'єднанні* кажуть, що дані переміщуються тільки в одному напрямку. *Напівдуплексне з'єднання* дозволяє даним переміщуватися в обох напрямах, але в різний час. *Дуплексне з'єднання* дозволяє даним переміщуватися в обох напрямах одночасно.

Топологія локальних обчислювальних мереж

Топологія - геометричне відображення з'єднань у мережі. Розрізняють декілька основних типів мережевих топологій.

Перший вид - **топологія типу «шина»** (рис. 1.1). У цьому випадку всі мережеві вузли (комп'ютери) пов'язані лінійно. Це найпростіший тип топології (daisy chain), але він має свої недоліки. Якщо відбудеться ушкодження кабелю (розмикання контакту) де-небудь посеред ланцюга, мережа розірветься на окремі ділянки, і порушиться її працездатність.

Наступний вид топології - **топологія типу «кільце»** (рис. 1.2).

«Кільце» (ring) дуже схоже на «шину», проте в цьому випадку в мережі немає ні початку, ні кінця: останній вузол сполучений із першим, замикаючи в такий спосіб ланцюг у кільце.

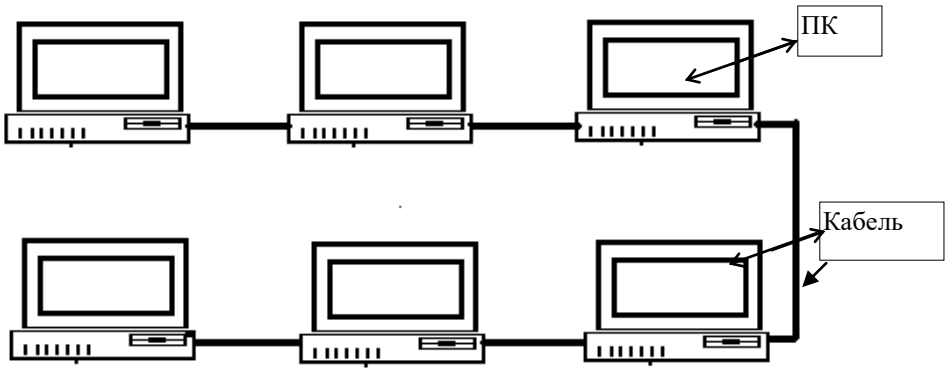


Рис. 1.1. Топологія типу « шина»

Наступний вид топології - **топологія типу «зірка»** (star) (рис. 1.3). При такому з'єднанні всі вузли пов'язані із центральним хабом (концентратором). Іншими словами, кожна мережева машина під'єднана до мережі незалежно від інших, і несправності на одній із ділянок кабелю ніяк не позначаться на роботі інших користувачів.

Наступний вид топології - **топологія типу «крапка-крапка»** (рис. 1.4).

Топологія типу крапка-крапка використовує прокладку каналів зв'язку між усіма крапками мережі, що призводить до надмірної кількості каналів зв'язку. Указаний недолік перевищує переваги даного виду з'єднання, які полягають у дуже високій надійності, за винятком випадку, коли один пристрій передає пакет усім іншим устроям при мінімальній затримці поширення сигналів.

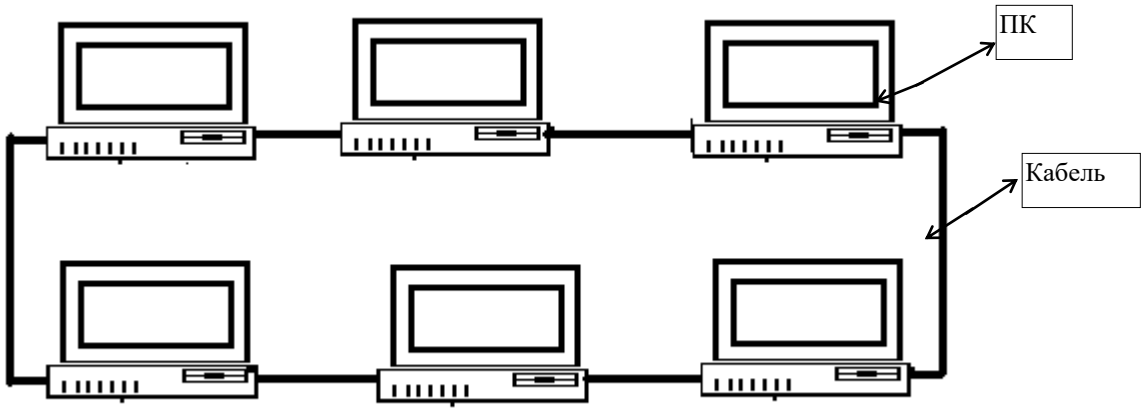


Рис. 1.2. Топологія типу « кільце»

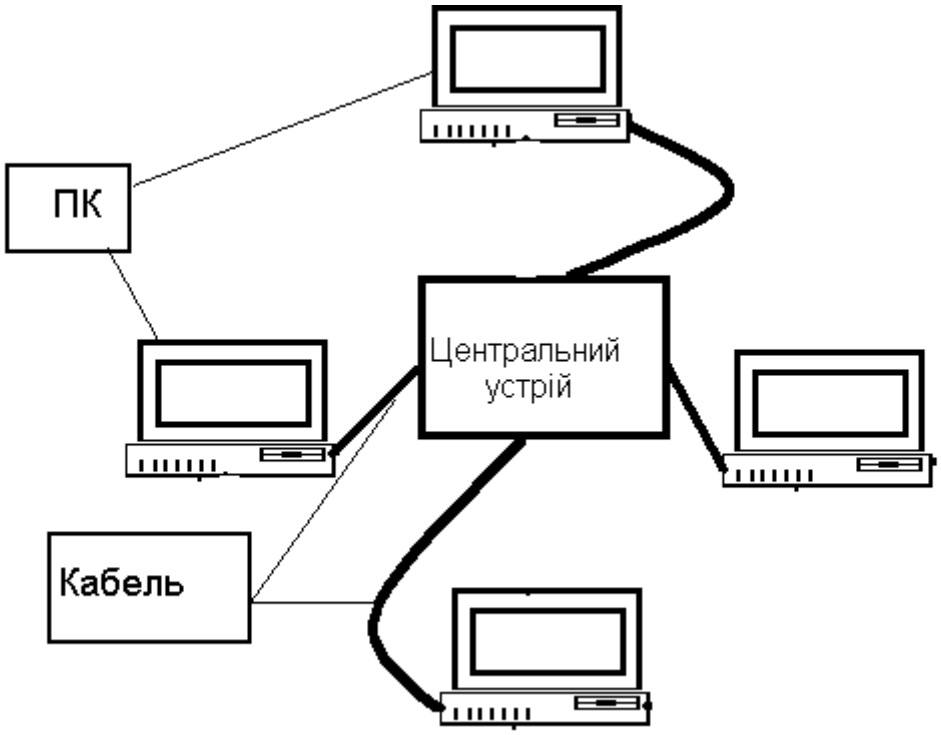


Рис. 1.3. Топологія типу « зірка»

Класифікація комп'ютерних кабельних мереж

Обчислювальні мережі класифікуються за рядом ознак. Залежно від відстаней між вузлами розрізняють такі обчислювальні мережі:

територіальні – охоплюють значний географічний простір; серед територіальних мереж можна виділити мережі регіональні й глобальні, що мають відповідно регіональні або глобальні масштаби; регіональні мережі іноді називають мережами MAN (Metropolitan Area Network), а загальна англомовна назва для територіальних мереж - WAN (Wide Area Network);

локальні (ЛОМ) – охоплюють обмежену територію (звичайно, у межах кількох десятків або сотень метрів один від одного, рідше – 1-2 км); локальні мережі позначають LAN (Local Area Network);

корпоративні (масштабу підприємства) – сукупність зв'язаних між собою ЛОМ, що охоплюють територію, на якій розміщене одне підприємство або установа в одному або декількох близько розташованих будинках.

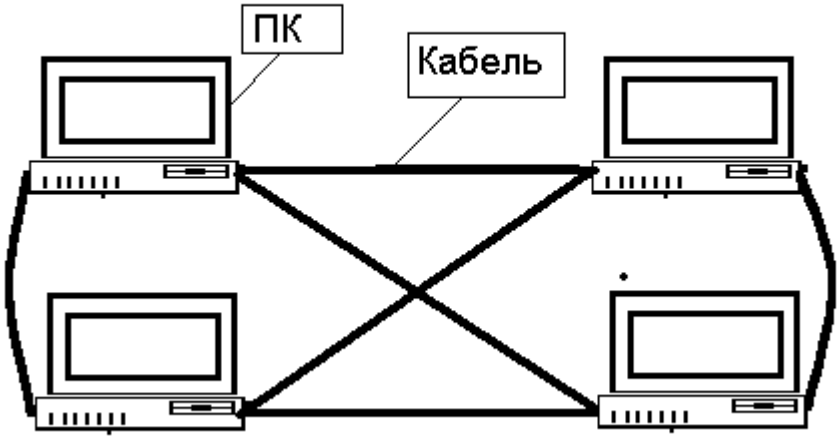


Рис. 1.4. Топологія типу «крапка-крапка»

Усі комп'ютерні мережі можуть бути класифікованими за певними ознаками:

- за порядком доступу до інформаційних ресурсів – відкриті й закриті;
- за розміщенням елементів мереж – локальні й розподілені;
- за масштабом використання – корпоративні, регіональні, державні, глобальні;
- за призначенням – загальні й спеціалізовані;
- за рівнем побудови – однорангові та із виділеними серверами (серверні);
- за використовуваним обладнанням – однорідні й різнорідні;
- за використовуваними засобами зв'язку – виділені й комутовані.

Варіанти класифікації мереж можуть бути й іншими.

Розглянемо класифікацію комунікаційних мереж за обсягом дії. Згідно поширеному підходу за обсягом дії мережі поділяються на:

- Локальні (Local Area Networks, LAN).
- Кампусні або міські (Metropolitan Area Networks, MAN).
- Глобальні (World Area Networks, WAN).

В якості критерію для оцінки обсягу мережі може бути використана максимальна відстань між будь-якою парою сусідніх пристроїв мережі (табл. 1.1).

Таблиця 1.1

Обсяг мережі

Максимальна відстань між пристроями	**Область дії**	**Тип**
10 м	Кімната	LAN
100 м	Будівля	LAN
1 км	Кампус, місто	LAN/MAN
1 ... 10 км	Місто	MAN
100 км	Країна	WAN
1.000 км	Континент	WAN
10.000 км	Планета	WAN
100.000 км	Земля та супутники	WAN

Глобальні (розподілені) мережі об'єднують у єдину систему інформаційні ресурси регіонів планети, забезпечуючи їх використання в реальному масштабі часу для всіх користувачів глобального інформаційного простору. Повністю такий простір буде сформовано, якщо інформаційні простори регіонів (країн) за своїми характеристиками досягнуть загального рівня.

Головними ознаками локальних мереж є:

- відносна простота структур мереж;
- використання каналів передавання даних зі значною швидкодією;
- високий рівень функціональної взаємодії користувачів мережі;
- розташування мережі на обмеженій території;
- відносно незначні витрати на створення мережі.

Особливо виділяють єдину у своєму роді **глобальну** мережу Internet. Це всесвітня комп'ютерна мережа, мережа мереж, що поєднує за допомогою міжмережевих інтерфейсів багато мереж. Internet охоплює американський континент, Європу, Азію. Деякі мережі, що входять до складу Internet, самі по собі великі, інші мають свої підмережі.

Вимоги до мереж

Для мереж висувається ряд вимог, серед яких треба виділити:

- конструктивну надійність;
- продуктивність;
- модульність;
- гнучкість;
- можливість масштабування;
- відсутність однієї «крапки завалення» у конструкції модульних виробів;
- маршрутизація в мережі з довільною топологією;
- локалізація трафіка й ізоляція мереж;
- узгодження різноманітних протоколів;
- керованість.

Конструктивна надійність – характерна відмінність устаткування. Вона полягає в забезпеченні працездатності мережі на визначений термін не тільки в нормальному режимі роботи, але й у режимах, коли параметри мережі виходять за межі робочих. Це досягається за рахунок застосування обладнання з визначеними характеристиками надійності та можливістю дублювання. Будь-який блок може бути продубльований. Крім того, усе устаткування, що встановлюється для виконання функцій дублювання або «гарячого резервування» для підвищення надійності не чекає часу «Ч» для того, щоб почати виконання функцій модуля, що вийшов із ладу. Воно й у звичайному режимі виконує функції основного модуля, знімаючи з нього половину навантаження, а в аварійному - цілком замінює.

Продуктивність – це спроможність мереж задовольняти потреби користувачів, тобто якісно виконувати команди з максимально можливою швидкістю на даному етапі розвитку мереж в одиницю часу з урахуванням росту числа користувачів, збільшенням кількості додатків, розширення мережевої структури.

Модульність устаткування – може мати багато рівнів вкладеності та можливості розширення мережі за рахунок нарощування модулів, що дозволяє оптимізувати витрати при переконфігурації встаткування. Завдяки цій якості виявляється така характеристика мереж **як гнучкість** та **можливість масштабування.** Блоки підтримують технології Ethernet, Fast Ethernet, Token Ring, FDDI і ATM, і т.д., забезпечуючи маршрутизацію пакетів між собою. Це дозволяє, наприклад, перейти з технології застарілої на сучасну з мінімальними витратами.

Гнучкість – структура мережі повинна дозволяти, по-перше, у разі потреби об'єднувати мережі з різною топологією, причому не тільки засобами модульних пристроїв, але й через додаткові порти в автономних концентраторах і, по-друге, без зупинки всієї системи змінювати дислокацію як окремих робочих місць із комп'ютерами, так і цілих груп комп'ютерів.

Можливість масштабування – особлива властивість устаткування, яка дозволяє розширення мережевої структури, як правило, без зупинки роботи мережі та особливих конструктивних змін, що досягається за рахунок стандартизації (уніфікації) обладнання та його модульності.

Відсутність крапки завалення. Це означає, що в мережах відсутній якийсь елемент або функціональний вузол, вихід із ладу якого призводить до припинення роботи всієї мережі.

Маршрутизація в мережах із довільною топологією. Серед протоколів канального рівня деякі забезпечують доставку даних у мережах із довільною топологією, але тільки між парою сусідніх вузлів (наприклад, протокол PPP), а деякі – між будь-якими вузлами (наприклад, Ethernet), але при цьому мережа повинна мати топологію визначеного й дуже простого типу, наприклад, деревоподібну.

При об'єднанні в мережу декількох сегментів за допомогою, наприклад, комутаторів продовжують діяти обмеження на її топологію: у мережі, що утворилася, повинні бути відсутні петлі. Дійсно, міст або його функціональний аналог - комутатор - можуть вирішувати задачу доставки пакета адресату тільки тоді, коли між відправником і одержувачем існує єдиний шлях.

У той же час наявність надлишкових зв'язків, що утворяють петлі, часто необхідна для кращого балансування навантаження, а також для підвищення надійності мережі за рахунок існування альтернативного маршруту на додаток до основного. Реалізація протоколу мережевого рівня припускає наявність у мережі спеціального пристрою - ***маршрутизатора.*** Маршрутизатори об'єднують окремі мережі в загальну складову мережу. До кожного маршрутизатора можуть бути приєднані декілька мереж (принаймні дві).

У складних мережах майже завжди існує декілька альтернативних маршрутів для передавання пакетів між двома кінцевими вузлами. Задачу вибору маршрутів із декількох можливих вирішують маршрутизатори, а також кінцеві вузли.

Керовані мережі повинні мати інтелектуальні складові, наприклад, програмні агенти для збору інформації про стан будь-яких засобів менеджменту мережі (Novell, NMS, HP OpenView, IBM NetView, Sun Net Manager і ін.). Концентратори повинні дозволяти керування й діагностику на рівні окремих портів, модулів і всього пристрою в цілому.

Локалізація трафіка й ізоляція мереж. Трафік у мережі укладається випадковим чином, проте, у ньому відбиті й деякі закономірності. Як правило, деякі користувачі, що працюють над загальною задачею (наприклад, співробітники одного відділу), найчастіше звертаються із запитами один до одного або до загального серверу, і тільки іноді вони відчувають необхідність доступу до ресурсів комп'ютерів іншого відділу. Бажано, щоб структура мережі відповідала структурі інформаційних потоків. Комп'ютери об'єднуються в групу, якщо велика частина породжуваних ними повідомлень адресується комп'ютерам цієї ж групи.

Узгодження різноманітних протоколів. Сучасні обчислювальні мережі часто будуються з використанням декількох різноманітних базових технологій - Ethernet, Token Ring або FDDI. Така неоднорідність виникає або при об'єднанні мереж, що раніше існували, які використовують у своїх транспортних підсистемах різноманітні протоколи канального рівня, або при переході до нових технологій, таких як Fast Ethernet , 100VG-AnyLAN і т.п.

Саме для утворення єдиної транспортної системи, що об'єднує декілька мереж із різноманітними принципами передавання інформації між кінцевими вузлами, і служить мережевий рівень. Коли дві або більше мережі організовують спільну транспортну службу, то такий режим взаємодії, звичайно, називають *міжмережевою взаємодією (internetworking)*. Для позначення складової мережі в англомовній літературі часто також використовується термін *інтермережа* (*internetwork* або *internet).*

Керованість. Це здатність мережі адекватно реагувати на керуючі впливи адміністраторів мережі, у тому числі, у нештатних та аварійних ситуаціях, і забезпечувати основні показники (надійність, трафік, адресацію й т.п.) у встановлених межах.

Подальший розвиток локальних мереж

Найперші типи локальних мереж не могли відповідати потребам великих підприємств, офіси котрих розташовані в різноманітних місцях. Але як тільки переваги комп'ютерних мереж стали незаперечні, і мережеві програмні продукти почали заповнювати ринок. Перед корпораціями - для зберігання конкурентноздатності - постала задача розширення мереж. З появою **Ethernet** і методу доступу **CSMA/CD**, коли всі робочі станції постійно прослуховують лінію з метою виявлення переданої інформації, була досягнута швидкість передавання до 10 Мбіт/с. Якщо в лінії виявляється сигнал, станція починає аналізувати його на предмет адреси призначення. Якщо ця інформація призначалася не їй, то станція переходить на якийсь час у режим очікування, після котрого знову "слухає" лінію. Коли станція хоче передати свої дані, вона чекає закінчення передавання, після цього починає передавати інформацію порціями визначеної довжини (пакетами або кадрами). Іноді пакети змішуються, викликаючи "**колізію**".

Мережі створюють відмінні умови для уніфікації програмного забезпечення, додатків (наприклад, текстових процесорів). Це значить, що на всіх комп'ютерах у мережі використовуються програми, додатки одного типу й однієї версії.

Інша приваблива сторона мереж - наявність програм електронної пошти й планування робочого дня. Завдяки їм керівники великих підприємств швидко й ефективно взаємодіють із численним штатом своїх співробітників або партнерів за бізнесом, а планування і коригування діяльності всієї компанії здійснюється зі значно меншими зусиллями, ніж колись.

Незважаючи на визначені подібності, мережі розділяються на чотири типи:

- Реальні (real network).
- Штучні.
- Однорангові (peer-to-peer).
- На основі серверу (server based).

Реальні мережі

Вважається, що не можна віднести до реальних мереж ту, що не потребує для своєї нормальної роботи одного-двох спеціалістів, що постійно стежать за нею. Такі мережі називаються реальними (real network або Network an Attityde (NWA)).

Одними з найпопулярніших реальних мереж є мережі NetWare фірми Novell.

Штучні мережі

Штучні мережі, виглядають і працюють як реальні мережі, але для них не потрібно спеціального мережевого жорсткого диска. Такі мережі дозволяють зв'язувати разом комп'ютери через послідовні й рівнобіжні порти й не потребують спеціальних мережевих адаптерів. Іноді зв'язок у такій мережі називають зв'язком за нуль-модемом або через нуль-слот, оскільки жодний слот машини не зайнятий мережевою платою. Самі мережі називають мережами на нуль-модемі або через нуль-слот (zero-slot networks). Представник такої мережі – мережа Laplink.

Однорангові мережі

В одноранговій мережі всі комп'ютери рівноправні: немає ієрархії серед комп'ютерів і немає виділеного серверу. Як правило, кожний комп'ютер функціонує і як клієнт, і як сервер; інакше кажучи, немає окремого комп'ютера, відповідального за адміністрування всієї мережі. Оскільки в одноранговій мережі кожний комп'ютер функціонує і як клієнт, і як сервер, користувачі повинні мати достатній рівень знань, щоб працювати і як користувачі, і як адміністратори свого комп'ютера. Усі користувачі самостійно вирішують, які дані на своєму комп'ютері зробити загальнодоступними в мережі. Однорангові мережі називають також **робочими групами**. Робоча група – це невеличкий колектив, тому в однорангових мережах найчастіше не більше 10 комп'ютерів.

Однорангові мережі відносно прості. Оскільки кожний комп'ютер є одночасно й клієнтом, і сервером, немає необхідності в потужному центральному сервері, або в інших компонентах, обов'язкових для складніших мереж. Однорангові мережі, звичайно, дешевші за мережі на основі серверу, але потребують потужніших (і дорожчих) комп'ютерів.

В одноранговій мережі вимоги до продуктивності й до рівня захисту для мережевого програмного забезпечення, як правило, нижчі, ніж у мережах із виділеним сервером.

Однорангова мережа характеризується стандартними рішеннями: користувачі самі виступають у ролі адміністраторів і забезпечують захист інформації; для об'єднання комп'ютерів у мережу застосовується проста кабельна система.

Однорангова мережа цілком підходить там, де: кількість користувачів не перевищує 10 чоловік; користувачі розташовані компактно; питання захисту даних не критичні; у доступному для огляду майбутньому не очікується значного розширення фірми й, отже, мережі. Якщо ці умови виконуються, тобто, швидше за все, вибір однорангової мережі буде правильним (ніж мережі на основі серверу). Незважаючи на те, що однорангові мережі цілком задовольняють потребам невеличких фірм, іноді виникають ситуації, коли їхнє використання може виявитися не доречним.

Можна зазначити деякі недоліки однорангових мереж, що треба мати на увазі, обираючи тип мережі. В одноранговій мережі кожний комп'ютер повинен: велику частину своїх обчислювальних ресурсів надавати локальному користувачу (який працює за цим комп'ютером); для підтримки доступу до ресурсів віддаленого користувача (який звертається до серверу) підключати додаткові обчислювальні ресурси. Усі користувачі можуть «поділитися» своїми ресурсами з іншими. До спільно використовуваних ресурсів відносять каталоги, принтери, факси-модеми й т.п. Захист ресурсів проводиться, як правило, шляхом встановлення пароля, наприклад, на каталог. Централізовано керувати захистом в одноранговій мережі дуже складно, тому що кожний користувач установлює його самостійно, та й «загальні» ресурси можуть знаходитися на всіх комп'ютерах. Така ситуація становить серйозну загрозу для всієї мережі, крім того, деякі користувачі можуть узагалі не встановити захист. Якщо

питання конфіденційності є принциповими, рекомендується вибрати мережу на основі серверу.

Мережі на основі серверу

Якщо до мережі залучено більше 10 користувачів, то однорангова мережа, де комп'ютери виступають у ролі й клієнтів, і серверів, може виявитися недостатньо продуктивною. Тому більшість мереж використовує виділені сервери. Мережа на основі серверу потребує потужніших серверів, оскільки вони повинні опрацьовувати запити всіх клієнтів мережі.

Виділеним називається такий сервер, що функціонує тільки як сервер (без функції клієнта або робочої станції). Вони спеціально оптимізовані для швидкого опрацювання запитів від мережевих клієнтів і для керування захистом файлів і каталогів.

Зі збільшенням розмірів мережі й обсягу мережевого трафіка необхідно збільшувати кількість серверів. Розподіл задач серед декількох серверів гарантує, що кожна задача буде виконуватися найефективнішим способом з усіх можливих. Задачі, що повинні виконувати сервери, різноманітні і складні. Щоб пристосуватися до зростаючих потреб користувачів, сервери у великих мережах стали спеціалізованими. Наприклад, у мережі Windows NT існують різноманітні типи серверів: файли-сервери й принт-сервери.

Файли-сервери й принт-сервери управляють доступом користувачів до файлів і принтерів відповідно. Наприклад, щоб працювати з текстовим процесором, насамперед треба запустити його на своєму комп'ютері. Документ текстового процесора, що зберігається на файлі-сервері, завантажується в пам'ять Вашого комп'ютера і, таким чином, можна працювати із цим документом на своєму комп'ютері. Іншими словами, файл-сервер призначений для збереження файлів і даних.

На серверах додатків виконуються прикладні частини клієнт-серверних додатків, а також знаходяться дані, доступні клієнтам. Наприклад, щоб спростити отримання даних, сервери зберігають великі обсяги інформації в структурованому виді. Ці сервери відрізняються від файл- і принт-серверів, в яких файл або дані цілком копіюються на комп'ютер, що здійснює запит.

Відмінності між одноранговими мережами й мережами на основі серверу мають принципове значення, оскільки визначають різні можливості вказаних мереж. Вибір типу мережі залежить від багатьох чинників: розміру підприємства; необхідного рівня безпеки: виду бізнесу; рівня доступності адміністративної підтримки; обсягу мережевого трафіка; потреб мережевих користувачів; фінансових витрат.

Кабельні системи локальних обчислювальних мереж

У проекти локальних обчислювальних мереж (стандартних) закладаються на сьогодні всього три види кабелів:

Коаксіальний (рис. 1.5) двох типів: тонкий коаксіальний кабель (thin coaxial cable); товстий коаксіальний кабель (thick coaxial cable). Тонкий коаксіальний кабель, це історично перший тип кабелів, який застосовувався в локальних мережах. Використання коаксіального кабелю вважається застарілою технологією, яка, наприклад, навіть не підтримується протоколом Fast Ethernet, але використовується в локальних мережах, які були установлені раніше.

RG-58/U, RG-58 A/U і RG-58 C/U – різновиди тонкого коаксіального кабелю для мереж Ethernet 10Base-2. Кабель RG-58/U має суцільний внутрішній провідник, а кабель RG-58 A/U — багатожильний. Усі ці різновиди кабелю мають опір 50 Ом, але володіють гіршими механічними і електричними характеристиками у порівнянні з товстим коаксіальним кабелем. Для з'єднання кабелів з устаткуванням використовується роз'єм типу BNC.

Товстий коаксіальний кабель (RG-8 і RG-11) має діаметр 12 мм і буває двох різновидів: гнучкий і жорсткий. Він має великий ступінь захисту та механічну міцність, а також дозволяє підключати новий комп'ютер до кабелю, не зупиняючи роботу мережі. Проте він складний при прокладанні, а для підключення до нього потрібний спеціальний пристрій (трансивер). Основна сфера застосування товстого коаксіального кабелю — магістральні лінії, що сполучають поверхи будівлі.

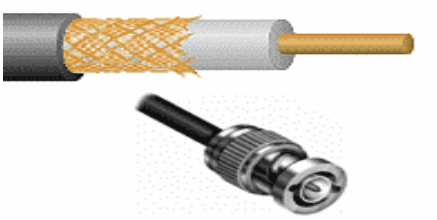


Рис. 1.5 Коаксіальний кабель

Скручена пара (рис. 1.6) двох основних типів: неекранова скручена пара (unshielded twisted pair - UTP); екранована скручена пара (shielded twisted pair - STP). Скручена пара не була новим винаходом, вона вже багато десятків років успішно використовувалася в телефонії, і залишається лише дивуватися, чому її перенесення на ґрунт Ethernet тільки в вересні 1990 року, коли був офіційно прийнятий стандарт 10baseT. Мідний неекранований кабель UTP залежно від електричних і механічних характеристик розділяється на 5 категорій. Кабелі категорій 1 і 2 були визначені в стандарті EIA/TIA-568, але до стандарту 568A вже не увійшли як застарілі.

Кабелі *категорії 1* застосовуються там, де вимоги до швидкості передавання мінімальні. Звичайно, це кабель для цифрового й аналогового передавання голосу й низькошвидкісного (до 20 Кбіт/с) передавання даних. До 1983 року це був основний тип кабелю для телефонних мереж.

Кабелі *категорії 2* були вперше застосовані фірмою IBM при побудові власної кабельної системи. Головна вимога до кабелів цієї категорії — здатність передавати сигнали зі спектром до 1 МГц.

Кабелі *категорії 3* були стандартизовані в 1991 році, коли розроблений *Стандарт телекомунікаційних кабельних систем для комерційних будівель* (EIA-568), на основі якого створений стандарт EIA-568A. Стандарт EIA-568 визначив електричні характеристики кабелів категорії 3 для частот в діапазоні до 16 МГц, що підтримують високошвидкісні мережі. Кабель категорії 3 призначений як для передавання даних, так і для передавання голосу. Крок скручування проводів рівний приблизно 3 витки на 1 фут (30,5 см). Кабелі категорії 3 зараз складають основу багатьох кабельних систем будівель.

Кабелі *категорії 4* це дещо покращений варіант кабелів категорії 3. Кабелі категорії 4 зобов'язані витримувати тести на частоті передавання сигналу 20 МГц і забезпечувати підвищену перешкодостійкість і низькі втрати сигналу. Кабелі категорії 4 добре підходять для застосування в системах зі збільшеними відстанями (до 135 метрів) і в мережах Token Ring із пропускною спроможністю 16 Мбіт/с. На практиці використовуються рідко.

Кабелі *категорії 5* були спеціально розроблені для підтримки високошвидкісних протоколів. Тому їх характеристики визначаються в діапазоні до 100 МГц. Більшість нових високошвидкісних стандартів орієнтуються на використання скрученої пари 5 категорії. На цьому кабелі працюють протоколи зі швидкістю передавання даних 100 Мбіт/с – FDDI (із фізичним стандартом TP-PMD), Fast Ethernet, 100VG-AnyLAN, а також швидші протоколи – ATM на швидкості 155 Мбіт/с, і Gigabit Ethernet на швидкості 1000 Мбіт/с (варіант Gigabit Ethernet на витій парі категорії 5 став стандартом у червні 1999 р.). Кабель категорії 5 прийшов на заміну кабелю категорії 3, і сьогодні все нові кабельні системи великих будівель будуються саме на цьому типі кабелю (у поєднанні з волоконно-оптичним кабелем).

За наявності (або відсутності) екрану, розрізняють декілька типів кабелів:

- UTP (unshielded twisted pair), що означає незахищена скручена пара (НЗВП), тобто кабель, скручені пари якого не мають індивідуального екранування;
- FTP (Foiled Twisted Pair) - фольгована скручена пара. Має загальний екран з фольги, проте у кожної пари немає індивідуального захисту;
- STP (shielded twisted pair) - захищена скручена пара (ЗВП), кожна пара має екран;
- SCTP (Screened Twisted Pair) - екранований кабель, який може як мати, так і не мати захисту окремих пар.

Екран виконується або плетеним із мідного дроту (захищає від низькочастотних наведень), або із струмопровідної фольги (плівки), яка блокує високочастотне електромагнітне випромінювання. Так само на практиці часто використовують подвійні екрани (HIGHT Screen), в яких використовуються обидва способи.

Рис. 1.6 Кабель типу «Скручена пара»

Волокнисто-оптичний кабель (рис. 1.7) буває двох типів: багатомодовий кабель (fiber optic cable multimode) і одномодовий кабель (fiber optic cable single mode). У цих типах кабелів сигнали передаються за допомогою світла, а не електрики, як в інших видах кабелів.

В одномодовому кабелі (Single Mode Fiber, SMF) використовується центральний провідник дуже малого діаметру, який можна порівняти з довжиною хвилі світла, — від 5 до 10 мкм. При цьому практично всі промені світла розповсюджуються уздовж оптичної осі світловода, не відбиваючись від зовнішнього провідника. Як джерело світла використовується напівпровідниковий лазер. Це найдорожчий тип кабелю з найвищими показниками.

У багатомодових кабелях (Multi Mode Fiber, MMF) використовуються ширші внутрішні сердечники, які легко виготовити технологічно. У багатомодових кабелях у внутрішньому провіднику одночасно існує декілька світлових променів, що відбиваються від зовнішнього провідника під різними кутами. Кут віддзеркалення променя називається модою. Як джерела випромінювання в багатомодових кабелях застосовуються світлодіоди, оскільки вони дешевші. У цілому, багатомодове волокно дешевше одномодового, хоча його характеристики гірші (більше загасання сигналу, нижча смуга пропускання).

Рис. 1.7 Волокнисто-оптичний кабель

Максимальна довжина сегмента

100 м - у кабелю із скрученими парами (табл. 1.2);
185 м - у тонкого коаксіального кабелю;
500 м - у товстого коаксіального кабелю;
1000 м - у багатомодового оптоволокнистого кабелю;
2000 м - в одномодового оптоволокнистого кабелю (із застосуванням спеціальних засобів до 40 - 90 км).

Кількість вузлів на сегменті

2 - у кабелю з скрученимиі парами; 30 - у тонкого коаксіального кабелю; 100 - у товстого коаксіального кабелю; 2 - в оптоволокнистого кабелю.

Таблиця 1.2

Характеристики кабелю для побудови локальних мереж

Тип кабелю	**Максимальна швидкість передавання**	**Максимальна довжина відрізку**	**Вартість**	**Надійність**
Скручена пара категорії 3 або 5	100 Мбіт/с	100 м	Низька	Висока
Скручена пара категорії 5, 6 або 7	1000 Мбіт/с	100 м	Середня	Висока
Багатомодовий волоконно-оптичний	1000 Мбіт/с	550 м	Висока	Висока
Одномодовий волоконно-	10000 Мбіт/с	5000 м	Висока	Висока

оптичний				
Твінаксіальний	1000 Мбіт/с	25 м	Середня	Висока
Тонкий коаксіальний	10 Мбіт/с	185 м	Низька	Низька
Товстий коаксіальний	10 Мбіт/с	500 м	Висока	Низька

Мережеві адаптери Ethernet

Мережеві адаптери виступають у якості фізичного інтерфейсу між комп'ютером і мережевим кабелем. Зазвичай вони вставляються в слоти материнських плат робочих станцій і серверів.

Щоб забезпечити фізичне з'єднання між комп'ютером і мережею, до відповідного порту адаптеру після його установки підключається мережевий кабель.

LAN-адаптери служать для виконання наступних функцій:

- підготування даних, що надходять від комп'ютера, до передавання мережевим кабелем;
- передавання даних іншому устаткуванню (комп'ютеру, концентратору, комутатору й т.п.);
- здійснює перетворення паралельного потоку даних у послідовний при передаванні в мережу й обернене перетворення при прийомі, завершуючи це перетворенням цифрових даних в електричні або оптичні за допомогою трансиверів;
- управління потоком даних між робочою станцією й кабельною системою (приймає/передає дані з кабелю й переводить їх у форму, «зрозумілу» центральному процесору).

Плата будь-якого мережевого адаптеру складається з апаратної частини й умонтованих програм, записаних у ПЗУ. Програми реалізують функції підрівнів управління логічним зв'язком і управління доступом до середовища канального (другого) рівня моделі OSI. Тим самим LAN-адаптери «покривають» собою перший (фізичний) і другий (канальний) рівні цієї моделі.

Існує велика кількість мережевих карт різних виробників, проте, за типом використовуваного протоколу канального рівня можна виділити наступні типи:

1. **Мережева карта Ethernet (Fast Ethernet).** Найпоширеніша мережева карта. Використовується в невеликих офісних і середнього розміру ЛОМ. Використання протоколу Ethernet дозволяє карті працювати на швидкості 10 Мбіт/с, а протоколу Fast Ethernet — 100 Мбіт/с.

2. **Мережева карта Token Ring (High Speed Token Ring).** Мережева карта для великих ЛОМ. Використання протоколу Token Ring дозволяє карті працювати на швидкостях 4 і 16 Мбіт/с, а протоколу High Speed Token Ring - на швидкостях 100 і 155 Мбіт/с.

3. **Мережева карта FDDI (Fiber Distributed Data Interface).** Використовується в волоконно-оптичних мережах. Протокол FDDI працює на швидкості 100 Мбіт/с.

Мережеві адаптери Ethernet пройшли в своєму розвитку три покоління.

Адаптери першого покоління були виконані на дискретних логічних мікросхемах, внаслідок чого володіли низькою надійністю. Вони мали буферну пам'ять тільки на один кадр, що приводило до низької продуктивності адаптера, оскільки всі кадри передавалися з комп'ютера в мережу або з мережі в комп'ютер послідовно. Окрім цього, конфігурування адаптера першого покоління здійснювалось уручну, за допомогою перемичок. Для кожного типу адаптерів використовувався свій драйвер, причому інтерфейс між драйвером і: мережевою операційною системою не був стандартизований.

У мережевих адаптерах другого покоління для підвищення продуктивності почали застосовувати метод багатокадрової буферизації. При цьому наступний кадр завантажується з пам'яті комп'ютера в буфер адаптера одночасно з передаванням попереднього кадру в мережу. У режимі прийому, після того як адаптер повністю прийняв один кадр, він може почати передавати цей кадр із буфера в пам'ять комп'ютера одночасно із прийомом іншого кадру з мережі.

У мережевих адаптерах другого покоління широко використовуються мікросхеми з високим ступенем інтеграції, що підвищує надійність адаптерів. Крім того, драйвери цих адаптерів засновані на стандартних специфікаціях. Адаптери другого покоління зазвичай поставляються з драйверами, що працюють як в стандарті NDIS (специфікація інтерфейсу

мережевого драйвера), розробленому фірмами 3Com і Microsoft і схваленому IBM, так і в стандарті ODI (інтерфейс відкритого драйвера), розробленому фірмою Novell.

У мережевих адаптерах третього покоління реалізована конвеєрна схема обробки кадрів. Вона полягає в тому, що процеси прийому кадру з оперативної пам'яті комп'ютера й передавання його в мережу поєднуються в часі. Таким чином, після прийому декількох перших байтів кадру починається їх передача. Це істотно (на 25-55 %) підвищує продуктивність ланцюжка оперативна *пам'ять — адаптер — фізичний канал — адаптер — оперативна пам'ять.* Така схема дуже чутлива до порогу початку передавання, тобто до кількості байтів кадру, яка завантажується в буфер адаптера перед початком передавання в мережу. Мережевий адаптер третього покоління здійснює самоналагодження цього параметра шляхом аналізу робочого середовища, а також методом розрахунку, без участі адміністратора мережі. Самоналагодження забезпечує максимально можливу продуктивність для конкретного поєднання продуктивності внутрішньої шини комп'ютера, його системи переривань і системи прямого доступу до пам'яті.

Адаптери третього покоління базуються на спеціалізованих інтегральних схемах (ASIC), що підвищує продуктивність і надійність адаптера при одночасному зниженні його вартості. Компанія 3Com назвала свою технологію конвеєрною обробкою кадрів Parallel Tasking, інші компанії також реалізували схожі схеми в своїх адаптерах.

Мережеві адаптери (рис. 1.8-1.10), що випускаються сьогодні, можна віднести до четвертого покоління. У ці адаптери обов'язково входить інтегральна схема ASIC, яка виконує функції MAC-рівня, а також велика кількість високорівневих функцій.

Мережеві карти також можна умовно розділити на мережеві карти для клієнтських комп'ютерів і мережеві карти для серверів. У мережевих картах, для клієнтських комп'ютерів значна частина роботи перекладається на драйвер мережевої карти. Наприклад, на стандартний драйвер NDIS (Network Driver Interface Specification) фірм Microsoft і 3Com, або драйвер ODI (Open Datalink Interface) фірми Novell, що використовується в мережах NetWare. Завдяки такому підходу мережева карта виявляється простішою і дешевшою, проте сильніше завантажує центральний процесор комп'ютера, який вимушений виконувати частину функцій мережевої карти замість виконання прикладних завдань користувача. Тому мережеві карти, призначені для серверів, зазвичай забезпечуються власними процесорами, які самостійно виконують велику частину функцій мережевої карти. Прикладом такої мережевої карти може слугувати мережева карта SMS EtherPower з вбудованим процесором Intel i960.

Рис. 1.8. Мережева плата Ethernet, 10 Мбіт/с з портами для кабелю на витій парі і коаксіального кабелю

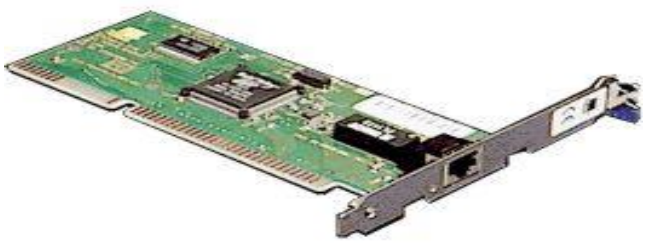


Рис. 1.9. Мережева плата Fast Ethernet, 10/100 Мбіт/с з портом для кабелю на витій парі

Рис. 1.10. Зовнішній мережевий адаптер, що приєднується до порту USB

Коротка характеристика поколінь мережевих адаптерів:

1 покоління

- Інтегральні схеми (IC).
- Буферна пам'ять на 1 кадр (~2 Кб).
- Ручне конфігурування.
- Унікальний драйвер.
- ISA (8 розрядів).
- Швидкість ~ 2 Мб/с.

2 покоління

- БІС, СБІС.
- Пам'ять на декілька кадрів (~8 Кб).
- Конфігурування за допомогою 3 параметрів для СА.
- NDIS/ODI.
- EISA (16 розрядів).
- Швидкість ~ 16 Мб/с.

3 покоління

- Спеціалізована СБІС.
- Конвеєр.
- P&P (Plug & Play) – спосіб створення або реконструкції абонентської системи швидким встановленням або заміною її компонентів. Заснована на використанні об'єктно-орієнтованої архітектури, її об'єктами є зовнішні пристрої і програми. Операційна система автоматично розпізнає об'єкти, і вносить зміни в конфігурацію абонентської системи.
- Full duplex.
- PCI (32/64 розряди).
- Швидкість 10/100 Мбіт/с.

4 покоління

- Реалізація на апаратному рівні високорівневих функцій.
- Технологія RMON.

Встановлення мережевої карти

Мережева карта вставляється у відповідний роз'єм шини даних, розташований на материнській платі. Якщо мережева карта призначена для шини даних ISA, то вставляти треба в будь-який вільний роз'єм ISA. Якщо мережева карта призначена для шини даних PCI, то вставляти треба в будь-який вільний роз'єм PCI.

Роз'єм ISA - 16bit

Роз'єм PCI

Конфігурування мережевої плати

Для нормальної роботи кожної мережевої плати їй необхідні адреса введення-виводу (In/Out port) і номер переривання (IRQ).

Конфігурування мережевої плати полягає в налаштуванні її на вільну адресу і переривання, які потім використовуватимуться операційною системою. Адреса (i/o port) і переривання (IRQ) для кожної мережевої плати повинні бути своїми, відмінними від інших пристроїв комп'ютера. Сучасні мережеві карти, що підтримують технологію Plug-n-play самі виконують цю операцію, для всіх інших необхідно самостійно проробити її.

Пошук незайнятої адреси й переривання залежить від вашого знання апаратної частини комп'ютера або програмного забезпечення на нім установленого.

Мережевий рівень і модель OSI

У моделі OSI, яку також називають *моделлю взаємодії відкритих систем* (Open Systems Interconnection - OSI) і розробленою *Міжнародною Організацією за Стандартами* (International Organization for Standardization - ISO), засоби мережевої взаємодії поділяться на **сім рівнів**, для яких визначені стандартні назви й функції.

Фізичний рівень виконує передачу бітів фізичними каналами, такими як коаксіальний кабель, скручена пара або волоконно-оптичний кабель. На цьому рівні визначаються характеристики фізичних середовищ передавання даних і параметрів електричних сигналів. Наприклад, у новій технології 100Base-TX - Fast Ethernet із передачею даних зі швидкістю до 100Мбіт/с, передавання даних провадиться двома парами проводів кабелю типу «скручена пара» категорії 5. Одна пара слугує для передавання, а інша для виявлення колізій і приймання інформації (**напівдуплексний режим**). Можливість застосування **повнодуплексного режиму** роботи з використанням чотирьох пар проводів дозволяє досягти швидкості роботи 200 Мбіт/с.

Канальний рівень забезпечує передачу кадру даних між будь-якими вузлами в мережах із типовою топологією або між двома сусідніми вузлами в мережах із довільною топологією. У протоколах канального рівня закладена визначена структура зв'язків між комп'ютерами й засоби їхніх адресацій. Адреси, що використовуються на канальному рівні в локальних мережах, часто називають MAC-адресами.

Мережевий рівень забезпечує доставку даних між будь-якими двома вузлами в мережі з довільною топологією, при цьому він не бере на себе ніяких зобов'язань щодо надійності передавання даних.

Транспортний рівень забезпечує передавання даних між будь-якими вузлами мережі з необхідним рівнем надійності. Для цього на транспортному рівні є засоби встановлення з'єднання, нумерації, буферизації й упорядкування пакетів.

Сеансовий рівень надає засоби керування діалогом, що дозволяють фіксувати, яка із взаємодіючих сторін є активною в даний момент, а також надає засоби синхронізації в рамках процедури обміну повідомленнями.

Рівень представлення. На відміну від рівнів, що лежать нижче, і які мають справу з надійним й ефективним передаванням бітів від відправника до одержувача, рівень представлення має справу із зовнішнім представленням даних. На цьому рівні можуть виконуватися різноманітні види перетворення даних, такі як компресія й декомпресія, шифрування й дешифрування даних.

Прикладний рівень - це, за суттю, набір різноманітних мережевих сервісів, наданих кінцевим користувачам і додаткам. Прикладами таких сервісів є, наприклад, електронна пошта, передавання файлів, підключення віддалених терміналів до комп'ютера в мережі.

При побудові транспортної підсистеми найбільший інтерес представляють функції фізичного, канального й мережевого рівнів, тісно пов'язані з використовуваним у даній мережі встаткуванням: мережевими адаптерами, концентраторами, мостами, комутаторами, маршрутизаторами. Функції прикладного й сеансового рівнів, а також рівня представлення реалізуються операційними системами й системними додатками кінцевих вузлів. Транспортний рівень виступає посередником між вказаними двома групами протоколів.

Мережеві операційні системи

Нижче наведено список деяких мережевих операційних систем із зазначенням їх виробників (табл. 1.3):

Таблиця 1.3

Операційні системи та їх розробники

Операційна система	**Виробник**
Apple	Apple Talk
LANtastic	Artisoft
NetWare	Novell
NetWare Lite	Novell
Personal NetWare	Novell
NFS	Sun Microsystems
OS/2 LAN Manager	Microsoft
OS/2 LAN Server	IBM
Windows	Microsoft
POWERfusion	Performance Technology
POWERLan	Performance Technology
Vines	Ba

Структура мережевої операційної системи

Мережева операційна система складає основу будь-якої обчислювальної мережі. Кожний комп'ютер у мережі в значній мірі автономний, тому під мережевою операційною системою в широкому змісті розуміється сукупність операційних систем окремих комп'ютерів, що взаємодіють із метою обміну повідомленнями й поділу ресурсів за єдиними правилами - протоколами. У вузькому змісті мережева ОС – це операційна система окремого комп'ютера, що забезпечує йому можливість працювати в мережі.

У мережевій операційній системі окремої машини можна виділити декілька частин.

- Засоби керування локальними ресурсами комп'ютера: функції розподілу оперативної пам'яті між процесами, планування й диспетчеризація процесів, керування процесорами в мультипроцесорних машинах і периферійними пристроями й інші функції управління ресурсами локальних ОС.
- Засоби надання власних ресурсів і послуг у загальне користування - серверна частина ОС (сервер). Ці засоби забезпечують, наприклад, блокування файлів і записів, що

необхідно для їхнього спільного використання; ведення довідників імен мережевих ресурсів; опрацювання запитів віддаленого доступу до власної файлової системи й бази даних; управління чергами запитів віддалених користувачів до своїх периферійних пристроїв.

- Засоби запиту доступу до віддалених ресурсів і послуг використання - клієнтська частина ОС (редиректор). Ця частина виконує розпізнавання й перенаправлення в мережу запитів до віддалених ресурсів від додатків і користувачів, при цьому запит надходить від додатка в локальній формі, а передається в мережу в інший формі, що відповідає вимогам серверу. Клієнтська частина також здійснює прийом відповідей від серверів і перетворення їх у локальний формат, так що для додатка виконання локальних і віддалених запитів нероздільне.
- Комунікаційні засоби ОС, за допомогою яких відбувається обмін повідомленнями в мережі. Ця частина забезпечує адресацію і буферизацію повідомлень, вибір маршруту передавання повідомлення мережею, надійність передавання і т.п., тобто є засобом транспортування повідомлень.

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

У такі операційні системи як Microsoft Windows NT Workstation, Microsoft Windows for Workgroups, Microsoft Windows 95, Microsoft Windows 2000, Microsoft Windows XP умонтована підтримка однорангових мереж. Для того щоб установити однорангову мережу, додаткового програмного забезпечення не потрібно.

Операційна система OS/2

Обидві мережеві ОС LAN Manager і LAN Server працюють, опираючись на OS/2. Для роботи ОС LAN Manager 2.2 потрібна OS/2 версії 1.21 або пізніші, тоді як LAN Server 3.0 вимагає OS/2 2.0. Робочі станції можуть управлятися DOS версії 3.3 або OS/2 версії 1.21.

При використанні OS/2 як операційної системи для управління файловим сервером ЛОМ з'являється можливість обслуговування запитів робочих станцій в багатозадачному середовищі, заснованому на принципі розділення пам'яті. Кожному завданню або прикладній програмі виділяються певні області пам'яті, які обслуговуються паралельно. При цьому прикладна програма складається з процесів. Важливою перевагою є простота програмного управління комп'ютерами в середовищі OS/2, навіть якщо вони використовуються як файлові сервери. Сама система OS/2 має такі позитивні риси як:

- немає обмеження пам'яті на рівні 640 Кб для прикладних програм - OS/2 версії 2.x надає користувачеві одночасний доступ до декількох сеансів DOS, кожен з яких може мати об'ємом ОЗУ 620 Кб;
- система OS/2 допускає можливість роботи в середовищі Microsoft Windows;.
- проста інсталяція з використанням графічного інтерфейсу;
- наявність віртуальної пам'яті;
- швидкий доступ до диска;
- високопродуктивна файлова система (HPFS - High Performance File System);
- підтримка національних мов (NLS - National Language Support);
- підтримка вдосконаленого механізму управління системою живлення (APM - Advanced Power Management);
- захист цілісності системи;
- швидка 32-х розрядна архітектура;
- підтримка карт розширення PCMCIA. Система OS/2 надає в розпорядження користувачеві поіменовані канали (named pipes). Користувач може інтерпретувати ці канали як файли, але насправді поіменовані канали містять повідомлення. Вони рухаються від робочих станцій до файлового сервера. На сервері прикладна програма може виконувати їх обробку.

Інтерфейс командного рядка

Для введення мережевих команд необхідно запустити програму NET з деякими параметрами. Далі наводяться найважливіші і часто використовувані варіанти команди NET з параметрами.

Команди для звичайної робочої станції

LOAD - завантажує різні мережеві протоколи;

NET CONTINUE - продовжує припинене обслуговування;
NET HELP - виводить підказку для команди;
NET NAME - надає ім'я комп'ютеру;
NET PAUSE - припиняє зв'язок з мережею;
NET PRINT - виводить чергу завдань друку або відправляє файл на друк;
NET START - запускає мережу;
WORKSTATION NET USE - виводить на екран ресурси або присвоює буквені позначення дискам або імена новим ресурсам;
UNLOAD - вивантажує мережевий протокол.

Додаткові команди для потужної робочої станції

NET ACCESS - проглядає дозвіл допуску;
NET COPY - копіює мережеві файли;
NET LOGON - приєднує до мережі;
NET LOGOFF - від'єднує від мережі;
NET PASSWORD - змінює пароль;
NET START - запускає робочу станцію або визначає, з якими робочими станціями існує з'єднання;
NET TIME - проводить синхронізацію годинників робочих станцій з годинником файлового сервера;
NET USE - виводить на екран ресурси або привласнює буквені позначення дискам;
NET VIEW - виводить на екран список серверів і їх ресурсів;
NET WHO - показує список користувачів, приєднаних до мережі.

При використанні накопичувачів адміністратор визначає, які ресурси файлового сервера можуть бути такими, що доступні.

Однією з істотних причин, через які LAN Manager і LAN Server виявилися менш популярними, ніж мережева ОС NetWare, є великий об'єм дискового простору, необхідний для зберігання програмних і конфігураційних файлів LM і LS.

NETBIOS

Поява терміну NETBIOS пов'язана з випуском фірмою IBM у 1984 році локальної мережі PCNet. NETBIOS було названо програмне забезпечення, "зашите" у мережеві адаптери, які встановлювалися на кожному комп'ютері мережі, і що дозволяє реалізувати п'ять рівнів протоколів передавання даних (включаючи сеансовий).

UNIX

Майже відразу після народження Unix розколовся на дві гілки: "прабатьківська" гілка, якою володіє "офіційний" власник торгової марки Unix - Unix System Laboratory - фактично комерційна гілка. І проект Дослідницького інституту Берклі - гілка в основному безкоштовних Unix'ів.

Некомерційні або умовно безкоштовні

BSD/OS 2.0 BSDi/386 – недорога комерційна. Добре підтримується. Підтримує бінарну сумісність з SCO.

Unix 386bsd BSD 4.3 для інтернетівської платформи NetBSD, похідна від 386bsd FreeBSD 2.1. Якісна мережа. Щоб не зв'язуватися з USL, у ньому цілком наново переписані частини ядра, на яких стояв копірайт AT&T.

Linux 2.0.30. Найпопулярніший серед безкоштовних Unix'ів. Число інсталяцій приблизно між 100 тисяч і 1 млн. Безупинне вдосконалювання силами сотень добровольців довели його до рівня досить надійної, швидкої, якісної й зручної системи, придатної для роботи як у якості графічної робочої станції, так і інтернет-сервера. Підтримує більше всіх додатків, і hardware. Підтримує специфікації iBCS, і тому може виконувати комерційні додатки для SCO, зокрема, Oracle і Informix. У Linux реалізований клієнт і сервер Netware, і Samba. Емулятором MS Windows WABI користуватися може.

Комерційні UNIXи

UnixWare 2.1 SVR4. 2 від SCO. Сумісно з Windows і Netware підтримує мультипроцесорні ПК.

Solaris 2.5 SVR4. 0 від SunSoft. Починаючи з 5-ї версії в Solaris, нарешті, прийшов Motif.

SCO Unix 4.0 SVR3. 2. Поки лідер за кількостю встановлювання серед усіх Unix'ів для ПК. Стара надійна налагоджена система. Підтримує достатньо багато hardware. Підтримує мультипроцесорні ПК. Достатньо дорога. Морально застаріла. Має проблеми з русифікацією.

Повільний ISC Unix 3.2. Надійний і компактний у роботі. Морально застарів.

Linux

Linux - це сучасна POSIX-сумісна й Unix-подібна операційна система для персональних комп'ютерів і робочих станцій.

Це мережева операційна система з мережевою віконною графічною системою X Window System. ОС Linux підтримує стандарти відкритих систем та протоколи мережі Internet, і сумісна із системами Unix, DOS, MS Windows. Усі компоненти системи, включаючи вихідні тексти, поширюються з ліцензією на вільне копіювання й встановлення для необмеженого числа користувачів.

ОС Linux широко поширена на платформах Intel PC 386/486/Pentium/Pentium Pro і завойовує позиції на ряді інших платформ (DEC AXP, Power Macintosh і ін.).

Розробка ОС Linux виконана Лінусом Торвальдсом (Linus Torvalds) з університету Хельсінкі й незліченною командою із тисяч користувачів мережі Internet, співробітників дослідницьких центрів, фондів, університетів і т.д.

Можливості ОС Linux

- надає можливість безкоштовно й легально мати сучасну ОС для використання як на роботі, так і вдома;
- має високу швидкодію;
- працює надійно, стійко, цілком без зависань;
- не схильна до вірусів;
- дозволяє використовувати цілком можливості сучасних ПК, знімаючи обмеження, властиві DOS і MS Windows із використання пам'яті машини й ресурсів процесора(ів);
- ефективно управляє багатозадачністю й пріоритетами, фонові задачі (тривалий розрахунок, передача електронної пошти за модемом, форматування дискети й т.д., і т.п.) не заважають інтерактивній роботі;
- дозволяє легко інтегрувати комп'ютер у локальні й глобальні мережі, у т.ч. у Internet; працює з мережами на базі Novell і MS Windows;
- дозволяє виконувати подані у форматі завантаження прикладної програми інших ОС - різноманітних версій Unix, DOS і MS Windows;
- забезпечує використання великого числа різноманітних програмних пакетів, накопичених у світі Unix, які вільно поширюються разом із вихідними текстами;
- надає багатий набір інструментальних засобів для розробки прикладних програм будь-якого ступеня складності, включаючи системи класу клієнт-сервер, об'єктно-орієнтовані, із багатовіконним текстовим або графічним інтерфейсом;
- надає можливість всім бажаючим спробувати свої сили в розробці, організувати спілкування і спільну роботу через Internet із будь-якими з розроблювачів ОС Linux і зробити свій внесок, ставши співавтором системи.

Мережі NETWARE

Однією з перших комерційних мережевих ОС, що дозволили будувати мережі довільної топології, і такі, що складаються з різнорідних комп'ютерів, була ОС Nowell NetWare. Якщо раніше мережеві ОС сильно залежали від конкретної конфігурації мережі, то ОС Nowell NetWare стала першою універсальною мережевою ОС. У цих системах один із мережевих комп'ютерів повинен функціонувати винятково як сервер. Після з'єднання з мережею NetWare отримується доступ до фізичних і логічних ресурсів усередині мережі. Визначення кожного ресурсу втримується в базі даних, що використовується операційною системою NetWare. Засіб взаємодії з ресурсами бази даних багато в чому залежить від того, яка версія операційної системи NetWare використовується. Після

вмикання комп'ютера, необхідно провести його реєстрацію, яка проводиться в діалоговому режимі. ОС NetWare здатна підтримувати робочі станції, керовані DOS, Windows, OS/2, UNIX, Mac System 7 і іншими ОС.

Будь-яка мережева карта, що має драйвер ODI (Open Datalink Interface) може використовуватися в мережах Nowell. NetWare допускає використання понад 200 типів мережевих адаптерів, більш ніж 100 типів дискових підсистем для зберігання даних, пристроїв дублювання даних і файлових серверів. У NetWare розрізняють три типи накопичувачів: локальні накопичувачі, мережеві накопичувачі і пошукові накопичувачі. Локальні накопичувачі фізично підключені до робочих станцій. Мережеві накопичувачі - це накопичувачі на жорстких дисках файлового сервера. Аналогічно тому, як в DOS застосовується засіб PATH для завдання списку накопичувачів і директорій, в яких за замовчуванням розшукуються прикладні програми, в ОС NetWare використовується поняття пошукового накопичувача.

Завдяки такій універсальності ОС швидко завоювала ринок, і довгий час залишалася основною ОС для локальних мереж. З 1990 року навіть фірма IBM почала перепродувати NetWare, і по сьогоднішній день ця ОС використовується достатньо широко.

Поточною версією ОС є NetWare 5.x. Окрім зручного графічного інтерфейсу, ця версія NetWare має ряд інших характерних особливостей:

1) NetWare 5.0 використовує як основний мережевий протокол TCP/IP (протокол, використовуваний в мережі Internet). Якщо попередні версії NetWare працювали на власному протоколі фірми Novell - протоколі IPX/SPX, а протокол TCP/IP міг використовуватися тільки поверх IPX/SPX (також емулювався NETBIOS), то тепер NetWare 5.0 пропонує наступні варіанти:

- тільки протокол TCP/IP;
- сумісне використання протоколів TCP/IP і IPX/SPX (обидва протоколи працюють паралельно й незалежно);
- тільки протокол IPX/SPX.

2) У NetWare використовується служба каталогу NDS (Nowell Directory Service), яка є єдиною розподіленою базою даних у вигляді дерева каталогів, в якій описуються всі об'єкти мережі (користувачі, групи користувачів, принтери і так далі) з вказівками прав доступу. База даних NDS є загальною для всієї мережі. Якщо в попередніх версіях NetWare 3.x і 2.x необхідно було створювати обліковий запис користувача (ім'я і пароль) на кожному сервері мережі, то в NetWare 5.0 достатньо один раз зареєструвати користувача в NDS і він дістане доступ до всіх серверів мережі.

3) У NetWare використовується потужна й гнучка модель розмежування доступу. Система безпеки підключення до мережі включає: обмеження на термін дії і частоту зміни пароля, заборону на повторне використання старих паролів, обмеження часу доби і адрес комп'ютерів, з яких користувач може підключатися до мережі, заборона одному і тому ж користувачеві на підключення до мережі з декількох машин одночасно. Система безпеки файлової системи дозволяє для кожного файлу й каталогу призначити різним користувачам будь-яку комбінацію наступних прав доступу: читання, запис, створення, видалення, модифікація (імені файлу і його атрибутів), перегляд вмісту каталогу), зміна прав доступу, супервізор (повний набір всіх прав). Аналогічно регулюється доступ і до будь-яких інших об'єктів NDS (права на перегляд, створення, видалення, перейменування об'єктів, читання, запис, порівняння і додавання їх властивостей, права супервізора). NetWare має також двосторонню систему аудиту: зовнішні незалежні аудитори можуть аналізувати події в мережі, не маючи доступу до секретних даних, у той же час і мережі не мають доступу до даних аудиту.

4) У NetWare 5.0 підтримуються як традиційні томи (аналог логічних дисків), так і томи NSS (Novell Storage Services). Традиційні томи забезпечують надійну файлову систему, засновану на обробці транзакцій (при збої файли відновлюються в стан "до збою"), стискування файлів і систему віддзеркалення дисків (дані паралельно пишуться на два різні вінчестери: при пошкодженні одного інформація буде читатися з іншого). Томи NSS можуть мати розмір до 8 терабайт і зберігати до 8 трильйонів файлів. Доступ до томів NSS здійснюється набагато швидше, ніж до традиційних томів. CD-ROM і розділи DOS можуть вмонтовуватися як томи NSS .

5) У NetWare 5.0 реалізована розподілена система друку NDPS (Novell Distributed Print Services), яка була розроблена спільно з компаніями Hewlett-Packard і Xerox і дозволяє реалізувати:

- двосторонній обмін даними (комп'ютер має можливість передавати дані на принтер і принтер має можливість передавати дані в комп'ютер).

- сповіщення про події (принтер в мережі має можливість оповістити технічний персонал, наприклад, про те, що кінчився тонер).
- автоматичне завантаження драйверів принтера, шрифтів і ін. ресурсів на комп'ютери, яким потрібно проводити друк документів.

6) У комплект постачання NetWare 5.0 входить потужний і простий у використанні Web-сервер FastTrack Server for NetWare, тісно інтегрований з NDS і такий, що підтримує більшість мов розробки застосувань для Web. FastTrack Server покликаний замінити собою Novell Web Server, що використовувався в попередніх версіях NetWare.

7) До складу сервера NetWare 5.0 входить віртуальна машина Java, що дозволяє запускати застосування і аплети Java на сервері. Наприклад, графічна утиліта управління сервером ConsoleOne написана на мові Java.

Мережа LANtastic

Artisoft LANtastic найпопулярніша операційна система для однорангових мереж, які базуються на DOS і не потребують виділення під сервер спеціальної машини. Вона ідеально підходить для мережі, що включає від 2 до 15 користувачів, хоча може підтримувати 100 і більше машин. Система LANtastic розроблена фірмою Artisoft. При збільшенні кількості комп'ютерів, які працюють в мережі, продуктивність мережі різко знижується. Для покращення вказаного показника використовують декілька файл-серверів в мережі. При введені команди *net* без параметрів з командного рядка автоматично активізується ОС LANtastic, *net mgr* ОС вимагає введення паролю. Можливий захист даних на рівні доступу до файлів та каталогів, в тому числі, за годинниковим графіком.

ОС LANtastic вимагає дуже невеликого об'єму пам'яті і має засоби для розділення накопичувачів типу CD-ROM. Фірма Artisoft пропонує мережеві адаптери Ethernet, які працюють особливо добре з ОС LANtastic. Є можливість включення комп'ютерів Macintosh в ЛОМ, керовану ОС LANtastic. Ця система сумісна із Windows.

Технічна підтримка ОС LANtastic включає електронну дошку оголошень, до якої можна дістати доступ за допомогою модему, і телефонні консультації фірми Artisoft у відділі підтримки користувачів.

Можливості ОС LANtastic

Версія 4.0, випущена в липні 1991 року, дає можливість роботи з прикладними програмами Windows. Працюючи в ній, можна керувати мережею, чергами друку, електронною поштою простим натисненням кнопок миші. Фірма Artisoft почала продаж версії 5.0 ОС LANtastic в березні 1993 року. У цій версії додані засоби для організації роботи ОС LANtastic в ЛОМ NetWare на базі файлових серверів і можливості для розділення в ЛОМ графічних і текстових даних прикладних програм пакету Windows. У квітні 1994 року фірма Artisoft випустила версію 6.0 ОС LANtastic. Нова версія має більшу швидкодію, чим попередні, і надає орієнтовані на застосування в середовищі Windows утиліти для управління ресурсами ЛОМ. Є шлюз до цифрового текстового пейджера - можна викликати з допомогою пейджера співробітників, відсутніх в даний момент за робочими станціями.

У версії 6.0 ОС LANtastic передбачено засоби для роботи з факсами в ЛОМ. Для цього необхідно встановити факс/модем на ПК, що являється сервером, завантажити додатковий модуль LANtastic для обслуговування факсимільного апарату і можна починати приймати і відправляти факси зі всієї ЛОМ. Нова версія ОС LANtastic надає більше засобів для управління сервером, включаючи контроль використання його ОЗУ. Цей засіб дозволяє максимізувати об'єм пам'яті, яку може використовувати сервер для прискорення обробки запитів файлів. Версія 6.0 ОС LANtastic також містить власний модуль SHAR.EXE, що має вищу швидкодію, ніж програма SHARE з DOS, хоча із нею ця ОС також може працювати.

У своєму складі ОС LANtastic містить багато корисних мережевих утиліт, що мають інтерфейс з користувачем через систему меню або із командного рядка DOS. Є також засоби для організації між користувачами ЛОМ діалогу за допомогою клавіатури, електронна пошта і засоби для виконання адміністративних функцій. Окрім цього, ОС LANtastic включає резидентну програму LANPUP використання "гарячих клавіш" для доступу до системи меню мережевих утиліт.

Система меню в ОС LANtastic

При запуску команди NET без параметрів автоматично активується система меню ОС LANtastic. Меню Main Functions в ОС LANtastic має наступні опції та команди (табл. 1.4):

- мережеві накопичувачі і принтери;
- управління чергами друку;
- поштова служба;
- переговори з іншими користувачами;
- приєднання/вихід з системи;
- управління реєстрацією користувачів;
- огляд дій сервера Команди мережевої ОС LANtastic.

Таблиця 1.4

Деякі команди ОС LANtastic.

Команда	**Функція**
ATTACH	Виділити всі доступні диски на сервері
AUDIT	Помістити контрольну інформацію в log-файл
CHANGEPW	Змінити пароль
CHAT	Почати набирати повідомлення іншому користувачеві
CLOCK	Синхронізувати годинник робочої станції з годинником файлового сервера
COPY	Копіювати файл з сервера на робочу станцію
DETACH	Відмінити перепризначення мережевих накопичувачів
DIR	Аналог команди DIR DOS, але показує також мережеву інформацію і атрибути файлів
DISABLEA	Відмінити псевдонім
EXPAND	Визначити повний шлях до файлу
HELP	Видати підказку
INDIRECT	Дозволяє створити непрямий (indirect) файл, тобто що містить посилання на файл в іншій директорії. Якщо вказати прикладній програмі використовувати непрямий файл, то ОС LANtastic, переприз-

	начивши його, в дійсності звертатиметься до того файлу, на який наведено посилання. Таким чином, ця команда дозволяєте дістати доступ до файлів в інших директоріях без зміни поточної директорії.
LOGIN	Почати мережевий сеанс
LOGOUT	Закінчити роботу ЛОМ
LPT TIMEOUT	Задати тривалість перерви для спулера друку ОС LANtastic, після закінчення якого друк файлу вважається закінченим
MAIL	Передати поштове повідомлення
MESSAGE	Вирішити дозволити або заборонити повідомлення про надходження чергового поштового повідомлення
POSTBOX	Повідомити про поштові повідомлення, що надійшли
PRINT	Аналогічна команді PRINT в DOS
QUEUE HALT	Зупинити мережевий спулер друку
QUEUE PAUSE	Тимчасово припинити мережевий спулер друку
QUEUE RESTART	Відновити роботу спулера друку
QUEUE STATUS	Показати чергу друку
RECEIVE	Показати останнє мережеве повідомлення
RUN	Запустити DOS-програму на вказаному сервері
SEND	Послати повідомлення іншому користувачеві ЛОМ
SHOW	Повідомити про конфігурацію робочої станції в ЛОМ, до яких серверів вона приєднана, і показати список серверів

SHUTDOWN	Задати зупинку або перезавантаження файлового сервера
UNUSE	Відмінити перепризначення накопичувачів на жорстких дисках і принтерів
USE	Провести перепризначення накопичувачів на жорстких дисках і принтерів ЛОМ

Мережа Windows for Workgroups

Робота мережі забезпечується програмами операційних систем **Windows 3.X, Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP.** Як правило, відразу при запуску системи машина автоматично запитує **Login** name (те ж саме, що й user ID) і **пароль**.

Налаштування мережі Windows for Workgroups проводиться через **панель керування**, піктограму "**мережа**". У діалогове віконце на робочій станції уводиться ім'я машини й номер робочої групи; проводиться налагодження відповідних служб і протоколів; налагоджуються мережеві адаптери, прив'язки; у протоколі TCP/IP для кожного мережевого адаптеру вказують IP адресу робочої станції, маску підмережі, основний шлюз, настроюють службу DNS, указуючи ім'я вузла, домен, порядок пошуку служби DNS, адреса WINS, параметри маршрутизації. Для одержання доступу до мережі двічі клацніть піктограму **"Мережеве оточення"** на робочому столі, а потім двічі клацніть значок комп'ютера, ресурси якого необхідно використати. Якщо потрібного комп'ютера немає в списку, двічі клацніть піктограму "**Вся мережа"**.

Мережеві протоколи
Стек протоколів TCP/IP

Стек TCP/IP включає два основні протоколи:

- TCP (Transmission Control Protocol) – протокол для гарантованої доставки даних, розбитих на послідовність фрагментів. Відповідає транспортному рівню.
- IP (Internet Protocol) – протокол для передавання пакетів, відноситься до розряду мережевих протоколів.

Стек був розроблений з ініціативи Міністерства оборони США (Department of Defence, Do) близько 30 років тому для зв'язку експериментальної мережі ARPAnet з іншими сателітними мережами як набір загальних протоколів для різнорідного обчислювального середовища. Мережа ARPA підтримувала розроблювачів і дослідників у військових областях. У мережі ARPA зв'язок між двома комп'ютерами здійснювалася з використанням протоколу Internet Protocol (IP), що й донині є одним з основних у стеку TCP/IP і фігурує в назві стека.

Великий внесок у розвиток стека TCP/IP вніс університет Берклі, реалізувавши протоколи стека у своїй версії ОС UNIX. Широке поширення ОС UNIX призвело й до широкого поширення протоколу IP і інших протоколів стека. На цьому ж стеку працює всесвітня інформаційна мережа Internet, чий підрозділ Internet Engineering Task Force (IETF) вносить основний внесок в удосконалювання стандартів стека, що публікуються у формі специфікацій RFC.

Стек TCP/IP є промисловим стандартним набором протоколів, які забезпечують зв'язок у неоднорідному середовищі (рис. 1.11), тобто забезпечують сумісність між комп'ютерами різних типів. Крім того, TCP/IP:

- представляє доступ до ресурсів Інтернет;
- підтримує маршрутизацію й зазвичай використовується як міжмережевий протокол.

Документи RFC описують внутрішню роботу мережі Internet. Деякі RFC описують мережеві сервіси або протоколи, і їхню реалізацію, у той час як інші узагальнюють умови

застосування. Стандарти TCP/IP завжди публікуються у вигляді документів RFC, але не всі RFC визначають стандарти мереж.

У даний час стек TCP/IP поширений не тільки в мережах з ОС UNIX, але й в мережах Windows.

Роль стека TCP/IP пояснюється наступними його властивостями:

- Це найбільше завершений стандартний і в той же час популярний стек мережевих протоколів, що має багаторічну історію.
- Майже всі великі мережі передають основну частину свого трафіка за допомогою протоколу TCP/IP.
- Це метод одержання доступу до мережі Internet.
- Цей стек є основою для створення Intranet-корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet.
- Усі сучасні операційні системи підтримують стек TCP/IP.
- Це гнучка технологія для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів.
- Це стійке міжплатформове середовище, яке масштабується, для додатків клієнт-сервер.

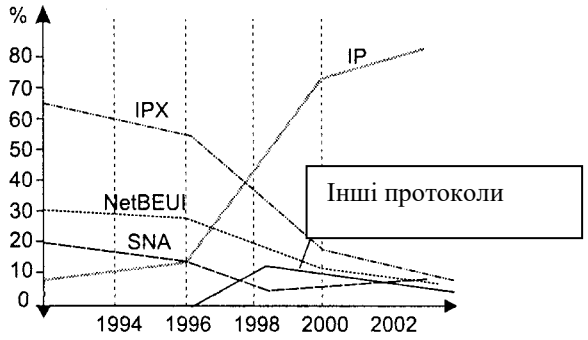


Рис. 1.11. Стек TCP/IP стає основним засобом побудови мереж

Структура стека TCP/IP

Оскільки стек TCP/IP був розроблений до появи моделі взаємодії відкритих систем ISO/OSI, хоча він також має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделі OSI достатньо умовне.

Протоколи TCP/IP діляться на 4 рівні.

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

Наступний рівень (***рівень III***) – це рівень міжмережевої взаємодії, що займається передаванням пакетів із використанням різноманітних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку й т.п. В якості основного протоколу мережевого рівня (у термінах моделі OSI) у стеку використовується протокол **IP**, що споконвічно проектувався як протокол передавання пакетів у складних 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 спроможність низькошвідкисних ліній зв'язку. Протокол IP є дейтаграмним протоколом, тобто

він не гарантує доставку пакетів до вузла призначення, але намагається це зробити. Протокол RIP слугує для знаходження найкращого шляху між відправником та отримувачем повідомлення. Він розраховує число переходів від даного маршрутизатора до інших. Підтримує не більше п'ятнадцяти переходів, в разі необхідності посилає широкомовні запити в мережі. Протокол OSPF також призначений для обміну інформацією маршрутизаторами. Він зберігає схему маршруту і передає повідомлення машрутизаторам в разі її зміни.

Наступний рівень (***рівень II***) називається основним. На цьому рівні функціонують протокол керування передаванням **TCP** (Transmission Control Protocol) і протокол дейтаграм користувача **UDP** (User Datagram Protocol). Протокол TCP забезпечує надійне передавання повідомлень між віддаленими прикладними процесами за рахунок утворення віртуальних з'єднань. Для передавання даних між комп'ютерами встановлюється зв'язок:

- комп'ютер-відправник посилає сегмент TCP отримувачу, де міститься початковий номер сегментів, які передаються, та розмір вікна TCP;
- комп'ютер-отримувач повертає сегмент TCP та повідомляє свій розмір вікна TCP і повідомлення про отримання сегмента TCP;
- комп'ютер-відправник посилає сегмент TCP, який підтверджує номер сегмента TCP відправника.

Таким чином, встановлюється зв'язок між комп'ютерами. Після закінчення сеансу зв'язку сеанс обміну повідомленнями повторюється в зворотному порядку.

Протокол UDP забезпечує передавання прикладних пакетів дейтаграмним засобом, як і IP, і виконує тільки функції сполучного ланцюга між мережевим протоколом і численними прикладними процесами.

Верхній рівень (***рівень I***) називається прикладним. За довгі роки використання в мережах різноманітних країн і організацій стек TCP/IP нагромадив велику кількість протоколів і сервісів прикладного рівня. До них відносять такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, який використовується в електронній пошті мережі Internet, гіпертекстові сервіси доступу до віддаленої інформації, такі як WWW і багато інші. Для передавання даних в Windows XP використовуються два підход Net BIOS і сокет Windows в залежності від додатків, які використовуються.

Стисла характеристика інших протоколів

До рівня міжмережевої взаємодії відносять і всі протоколи, пов'язані з упорядкуванням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації **RIP** (Routing Internet Protocol) і **OSPF** (Open Shortest Path First), а також протокол міжмережевих керуючих повідомлень. **ICMP** (Internet Control Message Protocol) протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі й вузлом – джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості складання пакета із фрагментів, про аномальні розміри параметрів, про зміну маршруту пересилки й типу обслуговування, про стан системи й т.п.

Протокол пересилання файлів **FTP** (File Transfer Protocol) реалізує віддалений доступ до файлу. Для того щоб забезпечити надійне передавання, FTP використовує в якості транспорту протокол з установленням з'єднань – TCP. Крім пересилання файлів протокол FTP пропонує й інші послуги. Так, користувачу надається можливість інтерактивної роботи з віддаленою машиною, наприклад, він може роздрукувати вміст її каталогів. Нарешті, FTP виконує аутентифікацію користувачів. Для одержання доступу до файлу, відповідно до протоколу, користувачі повинні повідомити своє ім'я й пароль. Для доступу до спільних каталогів FTP-архівів Internet парольна аутентифікація не потрібна, і її обходять за рахунок використання для такого доступу визначеного імені користувача Anonymous (Анонімний).

У стеку TCP/IP протокол FTP пропонує найширший набір послуг для роботи з файлами, проте він є й найскладнішим для програмування. Додатки, яким не потрібні всі можливості FTP, можуть використовувати інший, більш економічний протокол – найпростіший протокол пересилання файлів **TFTP** (Trivial File Transfer Protocol). Цей протокол реалізує тільки передавання файлів, причому в якості транспорту використовується простіший, ніж TCP, протокол без установлення з'єднання – UDP.

Протокол **telnet** забезпечує передавання потоку байтів між процесами, а також між процесом і терміналом. Найчастіше цей протокол використовується для емуляції термінала віддаленого комп'ютера. При використанні сервісу telnet користувач фактично керує віддаленим комп'ютером так само, як і локальний користувач, тому такий вид доступу потребує гарного захисту. Тому сервери telnet завжди використовують як мінімум парольну аутентифікацію, а іноді й потужніший засіб захисту, наприклад, систему Kerberos.

Протокол **SNMP** (Simple Network Management Protocol) використовується для організації мережевого керування. З самого початку протокол SNMP був розроблений для віддаленого контролю й керування маршрутизаторами Internet, які традиційно часто називають також шлюзами. З ростом популярності протокол SNMP стали застосовувати й для керування будь-яким комунікаційним устаткуванням – концентраторами, мостами, мережевими адаптерами й т.д. Проблема керування в протоколі SNMP розділяється на дві задачі.

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

Друга задача пов'язана з контрольованими змінними, що характеризують стан керованого пристрою. Стандарти регламентують, які дані повинні зберігатися й накопичуватися в пристроях, імена цих даних і синтаксис імен. У стандарті SNMP визначена специфікація інформаційної бази даних керування мережею. Ця специфікація, відома як база даних MIB (Management Information Base), визначає ті елементи даних, які керований пристрій повинен зберігати, і припустимі операції над ними.

Стек IPX / SPX фірми Novell включає:

- IPX (Internetwork Packet Exchange) – протокол міжмережевого передавання пакетів, відповідає транспортному рівню й визначає формат кадрів, які передаються в мережі. На рівні IPX робочі станції обмінюються блоками даних без підтвердження.
- SPX (Sequenced Packet Exchange) – протокол послідовного обміну пакетами. Відповідає мережевому рівню. Перед початком обміну PC установлюють між собою зв'язок. На рівні протоколу SPX гарантована доставка передаваних в мережі кадрів. При необхідності виконується повторне передавання.
- Стек IPX / SPX підтримує маршрутизацію й використовується в мережах Novell.

Протокол NETBIOS

NETBIOS (Network Basic Input/Output System) – базова система введення/виводу. Призначений для передавання даних між ПК, виконує функції мережевого, транспортного й сеансового рівнів. Цей протокол надає програмам засобу здійснення зв'язку з іншими мережевими програмами.

NETBEIU – розширений інтерфейс NETBIOS – невеликий швидкий і ефективний протокол транспортного рівня, який поставляється зі всіма мережевими продуктами Microsoft. Основний недолік – він не підтримує маршрутизацію. NWLink – реалізація IPX / SPX фірмою Microsoft. Це транспортний протокол, що маршрутизується.

Методи доступу до мережі

CSMA/CD

Комп'ютери «прослуховують» канал. Найчастіше відразу декілька ПК мережі хочуть передати дані, звідси – множинний доступ. При передаванні прослуховується канал із метою виявлення колізії – накладання пакетів один на одного.

Маркерний доступ

Суть маркерного доступу полягає в тому, що пакет особливого типу (маркер) переміщається по замкнутому колу, минувши за чергою всі ПК, до тих пір, поки його не отримає той, який хоче передати дані. Алгоритм взаємодії робочих станцій ЛОМ при використанні маркерного методу полягає в наступному:

1. Передавальна робоча станція змінює стан маркера на зайнятий і додає до нього пакет даних.
2. Зайнятий маркер із пакетом даних проходять через усі ПК мережі, поки не досягне адресата.

3. Після цього ПК, що приймає, посилає передавальному ПК повідомлення, де підтверджується факт прийому.
4. Після отримання підтвердження, передавальний ПК створює новий вільний маркер і повертає його в мережу.

Пакет як основна одиниця інформації в мережах

При обміні даними як між ПК в ЛОМ, так і між ЛОМ будь-яке інформаційне повідомлення розбивається програмами передавання даних на невеликі блоки даних, які називаються *пакетами* (рис. 1.12). Зв'язано це з тим, що дані зазвичай містяться у великих за розмірами файлах і якщо комп'ютер, який передає, надішле його цілком, то він надовго заповнить канал зв'язку й «зв'яже» роботу всієї мережі, тобто перешкоджатиме взаємодії інших учасників мережі. Окрім цього, виникнення помилок при передаванні великих блоків викличе великі витрати часу.

Пакет – основна одиниця інформації в комп'ютерних мережах. При розбитті даних на пакети швидкість їх передавання зростає на стільки, що кожен комп'ютер мережі отримує можливість приймати, і передавати дані практично одночасно з останніми ПК.

При розбитті даних на пакети мережева ОС до даних, які передаються, додає спеціальну інформацію:

- заголовок, у якому указується адреса відправника, а також інформація зі збору блоків даних у початкове інформаційне повідомлення при їх прийомі одержувачем;
- трейлер, у якому міститься інформація для перевірки безпомилковості в передаванні пакету. При виявленні помилки передавання пакету повинно повторитися.

Перемикання з'єднань

Перемикання з'єднань використовується мережами для передавання даних. Воно дозволяє засобом мережі розділити один і той же фізичний канал зв'язку між багатьма пристроями. Розрізняють два основні способи перемикання з'єднань:

- перемикання ланцюгів (каналів);
- перемикання пакетів.

Перемикання ланцюгів (рис. 1.13) створює єдине безперервне з'єднання між двома мережевими пристроями. Поки ці пристрої взаємодіють, жодне інше не може скористатися цим з'єднанням для передавання власної інформації – воно вимушене чекати, поки з'єднання звільниться, і настане його черга приймати дані.

Простий приклад перемикання ланцюгів – це перемикачі для принтерів, що дозволяють декільком ПК використовувати один принтер. Одночасно із принтером може працювати тільки один ПК. Який саме – вирішить перемикач, який прослуховує сигнали ПК, і як тільки надходить сигнал з одного з них, він автоматично його під'єднує і зберігає це з'єднання, поки не закінчиться друкарська серія цього ПК. Утворюється з'єднання типу «крапка-крапка», при якому інші ПК не можуть скористатися з'єднанням, поки воно не звільниться і не настане їх черга. Більшість сучасних мереж, включаючи Інтернет, використовують перемикання каналів, будучи мережами з пакетною комунікацією.

Початкове інформаційне повідомлення від $ПК_1$ до $ПК_2$ залежно від його розміру може передаватися одночасно одним пакетом або декількома. Але оскільки в заголовку кожного з них є адреса одержувача, всі вони прибудуть в одне і те ж місце призначення, хоча вони передавалися абсолютно різними маршрутами (рис. 1.14).

Для порівняння схем перемикання ланцюгів і пакетів уявимо, що ми перервали канал у кожному з них. Наприклад, відключивши принтер від $ПК_1$ ми зовсім позбавили його можливості друкувати. З'єднання з перемиканням ланцюгів вимагає безперервного каналу зв'язку. Навпаки, в мережі з перемиканням пакетів дані можуть рухатися іншими шляхами, тобто не порушується працездатність мережі.

Обмін даними в мережі. Доступ до файлів і тек

Робота з файлами в мережі для користувача практично не відрізняється від роботи з файлами на локальному комп'ютері. Основна відмінність полягає в тому, що доступ до даних мережевого комп'ютера визначається користувачем цього комп'ютера, який призначає можливість доступу до окремих файлів і тек.

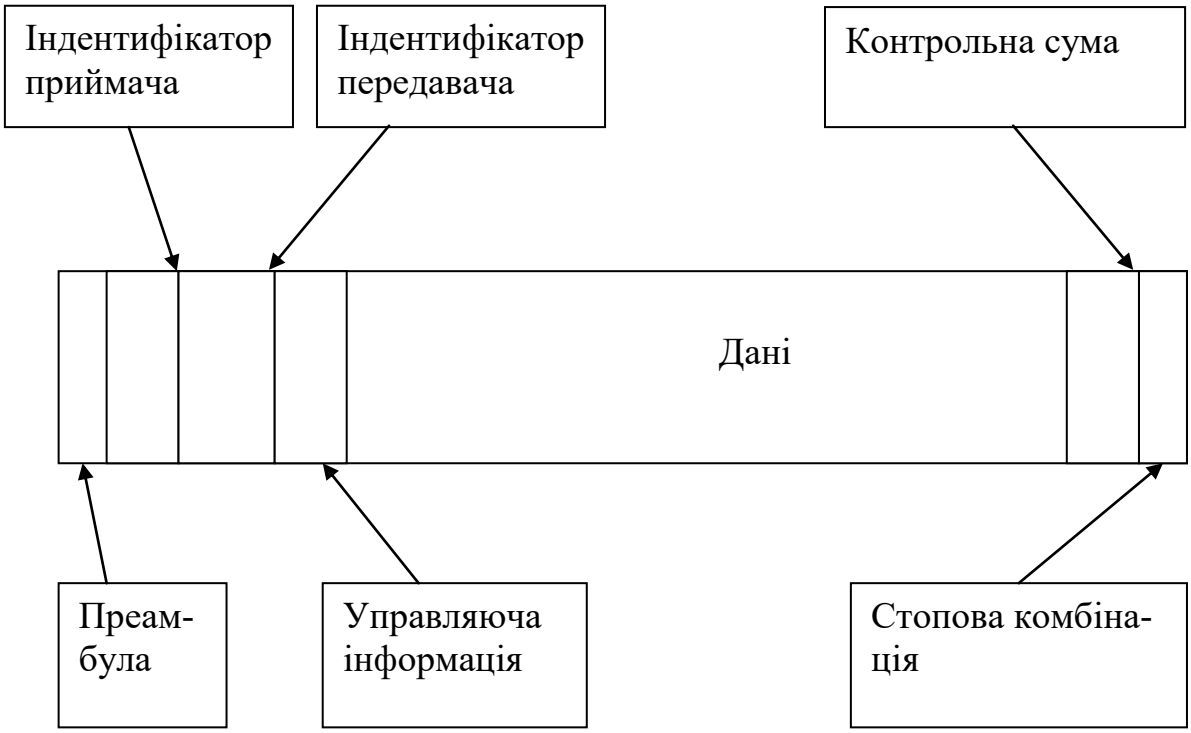


Рис. 1.12. Структура пакету

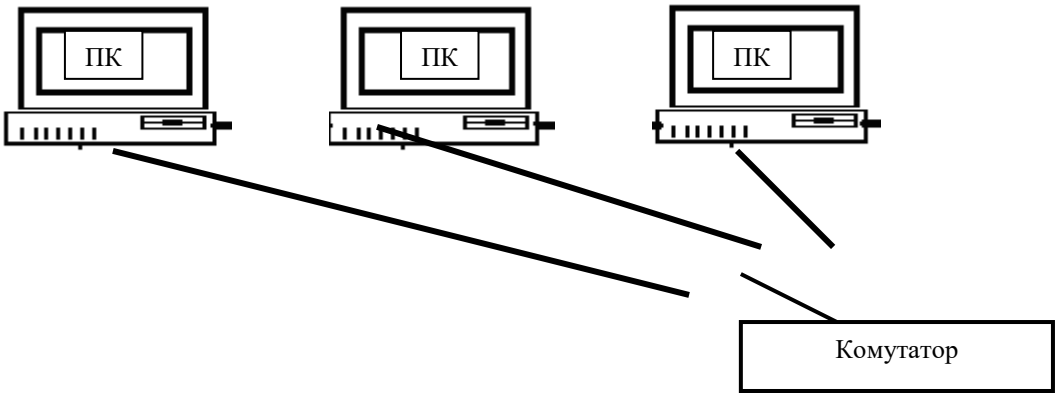


Рис. 1.13. Комутація каналів

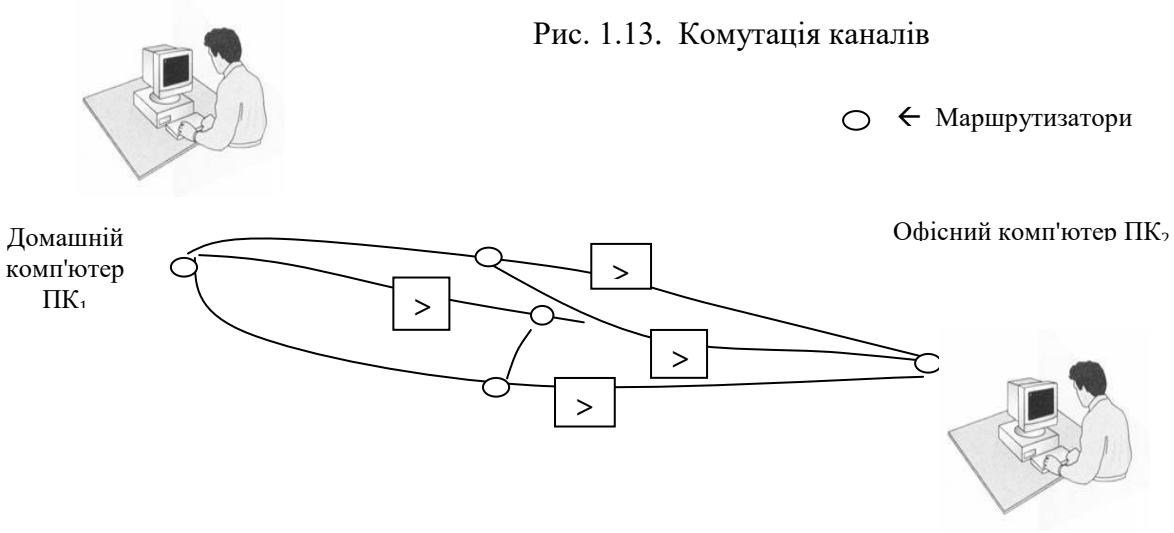


Рис. 1.14. Комутація пакетів

Ресурс, до якого наданий доступ, називається загальним.

Якщо викликати контекстне меню (праве клацання миші) для будь-якої теки, вибрати пункт «Свойства», то серед вкладок буде присутня "Доступ" (рис. 1.15), з допомогою якої можна управляти дозволом мережевого доступу до цієї теки.

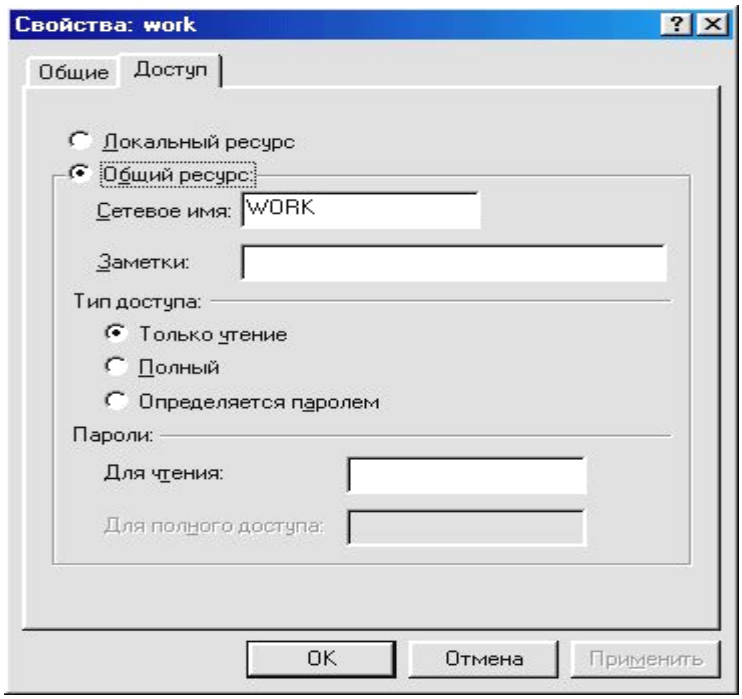


Рис. 1.15. Загальний вид вікна «Доступ»

Перемикач "Локальний ресурс" забороняє мережевий доступ до теки.

Перемикач "Загальний ресурс" дозволяє назначити параметри доступу до теки: поле "Мережеве ім'я" визначає мережеве ім'я теки, поле "Замітки" - визначає опис теки.

Група перемикачів "Тип доступу" визначає як буде здійснюватися мережевий доступ до теки.

- Тільки читання - можливо тільки читання даних.
- Повний доступ - можливе читання й зміна даних.
- Визначається паролем - для кожного з типів доступу визначається окремий пароль.

Область "Паролі" дозволяє призначити пароль для отримання мережевого доступу.

Використання майстра перенесення файлів і параметрів

Майстер перенесення файлів і параметрів допомагає переміщувати файли даних і особисті налагодження зі старого комп'ютера на новий без необхідності повторення на новому комп'ютері дій із налагодження. Наприклад, зі старого комп'ютера на новий можна перенести особисті властивості екрану, параметри тек і панелі завдань, налагодження оглядача Інтернету й електронної пошти. Даний майстер також переміщує деякі файли або цілі теки, такі як «Мої документи», «Мої малюнки» і «Вибране». При переміщенні властивостей програм за допомогою майстра перенесення файлів і параметрів перенесення паролів не відбувається. Ця функціональна можливість майстра перенесення файлів і параметрів допомагає зберегти конфіденційність паролів.

Рекомендується встановити на новий комп'ютер антивірусну програму до переміщення файлів зі старого комп'ютера. Це допоможе захистити новий комп'ютер від вірусів, які можуть міститися у файлах, які переносяться зі старого комп'ютера.

Запустіть майстра перенесення файлів і параметрів. Щоб відкрити майстра перенесення файлів і параметрів, натисніть кнопку **Пуск**, потім виберіть команди **Всі програми → Стандартні → Службові → Майстер перенесення файлів і параметрів.** З'явиться вікно (рис. 1.16). За допомогою кнопки **Далі** встановіть необхідні параметри перенесення файлів (рис 1.17-1.22).

Мережева архітектура – це комбінація стандартів топологій і протоколів, необхідних для створення працездатної мережі. Відповідно до стандартних протоколів фізичного рівня виділяють три основні мережеві архітектури: Ethernet (протокол 802.3) і Fast Ethernet (протокол 802.30); ArcNet (протокол 802.4); Token Ring (протокол 802.5).

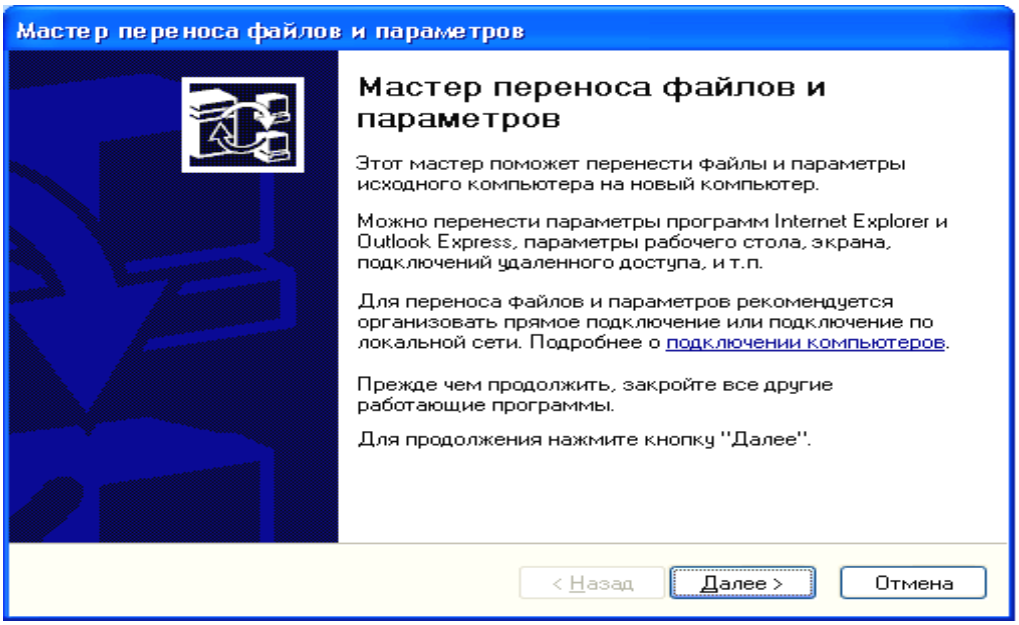


Рис 1.16. Вікно майстра

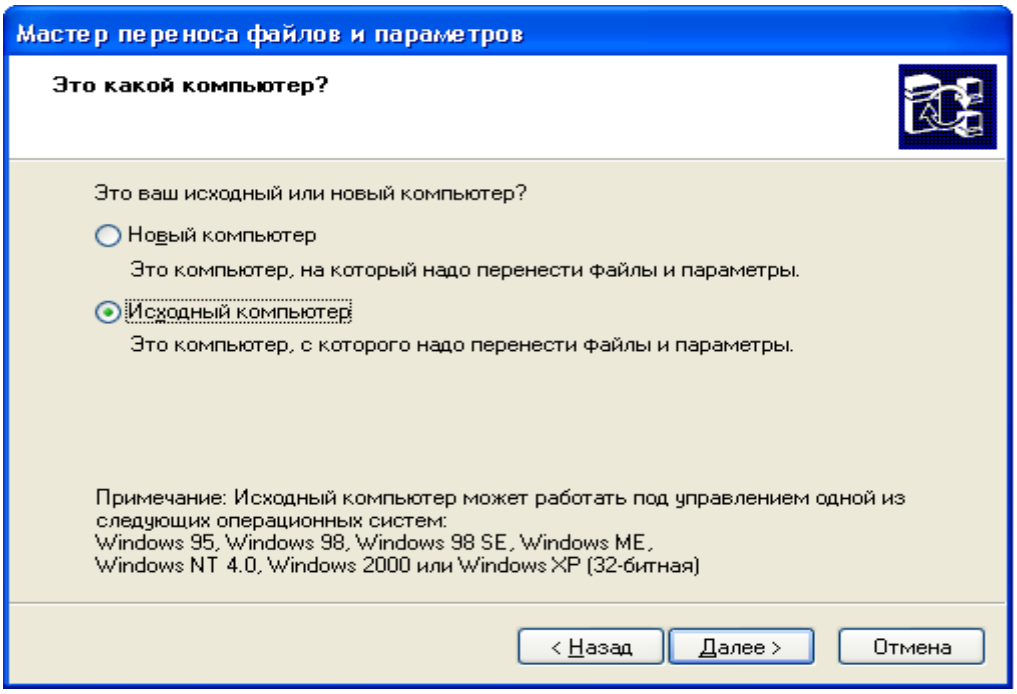


Рис. 1.17. Друге вікно майстра.

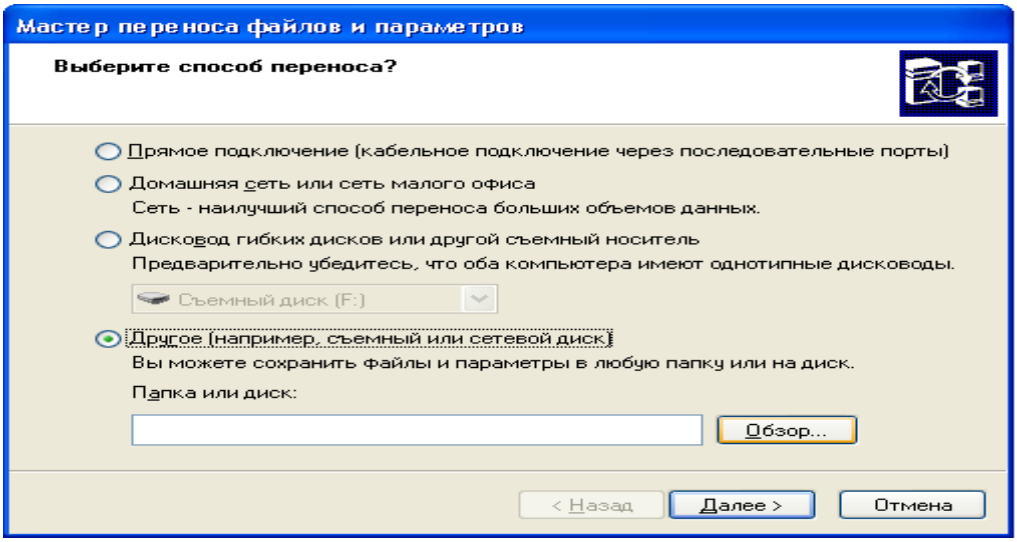


Рис. 1.18. Третє вікно майстра

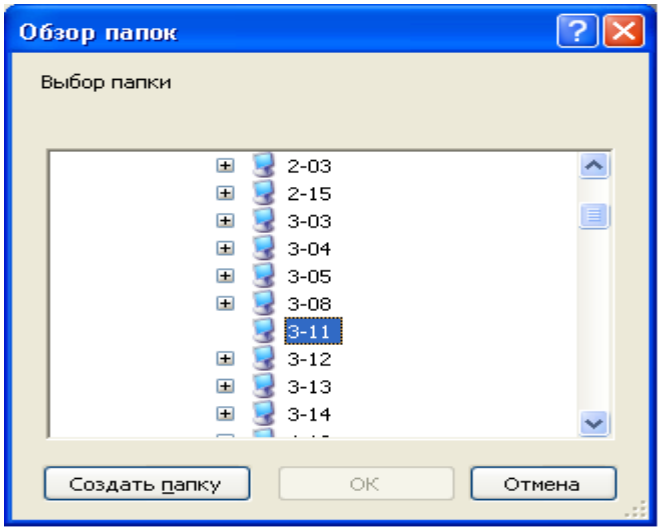


Рис. 1.19. Вікно вибору комп'ютера для передавання файлів

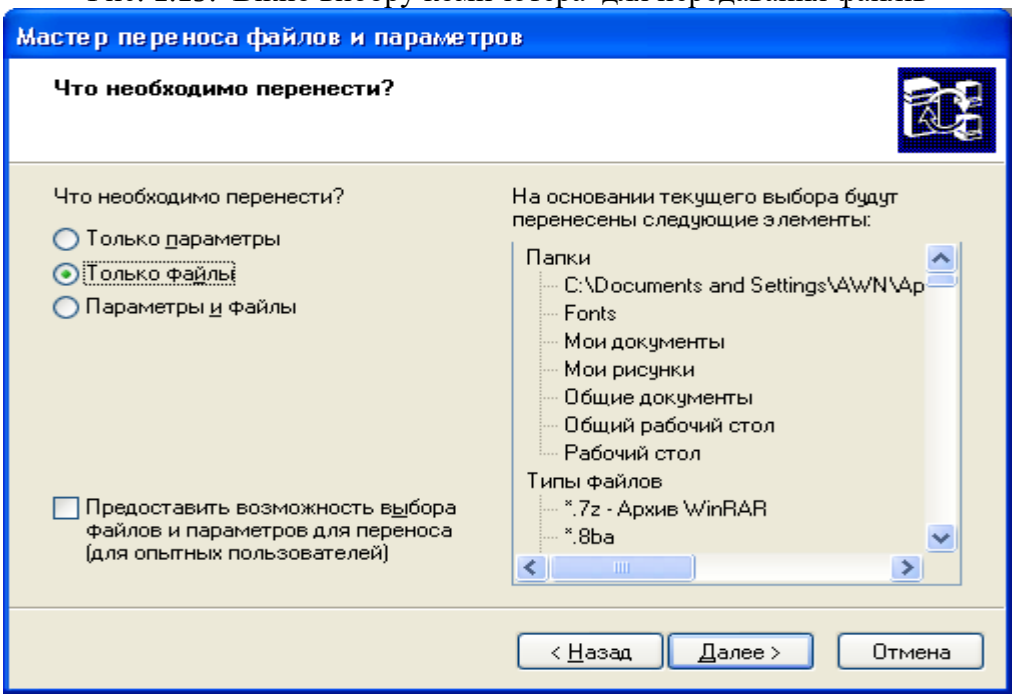


Рис. 1.20. Вікно майстра

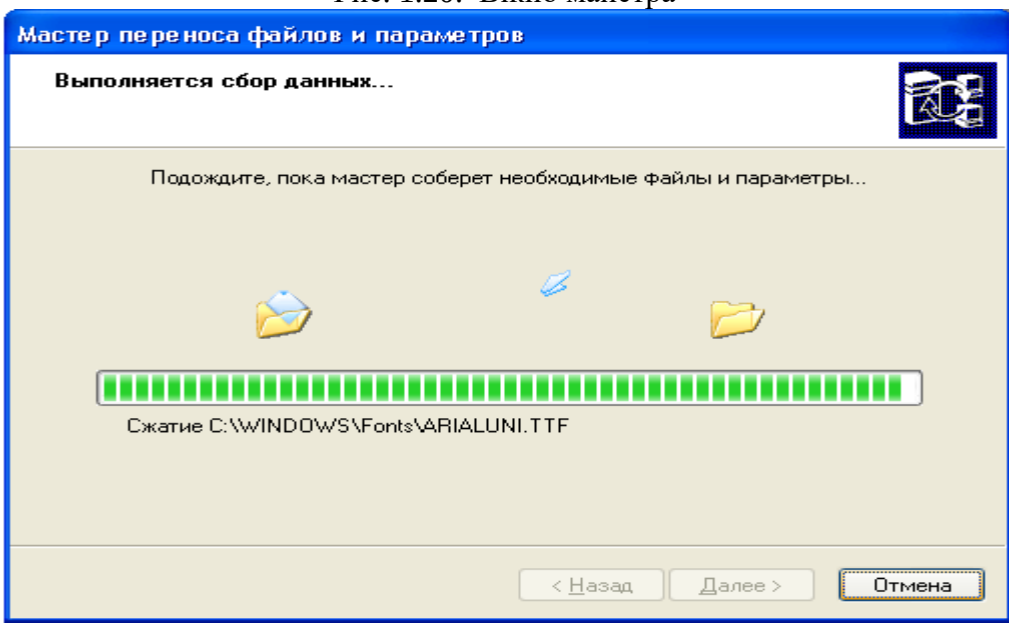


Рис. 1.21. Вікно майстра

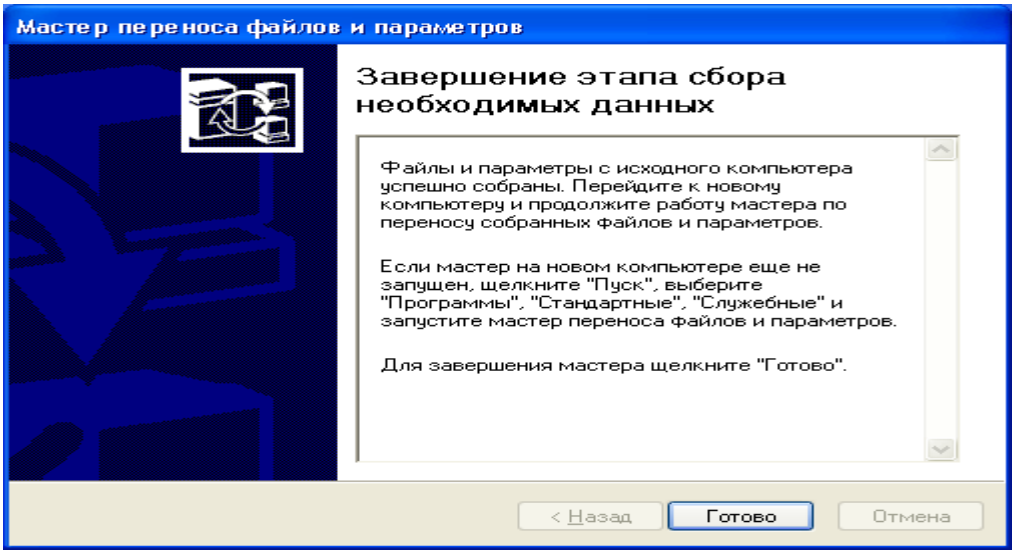


Рис. 1.22. Кінцеве вікно майстра.

Мережа Ethernet

Мережа отримала ім'я Ethernet, вона базувалася на товстому коаксіальному кабелі і забезпечувала швидкість передавання даних 2,94 Мбіт/с. У березні 1981 р. фірма 3Com представила 10 Мбіт/с Ethernet-трансивер, а у вересні 1982 р. – перший Ethernet-адаптер для ПК. Після виходу перших виробів, в червні 1983 р., IEEE затвердив стандарти Ethernet 802.3 і Ethernet 10Base5. Як середовище передавання передбачався "товстий" коаксіальний кабель, а кожен вузол мережі підключався за допомогою окремого трансивера. Така реалізація виявилася дорогою. Дешевою альтернативою із застосуванням менш дорогого і тоншого коаксіального кабелю став 10Base2 або ThinNet. Станції вже не вимагали окремих трансиверів для підключення до кабелю. Головними його перевагами була простота розгортання й мінімальна кількість активного мережевого у . Відразу ж визначилися недоліки На час підключення нових станцій доводилося зупиняти роботу всієї мережі. Для виходу мережі з ладу достатньо було обриву кабелю в одному місц, тому експлуатація кабельної системи вимагала від технічного персоналу великої уваги. Наступним кроком розвитку Ethernet стала розробка стандарту 10Base-T, що передбачав в якості середовища передавання неекрановану скручену пару (Unshielded Twisted Pair - UTP). В основу цього стандарту лягли розробки SynOptics Communications під загальною назвою LattisNet, які відносяться до 1985 р. У 10Base-T використовувалася топологія "зірка", у якій кожна станція з'єднувалася із центральним концентратором (hub). Такий варіант реалізації усував необхідність переривання роботи мережі на час підключення нових станцій і дозволяв локалізувати пошук обривів проводки на одній лінії концентратор-станція. Виробники дістали можливість вбудовувати в концентратори засобимоніторингу і управління мережею. У вересні 1990 р. IEEE затверджує стандарт 10Base-T.

Специфікація **Ethernet 10Base5** передбачає виконання наступних умов:

Середовище передавання – "товстий" (близько 12 мм в діаметрі) коаксіальний кабель (RG-8 або RG-11) з хвилевим опором 50 Ом. Довжина кабелю між сусідніми станціями – не менше 2,5 м. Максимальна довжина сегменту мережі – не більше 500 метрів. Загальна довжина всіх кабелів у сегментах не більше 2500 метрів. Загальне число вузлів на один сегмент мережі не більше 100.

Сегмент закінчується термінаторами, один з яких повинен бути заземлений. Кабелі, які відгалужуються, можуть бути скільки завгодно короткими, але відстань від трансивера до адаптера – не більше 50 метрів.

Основні переваги 10Base5: велика довжина сегменту, хороша перешкодозахисність кабелю і висока напруга ізоляції трансивера. Завдяки цим якостям "товстий" Ethernet найчастіше застосовувався для прокладки базових сегментів (Backbone). Зараз цей стандарт практично повністю витіснений дешевшими і продуктивнішими реалізаціями Ethernet.

Обмеження за специфікацією **Ethernet 10Base2.** Середовище передавання – "тонкий" (близько 6 мм в діаметрі) коаксіальний кабель (RG-58 різних модифікацій) з хвилевим опором 50 Ом. Довжина кабелю між сусідніми станціями не менше 0,5 м. Максимальна довжина сегменту мережі не більше 185 метрів. Загальна довжина всіх кабелів в сегментах (сполучених через повторювачі) не більше 925 метрів. Загальне число вузлів на один сегмент мережі не більше 30

(включаючи повторювачі). Сегмент закінчується термінаторами, один з яких заземляється. Відгалуження від сегменту недопустимі. У мережі не більше 1024 станцій.

Правила побудови мереж, що використовують фізичну топологію "загальна шина". У цьому випадку діє правило 5-4-3 тобто:

- не більше 5 сегментів мережі;
- можуть бути об'єднані не більше ніж чотирма повторювачами;
- при цьому станції можуть бути підключені не більше ніж до трьох сегментів, останні два можуть бути використані для збільшення загальної довжини мережі.

Ethernet 10BASE-T

Відповідає стандарту IEEE 802.3i, прийнятому в 1991 р.

Обмеження специфікації Ethernet 10Base-T:

Середовище передавання – неекранований кабель на основі скрученої пари (UTP - Unshielded Twisted Pair) категорії 3 і вище. При цьому використовуються 2 пари: одна для приймання, друга – для передавання. Фізична топологія "зірка". Довжина кабелю між станцією й концентратором не більше 100 м. Максимальний діаметр мережі не більше 500 метрів. Кількість станцій у мережі не більше 1024. У мережі 10Base-T термін "сегмент" застосовують до з'єднання станція-концентратор.

Ethernet 10BASE-F

Середовище передавання даних стандарту 10Base-F - оптично-волоконний кабель. У стандарті повторюється топологія й функціональні елементи 10Base-T: концентратор, до портів якого за допомогою кабелю підключаються мережеві адаптери станцій. Для з'єднання адаптера з повторювачем використовується два оптично-волоконних кабелі - один для приймання, другий для передавання.

Існує декілька різновидів 10Base-F. Першим стандартом для використання оптично-волоконного кабелю в мережах Ethernet був FOIRL (Fiber Optic Inter-Repeater Link). Обмеження довжини оптично-волоконних ліній між повторювачами складало 1 км при загальній довжині мереж не більше 2,5 км. Максимальне число повторювачів - чотири.

У стандарті 10Base-FL, призначеному для з'єднання станцій з концентратором, довжина сегменту оптично-волоконного кабелю становить до 2 км при загальній довжині мережі не більше 2,5 км. Максимальна кількість повторювачів також чотири. Обмеження довжин кабелів наведені для багатомодового кабелю. Застосування одномодового кабелю дозволяє прокладати сегменти завдовжки до 20 км.

Існує також стандарт 10Base-FB, призначений для магістрального з'єднання повторювачів. Обмеження на довжину сегменту становить 2 км при загальній довжині мереж 2,74 км. Кількість повторювачів - до 5. Характерною особливістю 10Base-FB є здатність повторювачів виявляти відмови основних портів і переходити на резервні за рахунок обміну спеціальними сигналами, які відрізняються від сигналів передавання даних.

Існує також стандарт 10Base-FP, призначений для з'єднання за топологією типу «зірка» може об'єднувати до 33 станцій з портами стандарту 10Base-FL.

Технологія Token Ring. Основні характеристики технології.

Мережі Token Ring, так само як і мережі Ethernet, характеризує середовище передавання даних, яке в даному випадку складається з відрізків кабелю, які сполучають усі станції мережі в кільце. Кільце розглядається як загальний ресурс і для доступу до нього потрібний не випадковий алгоритм, як у мережах Ethernet, а детермінований, заснований на передаванні станціям права на використання кільця в певному порядку. Це право передається за допомогою кадру спеціального формату, званого *маркером* або *токеном (token).*

Технологія Token Ring була розроблена компанією IBM в 1984 році, а потім передана як проект стандарту в комітет IEEE 802, який на її основі прийняв в 1985 році стандарт 802.5. Компанія IBM використовує технологію Token Ring як свою основну мережеву технологію для побудови локальних мереж на основі комп'ютерів різних класів — мейнфреймів, мінікомп'ютерів і персональних комп'ютерів. В даний час саме компанія IBM є основним законодавцем моди технології Token Ring, виготовляючи близько 60 % мережевих адаптерів цієї технології.

Мережі Token Ring працюють з двома бітовими швидкостями — 4 і 16 Мбіт/с. Використання станцій, що працюють на різних швидкостях, в одному кільці не допускається. Мережі

Token Ring, що працюють із швидкістю 16 Мбіт/с, мають деякі удосконалення в алгоритмі доступу в порівнянні із стандартом 4 Мбіт/с.

Технологія Token Ring є складнішою технологією, ніж Ethernet. Вона характеризується властивостями безвідмовності. У мережі Token Ring визначені процедури контролю роботи мережі, які використовують зворотний зв'язок кільцеподібної структури, – посланий кадр завжди повертається в станцію-відправник. У деяких випадках виявлені помилки в роботі мережі усуваються автоматично, наприклад, може бути відновлений втрачений маркер. В інших випадках помилки тільки фіксуються, а їх усунення виконується уручну обслуговуючим персоналом.

Для контролю мережі одна зі станцій виконує роль так званого *активного монітора.* Активний монітор вибирається під час ініціалізації кільця як станція з максимальним значенням MAC-адреси. Якщо активний монітор виходить із ладу, процедура ініціалізації кільця повторюється й вибирається новий активний монітор. Щоб мережа могла виявити відмову активного монітора, останній в працездатному стані кожні 3 секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється в мережі довше 7 секунд, то решта станцій мережі починає процедуру виборів нового активного монітора.

Методика розрахунку конфігурації мережі Ethernet

Дотримання численних обмежень, установлених для різних стандартів фізичного рівня мереж Ethernet, гарантує коректну роботу мережі (природно, при справності всіх елементів фізичного рівня).

Найчастіше доводиться перевіряти обмеження, пов'язані з довжиною окремого сегмента кабелю, а також кількістю повторювачів і загальною довжиною мережі.

Правила «5-4-3» для коаксіальних мереж, створених на основі коаксіальних кабелів (рис. 1.23), і «4 хабів» для мереж на основі скрученої пари (рис. 1.24) й оптичного-волокна не тільки дають гарантії працездатності мережі, але і залишають великий «запас міцності» мережі. Наприклад, якщо порахувати час подвійного обороту в мережі, що складається з 4 повторювачів 10Base-5 і 5 сегментів максимальної довжини 500 м, то виявиться, що воно складає 537 бітових інтервалів.

Рис. 1.23. Коаксіальний кабель.

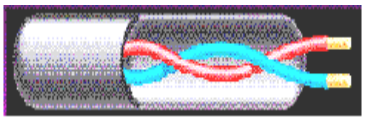


Рис. 1.24. Кабель типу "Скручена пара".

А так як час передавання кадру мінімальної довжини, разом із преамбулою, розмір якої складає 72 байти, дорівнює 575 бітовим інтервалам, то видно, що розробники стандарту Ethernet залишили 38 бітових інтервалів як запас для забезпечення надійності. Проте в документах комітету 802.3 стверджується, що і 4 додаткових бітових інтервали створюють достатній запас надійності.

Комітет IEEE 802.3 наводить вихідні дані про затримки, які вносяться повторювачами і різними середовищами передавання даних, для тих фахівців, які хочуть самостійно розраховувати максимальну кількість повторювачів і максимальну загальну довжину мережі, не задовольняючись тими значеннями, які приведені в правилах «5-4-3» і «4 хабів». Особливо такі розрахунки корисні для мереж, що складаються зі змішаних кабельних систем, наприклад, коаксиальних й оптично-волоконних (рис. 1.25), на які правила про кількість повторювачів не розраховані. При цьому максимальна довжина кожного окремого фізичного сегмента повинна суворо відповідати стандартові, тобто 500 м для «товстого» коаксіального кабелю, 100 м для «скрученої пари» й т.д.

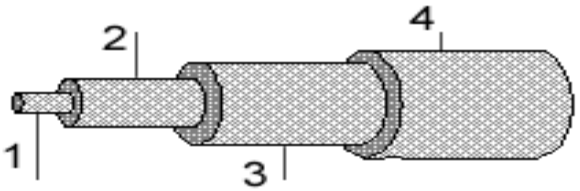


Рис. 1.25. Оптично-волоконний кабель (1 – сердечник; 2 - оболонка, що відбиває промінь; 3 - покриття первинного буфера; 4 - покриття вторинного буфера)

Щоб мережа Ethernet, яка складається із сегментів різної фізичної природи, працювала коректно, необхідне виконання чотирьох основних умов:

- кількість станцій у мережі — не більше 1024;
- максимальна довжина кожного фізичного сегмента — не більша величини, яка визначена у відповідному стандарті фізичного рівня;
- час подвійного обороту сигналу (Path Delay Value, PDV) між двома найвіддаленішими станціями мережі — не більше 575 бітових інтервалів;
- скорочення міжкадрового інтервалу IPG (Path Variability Value, PVV) при проходженні послідовності кадрів через усі повторювачі — не більше ніж 49 бітових інтервалів (тому що при відправленні кадрів кінцеві вузли забезпечують початкову міжкадрову відстань довжиною 96 бітових інтервали. Після проходження повторювача воно повинно бути не менше ніж 96 - 49 = 47 бітових інтервали).

Дотримання цих вимог забезпечує коректність роботи мережі навіть у випадках, коли порушуються прості правила конфігурування.

Розрахунок PDV

Для спрощення розрахунків, зазвичай, використовуються довідкові дані IEEE, які містять значення затримок поширення сигналів у повторювачах, приймально-передавальних пристроях і різних фізичних середовищах.

Таблиця 1.5

Дані для розрахунку значення PDV

Тип сегмента	База лівого сегмента, bt	База проміжного сегмента, bt	База правого сегмента, bt	Затримка середовища на 1 м, bt	Максимальна довжина сегменту, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	--	24,0	--	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI9 > 2m	0	0	0	0,1026	2+48

Позначення: bt –бітові інтервали.

У табл. 1.5 наведені дані, необхідні для розрахунку значення PDV для всіх фізичних стандартів мереж Ethernet.

Комітет 802.3 намагався максимально спростити виконання розрахунків, тому дані, наведені в таблиці, включають відразу кілька етапів проходження сигналу. Наприклад, затримки, внесені повторювачем, складаються із затримки вхідного трансивера, затримки блоку повторення й затримки вихідного трансивера. Проте в таблиці всі ці затримки представлені одною величиною, названою базою сегмента.

Щоб не потрібно було два рази додавати затримки, внесені кабелем, у таблиці даються подвоєні величини затримок для кожного типу кабелю.

У таблиці використовуються також такі поняття, як лівий сегмент, правий сегмент і проміжний сегмент. Пояснимо ці терміни на прикладі мережі, яка наведена на рис. 1.49.

Лівим сегментом називається сегмент, у якому починається шлях сигналу від виходу передавача (рис. 1.26) кінцевого вузла. На прикладі – це сегмент 1. Потім сигнал проходить через проміжні сегменти 2-5 і доходить до приймача (вхід Rx на рис. 1.27) найвіддаленішого вузла найвіддаленішого сегмента 6, який називається правим. Саме тут у гіршому випадку відбувається зіткнення кадрів і виникає колізія.

З кожним сегментом пов’язана постійна затримка, названа базою, що залежить тільки від типу сегмента й від положення сегмента на шляху сигналу (лівий, проміжний або правий). База правого сегмента, у якому виникає коллізія, набагато перевищує базу лівого й проміжних сегментів.

Крім цього, із кожним сегментом пов'язана затримка поширення сигналу уздовж кабелю сегмента, що залежить від довжини сегмента й обчислюється шляхом множення часу поширення сигналу на одному метрі кабелю (у бітових інтервалах) на довжину кабелю.

Розрахунок полягає в обчисленні затримок, внесених кожним відрізком кабелю (наведена в таблиці затримка сигналу на 1 м кабелю множиться на довжину сегмента), а потім підсумовування цих затримок із базами лівого, проміжних і правого сегментів. Загальне значення PDV не повинне перевищувати 575.

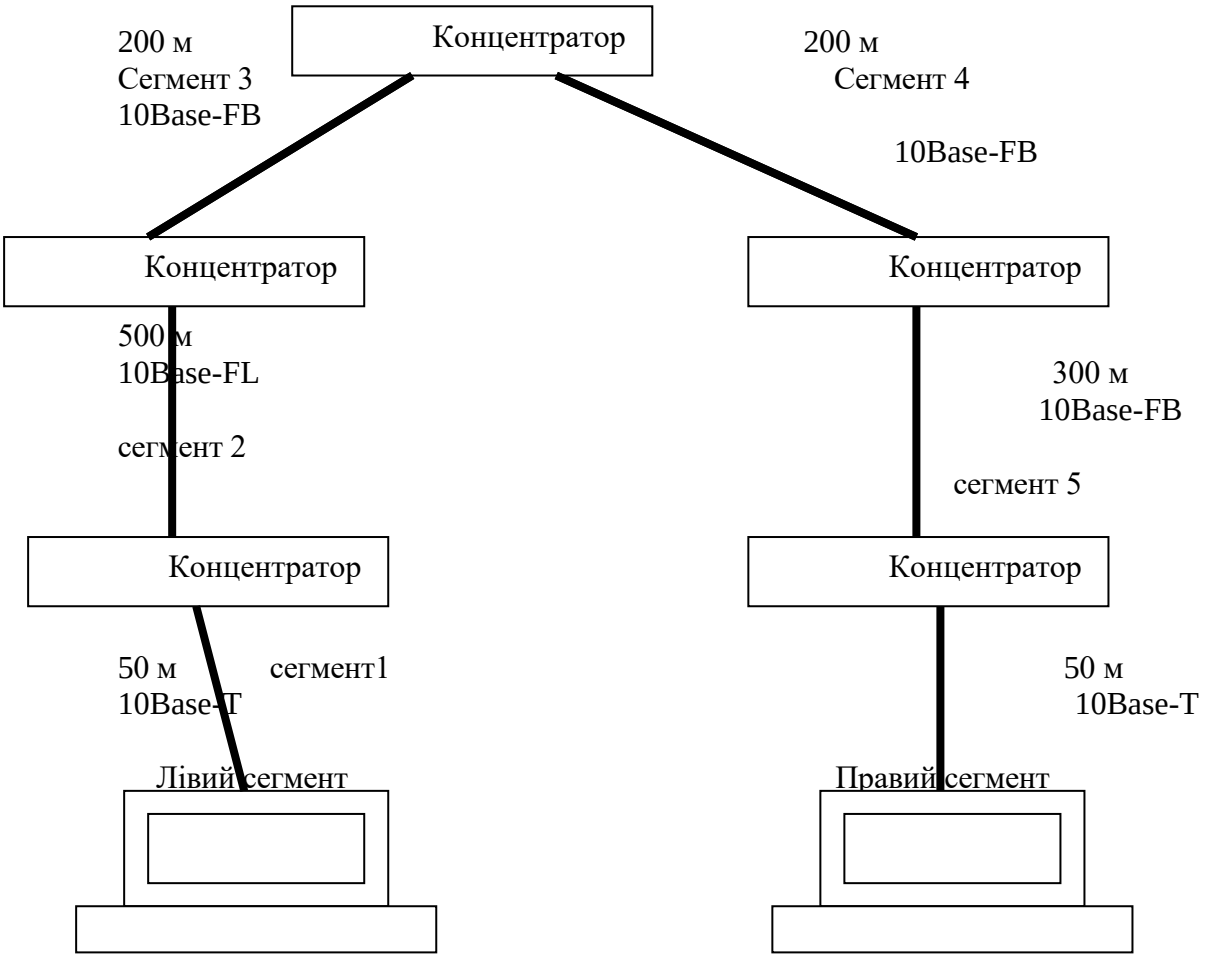


Рис. 1.26. Приклад мережі Ethernet

Так як лівий і правий сегменти мають різні величини базової затримки, то у випадку різних типів сегментів на віддалених краях мережі необхідно виконувати розрахунки двічі: один раз прийняти як лівий сегмент, сегмент одного типу, а в другий — сегмент іншого типу. Результатом можна вважати максимальне значення PDV. У нашому прикладі крайні сегменти мережі належать до одного типу – стандарту 10Base-T, тому подвійний розрахунок не вимагається, але якби вони були сегментами різного типу, то в першому випадку потрібно було б прийняти в якості лівий сегмент між станцією й концентратором 1, а в другому вважати лівим сегмент між станцією й концентратором 5.

Приведена на малюнку мережа відповідно до правила 4 хабів не являється коректною – у мережі між вузлами сегментів 1 і 6 знаходяться 5 хабів, хоча не всі сегменти є сегментами 10Base-FB. Крім того, загальна довжина мережі – 1200 м, що не порушує правило 2500 м. Розрахуємо значення PDV для нашого прикладу.

Лівий сегмент 1:

- 15,3 (база) + 50 x 0,113 = 20,95.

Проміжний сегмент 2:

- 33,5 + 500 x 0,1 = 83,5.

Проміжний сегмент 3:

- 24 + 200 x 0,1 = 44,0.

Проміжний сегмент 4:

- 24 + 200 x 0,1 = 44,0

Проміжний сегмент 5:

- 24 + 300 x 0,1 = 54,0.

Правий сегмент 6:

- 165 + 50x0,113 = 170,65.

Сума всіх складових дає значення PDV – 333,6.

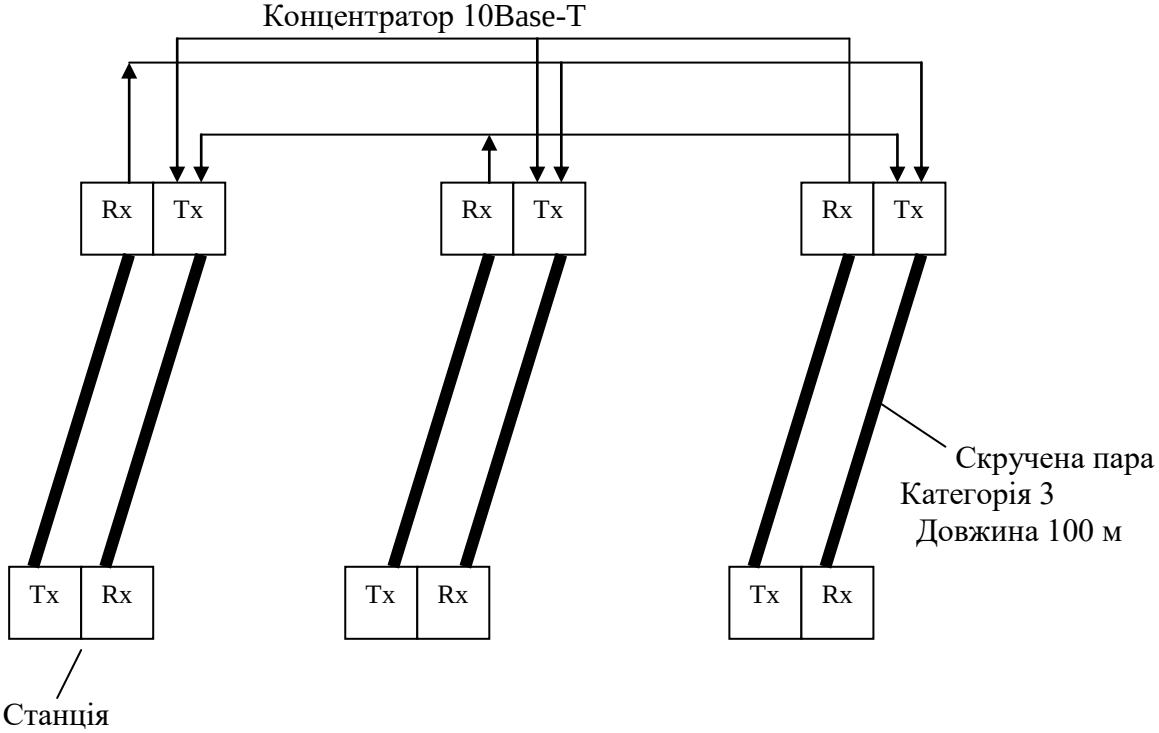


Рис. 1.27. Мережа стандарту 10Base-T
Позначення: Tx – передавач, Rx – приймач.

Оскільки значення PDV менше за максимально припустиму величину 575, то ця мережа відповідає критерію часу подвійного обороту сигналу незважаючи на те, що кількість повторювачів більша чотирьох.

Розрахунок PVV

Щоб визнати конфігурацію мережі коректною, потрібно розрахувати також зменшення міжкадрового інтервалу повторювачами, тобто величину PVV.

Для розрахунку PVV також можна скористатися значеннями максимальних величин зменшення міжкадрового інтервалу при проходженні повторювачів різних фізичних середовищ, рекомендованими IEEE і приведеними в табл. 1.6.

Відповідно до цих даних розрахуємо значення PVV для нашого прикладу.

- Лівий сегмент 1 10Base-T: скорочення в 10,5 bt.
- Проміжний сегмент 2 10Base-FL – 8 bt.
- Проміжний сегмент 3 10Base-FB – 2 bt.
- Проміжний сегмент 4 10Base-FB – 2 bt.
- Проміжний сегмент 5 10Base-FB – 2 bt.

Таблиця 1.6.

Зменшення міжкадрового інтервалу повторювачами

Тип сегмента	Передаючий сегмент, bt	Проміжний сегмент, bt
10Base-5, або 10Base-2	16	11
10Base-FB	--	2
10Base-FL	10,5	8
10Base-T	10,5	8

Сума цих величин дає значення PVV рівне 24,5, що менше граничного значення в 49 бітових інтервалів.

У результаті приведена в прикладі мережа відповідає стандартам Ethernet за всіма параметрами, пов'язаними і з довжинами сегментів, і з кількістю повторювачів.

Розрахунок мережі Fast Ethernet

Порядок розрахунку коректності конфігурації мережі Fast Ethernet (рис. 1.28)трохи відрізняється від розрахунку мережі Ethernet, як за параметрами, так і за схемою розрахунку. Стандарт Fast Ethernet не підтримує коаксіальний кабель, і мережа будується винятково за топологією зірка. Обмеження на довжину кабелю комп'ютер-повторювач, комп'ютер-комп'ютер приведені нижче (табл. 1.7).

Таблиця 1.7.

Обмеження на довжину кабелю в стандарті Fast Ethernet.

Тип кабелю	Стандарт	До повторювача підключений	Максимальна довжина кабелю, м
Скручена пара категорії 5	100Base-TX	—	100
Скручена пара категорії 3, 4	100Base-T4	—	100
Багатомодовий оптично-волоконний 62,5/125 мкм	100Base-FX	тільки оптично-волоконний кабель	412 (напівдуплекс) 2000 (повний дуплекс)
		один оптично-волоконний кабель і кілька кабелів скручена пара	160
		трохи оптично-волоконний кабелів і кілька кабелів скручена пара	136

Обмеження на кількість повторювачів

Повторювачі Fast Ethernet поділяються на два класи. Повторювачі класу 1 мають порти всіх типів (стандарт 100Base-TX, 100Base-FX і 100Base-T4). Повторювачі класу 2 мають або всі порти 100Base-T4, або порти 100Base-TX і 100Base-FX. Між будь-якими двома комп'ютерами в мережі може бути не більше двох повторювачів класу 2 або тільки один повторювач класу 1. Між собою повторювачі класу 1 повинні поєднуватися за допомогою комутаторів, мостів, маршрутизаторів. Приведених правил побудови мережі цілком достатньо для визначення коректності конфігурації мережі, тому що ці правила розроблені з мінімальним "запасом міцності".

Однак, при бажанні, можна провести й розрахунок PDV, виходячи з наступних підходів. Максимально припустима величина PDV = 512 бітових інтервалів. При розрахунку сегменти не поділяються на правий і лівий. Для розрахунку беруться затримки, що вносять дві взаємодіючих через повторювач мережеві карти комп'ютерів (або мережева карта комп'ютера й порт комутатора). Також ураховується затримка сигналу в повторювачі й затримка, внесена кабелем. Вихідні дані для розрахунку приведені в табл. 1.8.

Підрахуємо, для прикладу, PDV між двома комп'ютерами, підключеними до повторювача 1 класу, що розташований в правій частині (рис. 1.49). Припускаємо, що використовується скручена пари 5-ої категорії (TX). PDV=100*1,112 (кабель «скручена пара») + 136*1,0 (оптично-волоконний кабель) + 100 (мережеві карти) + 140 (повторювач) = 487,2 < 512. Розраховане значення PDV менше граничного значення 512 бітових інтервалів, відповідно розрахунки поки не виявили некоректність конфігурації мережі.

Таблиця 1.8.

Розрахунок затримок поширення сигналу.

Затримка, внесена кабелем		Затримка, внесена мережевими картами		Затримка, внесена повторювачем, мережевими картами	
Тип кабе-	Подвоєна	Тип мережевих карт,	Подвоєна	Клас повто-	Подвоєна

лю	затримка, bt на 1 м	які взаємодіють через повторювач	затримка, bt	рювача	затримка, bt
UTP Cat 3	l,14	Два адаптери TX/FX	114 (100 м)	1	140
UTP Cat 4	l,14	Два адаптери T4	114 (100 м)	2	138
UTP Cat 5	l,112	Один адаптер TX/FX і один – T4	111,2 (100 м)		128
оптично-волокон-ний	1,0	Два адаптери TX/FX	412 (412 м)		100

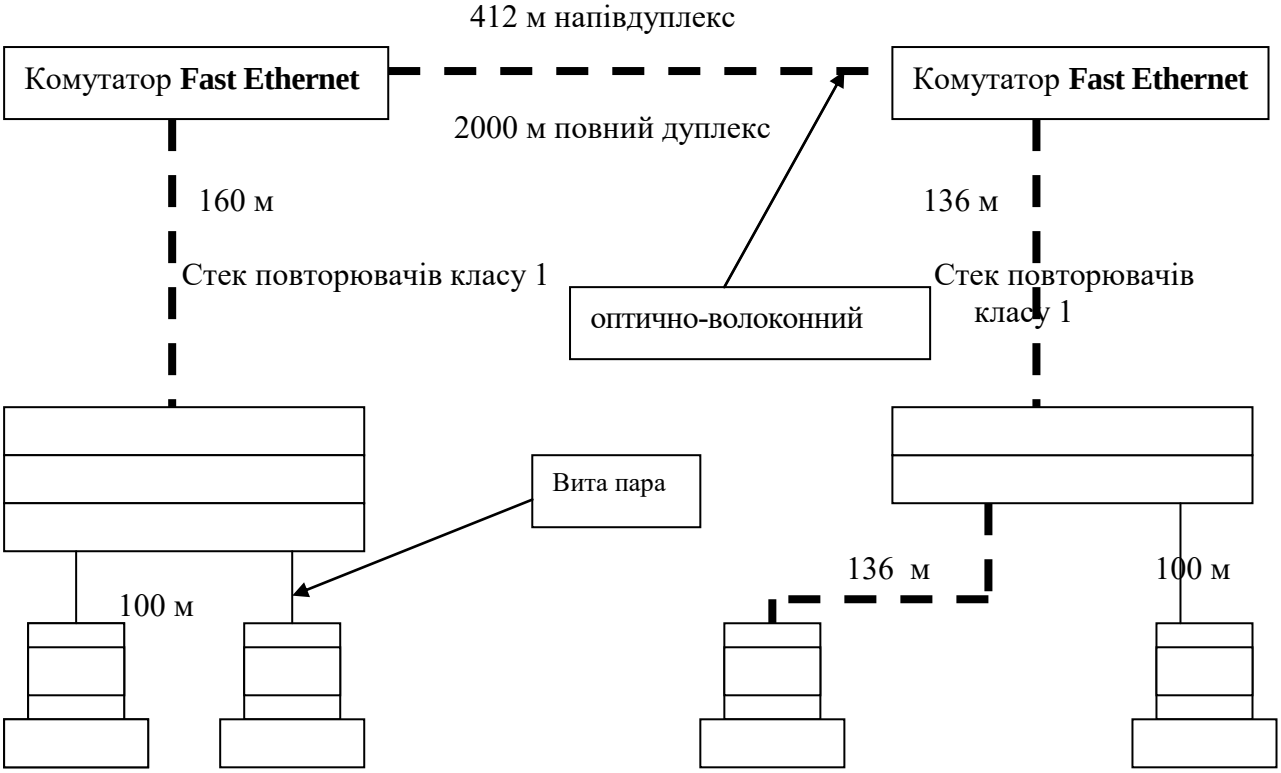


Рис. 1.28. Фрагмент мережі типу Fast Ethernet

Підключення до локальної мережі.
Встановлення й настроювання мережевого адаптера

Мережеві адаптери (рис. 1.29) виступають у якості фізичного інтерфейсу між комп'ютером і мережевим кабелем. Зазвичай вони вставляються в слоти розширення робочих станцій і серверів. Щоб забезпечити фізичне з'єднання між комп'ютером і мережею до відповідного порту адаптеру після його встановлення підключається мережевий кабель.

LAN-адаптери служать для виконання наступних функцій:

- підготування даних, що надходять від комп'ютера, для передавання мережевим кабелем;
- передавання даних іншому встаткуванню (комп'ютеру, концентратору);
- здійснює перетворення паралельного потоку даних у послідовний при передаванні в мережу й навпаки при прийманні, завершуючи ці перетворення перетворенням цифрових даних в електричні або оптичні за допомогою трансиверів;
- управління потоком даних між робочою станцією й кабельною системою (приймає/передає дані з кабелю й переводить їх у форму, «зрозумілу» центральному процесору встаткування).

Плата будь-якого мережевого адаптеру складається з апаратної частини й умонтованих програм, записаних у ПЗУ. Програми реалізують функції підрівнів управління логічним зв'язком і управління доступом до середовища канального (другого) рівня моделі OSI. Тим

самим LAN-адаптери «покривають» собою перший (фізичний) і другий (канальний) рівні цієї моделі.

Операції мережевих адаптерів

Усі види мережевих адаптерів виконують наступні операції при прийманні або передаванні даних (послідовність наведена для режиму передавання, при прийманні вона обернена наведеній):

Передавання даних. Дані передаються з ОЗУ комп'ютера в адаптер (або в ОЗУ при прийманні) через канал введення/виведення, який програмується, канал DMA або пам'ять.

Буферизація даних. Під час опрацювання у мережевому адаптері дані зберігаються в буфері. комутатору і т.п.).

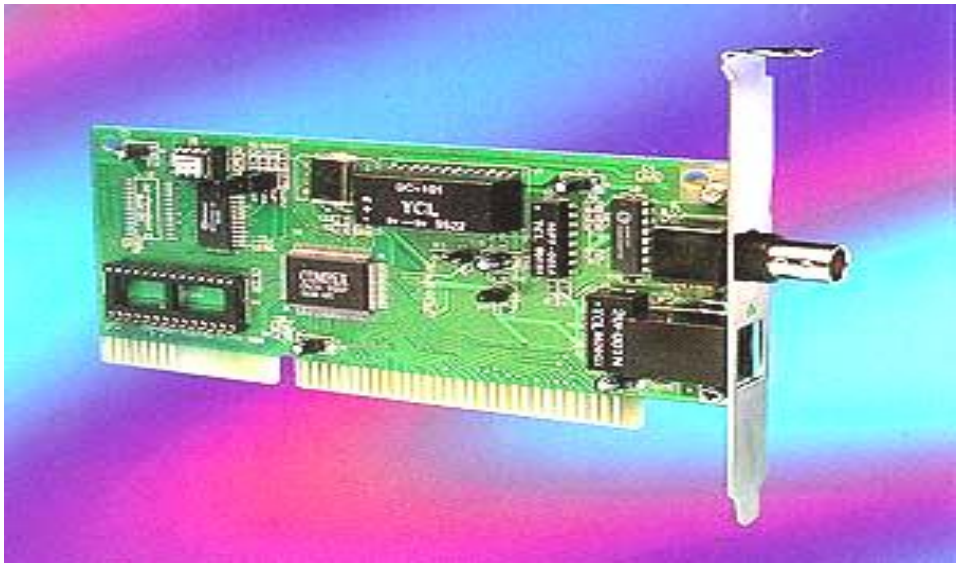


Рис. 1.29. Мережевий адаптер

Буфер дозволяє здійснити доступ до всього пакета. Тому буфер повинен мати об'єм, достатній для розміщення цілого пакета даних. Використання буферів необхідно для узгодження між собою швидкостей опрацювання інформації різноманітними компонентами мережі та комп'ютера.

Формування пакета даних. Мережевий адаптер повинен розділити дані на порції або блоки (при прийманні – зібрати). У мережах Ethernet розміри цих блоків складають 1500 байт, (для довідки, у мережах Token Ring – 4 Кб). Адаптер додає до пакета даних заголовок і закінчення. Заголовок і закінчення пакета є оболонками фізичного рівня. Після завершення цієї операції в буфері адаптеру лежить готовий до передавання пакет.

Доступ до кабелю. (Цю операцію адаптер виконує тільки в режимі передавання). В адаптерах типу Ethernet перед початком передавання адаптер переконується, що лінія не зайнята. У мережах Token Ring адаптер чекає надходження маркера, який він має право захопити, після чого можливий початок передавання даних.

Перетворення даних (при передаванні – із паралельного коду в послідовний, а при прийманні – із послідовного в паралельний). Цей етап необхідний тому, що дані передаються кабелем послідовно у формі бітів.

Кодування/декодування даних. На цьому етапі формуються електричні сигнали, які використовуються для представлення даних. Найпопулярнішим є Манчестерське кодування, при якому не потрібно синхронізувати сигнали, які предаються.

Передавання/приймання імпульсів. На цьому етапі кодовані електричні імпульси, що несуть у собі представлення даних, передаються в кабель.

Відмінності мережевих адаптерів

Адаптери поділяються на групи за протоколом, який використовується в їхній роботі: Ethernet, Token Ring, ArcNet і т.п. Але всередині будь-якої із груп завжди можна виділити адаптери, що працюють краще за інших. Мережевий адаптер може бути більш швидкодіючим

через те, що може мати великий об'єм власного ОЗУ або умонтований мікропроцесор, або продуктивніший інтерфейс для зв'язку з материнською платою комп'ютера й т.п. Тому цілком природно, що, наприклад, у сервер доцільно встановлювати найбільш швидкодіючі мережеві адаптери.

Мережеві адаптери відрізняються один від одного наступними основними можливостями:

- наявністю або відсутністю гнізда для встановлення ПЗУ програм самозавантаження (boot ROM) віддаленого клієнта;
- за типом системної шини, на застосування якої вони розраховані: ISA (8-ми й 16-ти розрядні), MCA (16-ти розрядні), EISA (32-х розрядні), PCI (32-х розрядні);
- наявністю альтернативних зовнішніх портів (UTP, BNC, AUI, FO). Зазначимо, що не дивлячись на можливу наявність альтернативних портів, активним може бути тільки один із них;
- кількістю каналів запиту переривань (IRQ), що може опрацьовувати адаптер;
- програмним конфігуруванням (jamper less) або конфігуруванням за допомогою перемичок (jampers);
- ємністю оперативної пам'яті, призначеної для буферизації пакетів;
- наявністю або відсутністю світодіодних індикаторів: передавання (Transmit), приймання (Receive), стану зв'язкового біту (Link Beat Status), обраного порту (Port Selected);
- можливістю підтримки декількох стандартів мереж (як правило 10Base-T і 100Base-TX або 10Base-T і 100VG-AnyLAN);
- засобом організації взаємодії з комп'ютером (bus master adapter, DMA adapter);
- режимом роботи адаптеру: режим поділу пам'яті (shared memory), циклічного вводу-виводу (Rep I/O), паралельної робота каналів приймання й передавання (full duplex), суміщення операцій передавання даних через трансивер зі зчитуванням даних з ОЗУ комп'ютера в буфер адаптеру (parallel tasking) і т.п.

Для визначення точки призначення пакетів (frames) у мережі Ethernet використовується **MAC-адреса**. Це унікальний серійний номер, який присвоюється кожному мережевому пристрою Ethernet для ідентифікації його в мережі. MAC-адреса присвоюється адаптеру його виробником, але може бути змінена за допомогою програми. Робити це не рекомендується (тільки в разі виявлення двох пристроїв у мережі з однаковою MAC-адресою). При роботі мережеві адаптери проглядають весь мережевий трафік і шукають у кожному пакеті свою MAC-адресу. Якщо такий знаходиться, то адаптер декодує цей пакет. Існують також спеціальні способи розсилання пакетів усім пристроям мережі одночасно (broadcasting). MAC-адреса має довжину 6 байт і, зазвичай, записується в шістнадцятирічному вигляді, наприклад, 12:34:56:78:90:AB

Двокрапки можуть бути відсутніми, але їх наявність робить число більш читабельним. Кожний виробник присвоює адреси з діапазону адрес, що належить йому. Перші три байти адреси визначають виробника.

При виборі мережевого адаптера слід брати до уваги наступні міркування.

- Тип шини даних, який установлений у вашому комп'ютері (ISA, VESA, PCI або який-небудь ще). Старі комп'ютери 286, 386 містять тільки ISA, відповідно й карту можна встановити тільки на шині ISA. 486 – ISA і VESA або ISA і PCI (хоча існує плата, яка підтримує всі три ISA, VESA і PCI). Дізнатись це, можна з опису або подивившись на саму материнську плату, після того як відкриєте корпус комп'ютера. Можливо встановити мережеву карту в будь-який відповідний вільний роз'єм. Pentium, Pentium Pro, Pentium-2 і ним подібні використовують ISA і PCI шини даних, причому шина ISA – для сумісності зі старими картами.
- Тип мережі, до якої будете підключатися. Якщо, наприклад, підключатися до мережі на коаксіальному кабелі (10Base-2, "тонкий" Ethernet), то потрібна мережева карта з відповідним роз'ємом (BNC).
- Його вартість, ураховуючи, що ціна на саме передове комп'ютерне встаткування падає дуже швидко. А вийти з ладу мережева карта, за несприятливих обставин, може дуже легко незалежно від того, скільки грошей за неї заплатили.

Ще треба враховувати підтримку вашого адаптера різними операційними системами.

У разі сумісних, наприклад, з NE2000 ISA адаптерів проблем, зазвичай, не виникає, просто вказуєте "NE2000 Compatible" не замислюючись яка фірма його зробила. Існує ще цілий ряд адаптерів, підтримка яких забезпечена практично у всіх операційних системах. Для того щоб перевірити які мережеві карти підтримує ваша ОС треба подивитися в "Compatibility List". Часто в такому списку вказаний чіп, який підтримується, тобто якщо мережевий адаптер зроблений на основі цієї мікросхеми, то працездатність, як правило, забезпечена.

Для нормальної роботи кожної мережевої плати їй необхідні адреса уведення-виведення й номер переривання (IrQ).

Конфігурація мережевої плати полягає в налагодженні її на вільну адресу й переривання, які потім використовуватимуться операційною системою. Адреса (i/o port) і переривання (IrQ) для кожної мережевої плати повинне бути своє, відмінне від інших пристроїв комп'ютера. Сучасні мережеві плати, що підтримують технологію Plug-n-play самі виконують цю операцію, для всіх інших необхідно самостійно виконати її.

Пошук незайнятої адреси й переривання залежить від апаратної частини комп'ютера або його програмного забезпечення.

Установлення мережевої карти

Для установлення мережевої карти необхідно виключити й знеструмити обчислювальну систему, зняти захисний кожух системного блоку і встановити мережеву карту в слот, що відповідає її інтерфейсові.

Установлення драйвера мережевої карти при наявності операційної системи Windows

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настроювання → Панель керування**.
2. Відкрийте об'єкт **Мережа**. У вікні, що з'явилося, на вкладці **Конфігурація** натисніть кнопку **Додати.**
3. Виберіть тип установлюваного компонента: **Мережева карта**. Натисніть кнопку **Додати.**
4. Виберіть відповідні пункти у вікнах **Виготовлювачі**: Виявлені мережеві драйвери й Мережеві плати: **Драйвер**, наприклад, **RTL8139.** Натисніть кнопку **OK**.
5. Відзначте, що в системі встановлені наступні компоненти: драйвер, наприклад, **RTL8139** і відповідні йому протоколи.
6. Перезавантажите систему.

Примітка: якщо встановлена операційна система Windows XP, то драйвер мережевої карти встановлюється операційною системою автоматично.

Видалення мережевої карти

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настроювання → Панель керування**.
2. У вікні, що з'явилося відкрийте об'єкт **Мережа**.
3. На вкладці **Конфігурація** у вікні **в системі встановлені наступні компоненти** виберіть тип компонента, що видаляється: **Драйвер RTL8139.** Натисніть кнопку **Видалити**.
4. Натисніть кнопку **OK**.
5. Відмітьте зникнення в системі наступних компонент Драйвера **RTL8139** і відповідних йому протоколів.
6. Перезавантажте систему.

Підключення до локальної мережі. Налагодження мережевих протоколів

Перед початком налагодження мережевого інтерфейсу необхідно встановити мережеву карту. Після коректного встановлення драйвера мережевої карти необхідно встановити мережеві протоколи, які використовуватимуться в даному інтерфейсі. Після налагодження протоколів перевіряється робота системи в мережі, починаючи з команд ping для перевірки зв'язку на фізичному й канальному рівні, tracert для перевірки роботи маршрутизації, і завершуючи роботою конкретних додатків (електронна пошта, веб-сервер) на прикладному рівні.

При роботі в мережі Internet можуть виникати ситуації, коли необхідно визначити працездатність того або іншого вузла, або каналу зв'язку, а також з'ясувати, яким конкретно каналом передаються повідомлення. Для цієї мети служать утиліти ping і traceroute. Ці утиліти, як і багато інших, були розроблені під ОС UNIX, але в даний час вони поширені практично у всіх ОС. Назви програмних файлів утиліт, а також формат їхнього командного рядка може змінюватися в залежності від версії ОС, але принципи роботи й призначення утиліт однакові (наприклад, під ОС типу Windows NT утиліта traceroute зветься tracert, однак, виконує вона ті ж дії).

Утиліта ping базується на протоколах ICMP (Internet Control Message Protocol) і UDP. Протокол ICMP перевіряє стан мережевих пристроїв і формує відповідні повідомлення. При виникненні несправності в якому-небудь пристрої він сповіщає про це іншим пристроям. ICMP працює на тім же рівні, що й протокол IP.

Вхідними даними для утиліти ping є адреса вузла, маршрут до якої підлягає трасуванню. Адреса вузла задається у вигляді IP-адреси або доменної адреси в командному рядку при запуску утиліти.

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

Локальна адреса вузла, яка визначається технологією, за допомогою якої побудована окрема мережа, у яку входить даний вузол. Для вузлів, що входять у локальні мережі, це MAC-адреса мережевого адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками встаткування і є унікальними адресами, оскільки управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байтів: старші 3 байти – ідентифікатор фірми виробника, а молодші 3 байти призначаються унікальним чином самим виробником. 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 мережевому рівні. Вона призначається адміністратором під час конфігурації комп'ютерів і маршрутизаторів. IP-адреса складається із двох частин: номера мережі й номера вузла. Номер мережі може бути вибраний адміністратором довільно або призначений за рекомендацією спеціального підрозділу Internet (Network Information Center, NIC), якщо мережа повинна працювати як складова частина Internet. Зазвичай провайдери послуг Internet одержують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами.

Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Розподіл IP-адреси на поле номера мережі й номера вузла - гнучкий, і межа між цими полями може встановлюватися дуже довільно. Вузол може входити в декілька IP-мереж. У цьому випадку вузол повинен мати декілька IP-адрес, за кількістю мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве 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, звана також DNS-ім'ям, використовується на прикладному рівні, наприклад, у протоколах FTP або telnet.

На основі відгуків протоколу ICMP утиліта будує протокол трасування з'єднання, з якого можна визначити через які вузли й протягом якого часу проходили пакети за мережею до заданої адреси. Версія BSD утиліти ping в ОС UNIX дозволяє виконувати дуже широкий набір функцій протоколювання і трасування з'єднань. В інших ОС (наприклад, у Windows NT) частина функцій трасування виділена в іншу утиліту - traceroute (у Windows NT - tracert), а утиліта ping дозволяє тільки перевірити наявність з'єднання.

Сервісні утиліти ping і traceroute найчастіше вимагають для свого запуску наявності в користувача адміністративних прав. Це пов'язано з тим, що при трасуванні з'єднань вони посилають у мережу велику кількість пакетів, які не несуть ніякої корисної інформації. Некваліфіковане або навмисне злочинне використання цих утиліт може привести до значного захаращення трафіка мережі, що у свою чергу може ускладнити роботу багатьох прикладних програм.

Зазначені сервісні утиліти виконують в основному налагоджувальні, а не прикладні функції. Вони найчастіше використовуються адміністративним персоналом мереж і вузлів для перевірки справності встаткування й правильності настроювань програмних систем. Вони також корисні розроблювачам прикладних програм, орієнтованих на роботу в мережі, для перевірки відгуку цих програм на вхідні повідомлення. Версії цих утиліт у багатьох ОС (насамперед - під ОС UNIX) дозволяють одержати додаткову налагоджувальну інформацію, корисну розроб-

лювачам програм при налагодженні. Наприклад, можлива роздруківка вмісту вхідних і вихідних пакетів, роздруківка заголовків пакетів (у стандартних утилітах ping і tracert під графічною оболонкою типу Windows такі налагоджувальні функції не надаються).

Порядок виконання: при наявності операційної системи Windows

Установлення протоколів

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настройка → Панель управління.**
2. Відкрийте об'єкт **Мережа**. У вікні, що з'явилося, на вкладці **Конфігурація** натисніть кнопку **Додати.**
3. Виберіть тип установлюваного компоненту: **Протокол.** Натисніть кнопку **Додати**.
4. Виберіть відповідні пункти у вікнах **Розробники,** наприклад**, Microsoft** і **Мережеві протоколи: IPX/SPX–протокол**. Натисніть кнопку **OK.**
5. Для коректного налагодження драйвера перезавантажте систему.

Видалення протоколів

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настройка -> Панель Управління**.
2. Відкрийте об'єкт **Мережа**. У вікні, що з'явилося, на вкладці **Конфігурація**, виберіть компонент **IPX/SPX-протокол**. Натисніть кнопку **Видалити**.
3. Для коректної настройки драйвера перезавантажте систему.

Налагодження мережевого протоколу TCP/IP

1. Виберіть компонент **TCP/IP**. У вікні, що з'явилося натисніть кнопку **Властивості**.
2. На вкладці **Адреса IP** видаліть значення параметрів **IP-адреса** й **Маска підмережі.**
3. На вкладці **Шлюз** видаліть значення параметра **Встановлені шлюзи.**
4. На вкладці **Конфігурація,** видаліть значення параметрів **Ім'я комп'ютера**, **Домен**, **Порядок проглядання серверів DNS**.
5. Натисніть кнопку **OK**.

Перевірка налагодження протоколу

Після перезавантаження комп'ютера перевірте роботу мережевого інтерфейсу командою ping IP-адреса й роботу серверу DNS командою ping доменне_ім'я, наприклад: ping carrier.kiev.ua; ping lincom.kharkiv.ua. Перевірте роботу маршрутизації командою tracert IP-адреса (tracert доменне_ім'я, наприклад: tracert vonter.nas.gov; tracert itc.kiev.ua).

Налагодження параметрів локальної мережі

Налагодження параметрів локальної мережі проводиться через **панель задач → Сеть** (рис. 1.30) команда **Состояние,** або мережеві підключення (рис. 1.31). З'явиться діалогове вікно із вкладками **Общие** (рис. 1.32) і **Поддержка** (рис. 1.33). При введені команди **Свойства** на вкладці **Общие** можна вибрати служби (рис. 1.34) та налагодити контролер мережі.

Налагодження параметрів служб та протоколу TCP/IP (рис. 1.35) проводиться введенням команди **Свойства.** При введені команди **Свойства** на вкладці **Общие** можна вибрати служби (рис. 1.36) та налагодити контролер мережі. При введенні команди **Дополнительно** з'являється можливість додаткового налагодження протоколу TCP/IP (рис.1.37), DNS сервера – (рис. 1.38), параметрів підключення – (рис. 1.39), фільтрацію трафіка мережі – (рис. 1.40) та налагодження її властивостей (рис. 1.41).

На вкладці **Проверка подлинности** та **Дополнительно** вибираються параметри захисту комп'ютера в мережі (рис. 1.42– 1.49).

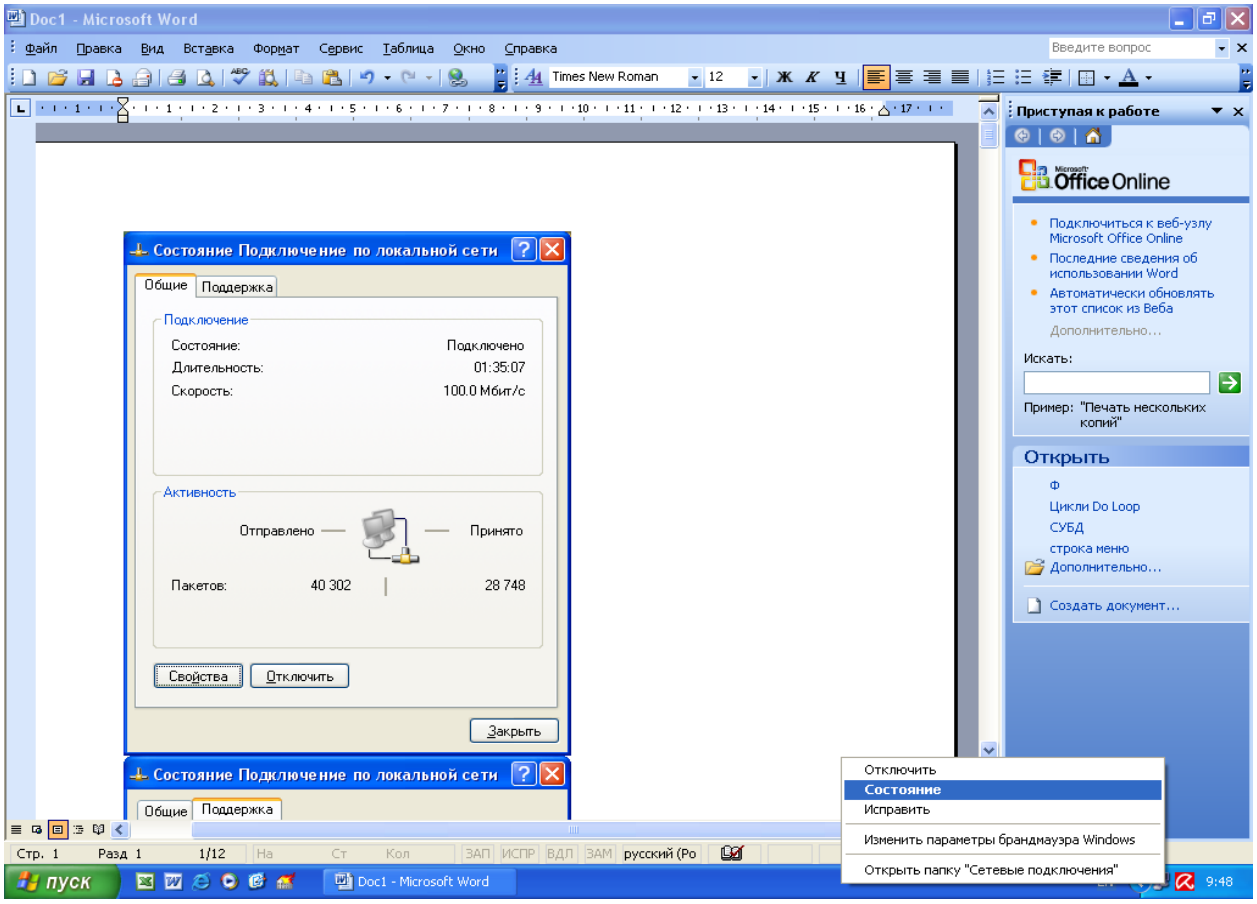


Рис. 1.30. Початок налагодження параметрів локальної мережі

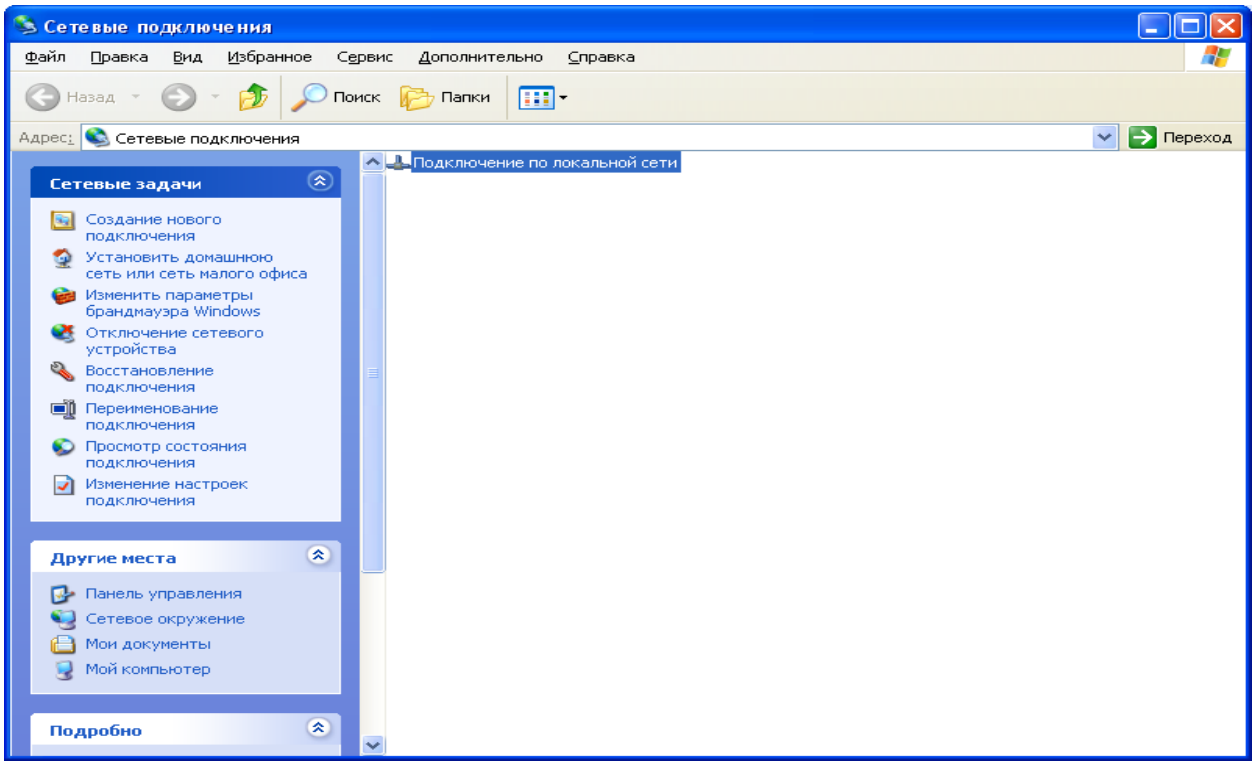


Рис. 1.31. Мережеві підключення

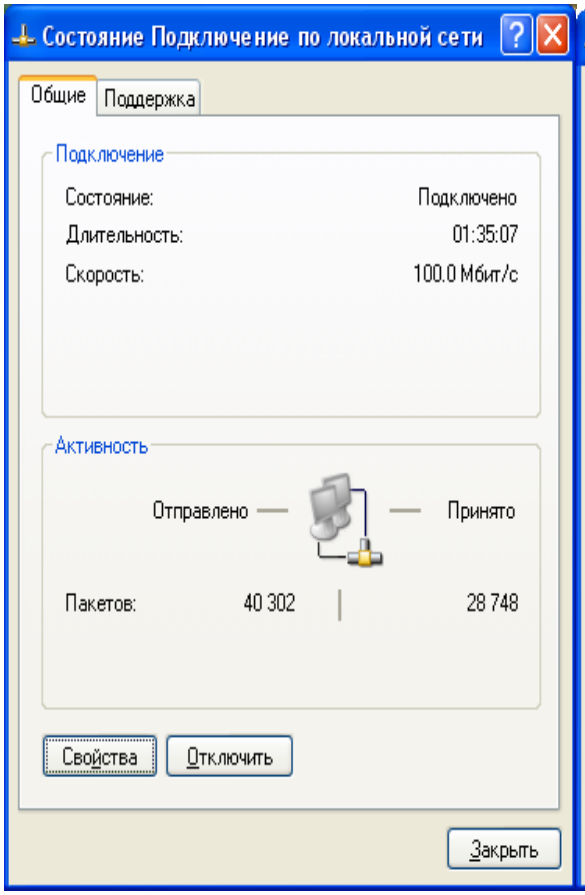


Рис. 1.32. Стан підключення до мережі вкладка **Общие**

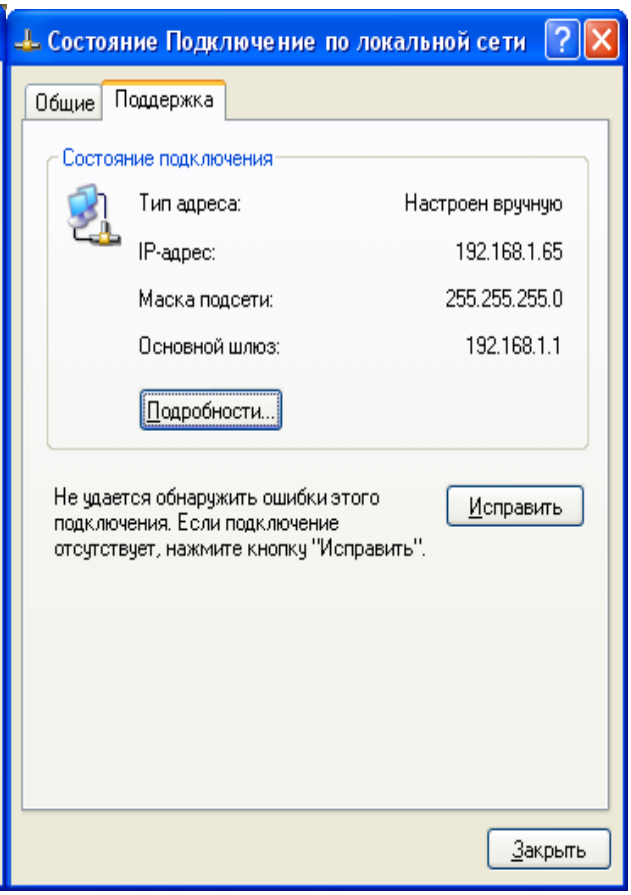


Рис. 1.33. Вкладка **Поддержка**

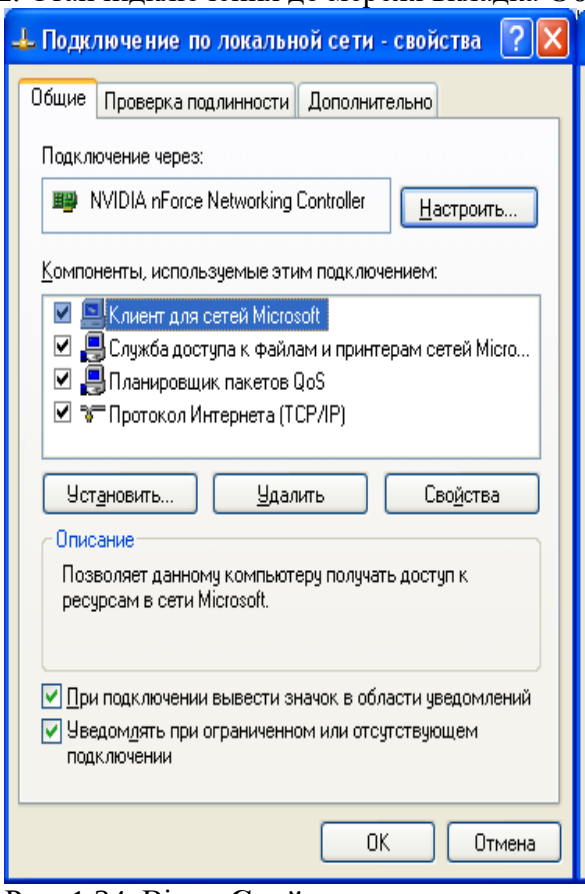


Рис. 1.34. Вікно **Свойства**.

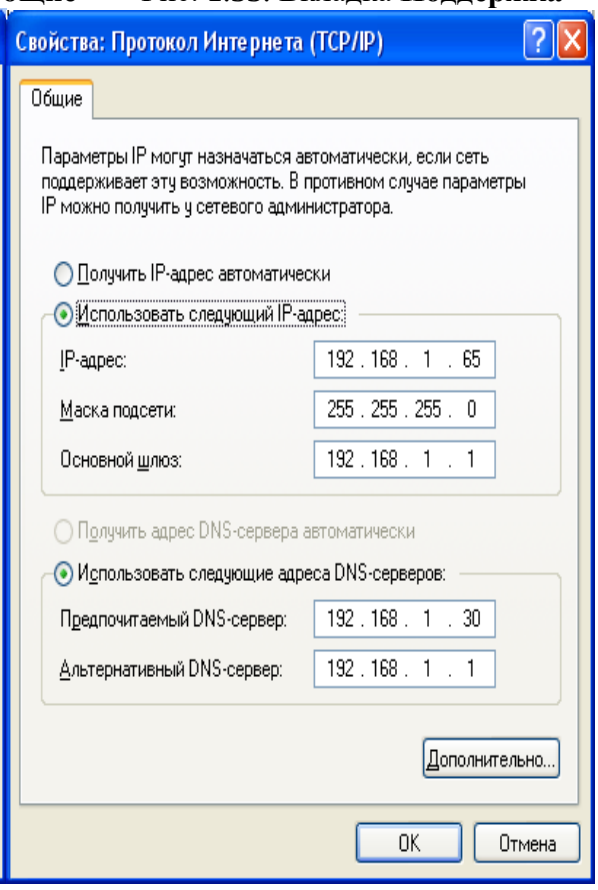


Рис. 1.35. Параметри протоколу TCP/IP

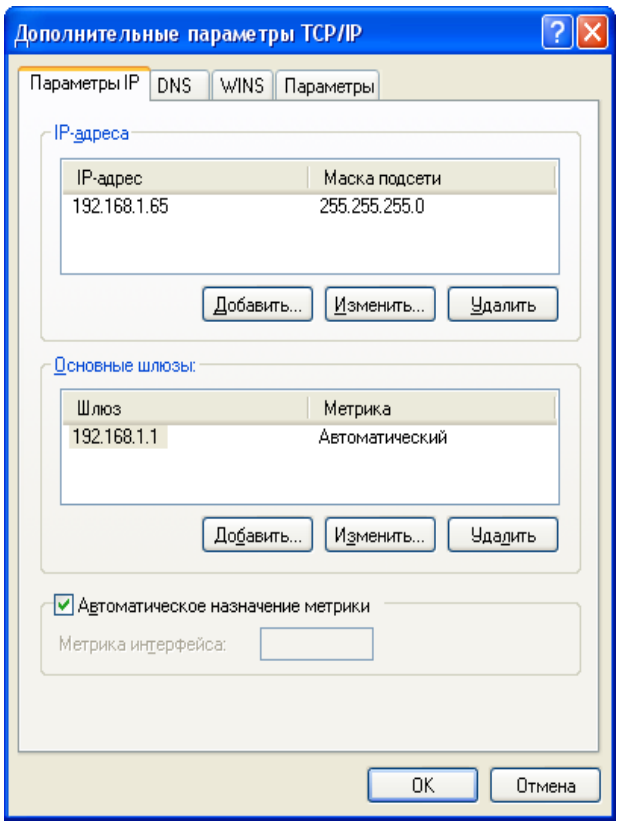


Рис. 1.36. Додаткові параметри протоколу TCP/IP

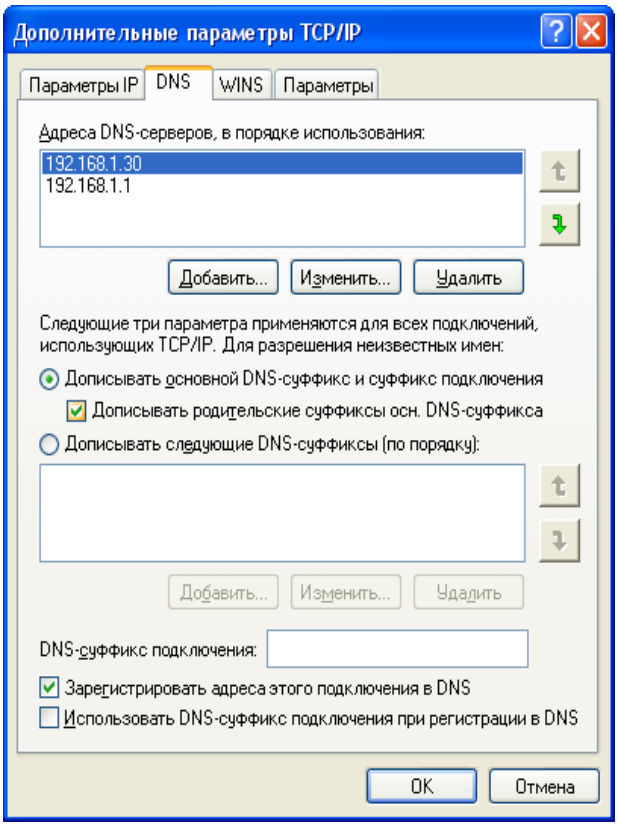


Рис. 1.37. Параметри DNS сервера

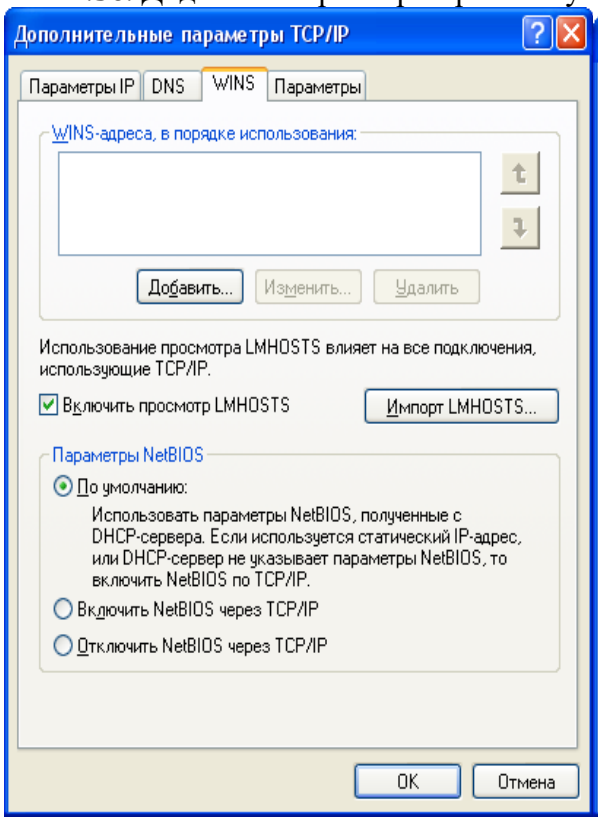


Рис. 1.38. Параметри підключення

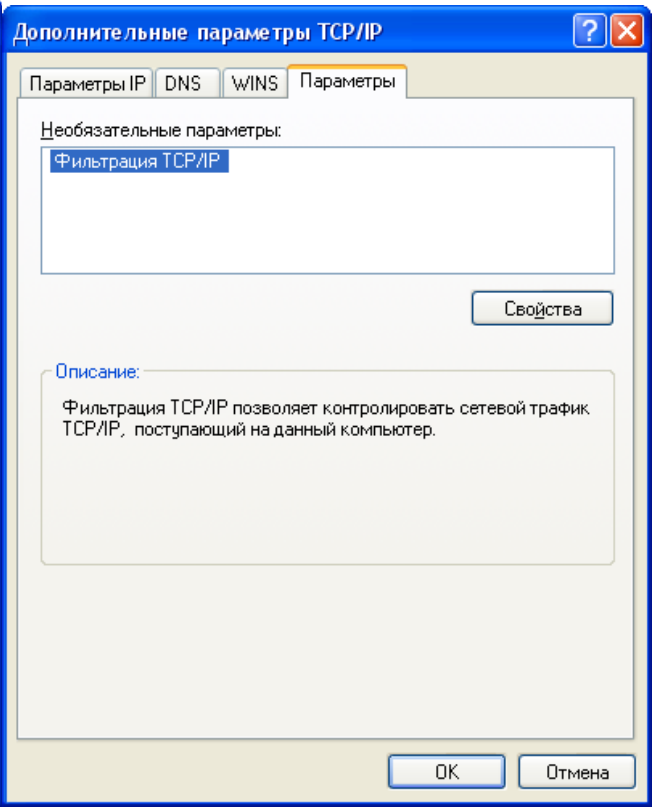


Рис. 1.39. Фільтрація трафіка

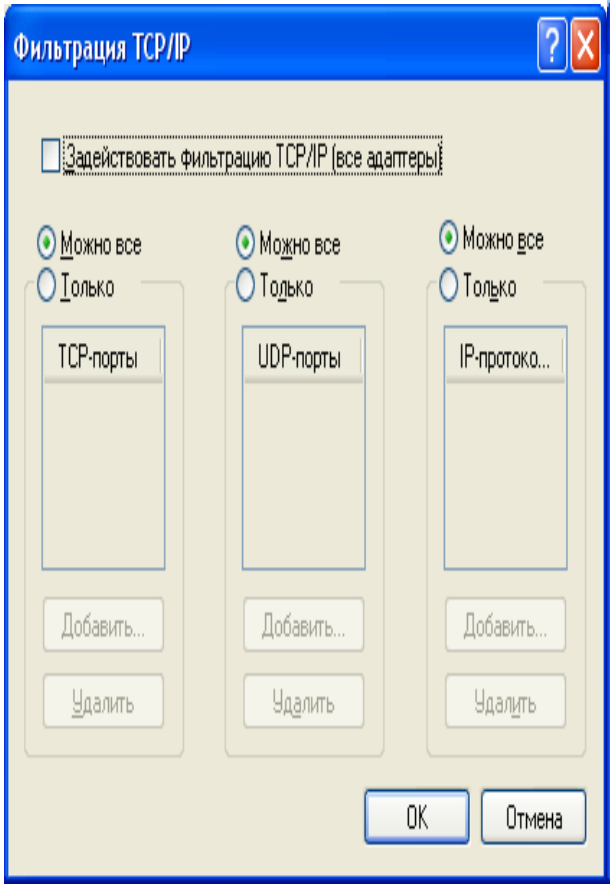


Рис. 1.40. Відбір параметрів фільтрації трафіка

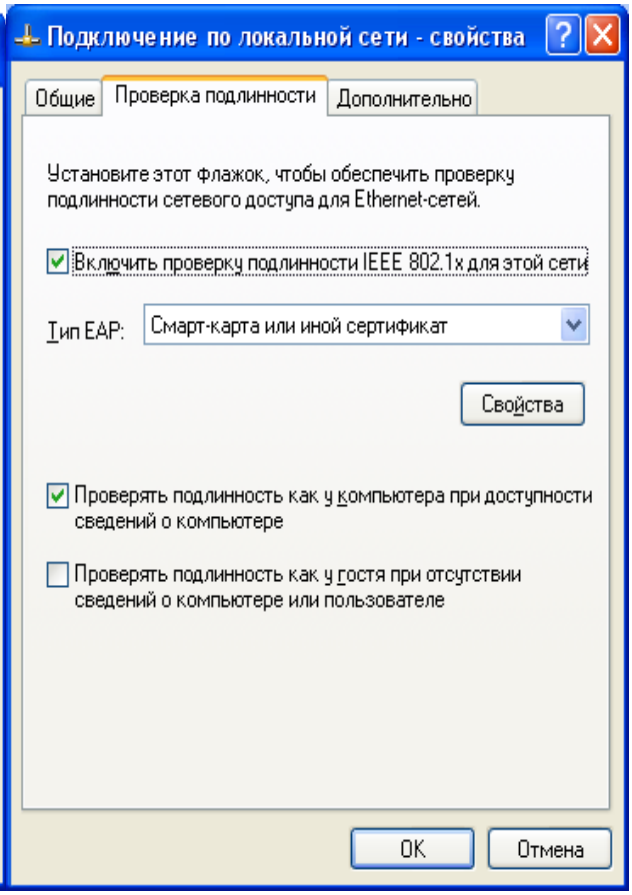


Рис. 1.41. Параметри захисту комп'ютера

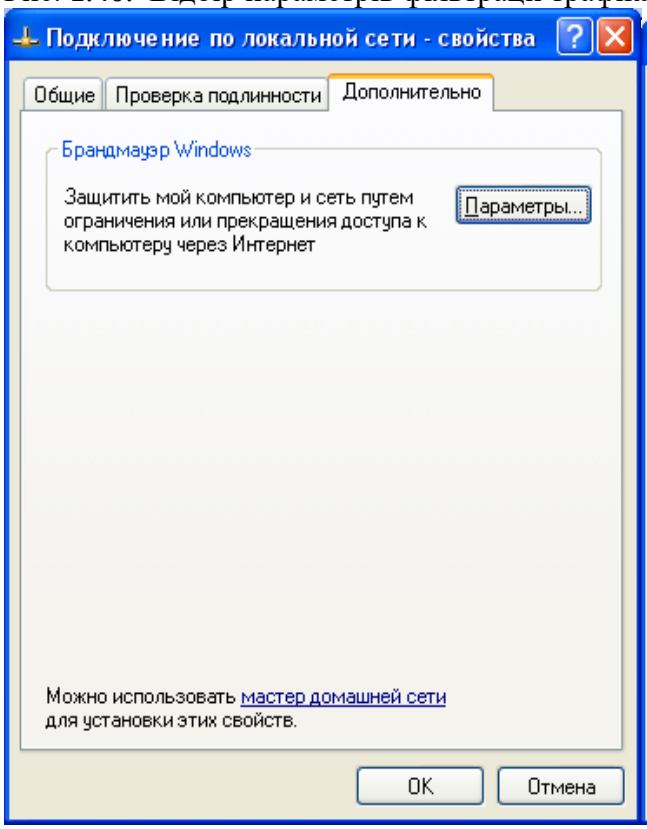


Рис. 1.42. Запуск брандмауера

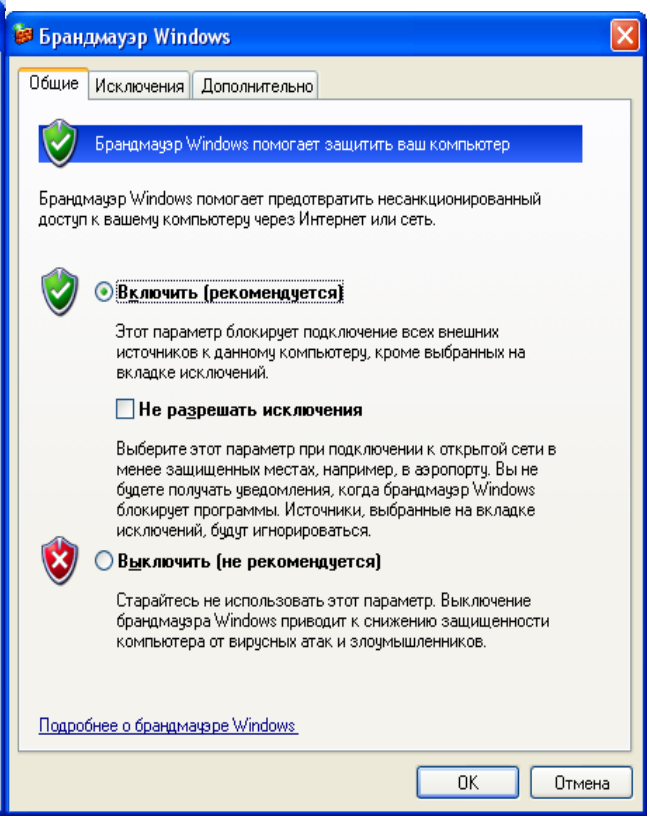


Рис. 1.43. Відбір параметрів брандмауера

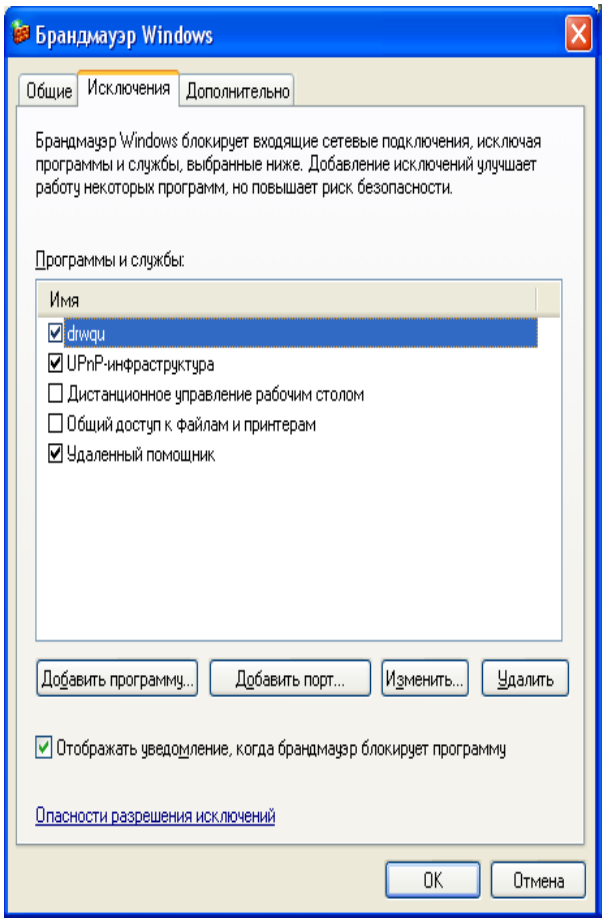


Рис. 1.44. Дозвіл виключень в захисті комп'ютера

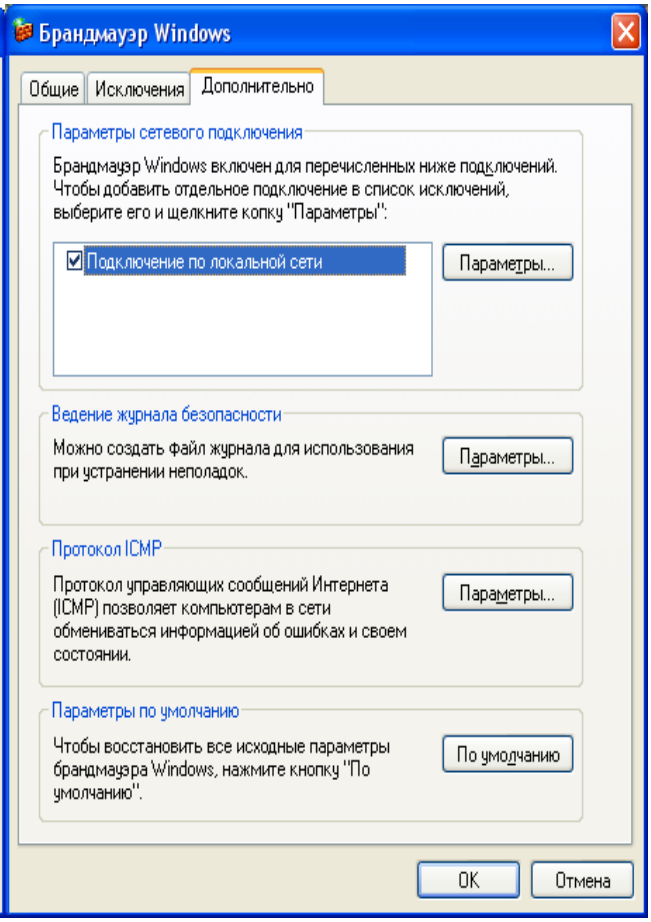


Рис. 1.45. Вибір параметрів захисту

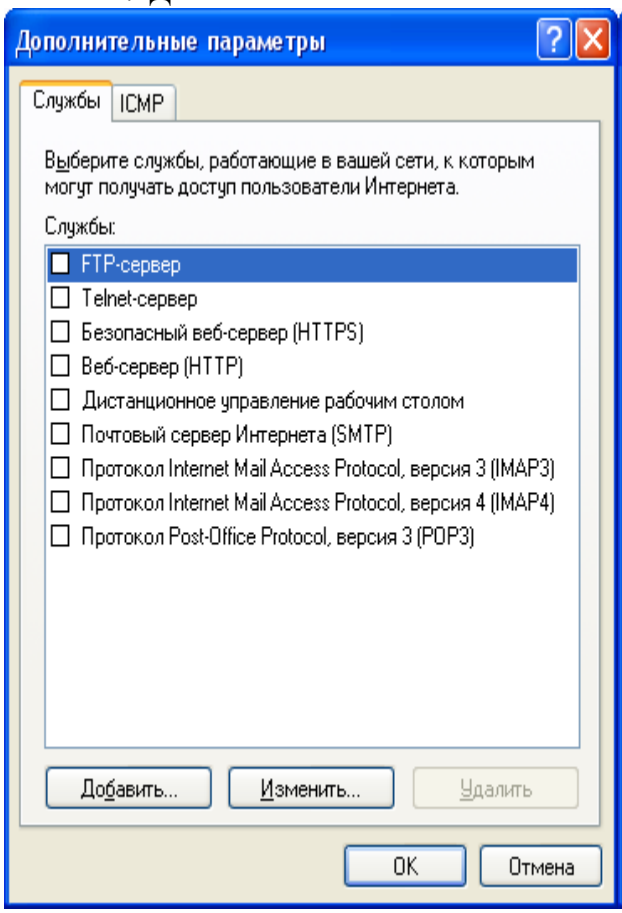


Рис. 1.46. Служби захисту

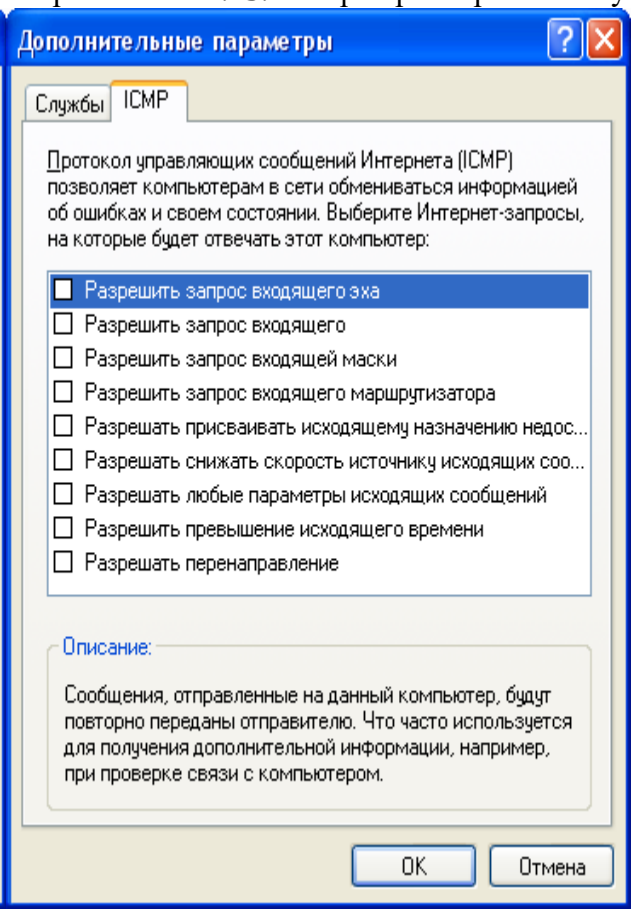


Рис. 1.47. Параметри відповіді на запити

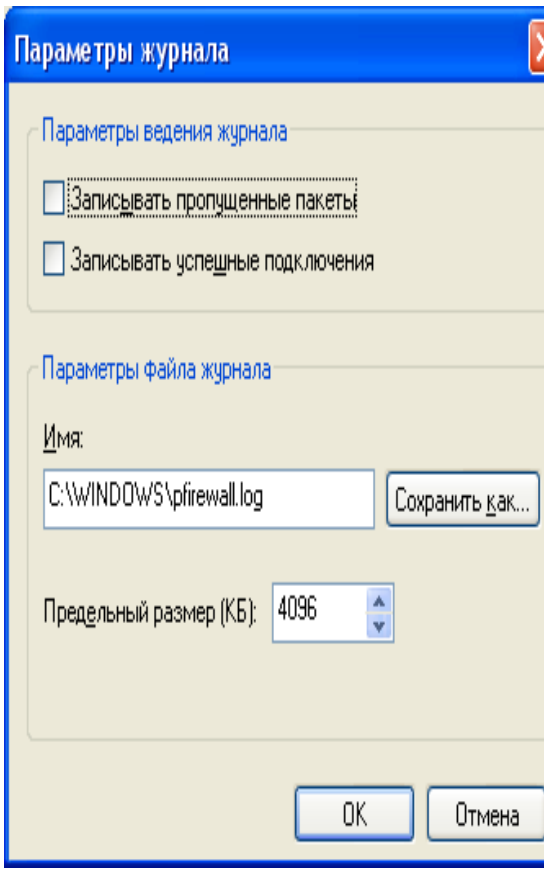


Рис. 1.48. Параметри журналу безпеки

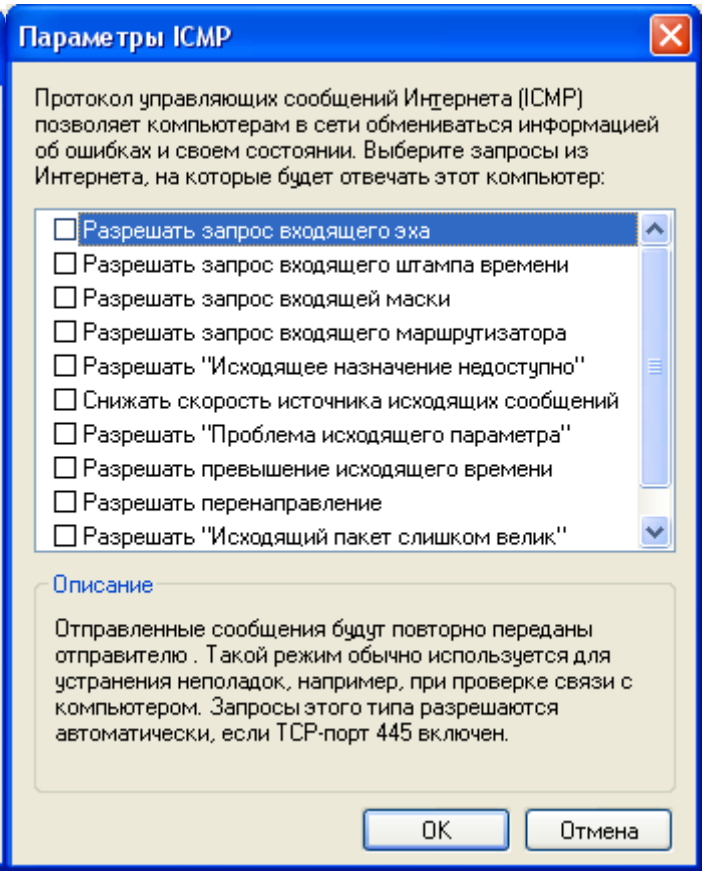


Рис. 1.49. Параметри відповіді на помилки

Мережа Windows for Workgroups

Робота мережі забезпечується програмами операційних систем Windows 3.X, Windows 95, Windows 98, Windows NT, Milenium, Windows 2000, Windows XP. Як правило, відразу при запуску системи машина автоматично запитує Login name (те ж саме, що й user ID) і пароль. Настроювання мережі Windows for Workgroups проводиться через панель керування, піктограму “мережа” або піктограму “сетевое окружение” на робочому столі Windows, шляхом вибору пункту властивості з контексно-залежного меню. У вкладці комп’ютер (рис. 1.50) можна визначити ім’я комп’ютера в мережі та робочу групу, до якої він входить. В інших діалогових віконцях провадиться налагодження відповідних служб і протоколів; настроюються мережеві адаптери, прив’язки; у протоколі TCP/IP для кожного мережевого адаптеру вказують IP-адресу робочої станції, маску підмережі, основний шлюз, настроюють службу DNS, указуючи ім’я вузла, домен, порядок пошуку служби DNS, адреса WINS, параметри маршрутизації.

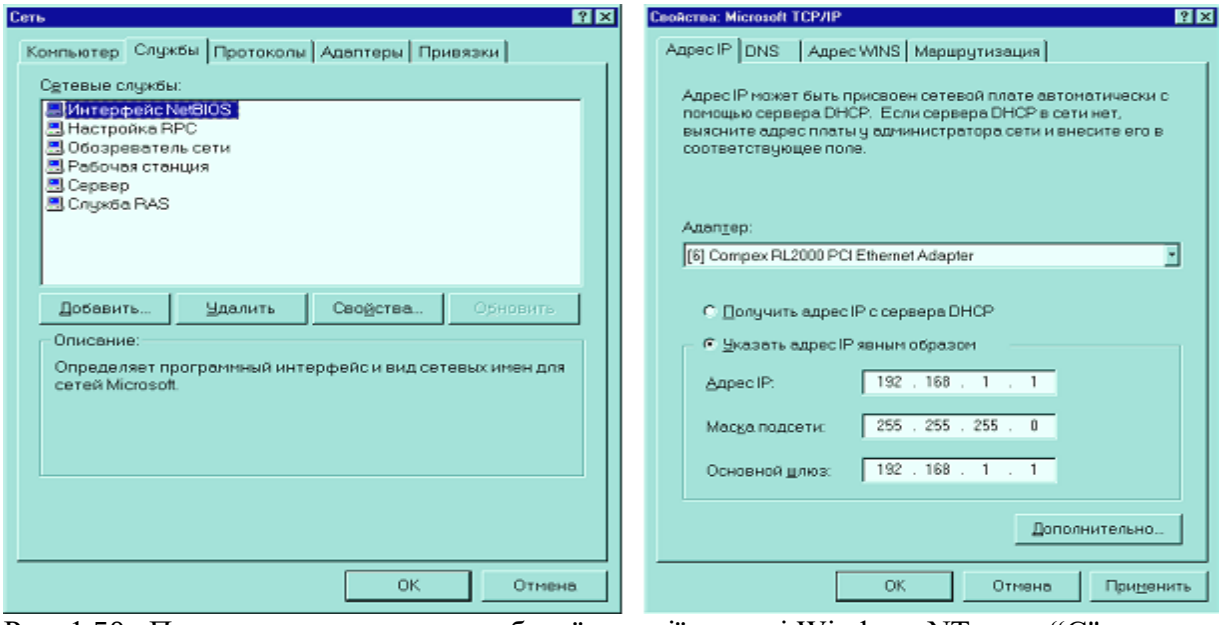


Рис. 1.50. Приклад настроювання робочої станції мережі Windows NT типу “С"

Для одержання доступу до мережі двічі клацніть піктограму "**Мережеве оточення**" на робочому столі , а потім двічі клацніть значок комп'ютера. Якщо потрібного комп'ютера немає в списку, двічі клацніть піктограму "**Вся мережа**".

Пошук комп'ютера в мережі

Натисніть кнопку **Пуск**, виберіть команду **Знайти**, а потім виберіть **Комп'ютер**. Якщо відомо ім'я комп'ютера, запишіть його в поле **Ім'я**. Наприклад: marketing.

Призначення загального каталогу

У вікні **Мій комп'ютер** або в провіднику Windows виберіть каталог, що потрібно зробити загальним. У меню **Файл** виберіть команду **Властивості**. Виберіть вкладку **Доступ**, а потім виберіть параметр **Загальний ресурс**. Виберіть тип доступу в групі **Тип доступу** й, при необхідності, уведіть пароль.

Призначення загального принтера

Натисніть кнопку **Пуск**, виберіть команду **Настроювання**, а потім виберіть **Принтери**.

Клацніть значок принтера, що потрібно зробити загальним.

У меню **Файл** виберіть команду **Властивості**. Виберіть вкладку **Доступ**, а потім виберіть параметр **Загальний ресурс** (рис. 1.51).

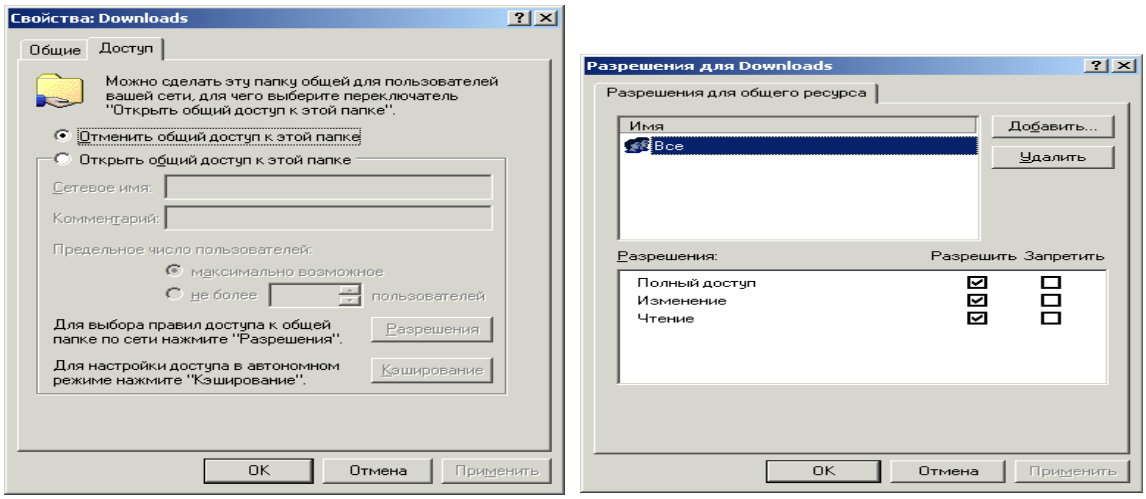


Рис. 1.51. Керування доступом до каталогів і принтерів

У вікні **Мій комп'ютер** або у вікні провідника виберіть загальну папку або принтер, доступ до яких потрібно обмежити. У меню **Файл** виберіть команду **Властивості**. Виберіть вкладку **Доступ**. Якщо застосовується керування доступом на рівні користувачів, натисніть кнопку **Додати** для додавання користувачів, яким дозволено використовувати принтер або каталог. Якщо застосовується керування доступом на рівні ресурсів, уведіть пароль для доступу до каталогу або принтера.

Призначення імені комп'ютера в мережі

Для відкриття діалогового вікна **Мережа** можна натиснути кнопку **Пуск**, вибрати команди **Настроювання → Панель керування**, а потім двічі клацнути значок **Мережа**.

Виберіть вкладку **Ідентифікація**. Уведіть ім'я комп'ютера. Ім'я комп'ютера повинно бути унікальним. Неможливо використовувати ім'я, що вже використовується в мережі. Можна також увести опис комп'ютера. Ці дані будуть доступні для інших користувачів при перегляді списку мережевих комп'ютерів.

Використання інспектора для контролю за використанням загальних ресурсів

Інспектор мережі дозволяє з'ясувати, хто саме використовує загальні ресурси вашого комп'ютера. Він також дає можливість відкривати спільний доступ до ресурсів і відключати інших користувачів від комп'ютера або окремих файлів.

Запуск інспектора установлення клієнта для мереж Microsoft, а також запуск служби доступу до файлів і принтерів комп'ютера

Для запуску інспектора натиснути кнопку **Пуск**, вибрати команди **Програми**, **Стандартні** й **Службові**, а потім вибрати команду **Інспектор**.

Використання системного монітора

Системний монітор використовують для спостереження за швидкодією комп'ютера або мережі. Кожний обраний показник відображається на діаграмі, що обновлюється кожні 5 секунд.

Для запуску системного монітора натиснути кнопку **Пуск**, вибрати команди **Програми**, **Стандартні** й **Службові**, а потім вибрати команду **Системний монітор**.

Робота в діалоговому режимі в мережі Windows NT

Уведіть команду **Розмова** із підменю **Стандартні**, підменю **Програми**, підменю **Старт**. У діалоговому віконці введіть, або виберіть зі списку ім'я комп'ютера мережі, з яким буде організовано діалоговий режим. Уведіть команду **Розпочати розмову** із підменю **Файл**. Користувач комп'ютера, з яким здійснюється зв'язок у режимі **Розмова,** при появі відповідного повідомлення в панелі задач повинен увести команду **Відповісти** із підменю **Файл**.

Створення мережевих дисків

Мережеві диски – це диски іншого комп'ютера мережі, який даний комп'ютер сприймає як свій додатковий зовнішній пристрій.

Операційна система Windows надає можливість користувачеві працювати з деякою мережевою папкою (каталогом), до якої призначений доступ, як із дисковим пристроєм. Логічний диск, отриманий у результаті такого підключення називають мережевим диском.

Будь-яка папка може бути призначена мережевим диском.

Для створення мережевого диска викличте контекстне меню папки **Сетевое окружение** і виберіть пункт **Підключити мережевий диск**, з'явиться діалогове вікно **Підключення мережевого диска** (рис. 1.52).

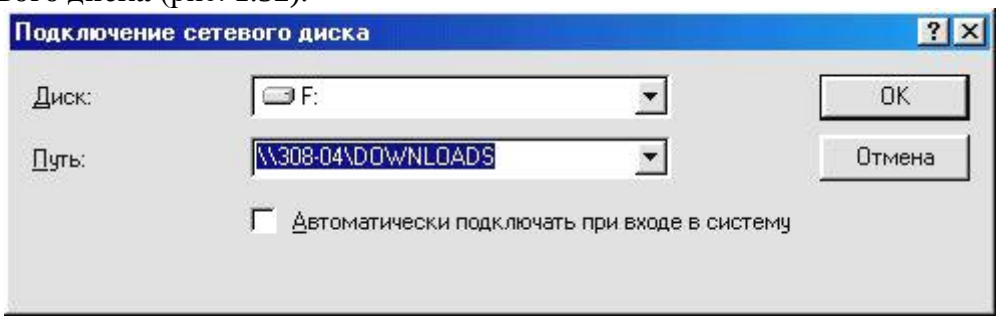


Рис. 1.52. Вікно створення мережевого диску

Поле **Диск** дозволяє призначити букву для мережевого диска.

Поле **Шлях** дозволяє вказати ім'я мережевого ресурсу для підключення в якості мережевого диску.

Якщо перемикач **Автоматично підключати при вході в систему** виключений, то диск буде підключатися за командою користувача, якщо ж він включений, то диск буде підключатися автоматично.

Після того як встановили необхідні параметри для підключення мережевого диска, підтвердіть своє рішення натисканням кнопки **ОК**.

Для перегляду змісту мережевого диска можна використовувати вікно **Мій комп'ютер** і працювати з ним як зі звичайним дисковим пристроєм.

Щоб відключити мережевий диск відкрийте його контекстне меню й виберіть пункт **Відключити**.

У Windows Vista зайдіть в розділ **Управління мережевими підключеннями** – його значок знаходиться на панелі **Центру управління мережами і загальним доступом.** Клацніть правою кнопкою мишки по значку вашого кабельного з'єднання і виберіть меню **Властивості**. У меню, що відкрилося, клацніть по рядочку **Протокол Інтернету версії 4 (TCP/IP v4)** – відкриється нове вікно, куди і зможете ввести відповідні параметри.

Перебудова мережі з виділеним сервером, наприклад, Windows 2000 Server на одноранговy

При необхідності можна перебудувати мережу з виділеним сервером (Windows 2000 Server) в одноранговy мережу:

1. Клацнути на Робочому столі на ярличку **Мій комп'ютер** правою кнопкою.
2. Вибрати з контекстного меню **Властивості.**

На вкладці **Загальні** вказано ім’я комп’ютера в локальній мережі. На вкладці **Мережева ідентифікація** вказано повне ім’я комп’ютера в мережі з виділеним сервером і робоча група в одноранговій мережі. Якщо ввести команду ідентифікація, з’явиться діалогове вікно (рис. 1.53).

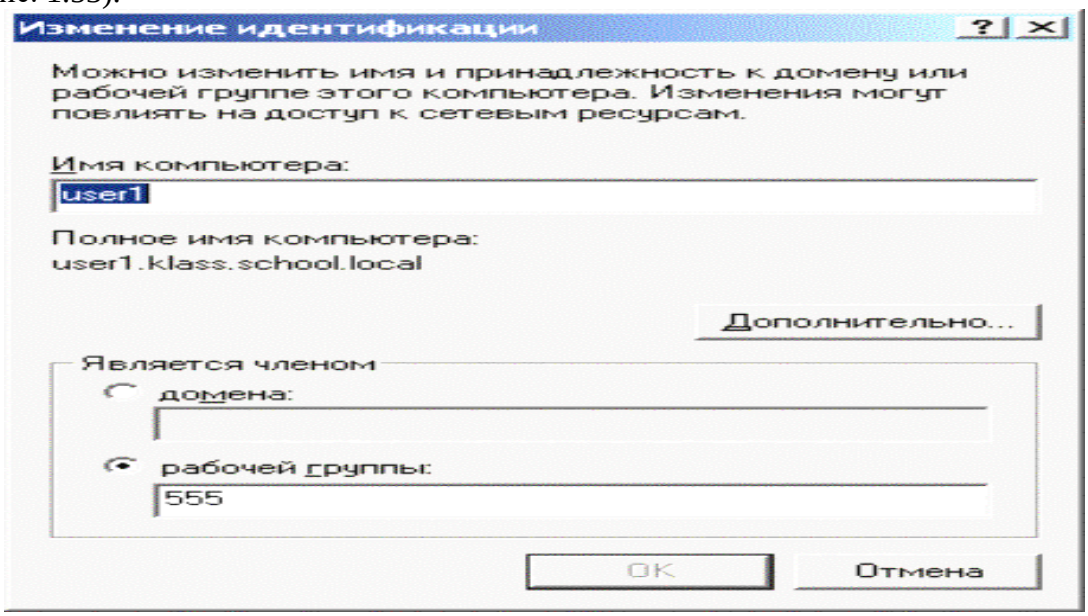


Рис. 1.53. Вибір параметрів мережі

Працюючи з мережею з виділеним сервером, вибираємо домен. Працюючи з одноранговою мережею, вибираємо робочу групу.

Підключення мережевого принтера.

1. Клацнути в панелі завдань на кнопці **Пуск**.
2. Вибрати в головному меню команду **Налагодження → Принтери**.
3. У вікні **Принтери** клацнути на ярличку **Установка принтера** (рис. 1.54).
4. Далі з’явиться вікно **Майстра установки** (рис. 1.55), в якому необхідно клацнути на кнопці **Далі.**
5. У наступному вікні майстра вибрати мережевий принтер і клацнути **Далі**.
6. У наступному вікні клацнути на перемикач **Введіть ім’я принтера** і клацнути подвійним клацанням в полі введення **Ім’я** (рис. 1.56).
7. Потім вибрати **мережевий** принтер і клацнути **Далі.**
8. У наступному вікні вибрати принтер одного з комп’ютерів мережі й клацнути **Далі,** а в останньому (рис. 1.57) – **Готово.**

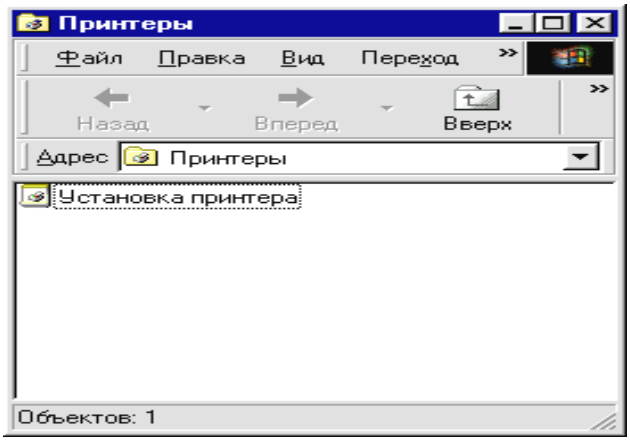


Рис. 1.54. Вікно установки принтера

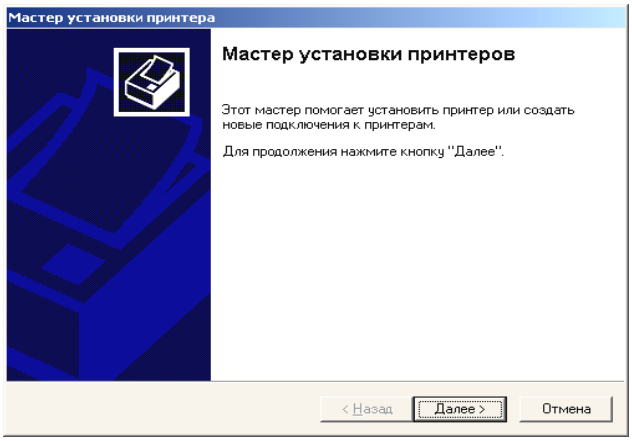
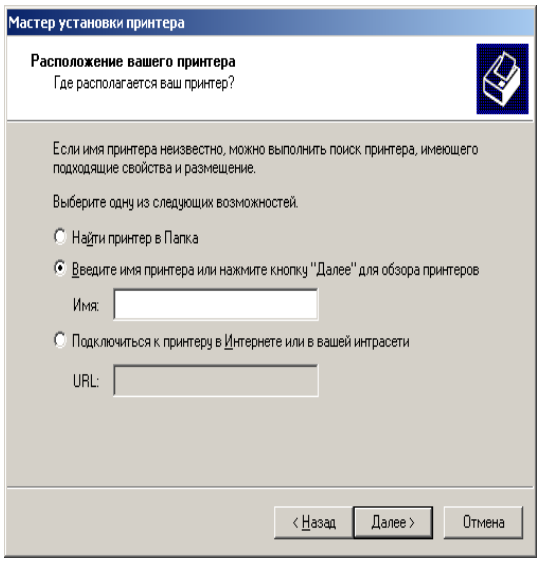


Рис. 1.55. Вікно майстра установки принтера



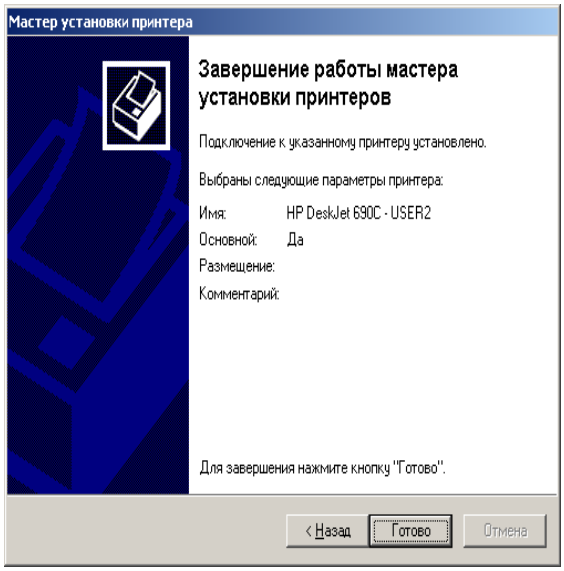


Рис. 1.56. Вікно введення імені принтера Рис. 1.57. Вікно завершення роботи майстра

Перевірка підключення мережі

1. Клацнути на робочому столі на ярличку **Мережеве оточення** правою кнопкою миші.
2. Вибрати з контекстного меню **Властивості** (Рис. 1.58, 1.59).

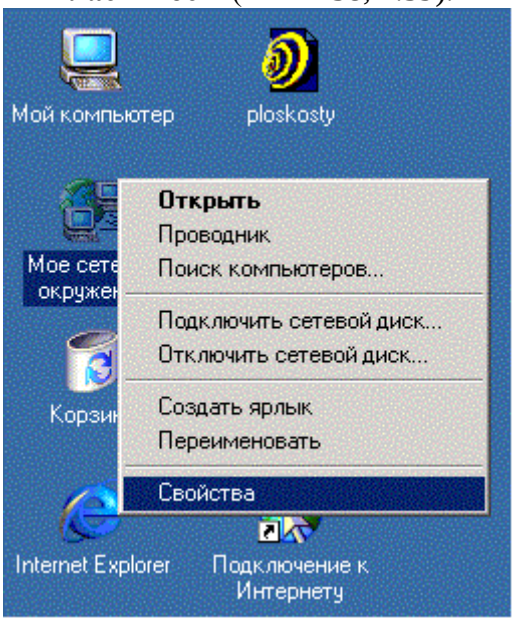


Рис. 1.58. Вікно контекстного меню

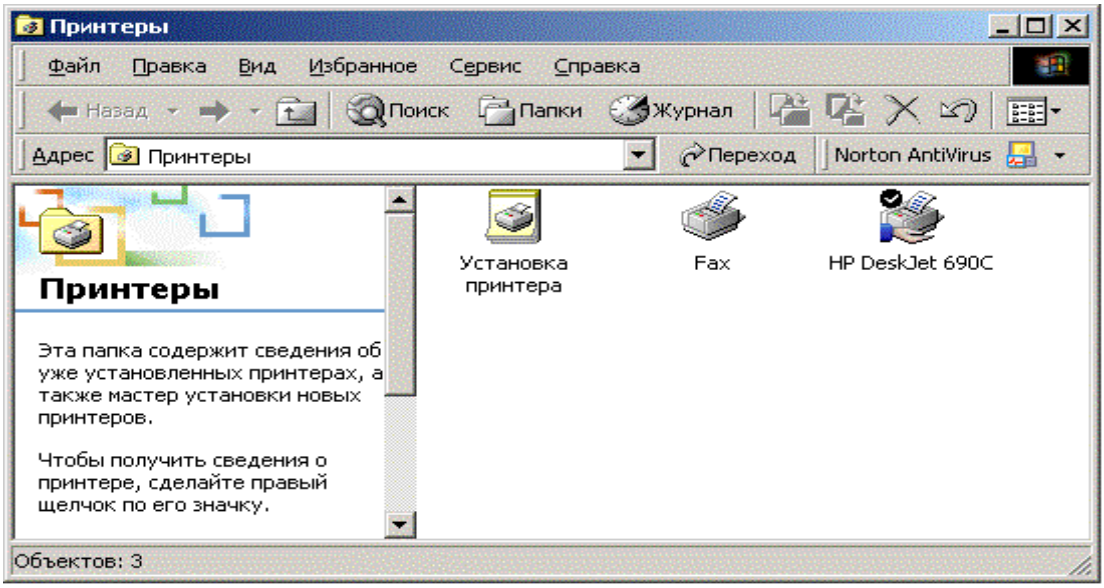


Рис. 1.59. Вікно властивостей

1. Клацнути у вікні **Мережа і віддалений доступ до мережі** на ярличку **Підключення за локальною мережею** правою кнопкою миші. Вибрати з контекстного меню **Стан** (рис. 1.60)

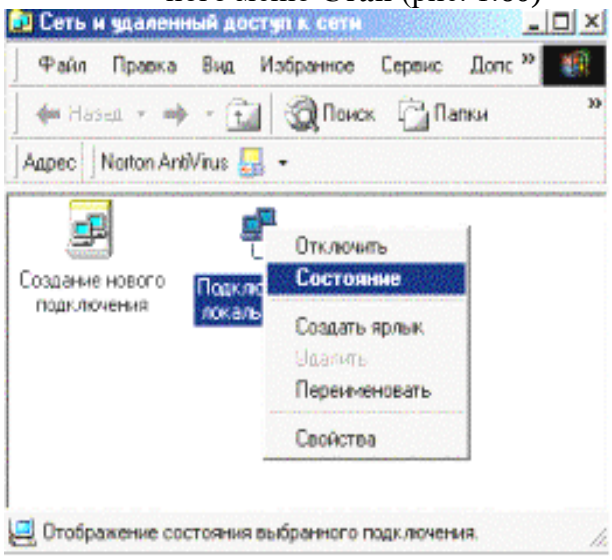


Рис. 1.60. Вікно вибору стану мережі

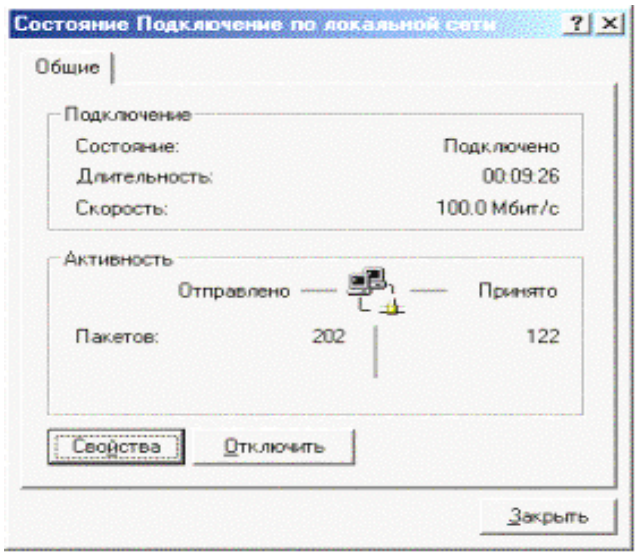


Рис. 1.61. Вікно перевірки стану мережі

2. Перевірити підключення у вікні, що з'явилося, **Стан підключення за локальною мережею** (рис. 1.61).

Якщо мережа відключена, то ярличок **Підключення за локальною мережею** буде блідим.

Відновлення підключення до мережі:

1. Клацнути на робочому столі на ярличку **Мережеве оточення** правою кнопкою миші.
2. Вибрати з контекстного меню **Властивості**.
3. Клацнути у вікні **Мережа й видалений доступ до мережі** на ярличку **Підключення за локальною мережею** правою кнопкою миші.
4. Вибрати з контекстного меню **Включити**.

Приклади роботи в локальній мережі Windows for Workgroups за допомогою різного програмного забезпечення

В операційних системах Windows існує убудована можливість роботи в локальній мережі за допомогою різноманітних програм, наприклад, провідника. При відкритті мережевого оточення (рис. 1.62) доступними є комп'ютери, наприклад, T_02… T_10, а також їхні логічні диски (C, D, E і т.д.) із каталогами й файлами. Подальша робота з каталогами й файлами нічим не відрізняється від звичайних операцій. Для забезпечення доступу до логічних дисків із мережі необхідно на робочому столі Windows відкрити піктограму **Мій комп'ютер** і з контекстно-залежного меню командою **доступ** установити загальний доступ до потрібних дисків. Програма-оболонка Far-manager при введенні команди **Drive** із підміню **Left** або **Right** із наступним вибором команди network (рис. 1.63) дозволяє одержати доступ до комп'ютерів, наприклад, T_02… T_10, а також до їхніх логічних дисків (C, D, E і т.д.) із каталогами й файлами (рис 1.64). Подальша робота з каталогами й файлами нічим не відрізняється від звичайних операцій.

Аналогічна робота в мережі з Norton Commander під Windows, де подається команда **Disconnect Network Drive** із підменю **Disk** для входу в локальну мережу, або **Map Network Drive** для створення мережевого диска. Подальша робота з каталогами й файлами нічим не відрізняється від звичайних операцій.

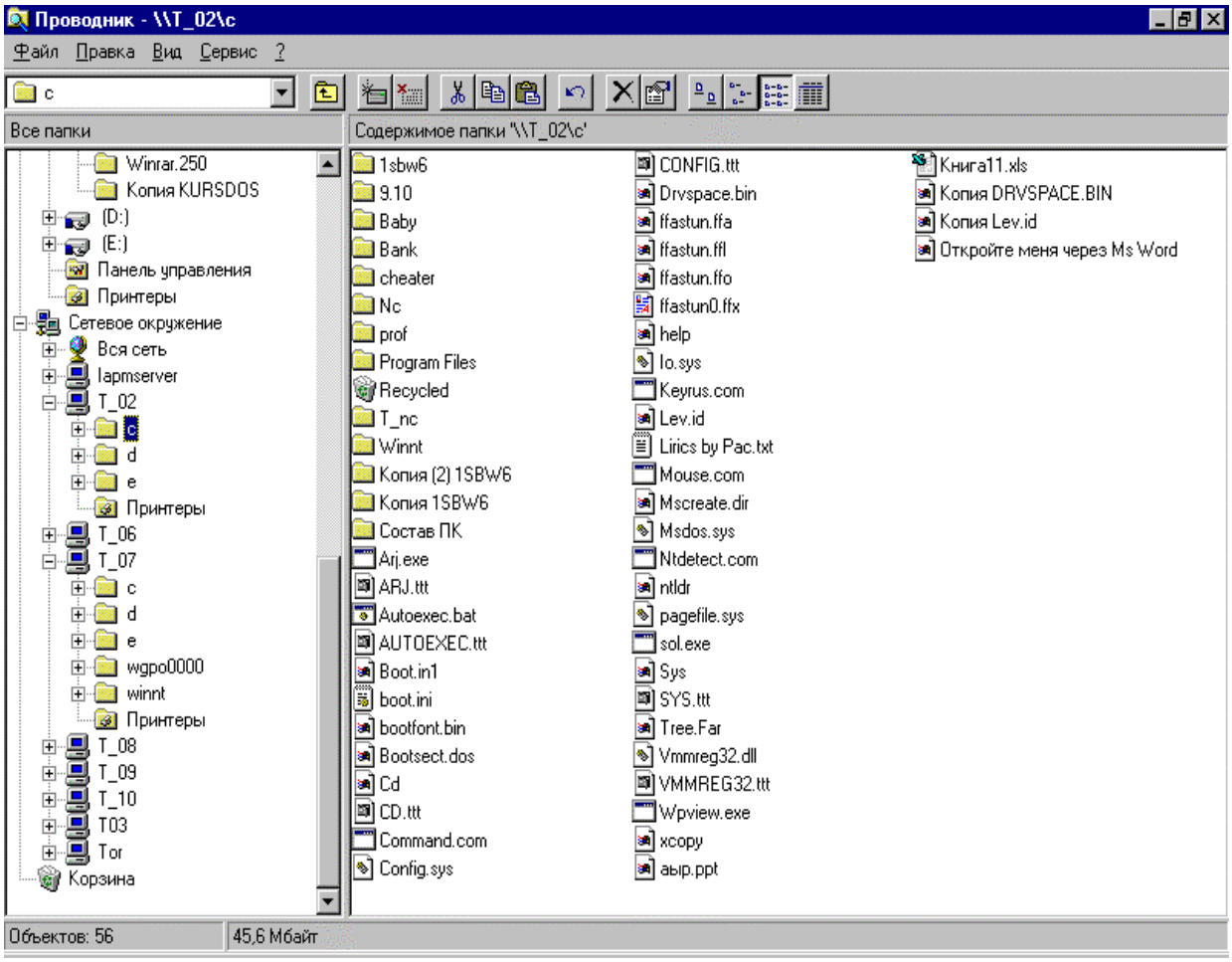


Рис. 1.62. Приклад роботи в локальній мережі за допомогою провідника.

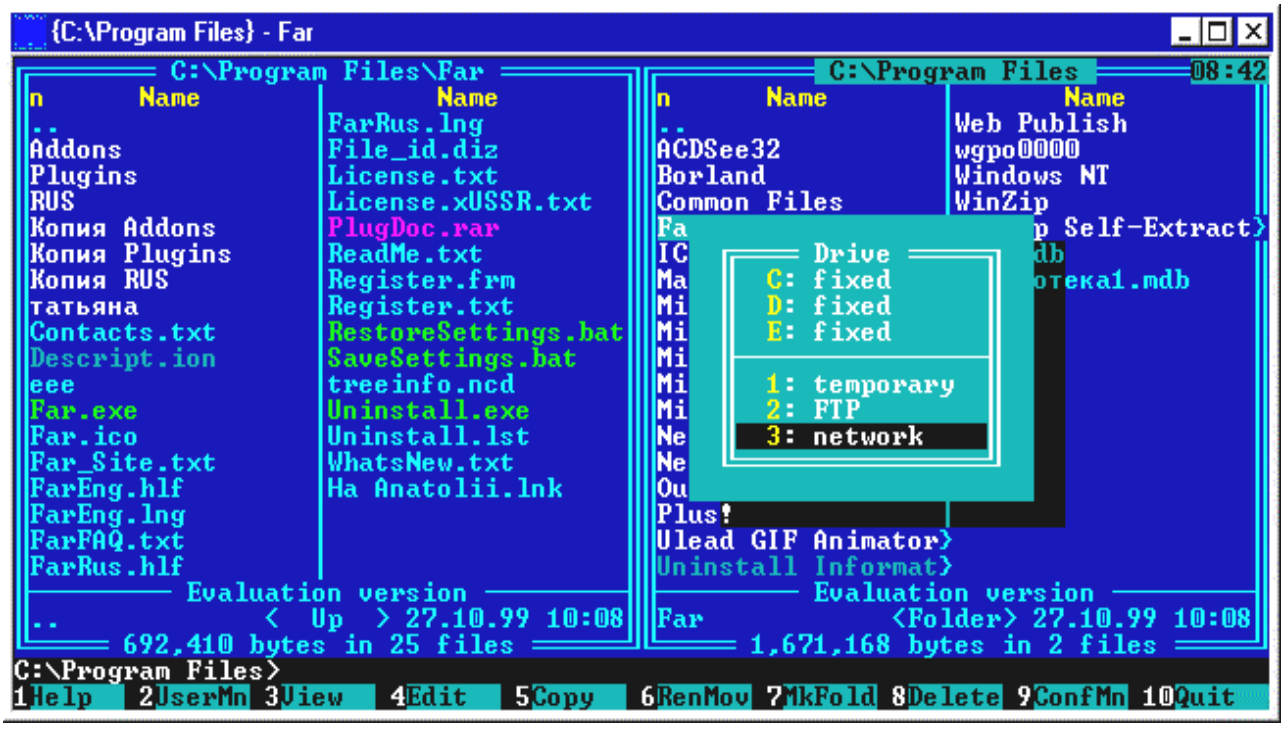


Рис. 1.63. Вибір локальної мережі

Рис. 1.64. Список комп'ютерів локальної мережі

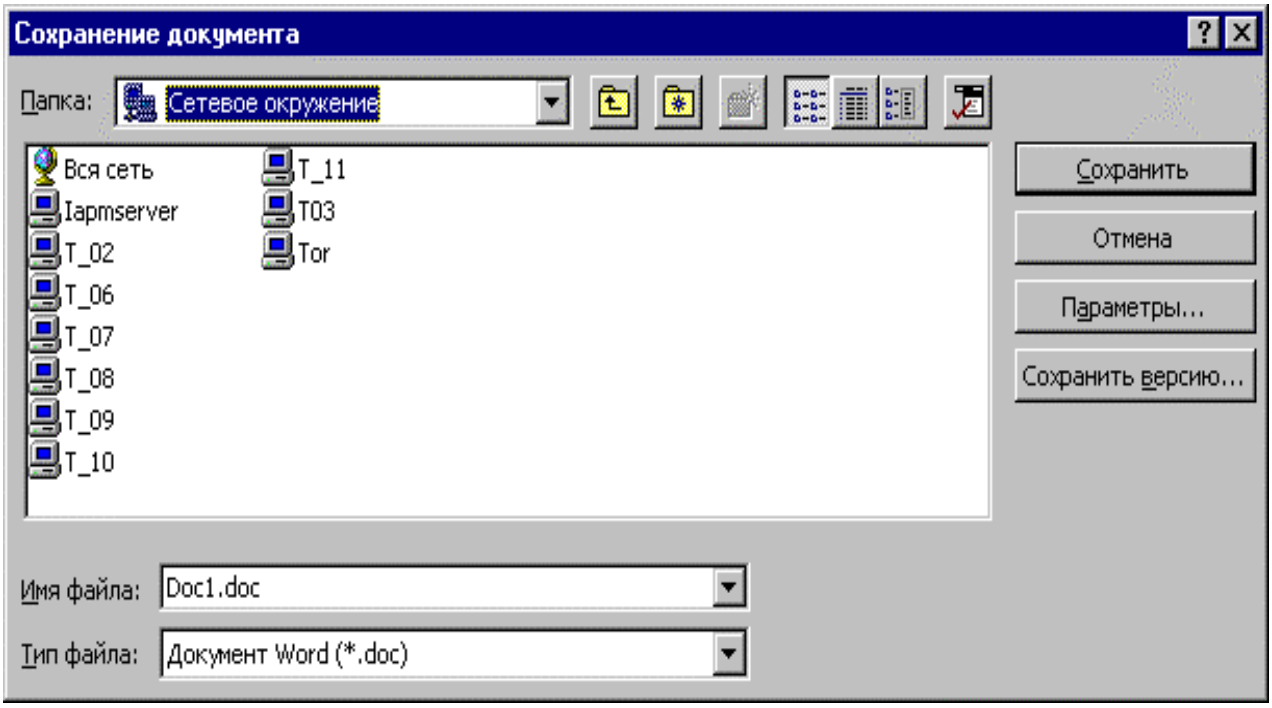


Рис. 1.65. Вибір мережевого оточення при зберіганні файлу в Microsoft Word

Аналогічна робота з локальною мережею програм із пакета Microsoft Office, які дозволяють зберігати і відкривати файли на комп'ютерах локальної мережі при введенні команд зберегти, зберегти як, відкрити із підміню Файл із наступним вибором мережевого оточення (рис 1.65).

Робота з віддаленим помічником Windows XP

В операційній системі Windows XP існує інструмент **Віддалений помічник,** що дозволяє користувачам допомагати один одному вирішувати різні проблеми.

Спочатку користувачеві, якому потрібна допомога, необхідно почати роботу з віддаленим помічником. Для цього слідуємо в **Мій комп'ютер → Властивості → Віддалені сеанси.**

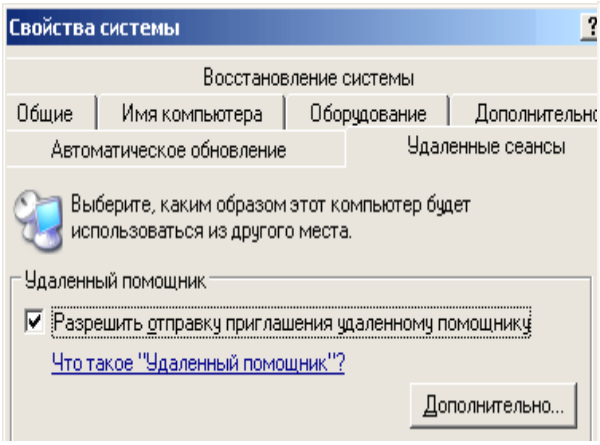


Рис. 1.66. Вікно помічника

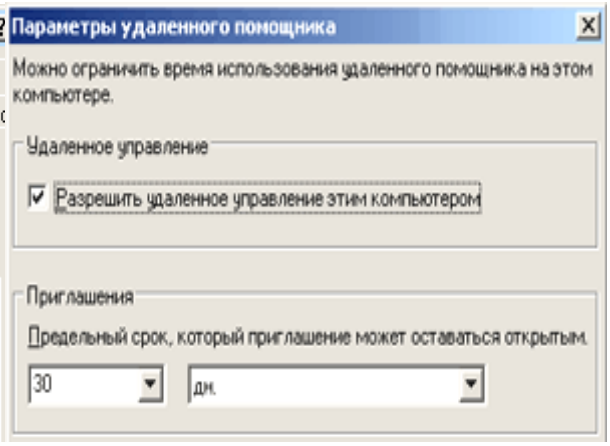


Рис. 1.67. Параметри помічника

Відбираємо **"Дозволити відправку запрошення віддаленому помічникові"**, (рис. 1.66), потім натискаємо кнопку **"Додатковий"** (рис. 1.67).

Тут можна дозволити віддаленому помічникові управляти комп'ютером, інакше він тільки бачитиме робочий стіл.

Тепер самий час налаштувати брандмауер. Якщо використовується стандартний брандмауер, вбудований в Windows XP SP2, то йдемо в **Панель управління**, знаходимо там **Брандмауер Windows** і на вкладці **Виключення** вирішуємо, яку команду вводимо: **Віддалений помічник** або **Дистанційне керування робочим столом** (рис.1.68).

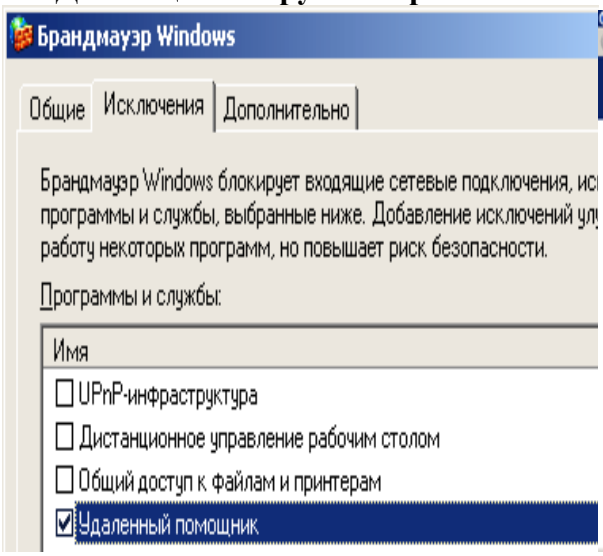


Рис. 1.68. Вікно брандмауера

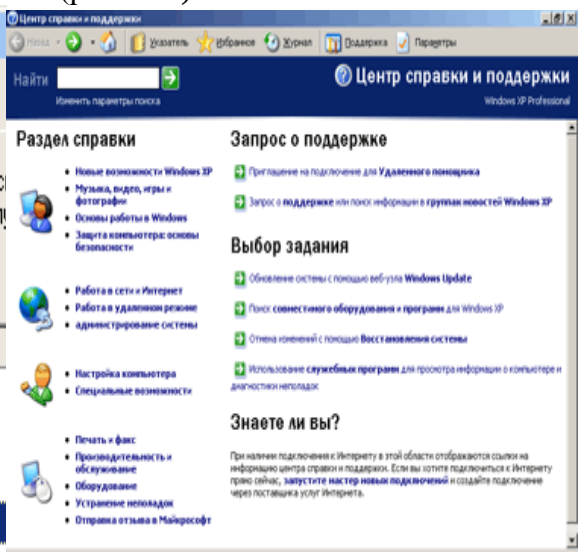


Рис. 1.69. Вікно довідки

Якщо використовується брандмауер стороннього виробника, то в налагодженнях мережевого екрану необхідно вказати вхідні TCP-з'єднання на порт 3389 для процесу C:\WINDOWS\system32\sessmgr.exe.

Той, кого покликали на допомогу, сам ініціюватиме установку з'єднання, тому, якщо доступ в Інтернет здійснюється через NAT (допустимо, у вигляді LAN ADSL-модема), то на NAT необхідно налагодити **форвардинг порту 3389,** потім (сформувавши запрошення) треба відкрити в **Блокноті** файл запрошення (**.msrcincident**), знайти в ньому поле **RCTICKET** і змінити в ньому **внутрішню IP-адресу** на **поточну зовнішню IP-адресу**. У разі відсутності можливості налагодження NAT можна заздалегідь установити VPN-з'єднання з тим, хто допомагатиме, і тоді сеанс допомоги проводитиметься за VPN-каналом.

Тепер починаємо запрошувати помічників.

Ідемо в **Пуск → Довідка й підтримка** (рис. 1.69). Там у розділі **Запит про підтримку** натискаємо посилання **Запрошення на підключення для віддаленого помічника** (рис. 1.70).

Далі вибираємо посилання **Відправити запрошення.** Там буде запропоновано використовувати MSN, або Outlook, або зберегти у файл. Запрошення – це звичайний файл з IP-адресою того, кому потрібна допомога. Файл можна доставити помічникові будь-яким способом: мережею, ICQ, як вкладений файл електронною поштою або навіть на дискеті. Для простоти й надійності вибираємо посилання **Зберегти запрошення у файл.**

Далі з'явиться пропозиція ввести своє ім'я й термін дії запрошення.

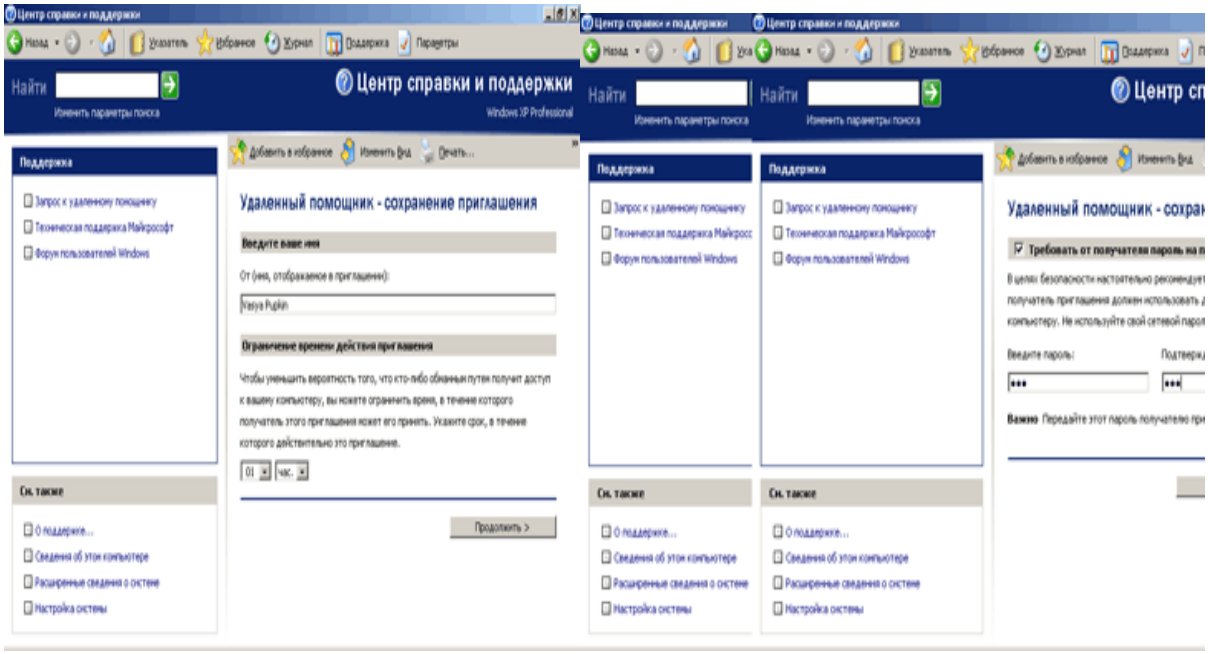


Рис. 1.70. Вікна виклику помічника

Ім’я може бути будь-яким, воно не пов’язане з ім’ям, указаним в Windows. Час дії, як сказано, служить для безпеки. Але ризикнемо припустити, що сенс його інший: річ у тому, що безпосередньо на початку сеансу допомоги у будь-якому випадку система запитає підтвердження. А ось за часом є сенс обмежити інтервал, через який вже допомога буде не потрібна.

Далі вводимо пароль (рис. 1.71).

Натискаємо кнопку **Зберегти запрошення**. Запрошення буде збережено у вигляді

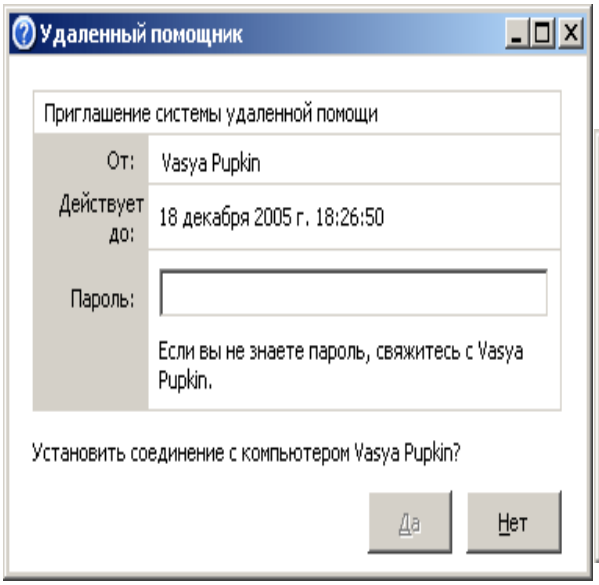


Рис. 1.71. Вікно введення паролю

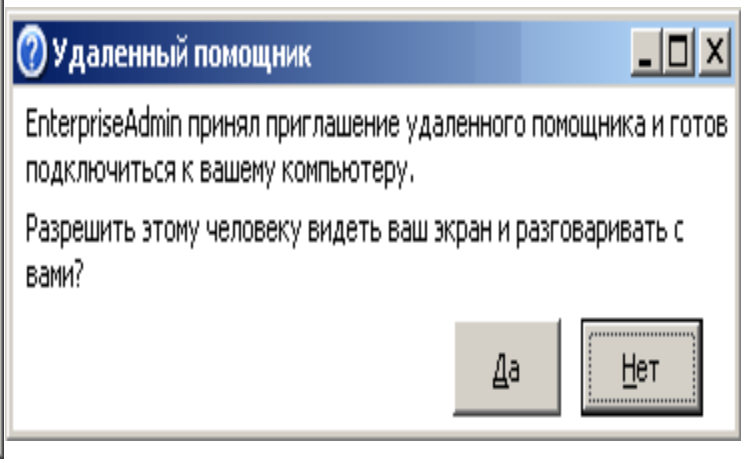


Рис.1.72. Вікно дозволу

файлу з розширенням .msrcincident. Готово, усі вікна можна позакривати. А файл запрошення й пароль до нього треба передати будь-яким способом тому, хто допомагатиме. Для виклику помічника, який допомагатиме, досить просто запустити в провіднику вказаний файл.

Потім, після встановлення зв’язку, він спочатку побачить порожній екран. Буде виданий запит на дозвіл початку сеансу допомоги (рис. 1.72). Після отримання згоди, помічник побачить ваш екран.

Він може писати повідомлення в нижньому лівому кутку свого вікна, а ви можете йому писати повідомлення у вікні діалогу **Віддалений помічник.**

Можливе відправлення один одному файлів за допомогою кнопки **Відправити файл**. Клавіша **Почати розмову** дозволяє спілкуватися голосом через мікрофон.

При необхідності помічник може не тільки спостерігати, але й теж управляти комп’ютером. Для цього йому треба натиснути кнопку **Узяти управління**, після чого буде запропоновано дозволити йому управління (рис. 1.73).

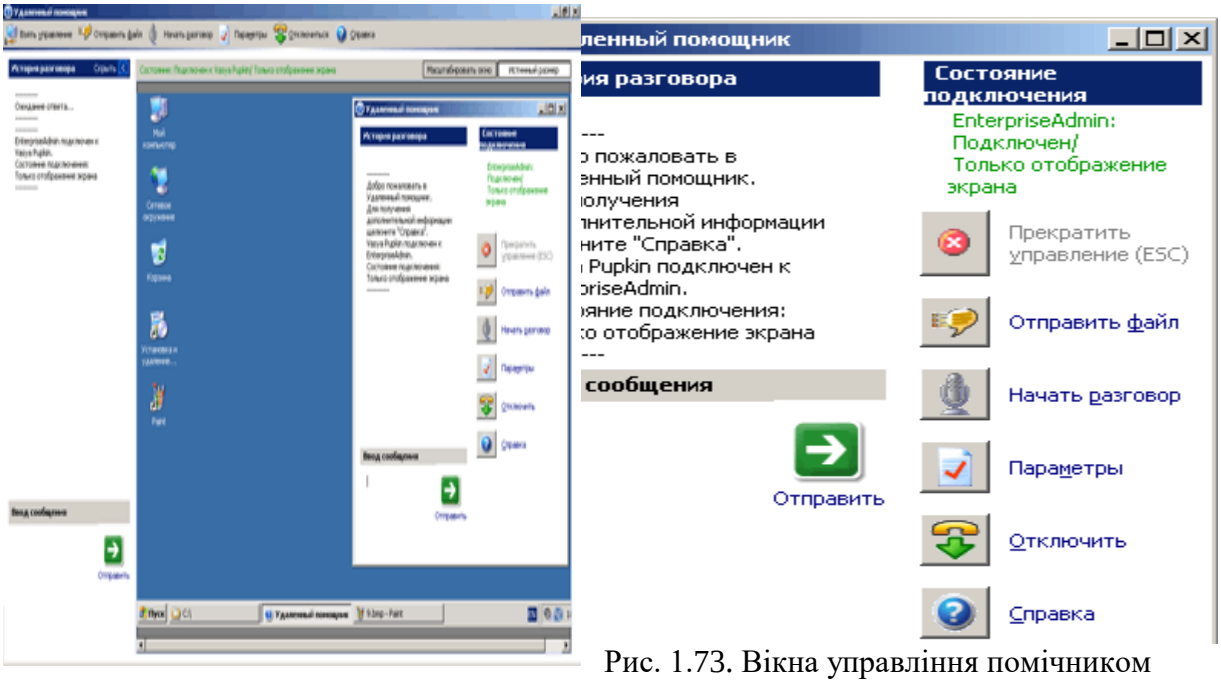


Рис. 1.73. Вікна управління помічником

Перервати сумісне управління можна кнопкою **Припинити управ**ління, а кнопка **Від-ключити** повністю завершує сеанс допомоги.

Захист інформації в мережах Microsoft Windows

Зміна мережевого пароля

Для відкриття діалогового вікна **Властивості: Паролі** можна натиснути кнопку **Пуск,** вибрати команди **Настроювання й Панель керування**, а потім двічі клацнути значок **Користувачі** (рис. 1.74).

Натисніть кнопку **Задати паролі.**

Виберіть пароль, який потрібно змінити, і натисніть кнопку **Змінити**.

Уведіть старий пароль.

Уведіть новий пароль, а потім знову введіть його в поле **Підтвердження пароля**.

Щоб дозволити іншому користувачу входити в мережу із цього комп'ютера, у вікні **Запровадження мережевого пароля** введіть нові значення в поля **користувач** і **Пароль**, а потім натисніть кнопку **OK**.

Призначення прав адміністратора, користувача, гостя.

На комп'ютері з операційною системою Windows NT натисніть кнопку **Пуск** і виберіть команди **Програми** й **Адміністрування, Локальна політика безпеки**, а потім **Політика враховуючих записів,** виберіть **Політика паролів,** аналогічно вибираються права користувача. Виконуйте інструкції, які виводяться на екран. На комп'ютері з операційною системою Windows 95 або більш пізньою натисніть кнопку **Пуск**, виберіть команди **Програми**, **Стандартні** й **Службові**, а потім виберіть **Призначені завдання.**

На комп'ютері з операційною системою Windows NT натисніть кнопку **Пуск** і виберіть команди **Програми** й **Адміністрування, Призначення прав користувача**. Виконуйте інструкції, які виводяться на екран під час роботи майстра. Аналогічно перегляньте локальну політику, політику відкритого ключа, політику безпеки IP. Натисніть кнопку **Пуск** і виберіть команди **Програми** й **Адміністрування, Управління комп'ютером** та перегляньте відповідні можливості діалогових вікон (рис. 1.75, 1.76).

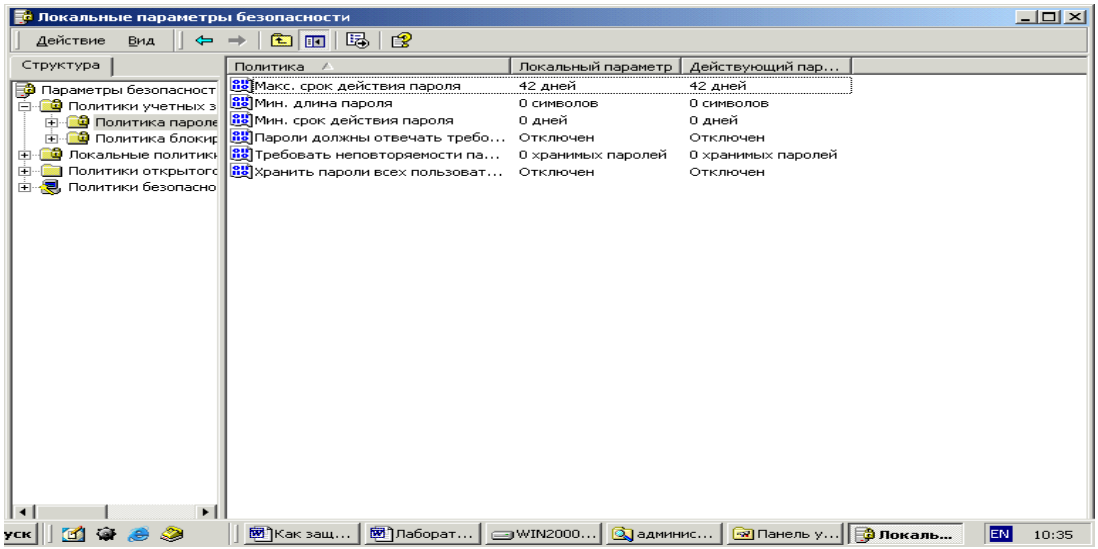


Рис. 1.74. Призначення параметрів паролів адміністратора, користувача, гостя.

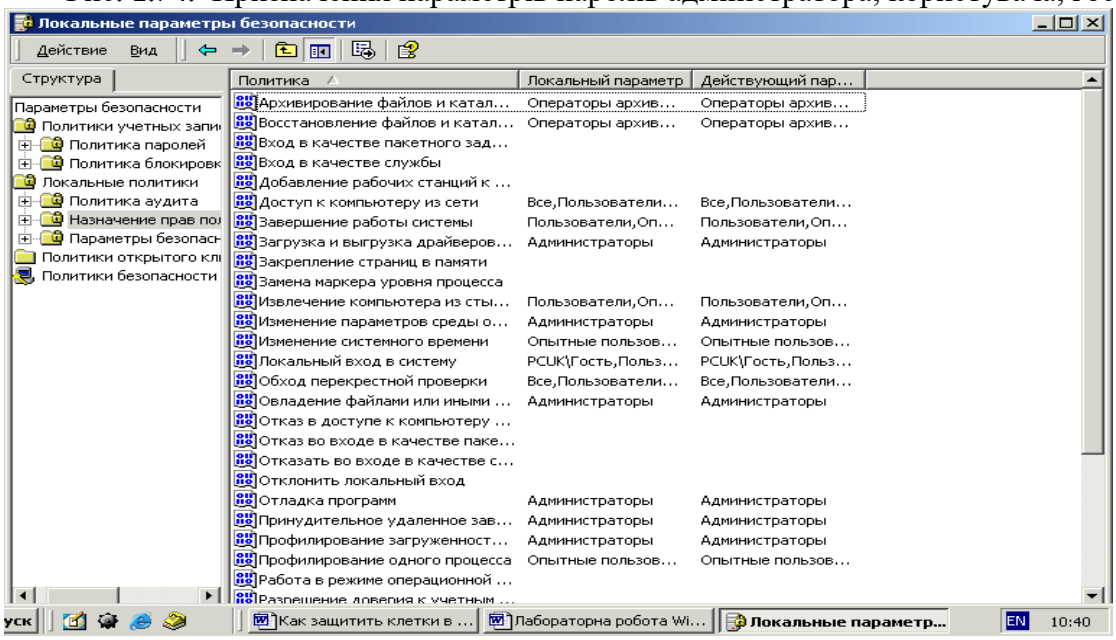


Рис. 1.75. Підбір прав користувачів.

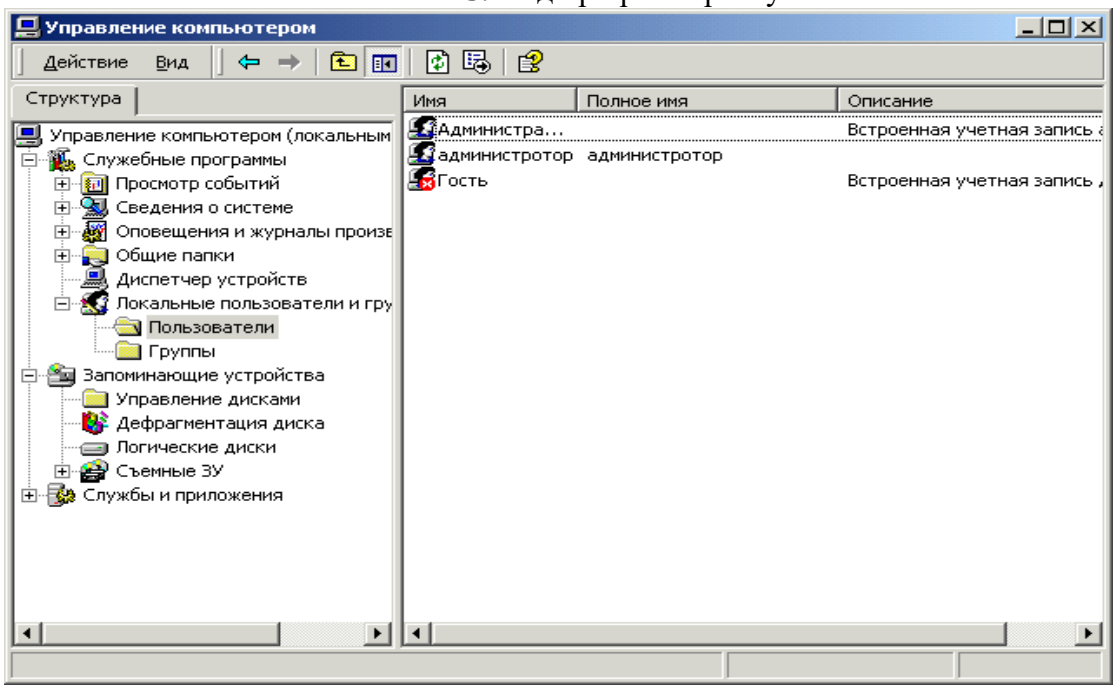


Рис. 1.76. Підбір параметрів безпеки.

Внутрішній мережевий захист із застосуванням програми LANguard Network Scanner

Як правило внутрішній мережевий захист недооцінюється адміністраторами. Дуже часто такого захисту навіть не існує. Багато користувачів, таких як, наприклад, працівники в межах компанії, не повинні мати доступу до машин один одного, адміністративних функцій, мережевих пристроїв або подібних прав. Зазвичай на практиці це не досягається і користувач із мінімальними навиками зможе здійснити успішне проникнення і досягти віддалених адміністративних прав у мережі за декілька хвилин. Через необхідну гнучкість, яка потрібна для проведення операцій, внутрішні мережі не можуть надати максимальний захист. Проте без захисту взагалі внутрішні користувачі можуть бути головною загрозою для багатьох корпоративних мереж. Користувач у межах компанії вже має доступ до багатьох ресурсів і йому не потрібно обходити мережевий захист або інші механізми захисту, які запобігають проникненню в мережу інтернетівським користувачам. Окрім внутрішніх користувачів, поганий мережевий захист означатиме, що якщо одного разу хакер одержить доступ до комп'ютера вашої мережі, то він також отримає доступ до решти частини внутрішньої мережі. Існує багато "дірок", які дозволяють хакерам проникнути у різні протоколи, як, наприклад, SMTP (електронна пошта) і http, до механізмів захисту обходу, наприклад, системи мережевого захисту. Такі напади дозволять досвідченішому хакеру легко проникнути і отримати адміністративні права через внутрішню мережу, читати зміст конфіденційної електронної пошти й документів, видаляти ділову інформацію на різних комп'ютерах й інші проблеми.

Перелік можливих точок входу хакера в локальну мережу:

- послуги користувачів і відкриті порти;
- дірки SNMP;
- закулісні користувачі;
- троянські коні або закулісне програмне забезпечення;
- відкриті акції;
- слабкі мережеві паролі;
- перелік користувачів, послуги і т.п.

Вирішенню вказаних проблем сприяє програма LANguard Network Scanner.

Програма призначена для сканування локальної мережі та її компонентів, вона, по-перше, гарантує виявлення хакерських атак, ідентифікацію всіх машин у локальній мережі, інформацію про Netbios, відкриті порти, нерадивих користувачів, диски й каталоги, відображає вже встановлені "хотфікси" (заплатки), які виправляють помилки в програмному забезпеченні, або латають дірки; у програму включена велика база даних з області відомих проблем безпеки, включаючи CGI, FTP і т. д.

Для встановлення програми LANguard Network Scanner необхідно:

- Windows (Windows 2000, NT або XP).
- Установлений мережевий протокол Netbios.
- Припинення роботи програмного забезпечення особистої системи мережевого захисту, оскільки це могло б блокувати комп'ютер, який сканується.

Інсталяційна процедура

1. Виконайте подвійне клацання по файлу **lannetscan.exe**. Далі виберіть параметри установки за допомогою майстра.

2. У діалоговому вікні ліцензійної угоди прийміть угоду й продовжуйте інсталяцію.

3. Виберіть місцеположення для LANguard і натисніть далі. LANguard будуть потрібні приблизно 10 МБ вільної пам'яті жорсткого диска.

4. Після того як LANguard буде встановлений, можна звертатися до програми за допомогою ярлика на робочому столі або з головного меню.

Сканування системи

Щоб запустити нове мережеве сканування:

В головному меню програми (рис. 1.77) введіть команду **нове сканування** з підменю **Файл**.

В діалоговому вікні, яке з'явиться (рис. 1.78) можна вибрати об'єкти сканування. Виберіть **локальну мережу**, щоб провести сканування внутрішньої мережі.

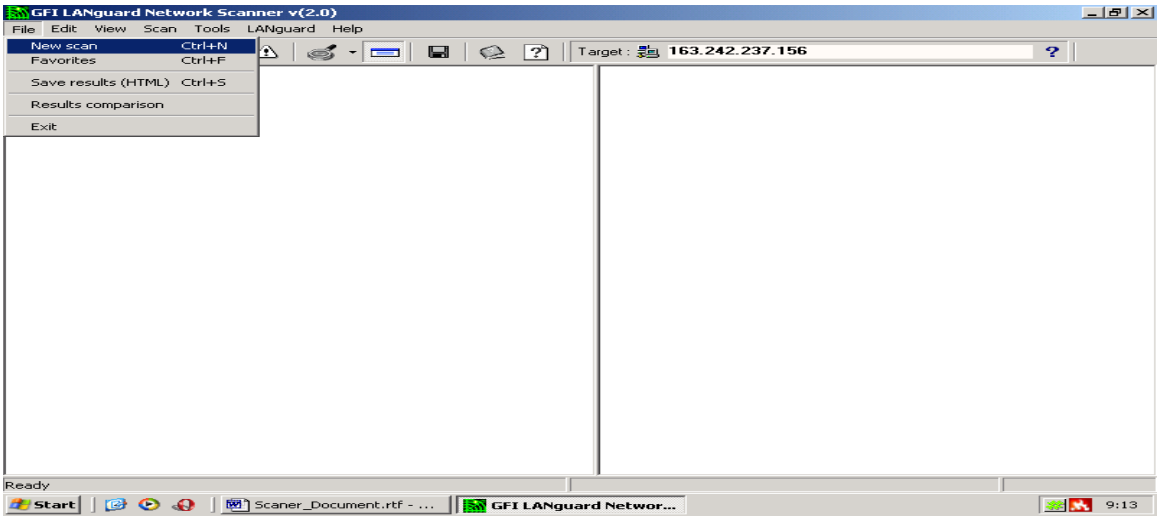


Рис. 1.77. Вікно програми.

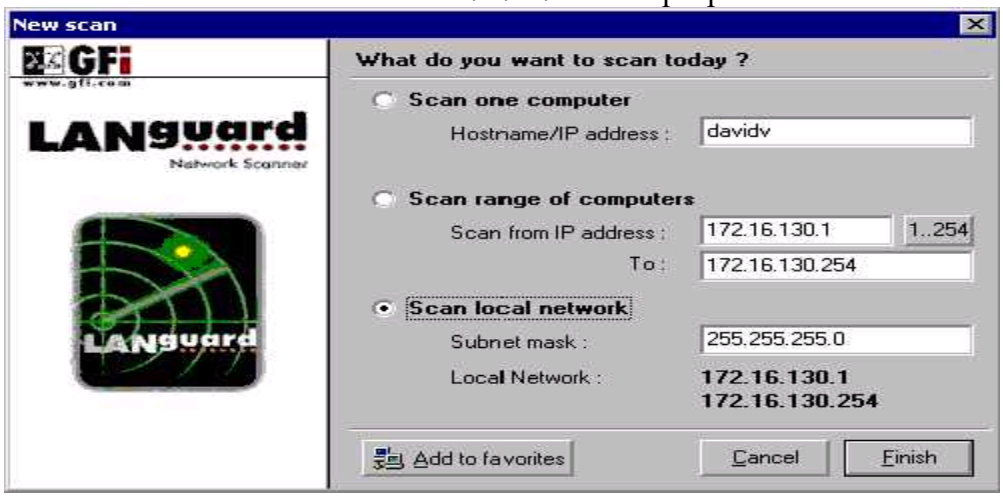


Рис. 1.78. Вікно вибору об’єктів для сканування

Натисніть кнопку **Finish**. На панелі інструментів натисніть кнопку **Start Scanning**. Буде проведено сканування вашої внутрішньої мережі, виконано дослідження Netbios, міжмережевого протоколу управління повідомленнями ICMP ping і запити SNMP.

Аналіз результатів

Приклад результатів сканування наведений на рис. 1.79.

Після мережевої перевірки можна бачити декілька рядків, що з’являються під кожним комп’ютером.

Дані, які можуть бути критичними:

1. Trusted Domains
2. Shares
3. Users, Groups and Services
4. Password Policy
5. Open Ports
6. Alerts

1. Trusted Domains (Довірені Домени)

Якщо цільовий комп’ютер(и) входить до домену, то він буде мати записи про довірені домени. Будьте впевнені, що довірені домени захищені і їм можна довіряти.

2. Shares (Мережеві ресурси)

Треба переконатися, що :

- Ніхто не може відкрити адміністративний ресурс комп'ютера.

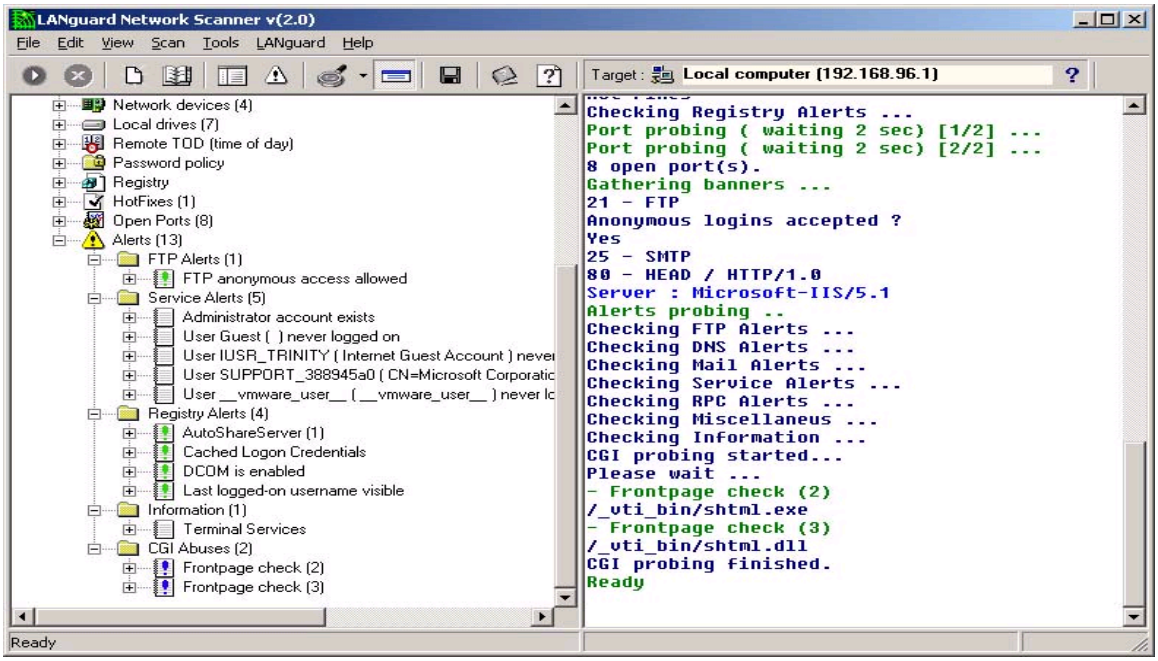


Рис. 1.79. Вікно результатів сканування мережі.

- Анонімний доступ заборонений.
- Теки автозапуску або подібні системні файли не відкриті. Це могло б дозволити менш привілейованим користувачам виконувати роботу на цільових машинах при запуску комп'ютера та наявності "трояна" у теці автозапуску.

Згадані вище роздуми дуже важливі для машин, які є критичними для системної цілісності, як, наприклад, публічний контролер домену. Уявіть адміністратора, що відкрив теку (або тека, що містить теку автозапуску) запуску на PDC (Public Domain Controller) для користувачів. Одержавши правильні дозволи, користувачі можуть легко копіювати програми, які будуть виконані на наступному діалоговому початку сеансу адміністратора.

3. Users, Groups and Services (Користувачі, групи й служби)

Скануючий комп'ютер перераховує користувачів і групи на машині для того, щоб виявити закулісних користувачів, які без підтримки в групах можуть отримати дозвіл доступу чорного ходу, та відповідні служби. Певні служби не повинні працювати на певних машинах, і тому повинні бути зупинені. Цей підхід виключає багато можливих "дірок", забороняючи хакерам вхід.

4. Password Policy (Політика паролів)

Рекомендовано, щоб політика паролів безпеки впроваджувалася, з тих пір як вона буде являтися основним проектом захисту. Мінімальна довжина пароля повинна бути практичною і мати число символів, наприклад, не менше восьми.

5. Open Ports (Відкриті порти)

У результаті роботи LANguard, який проводить сканування портів на цільових машинах, можна виявити які порти відкриті, а які – закриті. Звичайно, зрозуміло, що багато відкритих портів дозволяють проникнення через них до комп'ютерів. Кожен порт виконує визначену функцію обслуговування користувача, таким чином, що, якщо служба має проблему захисту, хакер міг би запустити напад проти тієї служби, підключаючись до вказаного порту на цільовій машині, і виконати вхід до комп'ютера через запуск exploit. Тому порти, які не потрібні для нормальної роботи, потрібно закрити.

6. Alerts (Попередження)

У сканері LANguard попередження містять відомості про загрози й додаткову інформацію. Такі загрози можуть включати проблеми http, Netbios, конфігурації, які можуть приводити до проблем захисту й так далі. Кожне із цих попереджень потрібно прийняти серйозно, і надати команди відповідно на те, як виключити проблему.

Дані, які можуть бути не критичними:

Указані дані, як правило, можуть забезпечити підказки/інформацію до проблем захисту у мережі. До них можна віднести:

1. NETBIOS Information
2. Username
3. MAC
4. TTL
5. LAN Manager
6. Domain
7. Computer Usage
8. Network devices
9. Remote TOD
10. Registry
11. Hot Fixes

1. **NETBIOS Information (Інформація Netbios).** Імена Netbios – це імена служб, зареєстрованих користувачів й комп'ютерів.
2. **Username (Ім'я користувача) –** це ім'я користувача, який працює в даний час на вказаній машині, або машинного імені.
3. **MAC** – це унікальна мережева адреса, яка присвоюється заводом-виробником мережевим платам.
4. **TTL** (Time To Live – час життя) – тривалість життя мережевих пакетів, яка вказує відстань, або час, між сканером LANguard і цільовою машиною.
5. **LAN Manager** – указує версію протоколу LAN Manager і операційної системи, яка використовується.
6. **Domain (Домен)**. Якщо цільова машина – член домену, це надасть можливість доступу до довіреного домену.
7. **Computer Usage (Комп'ютерне використання)**. Говорить про те, цільова машина – це робоча станція або сервер.
8. **Network devices (мережеві пристрої)** – указує список мережевих пристроїв, доступних на цільовій машині
9. **Remote TOD** – це мережевий час на цільовій машині, який, звичайно, установлений адміністратором.
10. **Registry** – надає ім'я власника, оригінальне машинне ім'я й різну іншу машинну інформацію. Указує список програм, що виконуються при запуску комп'ютера, програмне забезпечення як, наприклад, «троянські коні» й чорні ходи.
11. **Hot Fixes** (Оперативні виправлення) – указує на вже встановлені оперативні "заплатки" і т.п.

Налагодження параметрів програми

Для налагодження параметрів програми треба подати команду **Options** із під меню **Scan** з'явиться діалогове вікно рис. 1.80.

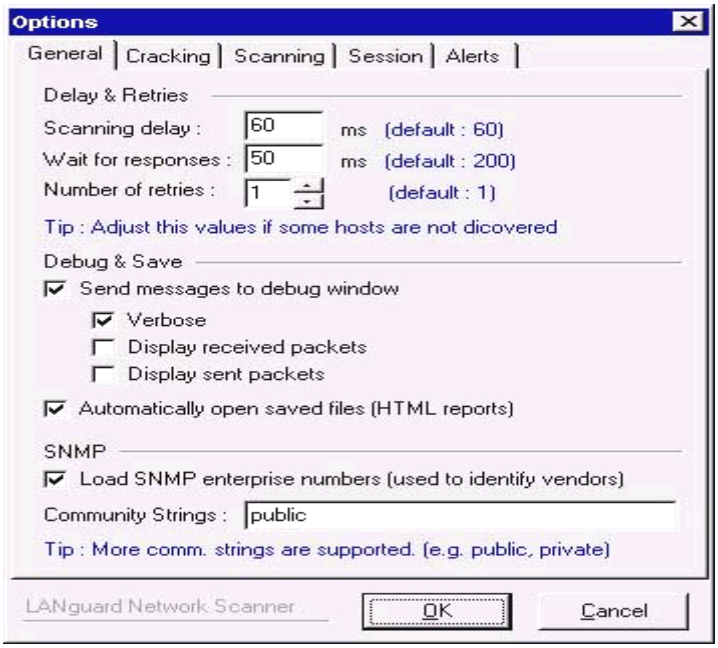


Рис. 1.80. Вікно налагодження параметрів програми

Загальні елементи налагодження сканування:

Delay & Retries (Повторення й затримки).

Scanning delay (Затримка сканування) – за умовчанням 60 мс.
Wait for responses (Очікування для відповідей) – за умовчанням 200 мс.
Number of retries (Кількість повторювань).
Debug & Save (Налагодження й збереження).
Send messages to debug windows (Посилати чи ні повідомлення у вікно налагодження).
Verbose (Докладно).
Display received packets (Відображати отримані пакети).
Display send packets (Відображати відправлені пакети).

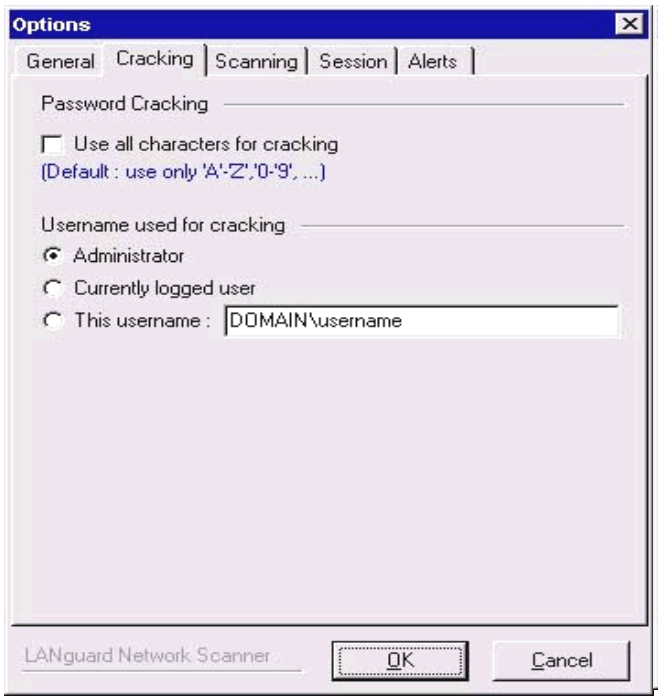


Рис. 1.81. Вікно вкладки злом.

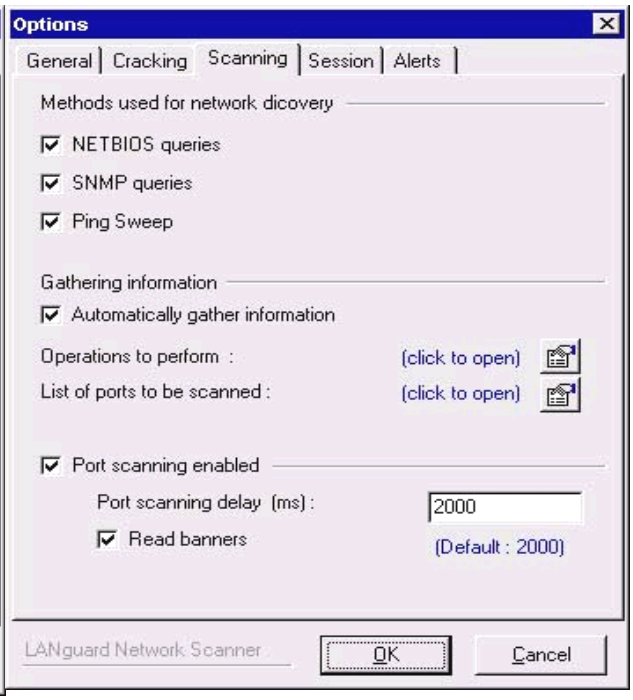


Рис. 1.82. Вкладка - сканування.

Automatically open saved files (HTML reports) (Автоматично відкривати збережені файли (Повідомлення html)).

SNMP

Load SNMP enterprise numbers (user to identify venders) (Завантажувати номери SNMP підприємства (використовується для ідентифікації виробника мережевого обладнання)
Community Strings (Указати назву сімейства SNMP).

Вкладка Cracking (Злом)

Ця секція (рис. 1.81) дозволяє користувачу формувати налагоджувальні елементи для злому мережевих ресурсів, щоб ідентифікувати слабкі паролі вказаних ресурсів.
User all characters for cracking (Використовувати всі символи для злому).
Username used for cracking (Ім'я користувача, яке використовується для злому). Це ім'я користувача, яке використовується програмою мережі LANguard для злому пароля на мережевому ресурсі.

Вкладка Сканування

На даній вкладці (рис. 1.82) користувач може конкретизувати методи дослідження мережі. Тобто виявляти, які машини працюють. Деякі сервери можуть не використовувати протоколи Netbios або SNMP, але вони відповідають на ping. Інколи пакети втрачаються при повільних нестабільних з'єднаннях. Користувач на таких мережах може використати більшу кількість спроб для отримання прийнятного результату. Тут формуються параметри, які порти переглядати, і які функції Netbios виконуються на цільовій машині. За умовчанням, скануючий комп'ютер виконуватиме сканування портів при виявленні комп'ютера, який працює. Можливо замінити задану за умовчанням установку параметрів сканування.

Вкладка Сесії

На вкладці (рис. 1.83) можна встановити ідентифікатор особи для сканування, її привілеї, щоб використовувати запити Netbios. Якщо немає доступу до мережі, це означає, що буде одержано мало або зовсім не одержано інформації. У такому випадку треба вибрати НУЛЬОВУ сесію, яка дозволить анонімному користувачу перерахувати служби й так далі.

Alerts probing enabled (дослідження попереджень включене).

Internal chechs enabled (ftp annon, weak passwords) (Внутрішні перевірки включені).

CGI probing enabled (Уключити перевірку скриптів CGI).

Proxy support (Підтримка Proxy, рис. 1.84).

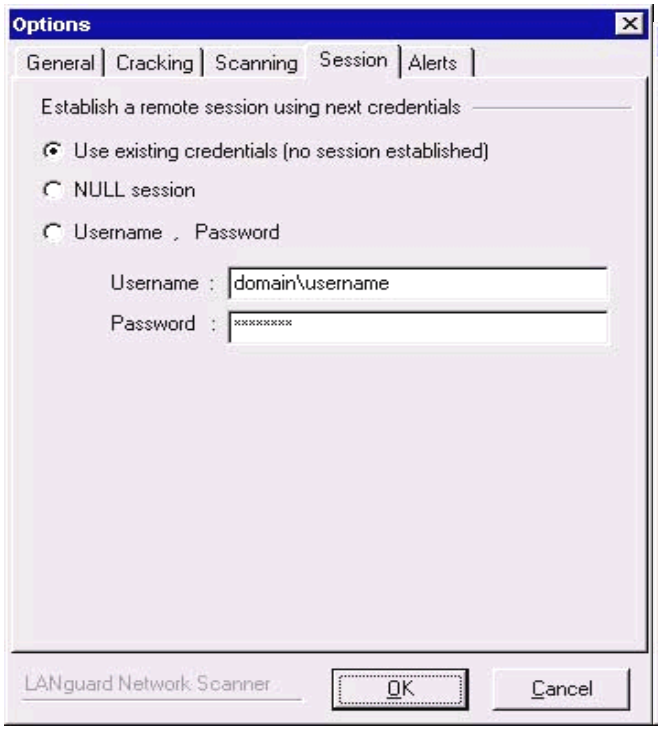


Рис. 1.83. Вкладка «Сесія»

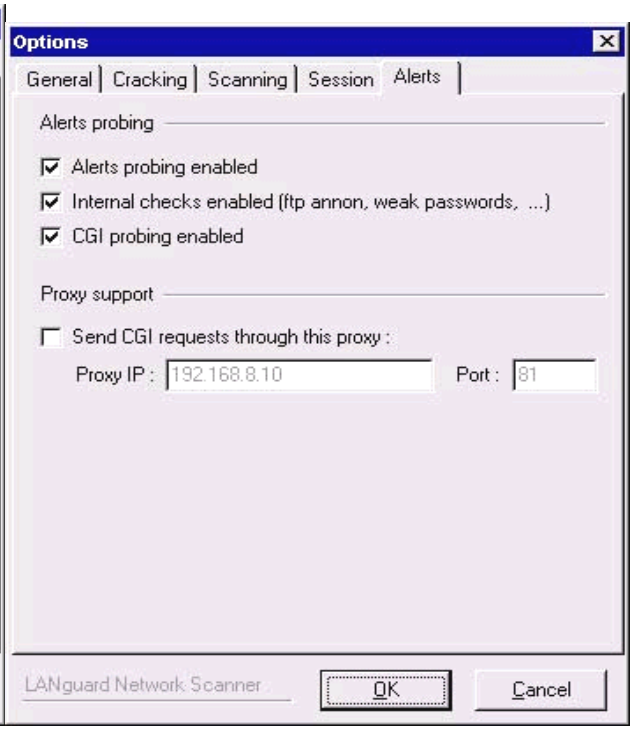


Рис. 1.84. Вкладка попередження

Вкладка «Підтримка проксі»

Send CGI reguests through this proxy (Посилати CGI запити через указаний Proxy).

Порівняння результатів

Вкладка Попередження

На вкладці вибираються параметри:

Alerts probing (Дослідження попереджень).

Коли сканер LANguard зберігає висновок html, то також зберігає файл із розширенням xml, який використовується в модулі порівняння результатів.

Щоб порівняти два зразки, виберіть із підменю **Файл** команду **порівняння результатів** (до того вікно результатів сканування повинно бути активним у програмі). З'явиться вікно (рис. 1.85). Виберіть два файли, що складаються з такого ж сканування в різний час, і введіть команду порівняння (клавіша **Compare** у даному вікні). Результати порівняння вкажуть що було добавлено або відключено й будь-які мережеві зміни, починаючи з останнього сканування.

Додаткові утиліти

Перевірка SNMP

Деякі мережеві пристрої мають рядки альтернативного або незаданого за замовчуванням сімейства. Перевірка SNMP дозволяє зламати слабкі загальні рядки (community strings). Уведіть команду SNMP **audit** із підменю **Tools** (рис. 1.86). Файл словника повинен містити список популярних загальних рядків для перевірки.

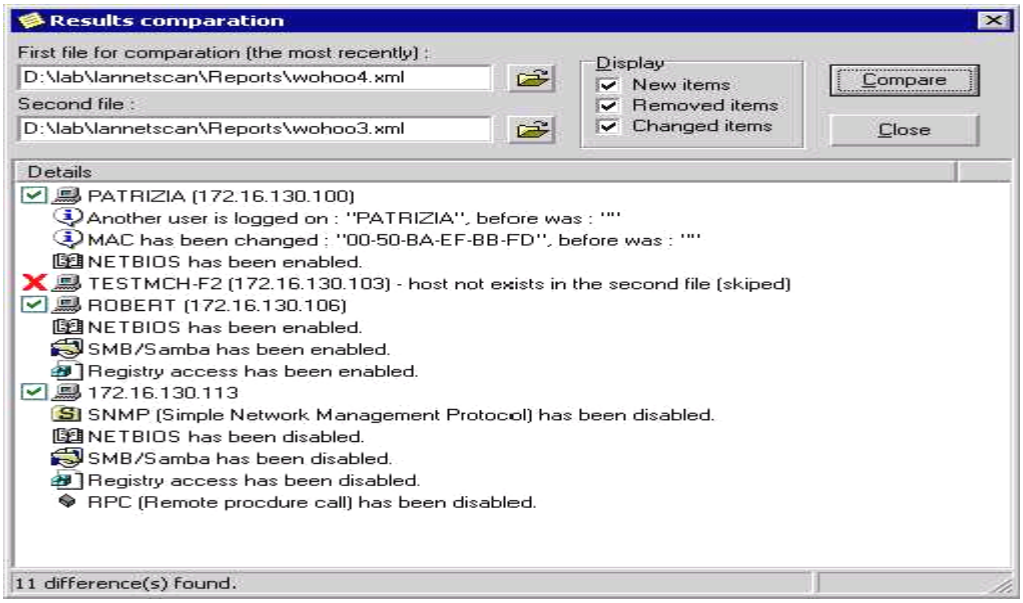


Рис. 1.85. Результати сканування

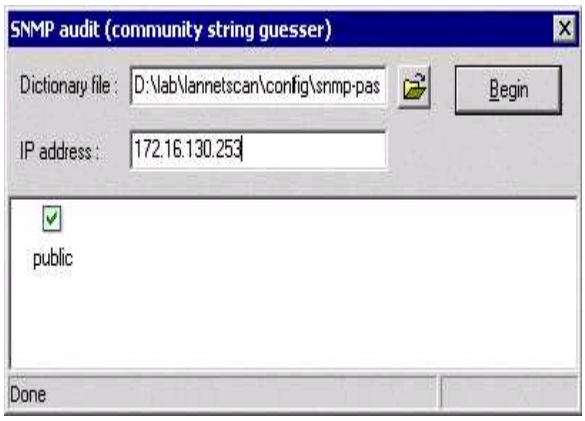


Рис. 1.86. Вікно аудиту SNMP

Рис. 1.87. Віно DNS lookup

Пошук сервера імен доменів (DNS)

Уведіть команду DNS **lookup** із підменю **Tools** (рис. 1.87). Цей інструмент визначає доменне ім'я комп'ютера за його відповідною IP адресою.

Показ траси

Уведіть команду **Traceroute** із підменю **Tools** (рис. 1.88). Це простий інструмент, який указує мережевий шлях між скануючим комп'ютером і цільовою машиною.

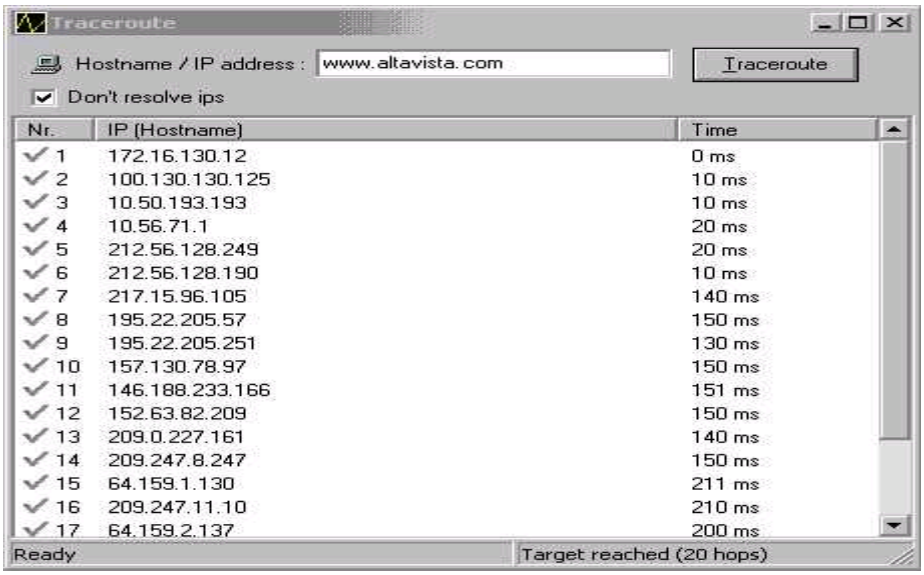


Рис. 1.88. Вікно виконання traceroute.

Команди контекстного меню

SNMPwalk

Виконання вказаної утиліти можливе, коли на комп'ютері, який сканується, установлено SNMP. Це надає можливість скануючому комп'ютеру надати запит службі SNMP та отри-

мати відповідну інформацію, таку як, наприклад, перелік відкритих портів, присутні служби, і так далі. Уведіть команду SNMPwalk із контекстного меню (рис. 1.89).

SNMP допоможе користувачам дізнатися багато про систему. За винятком випадків, коли це обслуговування потрібне, рекомендується вказану службу закрити назавжди.

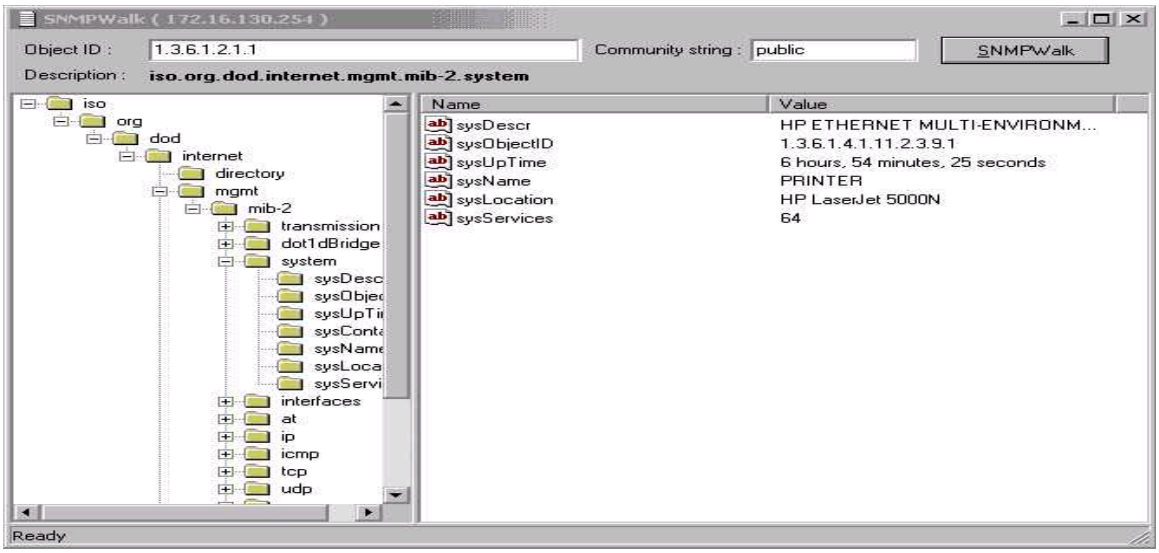


Рис. 1.89. Вікно програми SNMPwalk.

Збирання інформації

Уведіть команду **Gather Information** із контекстного меню. Вона дозволяє провести сканування одного вибраного комп'ютера зі списку.

Copy to clip board – цей налагоджувальний елемент просто копіюватиме інформацію в буфер обміну.

Resolve Address – дізнатись доменне ім'я комп'ютера можна, вибираючи цей налагоджувальний елемент.

Crack Password (Win9x). Уразливість у Windows 95, 98 і ME Netbios дозволяє користувачам легко визначити паролі на мережеві ресурси. Windows NT і 2000 не уразливі до цих нападів і цей налагоджувальний елемент не працюватиме для них.

Для більш конкретної інформації про цю проблему зверніться за адресою:
http://support.microsoft.com/support/kb/articles/Q273/9/91.ASP?LN=EN-US&SD=gn&FR=1

Dictionary Attack

Команда аналогічна попередній з тією різницею, що для збільшення швидкості визначення паролю використовується словник (рис. 1.90).

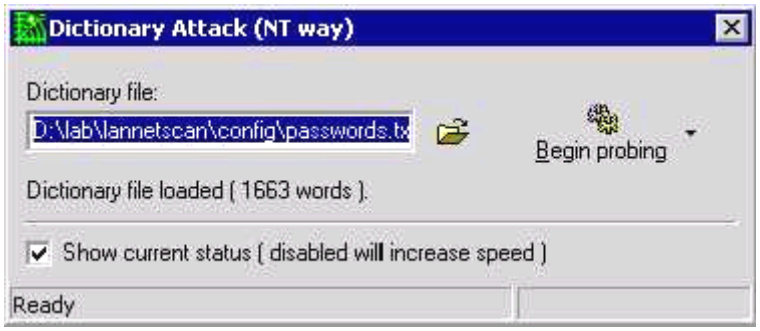


Рис. 1.90. Вікно Dictionary Attack

Send Message – цей налагоджувальний елемент дозволяє скануючому комп'ютеру посилати Netbios повідомлення з підробленою IP-адресою відправника.

Shutdown – дозволяє дистанційно вимкнути комп'ютер, який сканується, якщо в користувача, який сканує, є відповідні права.

Expand All. Вибір цього налагоджувального елементу відкриє дерево комп'ютерів у лівій панелі (рис. 1.110).

Saving Results. Щоб зберегти результати, виберіть **Файл** із меню, і виберіть **Результати (html) збереження**, або натисніть Control+S. Файл буде автоматично названий згідно вашому скануванню.

При збереженні файлу html, Internet Explorer або Netscape повинен запуститися на виконання і відобразити результуючий файл html.

List of Alerts – список попереджень і їх опис.

Introduction. Цей розділ складає список усіх налагоджувальних елементів меню сканера LANguard і короткого опису кожної функції.

Зміст команд головного меню

File Menu

- New scan – дозволяє вибирати новий діапазон для сканування.
- Favorites – вибране налагодження, яке використовується з попередніх сканувань.
- Save Results (HTML) – це збереже результати до файлу html після сканування.
- Results Comparison – дозволяє порівнювати сканування, щоб відзначити нові можливі проблеми захисту, будь-які мережеві зміни, і т.п.
- Exit – завершує програму.

Edit

- Add computer – дозволяє уручну додавати комп'ютер, щоб зібрати інформацію.
- Remove Computer – дозволяє уручну видаляти комп'ютер зі списку.
- Find Computer – дозволяє знаходити комп'ютер.
- Sort Computers – сортувати комп'ютери

View

Debug Window – показувати або не показувати праву панель.

Portscan.txt – цей текстовий файл містить список портів, які будуть скануватися.

Passwords.txt – цей текстовий файл містить список мережевих паролів, які будуть підставлятися зі словника.

Rpc.txt – цей текстовий файл містить список відомих послуг Rpc.

Object_Ids.txt – список ідентифікаторів об'єктів для запитів SNMP, для ідентифікації операційної системи.

Scan

Gather information – дозволяє збирати інформацію щодо вибраного комп'ютера.

Gather information from all – дозволяє збирати інформацію щодо всіх комп'ютерів.

Alerts – конфігурація попереджень. Дозволяє додавати нові попередження, видалити існуючі і конкретизувати, які попередження використовувати в скануванні.

Options – налагодження конфігурації сканера LANguard.

Tools

DNS lookup – дозволяє визначити доменне ім'я комп'ютера за його IP-адресою.

Traceroute – надає шлях між сканером і цільовою машиною.

SNMP audit – робить підбір за словником рядків сімейства SNMP.

КОНТРОЛЬНІ ПИТАННЯ

1. Чому дані передаються за допомогою пакетів?
2. Охарактеризуйте основні види мережевих топологій.
3. Назвіть характеристики поширеної мережевої архітектури.
4. Дайте коротку характеристику спеціального мережевого встаткування.
5. В яких областях і з якою метою застосовуються локальні мережі?
6. Які значення максимальної довжини різних видів фізичних сегментів для мережі Ethernet Ви знаєте?
7. Перерахуйте основні умови нормальної роботи мережі Ethernet, яка складається з різних видів фізичних сегментів.
8. В чому полягає правило «5-4-3»?
9. Перерахуйте основні умови нормальної роботи мережі Fast Ethernet, яка складається з різних видів фізичних сегментів.
10. Які значення максимальної довжини різних видів фізичних сегментів для мережі Fast Ethernet Ви знаєте?
11. Яка послідовність розрахунку показника PDV?

12. Яка послідовність розрахунку показника PW?
13. Що таке локальна мережа? Які ознаки класифікації мереж?
14. Охарактеризуйте фізичні середовища передавання даних.
15. Який порядок установки й настроювання мережевого адаптера?
16. В чому полягають функції мережевого адаптера?
17. Які операції здійснює мережевий адаптер?
18. Перерахуйте типи мережевих адаптерів.
19. Які типи шин передавання даних існують?
20. Якому рівневі моделі OSI відповідає: установлення мережевої карти й підключення до ЛОМ?
21. Який порядок роботи з майстром переносу файлів та каталогів в ОС Windows?
22. Яка історія стека протоколів TCP/IP?
23. Структура стека протоколів TCP/IP.
24. Які рівні адрес має кожний комп'ютер у мережі TCP/IP?
25. Дайте стислу характеристику інших протоколів мережі.
26. Який порядок налагодження стека протоколів TCP/IP?
27. Що таке: IP-адреса, маска підмережі, доменне ім'я, DNS-сервер, повторювач, концентратор, шлюз, маршрутизатор, міст, комутатор?
28. Охарактеризуйте безпровідні мережі.
29. Стандарти безпровідних мереж
30. Охарактеризуйте основні види топології безпровідних мереж.
31. Охарактеризуйте безпровідні ЛОМ із радіопередачею даних.
32. Як здійснюється підключення до безпровідної мережі?
33. Як здійснюється налагодження Wi-Fi-мережі на ПК і ноутбуках?
34. Опишіть налагодження роутера.
35. Охарактеризуйте режими роботи безпровідної мережі.
36. Як здійснюється безпека безпровідної мережі?
37. Еталонна модель взаємодії відкритих систем.
38. Що таке маршрутизація? Які принципи маршрутизації?
39. Як проводиться налагоджування мережі Windows for Workgroups?
40. Як отримати доступ до локальної мережі?
41. Як знайти комп'ютер у мережі?
42. Як використати мережевий принтер?
43. Як призначити загальний каталог для всіх користувачів мережі?
44. Як обмежити доступ до мережевих ресурсів?
45. Як призначити ім'я комп'ютера в мережі?
46. Які особливості використання інспектора для контролю за використанням загальних ресурсів?
47. Робота в діалоговому режимі в мережі Windows NT.
48. Який порядок створення мережевих дисків?
49. Робота в мережі за допомогою провідника.
50. Робота в мережі за допомогою програм, які входять до складу Microsoft Office.
51. Яка послідовність налагодження роботи комп'ютера в мережі?
52. Як проводиться пошук комп'ютера в мережі?
53. Як проводиться пошук принтера в мережі?
54. Яка послідовність надання доступу до файлу або каталогу в мережі?
55. Яка послідовність заборони доступу до файлу або каталогу в мережі?
56. Яка послідовність надання доступу до принтера в мережі?
57. Яка послідовність заборони доступу до принтера в мережі?
58. Яка послідовність зміни мереженого паролю?
59. Чому набуває важливості захист комп'ютерних мереж зсередини?
60. Перерахуйте можливі точки входу хакера в локальну мережу.
61. Яке призначення програми LANguard Network Scanner?
62. Який порядок сканування мережі?
63. Аналіз результатів сканування.
64. Охарактеризуйте критичні та некритичні параметри сканування, їх призначення.

65. Налагодження параметрів програми.
66. Порівняння результатів сканування.
67. Додаткові утиліти програми, їх призначення.
68. Команди контекстного меню програми.
69. Команди головного меню програми.
70. Еволюція обчислювальних систем. Системи пакетної обробки.
71. Еволюція обчислювальних систем. Багатотермінальні системи.
72. Еволюція обчислювальних систем. Перші локальні мережі.
73. Еволюція обчислювальних систем. Створення стандартних технологій локальних мереж.
74. Еволюція обчислювальних систем. Сучасні тенденції в розвитку обчислювальних систем.
75. Розподілені системи. Обчислювальні мережі.
76. Основні програмні й апаратні компоненти мережі.
77. Розподілені програми.
78. Переваги використання мереж.
79. Кабелі на основі неекранованої скрученої пари.
80. Кабелі на основі екранованої скрученої пари.
81. Коаксіальні кабелі.
82. Волоконно-оптичні кабелі.
83. Дайте загальну характеристику протоколів локальних мереж.
84. Яка структура стандартів IEEE 802.x?
85. Технологія Ethernet (802.3).
86. Метод доступу CSMA/CD. Етапи доступу до середовища.
87. Метод доступу CSMA/CD. Виникнення колізії.
88. Метод доступу CSMA/CD. Час подвійного обороту й розпізнавання колізій.
89. Яка максимальна продуктивність мережі Ethernet?
90. Охарактеризуйте оптично-волоконний Ethernet.
91. Що таке домен колізій у технології Ethernet?
92. Яка методика розрахунку конфігурації мережі Ethernet?
93. Поняття пакету. Його складові.
94. Які схеми передавання даних Ви знаєте?
95. Які особливості роботи з віддаленим помічником?

РОЗДІЛ 2
КОРПОРАТИВНІ МЕРЕЖІ

Причини розширення ЛОМ і пристрої, які використовуються для цього

ЛОМ мають властивість переростати початкові проекти. Із зростанням компаній ростуть і мережі. Зміни профілю діяльності організації або роботи компанії можуть зажадати переконфігурації мережі. Це стає очевидним, коли:

- неприпустимо довго документи стоять в черзі на мережевий принтер;
- збільшився час запиту до БД;
- змінилися вимоги із захисту інформації і так далі.

Мережі не можуть розширюватися за рахунок простого додавання робочих станцій і прокладання кабелю. Будь-яка топологія або архітектура має свої обмеження (табл. 2.1). Проте існують пристрої, які можуть:

- сегментувати ЛОМ так, що кожен сегмент стане самостійною ЛОМ;
- об'єднувати дві ЛОМ в одну;
- підключати ЛОМ до інших мереж для об'єднання їх в Інтернет.

Основне завдання мереж – транспортування інформації від ЕОМ-відправника до ЕОМ-одержувача. В більшості випадків для цього потрібно зробити декілька пересилань. Проблему вибору шляху вирішують алгоритми маршрутизації. Якщо транспортування даних здійснюється дейтаграмами, для кожної з них це завдання вирішується незалежно. При використанні віртуальних каналів вибір шляху виконується на етапі формування цього каналу. У Інтернет з його IP-дейтаграмами реалізується перший варіант (якщо не розглядати віртуальні мережі), а в ISDN і ATM – другий.

Алгоритми маршрутизації бувають *адаптивними* і *неадаптивними*. Другі, здійснюючи вибір маршруту, не приймають до уваги топологію, яка існує в даний момент, або завантаження каналів. Такі алгоритми називаються також статичними. Адаптивні ж алгоритми припускають періодичне вимірювання характеристик каналів і постійне дослідження топології маршрутів. Вибір того або іншого маршруту проводиться на підставі вимірювань.

Якщо адресат досяжний більше ніж одним шляхом, маршрутизатор повинен зробити вибір, який здійснюється на підставі оцінки маршрутів-кандидатів. Зазвичай кожному сегменту, що входить в маршрут, привласнюється деяка величина – оцінка цього сегменту. Кожен протокол маршрутизації використовує свою систему оцінки маршрутів. Оцінка сегменту маршруту називається *метрикою*. Тут слід звернути увагу на те, що при виборі маршруту всім сегментам шляху повинні бути надані зіставні значення метрики. Неприпустимо, щоб одні сегменти оцінювалися числом кроків, а інші – величиною затримки в мілісекундах. В межах автономної системи це зазвичай не створює проблем, адже це зона відповідальності одного адміністратора. Але в регіональних мережах, де працює багато адміністраторів, проблема вибору метрики може стати реальним утрудненням. Саме з цієї причини в таких мережах часто використовується вектор відстані, що виключає суб'єктивність оцінок метрики.

Окрім класичної схеми маршрутизації за адресою місця призначення, часто використовується варіант вибору маршруту відправником (даний варіант отримав подальший розвиток при введенні стандарту IPv6). В цьому випадку IP-пакет містить відповідний код опції і список проміжних адрес вузлів, які він повинен відвідати дорогою до місця призначення.

Існують і інші схеми, наприклад, що використовують широкомовні методи адресації (flooding), де кожен пакет, що приходить, надсилається всіма наявними каналами, за винятком того, за яким він отриманий. З тим щоб виключити безмежне розмноження пакетів в заголовок вводиться поле-лічильник числа кроків. У кожному вузлі вміст поля зменшується на одиницю. Коли значення поля стає рівним нулю, пакет ліквідовується. Початкове значення лічильника визначається розміром субмережі. Здійснюються спеціальні заходи проти можливого зациклення пакетів. Існує вдосконалена версія широкомовної маршрутизації, звана селективним широкомовним розсиланням. У цьому алгоритмі розсилання проводиться не за всіма можливими напрямами, а тільки за тими, які імовірно ведуть в правильну сторону. Широкомовні методи не відносяться до широко застосовуваних. Але вони використовуються там, де потрібна гранично можлива надійність, наприклад у військових застосуваннях, коли можуть бути пошкодження тих або інших каналів. Дані методи можуть використовуватися лише при формуванні віртуального каналу, адже вони завжди забезпечують найкоротший шлях,

оскільки перебираються всі можливості. Якщо шлях записується в пакеті, одержувач може вибрати оптимальний прохід і повідомити про це відправника.

Більшість алгоритмів враховують топологію зв'язків, а не їх якість (пропускну спроможність, завантаження і ін.). Але існують підходи до рішення проблеми статичної маршрутизації, що враховують як топологію, так і завантаження (flow-based routing). У деяких мережах потоки між вузлами відносно стабільні і передбачені. В цьому випадку з'являється можливість обчислити оптимальну схему маршрутів заздалегідь.

До таких пристроїв відносяться: репітери, мости, маршрутизатори, мости-маршрутизатори, шлюзи, комутатори.

Тоді в рамках підприємства мережі переростають з ЛОМ в корпоративні.

Епітет "корпоративний" часто використовується для характеристики продуктів обчислювальних систем. Корпоративними можуть бути названі майже всі типи елементів обчислювальної систем: від концентраторів і маршрутизаторів до серверів і операційних систем.

В англомовній літературі цей вид мереж часто називається "enterprise-wide networks" (дослівно – мережа масштабу підприємства), а в нашій країні прижився інший термін іноземного походження – корпоративні мережі.

Термін "корпоративна" відбиває з однієї сторони **розмір мережі**, тому що корпорація – це значне, велике підприємство. З іншого боку, цей термін несе в собі **зміст об'єднання**, тобто корпоративна **мережа – це мережа, що утворилася в результаті об'єднання декількох, як правило, різнорідних мереж**.

Мережі відділів або *робочих груп* (рис. 2.1) використовуються групою людей, об'єднаних рішенням загальної задачі, такої, наприклад, як бухгалтерський облік або маркетинг. Головною метою мереж відділів є поділ ресурсів, таких як додатки, дані, лазерні принтери й, можливо, низькошвидкісні модеми. Зазвичай, мережі відділів мають один або два файлових сервери й не більш ніж 30 користувачів.

Мережі кампусів можуть простиратися на декілька кілометрів, але при цьому глобального з'єднання не потребують. Мережі кампусів мають *хребет (backbone)* або головну мережу, і підмережі, що подібні ребрам. Для підвищення продуктивності підприємства іноді використовують маршрутизатори, проте, частіше підмережі приєднуються до хребта за допомогою мостів або швидкодіючих багатопортових мостів нового покоління – концентраторів, що комутуються (switching hubs). У мережі кампуса в кожному відділі здійснюється адміністрування своїми серверами, але співробітники відділу одержують доступ до деяких файлів і ресурсів мереж інших відділів. Послуги, надані мережами кампусів, не обмежуються простим поділом файлів і принтерів, а часто включають доступ і до серверів інших типів, наприклад, до факсів-серверів і до серверів високошвидкісних модемів. Важливим сервісом, наданим мережами кампусів, став доступ до корпоративних баз даних, незалежно від того розташовуються вони на серверах баз даних чи на мінікомп'ютерах.

Для створення корпоративних мереж (рис. 2.2) треба створити єдину інформаційну мережу підприємства. Вона повинна виконувати наступні функції:

1. Створення єдиного інформаційного простору, який здатний охопити і застосовувати для всіх користувачів інформацію, створену в різний час і різними способами зберігання і обробки даних, контролю виконання робіт.

2. Підвищення достовірності інформації й надійності її зберігання шляхом створення стійкої до збоїв і втрати інформації обчислювальної системи, а також створення архівів даних, які можна використовувати, але необхідності в яких на даний момент немає.

3. Забезпечення ефективної системи накопичення, зберігання й пошуку технологічної, техніко-економічної й фінансово-економічної інформації щодо поточної роботи й виконаної певний час назад (інформація архіву) за допомогою створення глобальної бази даних.

4. Обробка документів і побудова системи аналізу, прогнозування і оцінки обстановки з метою ухвалення оптимального рішення і вироблення глобальних звітів.

5. Забезпечення прозорого доступу до інформації авторизованому користувачеві відповідно до його прав і привілеїв.

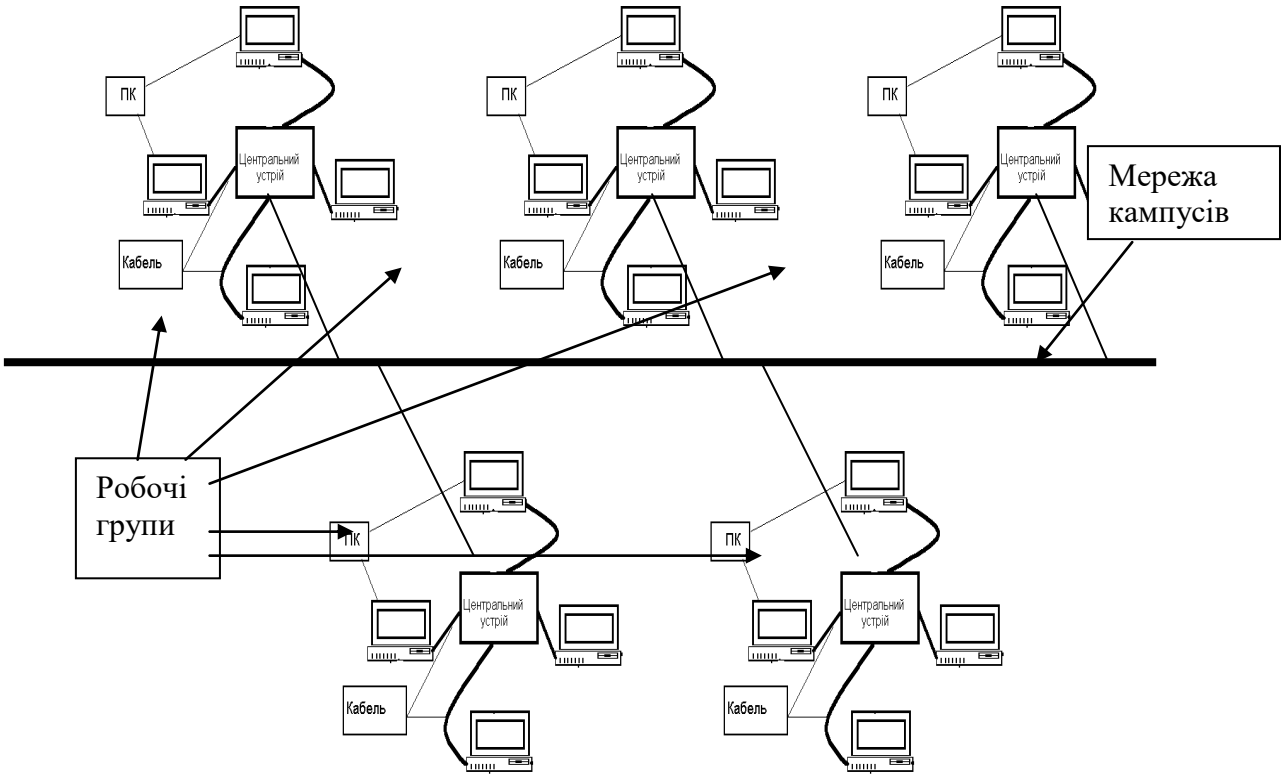


Рис. 2.1. Корпоративна мережа

Характеристики топологій обчислювальних мереж приведені в табл. 2.1.

Таблиця 2.1.

Характеристики топології мереж

Характеристики	**Топологія**		
	Зірка	**Кільце**	**Шина**
Вартість розширення	Незначна	Середня	Середня
Приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмов	Незначна	Незначна	Висока
Розміри системи	Будь-які	Будь-які	Обмежені
Захищеність від прослуховування	Хороша	Хороша	Незначна
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороше	Задовільне	Погане
Можливість роботи в реальному режимі часу	Дуже хороша	Хороша	Погана
Розводка кабелю	Хороша	Задовільна	Хороша
Обслуговування	Дуже хороше	Середнє	Середнє

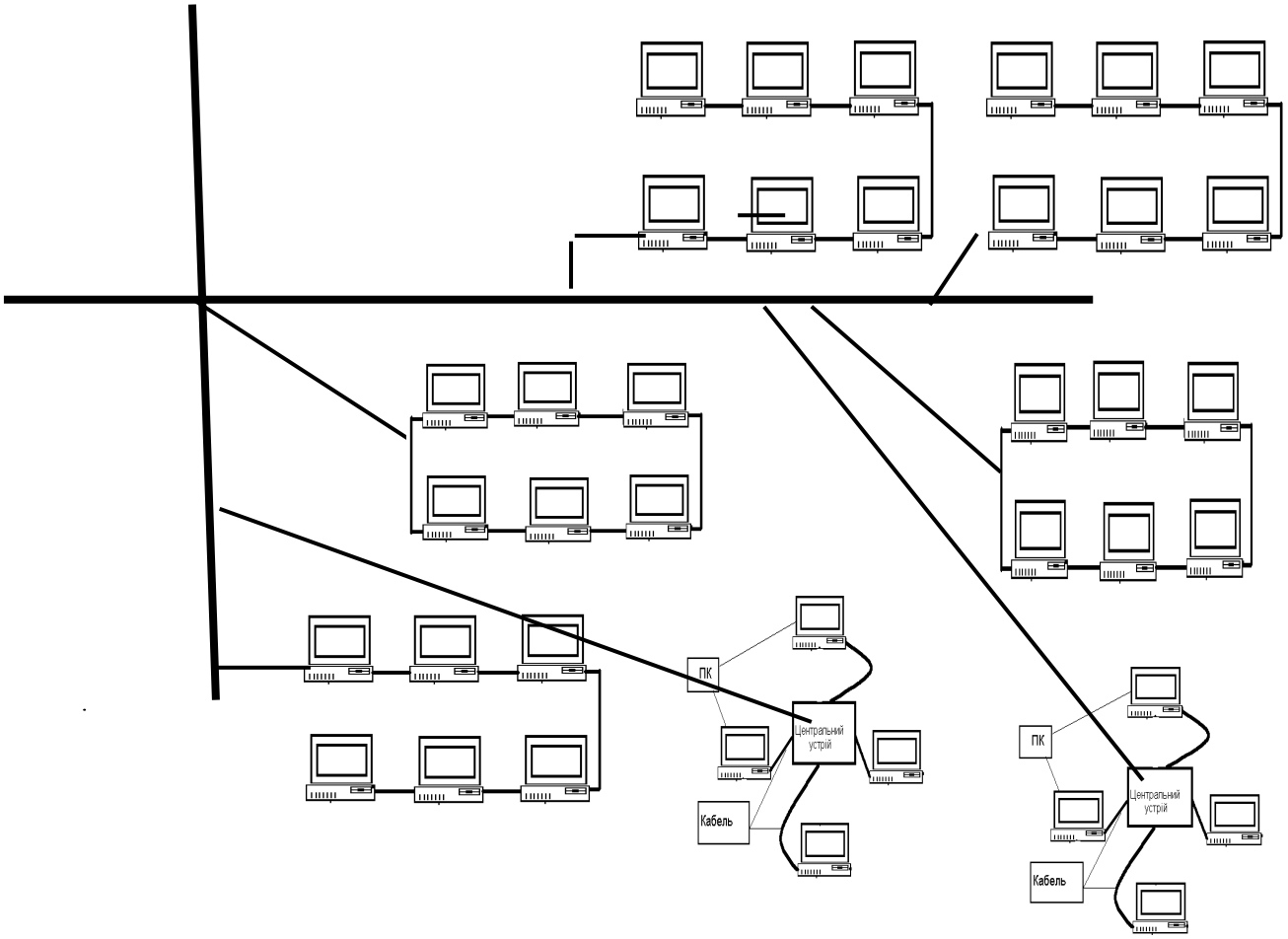


Рис. 2.2. Фрагмент деревовидної структури мережі

Якість обслуговування QoS

QoS (Quality of Service — якість обслуговування) — цим терміном в області комп'ютерних мереж називають вірогідність того, що мережа зв'язку відповідає заданій угоді про трафік, або ж, у ряді випадків, неформальне позначення вірогідності проходження пакета між двома крапками мережі.

Класи QoS

QOS Class 1 (званий також класом послуг A) має ті ж характеристики, що і виділений цифровий канал типу крапка-крапка

QOS Class 2 (званий також класом послуг B) забезпечує режим, прийнятний для аудіо і відео при видеоконференціях або передачах мультимедіа

QOS Class 3 (званий також класом послуг 3) забезпечує режим, прийнятний для передачі, орієнтованої на з'єднання, наприклад, через посередництво frame relay.

QOS Class 4 (званий також класом послуг 4) еквівалентний режиму IP-передачі в умовах якнайкращих зусиль (best efforts) за відсутності гарантії доставки

Механізм роботи

Для більшості випадків якість зв'язку визначається наступними параметрами:

- Смуга пропускання (Bandwidth), описує номінальну пропускну спроможність середовища передачі інформації, визначає ширину каналу. Вимірюється в bit/s (bps), kbit/s (kbps), Mbit/s (Mbps), Gbit/s (Gbps).
- Затримка при передачі пакету (Delay), вимірюється в мілісекундах.
- Коливання (тремтіння) затримки при передачі пакетів — джиттер (Jitter).
- Втрата пакетів (Packet loss). Визначає кількість пакетів, втрачених в мережі під час передачі.

Для простоти розуміння, канал зв'язку можна представити у вигляді умовної труби, а пропускну спроможність описати як функцію двох параметрів: діаметру труби і її довжини.

Коли передача даних стикається з проблемою «темно-зеленої шийки» для прийому і відправки пакетів , то зазвичай використовується метод FIFO: перший прийшов — перший

пішов (First In — First Out). При інтенсивному трафіку це створює затори, які вирішуються украй простим чином: всі пакети, що не увійшли до буфера черги FIFO (на вхід або на вихід), ігноруються маршрутизатором і, відповідно, втрачаються безповоротно. Розумніший метод — використовувати «розумну» чергу, в якій пріоритет у пакетів залежить від типу сервісу, — ToS. Необхідна умова: пакети повинні вже нести мітку типу сервісу для створення «розумної» черги. Звичайні користувачі найчастіше стикаються з терміном QOS в домашніх маршрутизаторах з підтримкою QOS. Наприклад, вельми логічно дати високий пріоритет пакетам VoIP і низький — пакетам, FTP, SMTP.

Моделі QoS

Негарантована доставка — Best Effort Service

Наявність марки TOS Best Effort Service не є механізмом тонкого регулювання і є ознакою простого збільшення пропускної спроможності без якого-небудь виділення окремих класів трафіку і регулювання. Вид послуг реалізується в мережі, коли робиться все можливе для доставки пакету, але при цьому нічого не гарантується (наприклад FTP або HTTP).

Інтегрований Сервіс — Integrated Service (IntServ)

Згідно RFC 1633, модель інтегрованого обслуговування забезпечує наскрізну (End-to-End) якість обслуговування, гарантуючи необхідну пропускну спроможність. IntServ використовує для своїх цілей протокол сигналізації RSVP, який забезпечує виконання вимог до всіх проміжних вузлів. Відносно IntServ часто використовується термін «резервування ресурсів» (Resource reservation). Протокол RSVP надає сигнальний механізм для конфігурації віддалених маршрутизаторів з метою отримання потрібного QoS. Протокол орієнтований на роботу з трьома видами трафіку: best efforts (звичайна передача IP-даних без встановлення з'єднання), чутливий до швидкості передачі і чутливий до затримок. Трафік чутливий до завантаження вимагає формування каналу з гарантованою пропускною спроможністю. Додаток при цьому вимушений миритися з певними затримками доставки (клас послуг з гарантованою швидкістю в бітах в сек.

Диференційоване обслуговування — Differentiated Service (DiffServ)

Описане в RFC 2474 і RFC 2475. Забезпечує QoS на основі розподілу ресурсів в ядрі мережі і певних класифікаторів та обмежень на межі мережі, комбінованих з метою надання необхідних послуг. У цій моделі вводиться розділення трафіку за класами, для кожного з яких визначається свій рівень QoS. DiffServ складається з управління формуванням трафіку (класифікація пакетів, маркіровка, управління інтенсивністю) і управління політикою (розподіл ресурсів, політика відкидання пакетів). DiffServ є найбільш відповідним прикладом «розумного» управління пріоритетом трафіку.

Протоколи, які надають послугу QoS

IP Differentiated services (DiffServ)
IP Integrated services (IntServ)
Resource reSerVation Protocol (RSVP)
Multiprotocol Label Switching (MPLS)
RSVP-TE
Frame relay
X.25
Asynchronous Transfer Mode (ATM)
IEEE 802.1p
IEEE 802.1Q
IEEE 802.11e
IEEE 802.11p

Велика мережа з топологією типу «зірка»

У міру розширення мережі доступна користувачу смуга (середня швидкість передавання) звужується за рахунок того, що канал 10Мбіт/с ділиться між усіма вузлами мережі.

У мережі типу велика мережа з топологією «зірка» з'єднання окремих робочих груп комп'ютерів проводиться через підсилювачі (хаби, рис. 2.3).

Підвищення продуктивності комп'ютерів і використання додатків з інтенсивним мережевим трафіком потребує розширення смуги для повної реалізації можливостей програм і встаткування. Розширення мереж і підвищення продуктивності комп'ютерів потребують розширення доступної користувачам смуги, яка забезпечується мережевим середовищем передавання.

Існує декілька засобів розширення смуги, доступної кожному користувачу. Одним з яких є зниження числа вузлів мережі, що мають доступ до середовища, яке розділяється, і, отже, розширення доступної вузлам смуги, що залишилися. У граничному випадку вся смуга каналу передавання може бути надана одному користувачу. Процес зниження числа вузлів у мережі називається **сегментацією** й здійснюється за рахунок розподілу великої мережі на декілька менших.

У мережі необхідні можливості забезпечуються за допомогою таких пристроїв як **репітери**, **маршрутизатори, комутатори, концентратори й мости**.

Репітер – це пристрій, який приймає затухаючий сигнал з одного сегменту мережі, відновлює його і передає в наступний сегмент, чим підвищує дальність передавання сигналів між окремими вузлами мережі. Репітери передають весь трафік в обох напрямах і працюють на фізичному рівні моделі OSI. Це означає, що кожен сегмент повинен використовувати однакові формати пакетів, протоколи і методи доступу. Тобто за допомогою репітера можливо об'єднати в єдину мережу два сегменти Ethernet і, наприклад, неможливо Ethernet і Token Ring.

Проте репітери дозволяють з'єднувати два сегменти, які використовують різні фізичні середовища передавання сигналів (оптично-волоконний кабель та кабель типу «скручена пара» і т. д.). Деякі багатопортові репітери працюють як багатопортові концентратори, що з'єднують різні типи кабелів.

Концентратор (повторювач) просто копіює (пересилає) усі пакети з одного сегмента у всі інші, приєднані до нього. Основною задачею повторювача є відновлення електричних сигналів для передавання їх в інші сегменти. За рахунок посилення й відновлення форми електричних сигналів повторювачем стає можливим розширення мереж, побудованих на основі коаксіального кабелю й збільшення загального числа користувачів мережі. При використанні повторювачів максимальна протяжність мережі складає 2500 метрів. Концентратор (Hub) служить центром (шиною) зіркоподібної конфігурації мережі й забезпечує підключення мережевих пристроїв.

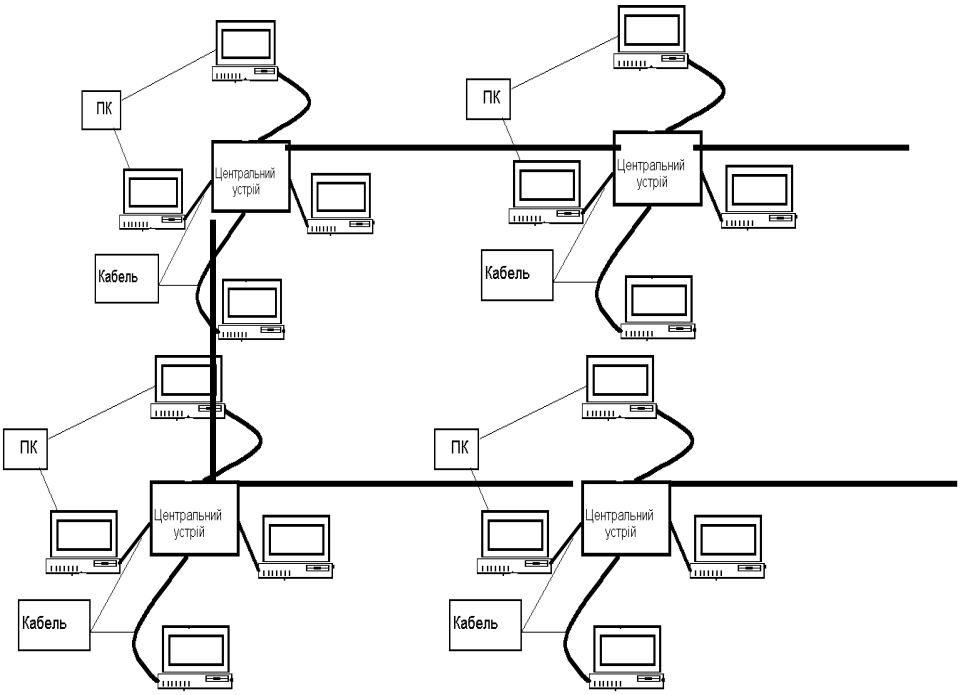


Рис. 2.3. Велика мережа з топологією типу «зірка»

У концентраторі для кожного вузла (ПК, принтери, сервери доступу, телефони й ін.) повинний бути передбачений окремий порт. Концентратори, що нарощуються, являють собою

окремі модулі, які об'єднуються за допомогою швидкодіючої системи зв'язку. Такі концентратори надають зручний засіб поетапного розширення можливостей і потужності ЛОМ. Концентратор здійснює електричну розв'язку відрізків кабелю до кожного вузла, тому коротке замикання на одному із відрізків не виведе з ладу всю ЛОМ. Для подолання цього обмеження потрібні інші пристрої, що називаються мостами. Мости мають багато відмінностей від повторювачів. Повторювачі передають усі пакети, а мости – тільки ті, що потрібно. Якщо пакет не потрібно передавати в інший сегмент, він фільтрується. Для мостів існують численні алгоритми (правила) передавання й фільтрації пакетів – мінімальною вимогою є фільтрація пакетів за адресою одержувача. Іншою важливою відмінністю мостів від повторювачів є те, що сегменти, залучені до повторювача, утворять середовище, що розділяється, а сегменти, залучені до кожного порту моста утворять своє середовище зі смугою 10Мбіт/с.

Міст – це пристрій, що дозволяє з'єднувати дві мережі, таким чином, щоб вони одержували повідомлення через один інтерфейс, визначає одержувача за тією або іншою таблицею, і передає його на інший інтерфейс. Також дозволяє збільшувати розмір мережі і кількість РС в ній та з'єднувати різнорідні мережеві кабелі. Проте принциповою їх відмінністю є те, що вони працюють на канальному рівні моделі OSI, тобто на вищому, ніж репітери і враховують більше особливостей даних, які передаються, дозволяючи:

- відновлювати форму сигналів, але роблять це на рівні пакетів;
- з'єднувати різнорідні сегменти мереж (наприклад, Ethernet і Token Ring) і переносити між ними пакети;
- підвищити продуктивність, ефективність, безпеку і надійність мереж.

Призначення мостів

1. Мости дозволяють збільшити розмір мережі, працюючи як повторювачі. При цьому допускається каскадне з'єднання різнорідних ЛОМ через мости.

2. Використання мостів підвищує продуктивність мережі унаслідок можливості її сегментації. Мости здатні фільтрувати пакети згідно деяких критеріїв. Два невеликі сегменти працюватимуть швидше, ніж один великий, оскільки трафік локалізується в межах кожного сегменту.

3. Застосування мостів підвищує ефективність роботи мережі, оскільки для кожної підмережі (сегменту) можна використовувати різні топології і середовища передавання, а потім їх об'єднувати мостами. Так, наприклад, якщо в окремих відділах ПК сполучені скрученимиі парами, то мостом ці підмережі можна з'єднати з корпоративною оптичною магістраллю.

4. Мости дозволяють збільшити безпеку (захист) даних за рахунок того, що їх можна програмувати на передавання тільки тих пакетів, які містять адреси певних відправників і одержувачів. Це дозволяє обмежити круг РС, здатних посилати і приймати інформацію з іншої підмережі. Наприклад, в мережі, що обслуговує бухоблік, можна поставити міст, який дозволить приймати інформацію лише деяким зовнішнім станціям.

5. Мости збільшують надійність і відмовостійкість мережі. При сегментації мережі відмова якої-небудь підмережі не приведе до зупинки всіх інших. Окрім цього, коли виходить з ладу єдиний файл-сервер, припиняє роботу вся мережа. Якщо за допомогою внутрішніх мостів зв'язати два файл-сервери, що страхують один одного, то зросте відмовостійкість мережі та знизиться рівень трафіку.

Розрізняють *локальні* і *віддалені мости*. Віддалені мости використовуються у великих мережах, коли її окремі сегменти зв'язуються телефонними (або іншими) каналами зв'язку.

Проте якщо для з'єднання двох кабельних сегментів ЛОМ використовують тільки один локальний міст, то в великих мережах доводиться використовувати два віддалені мости, що підключені через синхронні модеми до виділеного каналу зв'язку.

Маршрутизатори (router) – це «надрозумний міст», що визначає адреси комп'ютерів у мережі, і в залежності від того, звідкіля й куди слідує сигнал, переправляє інформацію. Маршрутизатор знає дуже добре, з якими пакетами він працює – з IP, IPX, CLNP або з усіма ними відразу (у випадку багатопротокольних маршрутизаторів). Він аналізує заголовки цих пакетів і приймає рішення відповідно до адресної інформації, що міститься там. З іншого боку, коли маршрутизатор передає пакет на канальний рівень, він не знає, і не повинен знати про те, у який кадр даний пакет буде приміщений – Ethernet, Token Ring або якийсь інший.

Працюючи на мережевому рівні моделі OSI, маршрутизатори можуть:

- комутувати і направляти пакети через декілька мереж;

- визначати якнайкращий шлях для їх передавання;
- обходити повільні і несправні канали;
- фільтрувати широкомовні повідомлення;
- діяти як бар'єр безпеки між мережами.

Маршрутизатор на відміну від моста має свою адресу і використовується як проміжний пункт призначення.

Вони бувають *статичні* й *динамічні*. Статичні маршрутизатори характеризуються ручним установленням й конфігуруванням усіх маршрутів. Жорстко заданий маршрут не завжди є найкращим. Статичні маршрутизатори вважаються безпечнішими, тому що адміністратор сам указує кожний маршрут.

Так само як і мости, маршрутизатори бувають *локальними* і *віддаленими*. Відмінність мостів і маршрутизаторів в тому, що:

- міст працює на канальному рівні і "бачить" тільки адресу вузла; розпізнає його, передає в потрібний сегмент мережі; не визначивши адресу, пересилає у всі сегменти;
- маршрутизатор працює на мережевому рівні, визначаючи і те, що потрібно передати, і те, куди потрібно; тобто він розпізнає не тільки адресу, але і тип протоколу;
- маршрутизатор встановлює адреси інших маршрутизаторів і вирішує, які пакети яким маршрутизаторам переадресувати.

Міст може розпізнати тільки один шлях між мережами, а маршрутизатор з багатьох знаходить кращий. В даний час почали використовуватися мости-маршрутизатори – пристрої, які поєднали в собі кращі властивості мостів і маршрутизаторів: для одних протоколів вони діють як мости; для інших – як маршрутизатори.

Шлюзи призначені для з'єднання в одну систему двох мереж абсолютно різних типів. Вони виконують функції маршрутизаторів і універсальних ретрансляторів, перетворюючи повідомлення з формату однієї мережі у формат іншої. Функції шлюзів, як правило, у мережі виконують сервери.

Головне їх призначення – здійснювати зв'язок між ПК. Звичайно, роль шлюзів в ЛОМ виконують виділені сервера, а решта всіх робочих станцій ЛОМ працюють з мейнфреймом так само просто, як зі своїми ресурсами. Шлюз зв'язує дві системи, які використовують різні:

- комунікаційні протоколи;
- структури і формати даних;
- мови і архітектуру.

Шлюзи приймають дані з одного середовища, видаляють протокольний стек і перетворюють їх в протокольний стек системи призначення. Обробляючи дані, шлюз виконує наступні операції:

- отримує дані з пакетів, що приходять, пропускаючи їх від низу до верху через повний стек протоколів передавального середовища;
- наново упаковує отримані дані, пропускаючи їх зверху вниз через стек протоколів мережі призначення.

Комутатор (switch) являє собою пристрій для організації мереж великого розміру. Комутатор може з'єднувати сервери в кластер і бути основою для об'єднання декількох робочих груп. Він спрямовує пакети даних між вузлами ЛОМ. Кожний сегмент, що комутує, одержує доступ до каналу передавання даних без конкуренції й бачить тільки той трафік, що направляється в його сегмент. Комутатор повинний надавати кожному порту можливість з'єднання з максимальною швидкістю конкуренції з боку інших портів (на відміну від спільно використовуваного концентратора). Зазвичай, у комутаторах є один або два високошвидкісних порти, а також інструментальні засоби керування. Комутатором можна замінити маршрутизатор, доповнити ним маршрутизатор, або використовувати комутатор у якості основи для з'єднання декількох концентраторів. Комутатор може слугувати відмінним пристроєм для спрямовування трафіка між концентраторами ЛОМ робочої групи й завантажених файлів-серверів.

Комутатори потіснили маршрутизатори тому, що їх показник "ціна/продуктивність", розрахований для одного порту, виявився набагато нижчим, ніж у маршрутизаторів при збереженні функціональних можливостей активної дії на передаваний трафік. Сьогоднішні корпоративні комутатори уміють багато що з того, що кілька років тому здавалося винятковою прерогативою маршрутизаторів: транслювати кадри різних технологій локальних мереж,

наприклад Ethernet в FDDI, здійснювати фільтрацію трафіку за різними умовами, ізолювати трафік одного сегменту від іншого і тому подібне. Комутатори ввели також і нову технологію, яка до їх появи не застосовувалася, – технологію віртуальних сегментів, що дозволяє переміщувати користувачів з одного сегменту в іншій чисто програмним шляхом, без фізичної перекомутації роз'ємів.

Брандмауер – це не просто маршрутизатор, хост або група систем, що забезпечують безпеку в мережі. Скоріше, брандмауер – це підхід до безпеки; він допомагає реалізувати політику безпеки, що визначає дозволені служби й типи доступу до них, і є реалізацією цієї політики в термінах мережевої конфігурації, декількох хостів і маршрутизаторів, і інших мір захисту, таких як посилена аутентифікація замість статичних паролів. Основна мета системи брандмауера – керування доступом до або з мережі, що захищається. Він реалізує політику мережевого доступу, примушуючи проходити всі з'єднання з мережею через брандмауер, де вони можуть бути проаналізовані й дозволені, або відкинуті.

Система брандмауера може бути маршрутизатором, персональним комп'ютером, хостом, або групою хостів, створеною спеціально для захисту мережі, або підмережі від неправильного використання протоколів і служб хостами, що знаходяться поза цією підмережею. Як правило, система брандмауера створюється на основі маршрутизаторів верхнього рівня, звичайно, на тих, що з'єднують мережу з Інтернетом, хоча може бути створена й на інших маршрутизаторах, для захисту тільки частини хостів або підмереж. Брандмауер також надає можливості з керування доступом до хостів мережі. Наприклад, деякі хости можуть бути досяжними із зовнішніх мереж, у той час як доступ до інших систем ззовні буде заборонений. Мережа може заборонити доступ до своїх хостів ззовні, за винятком особливих випадків, таких як поштові сервери або інформаційні сервери.

Вибір розміру й структури мережі

Під розміром мережі в даному випадку розуміється як кількість об'єднуваних у мережу комп'ютерів, так і відстані між ними. Треба чітко уявляти собі скільки комп'ютерів (мінімально й максимально) потребує підключення до мережі. При цьому необхідно залишати можливість для подальшого зростання кількості комп'ютерів у мережі, хоч би відсотків на 20–50.

До речі, зовсім не обов'язково раз і назавжди включати в мережу всі комп'ютери підприємства. Іноді має сенс залишити деякі з них автономними, наприклад, з міркувань безпеки інформації на їх дисках. Кількість підключених до мережі комп'ютерів сильно впливає як на продуктивність, так і на складність її обслуговування. Вона також визначає вартість необхідних програмних засобів, тому прорахунки можуть мати досить серйозні наслідки.

Необхідна довжина ліній зв'язку мережі також грає не малу роль у проектуванні мережі. Наприклад, якщо відстані дуже великі, може знадобитися використання дорогого встаткування. До того ж зі збільшенням відстані різко зростає значущість захисту ліній зв'язку від зовнішніх електромагнітних перешкод. Від відстані залежить і швидкість передавання інформації мережею (вибір між Ethernet і Fast Ethernet). Доцільно при виборі відстаней закладати невеликий запас (хоч би відсотків 10) для врахування непередбачених обставин. Подолати обмеження за довжиною іноді можна шляхом вибору *структури мережі*, розбиття її на окремі частини.

Під *структурою мережі* розуміється спосіб розділення мережі на частини (сегменти), а також спосіб з'єднання цих сегментів між собою. Мережа підприємства може включати робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі можуть використовуватися репітери, репітерні концентратори, комутатори, мости й маршрутизатори. Причому в ряді випадків вартість цього об'єднувального встаткування може навіть перевищити вартість комп'ютерів, мережевих адаптерів і кабелю, тому вибір *структури мережі* виключно важливий.

В ідеалі *структура мережі* повинна відповідати структурі будівлі або комплексу будівель підприємства. Робочі місця групи співробітників, що займаються одним завданням (наприклад, бухгалтерія, відділ продажів, інженерна група), повинні розміщуватися в одній або поряд розташованих кімнатах. Тоді можна комп'ютери цих співробітників об'єднати в один сегмент, у єдину робочу групу й установити поблизу їх кімнат сервер, з яким вони працюватимуть, а також концентратор або комутатор, що зв'язує всі їх машини. Так само робочі місця співробітників підрозділу, що займаються комплексом близьких завдань, краще розташувати на одному поверсі будівлі, що істотно спростить їх об'єднання в сегмент і подальше його адміністрування.

На цьому ж поверсі зручно розташувати комутатори, маршрутизатори й сервери, з якими працює даний підрозділ.

Як і в інших випадках, при виборі *структури* розумно залишати можливості для подальшого розвитку мережі. Наприклад, краще придбати комутатори або маршрутизатори з більшою кількістю портів, ніж потрібно зараз (хоч би на 10-20 відсотків). Це дозволить при необхідності легко включити в мережу один або декілька сегментів. Адже будь-яке підприємство завжди прагне до зростання (деколи абсолютно марно), і це зростання не повинне кожного разу приводити до необхідності проектувати мережу підприємства наново.

Нехай невелике підприємство займає два поверхи, на кожному по шість кімнат і включає чотири підрозділи по три групи. У цьому випадку можна побудувати мережу, таким чином:

- Робочі групи займають по 1-3 кімнати, їх комп'ютери об'єднані між собою репітерними концентраторами. Концентратор може використовуватися один на кімнату, один на групу або один на весь поверх. Концентратор доцільно розташувати в приміщенні, в яке має доступ мінімальна кількість співробітників.
- Підрозділи займають половину поверху. Усі чотири мережі робочих груп кожного підрозділу об'єднуються комутатором, а для зв'язку з мережами інших підрозділів використовується маршрутизатор. Комутатор разом з одним із концентраторів краще помістити в окремій кімнаті.
- Загальна мережа підприємства включає чотири сегменти мереж підрозділів, об'єднаних маршрутизатором. Цей же маршрутизатор може використовуватися для підключення до глобальної мережі.
- Сервери робочих груп розташовуються в кімнатах робочих груп, сервери підрозділів – на поверхах підрозділів.

У розглянутій ситуації області колізій (зони конфлікту) мережі включатимуть сегменти, розташовані в кімнатах кожної робочої групи, плюс сегмент, що зв'язує концентратор робочої групи з комутатором підрозділу. Усього таких областей колізій буде вісім. Саме для них необхідно проводити розрахунки працездатності мережі.

Широкомовні області включатимуть усі сегменти мережі кожного підрозділу плюс сегмент, що зв'язує комутатор підрозділу з маршрутизатором підприємства. Таких широкомовних областей буде всього чотири.

Якщо передбачувана інтенсивність обміну проектованою мережею не достатньо велика, комп'ютерів не дуже багато і розміри будівлі дозволяють, то цілком можливо обійтися без маршрутизаторів, досить складних і порівняно дорогих пристроїв.

Тоді мережі підрозділів будуть зв'язані концентраторами, а між собою вони з'єднуватимуться комутаторами.

Області колізій у даному випадку включатимуть усі сегменти мережі кожного підрозділу плюс сегмент, що сполучає концентратор підрозділу й комутатор підприємства. Таких областей колізій усього чотири. Для них треба проводити розрахунок працездатності мережі. До єдиної широкомовної області ввійде вся мережа підприємства.

За ситуації, коли комп'ютерів на підприємстві небагато (до 50), має сенс відмовитися не тільки від маршрутизаторів, але і від комутаторів, залишивши тільки репітерні концентратори. Більш того, при такій малій мережі і низькій інтенсивності обміну цілком може виявитися відповідною мережа Ethernet на тонкому коаксіальному кабелі (сегменти 10BASE2) без концентраторів або з 1-2 простими репітерами. Правда, в останньому випадку доведеться комп'ютери кожного сегменту розмістити на одному поверсі із-за обмежень на довжину кабелю сегменту 10BASE2. Слід ураховувати, що в новостворюваних мережах використання коаксіального кабелю не рекомендується.

Класи IP-адрес

IP-адреса має довжину 4 байти і зазвичай записується у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі і розділених крапками, наприклад, 128.10.2.30 – традиційна десяткова форма представлення адреси, а 10000000 00001010 00000010 00011110 – двійкова форма представлення цієї ж адреси.

Адреса складається із двох логічних частин – номера мережі й номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка – до номера вузла, визначається зна-

ченнями перших біт адреси. Значення цих біт є також ознаками того, до якого *класу* відноситься та або інша IP-адреса.

Якщо адреса починається з 0, то мережу відносять до *класу A* і номер мережі займає один байт, останні 3 байти інтерпретуються як номер вузла в мережі. Мережі класу А мають номери в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей.) Мереж класу А небагато, зате кількість вузлів у них може досягати 2^{24}, тобто 16 777 216 вузлів.

Якщо перші два біта адреси рівні 10, то мережа відноситься до *класу B.* У мережах класу В під номер мережі й під номер вузла відводиться по 16 бітів, тобто по 2 байти. Таким чином, мережа класу В є мережею середніх розмірів із максимальним числом вузлів 2^{16}, що складає 65 536 вузлів.

Якщо адреса починається з послідовності 110, то це мережа *класу C.* У цьому випадку під номер мережі відводиться 24 біта, а під номер вузла – 8 бітів. Мережі цього класу найпоширеніші, число вузлів у них обмежене 2^8, тобто 256 вузлами.

Якщо адреса починається з послідовності 1110, то вона є адресою *класу D і* позначає особливу, групову адресу – multicast. Якщо в пакеті як адреса призначення вказана адреса класу D, то такий пакет повинні отримати всі вузли, яким привласнена дана адреса.

Якщо адреса починається з послідовності 11110, то це означає, що дана адреса відноситься до *класу E*. Адреси цього класу зарезервовані для майбутніх застосувань.

Технології мереж

Модель STM

STM є мережевим механізмом з комутацією з'єднань, де з'єднання встановлюється перш, ніж почнеться передавання даних, і розривається після його закінчення. Таким чином, взаємодіючі вузли захоплюють і утримують канал, поки не вважатимуть необхідним роз'єднатися, незалежно від того, передають вони дані або "мовчать".

Дані в STM передаються за допомогою розділення всієї смуги каналу на базові трансмісійні елементи, звані *тимчасовими каналами* або *слотами*. Слоти об'єднані в обойму, що містить фіксоване число каналів, пронумерованих від 1 до N. Кожному слоту ставитися у відповідність одне з'єднання. Кожна з обойм (їх теж може бути декілька – від 1 до M) визначає свій набір з'єднань. Обойма надає свої слоти для встановлення з'єднання з періодом T. При цьому гарантується, що протягом цього періоду необхідна обойма буде доступна. Параметри N, M і T визначаються відповідними комітетами зі стандартизації й відрізняються в Америці і Європі.

У рамках каналу STM кожне з'єднання асоціюється з фіксованим номером слота в конкретній обоймі. Одного разу захоплений слот залишається у розпорядженні з'єднання протягом всього часу існування цього з'єднання.

Модель ATM

Asynchronous Transfer Mode (ATM, асинхронний режим передавання даних) – технологія, прообразом якої є технології, що розроблені раніше телефонними компаніями. Технологія ця розроблялася далеко не з розрахунку на комп'ютерні мережі передавання даних. ATM радикально відрізняється від звичайних мережевих технологій. Основна одиниця передавання в цьому стандарті – це комірка, на відміну від звичного пакету. Комірка містить в собі 48 байт даних і 5 байт заголовка. Частково це необхідно, щоб забезпечити дуже маленький час затримки передавання мультимедійних даних. (Фактично розмір комірки став компромісом між американським телефонними компаніями, які віддають перевагу розміру комірки 64 байти, і європейськими, у яких він дорівнює 32 байтам).

Пристрої ATM установлюють зв'язок між собою і передають дані віртуальними каналами зв'язку, які можуть бути тимчасовими або постійними. Постійний канал зв'язку – це шлях, яким передається інформація. Він завжди залишається відкритим незалежно від трафіку. Тимчасові канали створюються на вимогу й, як тільки передача даних закінчується, закриваються.

Із самого початку ATM проектувався як система комутації за допомогою віртуальних каналів зв'язку, які забезпечують заздалегідь специфікований рівень якості сервісу (Quality of Service, QOS) і підтримують постійну або змінну швидкість передавання даних. Модель QOS дозволяє додаткам запитати гарантовану швидкість передавання між приймачем і джерелом, не

беручи до уваги на те, наскільки складний шлях між ними. Кожен ATM-комутатор, зв'язуючись з іншим, вибирає такий шлях, який гарантує потрібну додаткам швидкість.

Дану технологію побудови високошвидкісних обчислювальних мереж з комутацією пакетів характеризує унікальна масштабованість: від невеликих локальних мереж зі швидкостями обміну 25-50 Мбіт/с до трансконтинентальних мереж.

Як передавальне середовище використовується або кабель типу «скручена пара» (до 155 Мбіт/с), або оптично-волоконний кабель.

ATM є розвитком STM (Synchronous Transfer Mode) – технології передавання пакетованних даних і мови на великі відстані, традиційно використовуваною для побудови телекомунікаційних магістралей і телефонної мережі. Тому перш за все ми розглянемо STM.

Дослідження застосування оптично-волоконних каналів у трансокеанських і трансконтинентальних масштабах виявили ряд особливостей передавання даних різних типів. У сучасних комунікаціях можна виділити два типи запитів:

- передавання даних, стійких до деяких втрат, але критичних до можливих затримок (наприклад, сигнали телебачення високої чіткості й звукова інформація);
- передавання даних, не дуже критичних до затримок, але не допускаючих втрат інформації (цей тип передавання, як правило, відноситься до міжкомп'ютерних обмінів).

Передавання різнорідних даних приводить до періодичного виникнення запитів на обслуговування, що вимагають великої смуги пропускання, але при малому часі передавання. Вузол, деколи, вимагає пікової продуктивності каналу, але відбувається це відносно рідко, займаючи, скажімо, одну десяту часу. Для такого виду каналу реалізується одне з десяти можливих з'єднань, на чому, природно, втрачається ефективність використання каналу. Було б чудово, якби існувала можливість передати тимчасово невикористовуваний слот іншому абонентові. На жаль, у рамках моделі STM це неможливо.

У мережі ATM два вузли знаходять один одного за «віртуальним ідентифікатором з'єднання» (Virtual Circuit Identifier, VCI), що використовується замість номерів слота і обойми в моделі STM. Швидкий пакет передається в такий же слот, як і раніше, але без будь-яких вказівок або ідентифікатора.

Формат даних ATM

Пакет ATM, визначений спеціальним підкомітетом ANSI, повинен містити 53 байти. П'ять байтів зайнято заголовком, останні 48 – змістовна частина пакету. У заголовку 24 біта віддано ідентифікатору VCI, вісім бітів – контрольні, відведені для контрольної суми. З 48 байт змістовної частини 4 байти може бути відведене для спеціального адаптаційного рівня ATM, а 44 – власне під дані. Адаптаційні байти дозволяють об'єднувати короткі пакети ATM у крупніші, наприклад, в кадри Ethernet. Контрольне поле містить службову інформацію про пакет.

Хоча фізичний рівень і не є частиною специфікації ATM, він враховується багатьма комітетами стандартизації. В основному, як фізичний рівень розглядається специфікація SONET (Synchronous Optical Network) – міжнародний стандарт високошвидкісного передавання даних. Визначено чотири типи стандартних швидкостей обміну: 51, 155, 622 і 2400 Мбіт/с, відповідних міжнародній ієрархії цифрового синхронного передавання (Synchronous Digital Hierarchy, SDH). SDH специфікує яким чином дані фрагментуються і передаються синхронно оптично-волоконними каналами, не вимагаючи при цьому синхронізації каналів і тактових частот всіх вузлів, що беруть участь в процесі передавання і відновлення даних.

100VG-AnyLAN

У липні 1993 року за ініціативою компаній AT&T і Hewlett-Packard був організований новий комітет IEEE 802.12, покликаний стандартизувати нову технологію 100BaseVG. Дана технологія була високошвидкісним розширенням стандарту IEEE 802.3 (відомого також як 100BaseT, або Ethernet на витій парі).

У вересні компанія IBM запропонувала об'єднати в новому стандарті підтримку Ethernet і Token Ring. Змінилася й назва нової технології – 100VG-AnyLAN.

Технологія повинна підтримувати як уже існуючі мережеві застосування, так і новостворювані. На це направлена одночасна підтримка форматів кадрів даних і Ethernet, і Token Ring, що забезпечує прозорість мереж, побудованих за новою технологією, для існуючих програм.

Стандарт 100VG-AnyLAN орієнтований як на скручені пари (для використання придатне будь-яке наявне кабельне господарство), так і на оптично-волоконні лінії, що допускають значну віддаленість абонентів. Втім, на швидкості обміну застосування оптоволокна не позначається.

Оскільки 100VG покликана замінити собою Ethernet і Token Ring, вона підтримує топології, вживані для цих мереж (логічно загальна шина і маркерне кільце, відповідно). Фізична топологія – обов'язково зірка, петлі або галуження не допускаються.

При каскадному підключенні хабів між ними допускається тільки одна лінія зв'язку. Утворення резервних ліній можливе лише за умови, що в кожен момент активна одна лінія.

Стандартом передбачено до 1024 вузлів в одному сегменті мережі, але із-за зниження продуктивності мережі реальний максимум скромніший – 250 вузлів. Схожими міркуваннями визначається й максимальне відстань між найвіддаленішими вузлами – два з половиною кілометри.

Fast Ethernet

Ідея технології Fast Ethernet народилася в 1992 році. У серпні наступного року група виробників об'єдналася в союз Fast Ethernet (Fast Ethernet Alliance, FEA). Метою FEA було якнайскоріше дістати формальне схвалення Fast Ethernet від комітету 802.3 Інституту інженерів електротехніки і радіоелектроніки (Institute of Electrical and Electronic Engineers, IEEE), оскільки саме цей комітет займається стандартами для Ethernet. Як і його попередник, Fast Ethernet використовує метод передавання даних CSMACD (Carrier Sense Multiple Access with Collision Detection). За цим довгим і незрозумілим акронімом ховається дуже проста технологія. Коли мережева плата Ethernet повинна послати повідомлення, то спочатку вона чекає настання тиші, потім відправляє пакет і одночасно слухає, чи не послав хто-небудь повідомлення одночасно з нею. Якщо це відбулося, то обидва пакети не доходять до адресата. Якщо колізії не було, а плата повинна продовжувати передавати дані, вона все-таки чекає декілька мікросекунд, перш ніж знову спробує послати нову порцію. Це зроблено для того, щоб інші плати також могли працювати, і ніхто не зміг захопити канал монопольно. У разі колізії обидва пристрої замовкають на невеликий проміжок часу, який згенеровано випадковим чином, а потім роблять нову спробу передати дані.

Із-за колізій ні Ethernet, ні Fast Ethernet ніколи не зможуть досягти своєї максимальної продуктивності 10 або 100 Мбіт/с. Як тільки починає збільшуватися трафік мережі, тимчасові затримки між посилками окремих пакетів скорочуються, а кількість колізій збільшується. Реальна продуктивність Ethernet не може перевищувати 70% його потенційної пропускної спроможності, а може ще нижче, якщо лінія серйозно переобтяжена.

Для того щоб понизити перевантаження, мережі стандарту Ethernet розбиваються на сегменти, які об'єднуються за допомогою мостів і маршрутизаторів. Це дозволяє передавати між сегментами лише необхідний трафік. Повідомлення, що передається між двома станціями в одному сегменті, не буде передано в іншій сегмент і не зможе викликати в ньому перевантаження.

Сьогодні при побудові центральної магістралі, що об'єднує сервери, використовують комутовані Ethernet. Ethernet-комутатори можна розглядати як високошвидкісні багатопортові мости, які можуть самостійно визначити, в який з його портів адресований пакет. Комутатор проглядає заголовки пакетів і таким чином складає таблицю, що визначає, де знаходиться той або інший абонент з такою фізичною адресою. Це дозволяє обмежити область розповсюдження пакету і понизити вірогідність переповнювання, посилаючи його лише в потрібний порт. Тільки широкомовні пакети розсилаються за всіма портами.

З легкої руки IEEE Fast Ethernet іменується 100BaseT. Пояснюється це просто: 100BaseT є розширенням стандарту 10BaseT з пропускною спроможністю від 10 Мбіт/с до 100 Мбіт/с. Стандарт 100BaseT включає протокол обробки множинного доступу і виявлення конфліктів CSMA/CD, який використовується і в 10BaseT. Крім того, Fast Ethernet може працювати на кабелях декількох типів, у тому числі і на витій парі. Обидві ці властивості нового стандарту дуже важливі для потенційних покупців, і саме завдяки ним 100BaseT виявляється вдалим шляхом переобладнання мереж на базі 10BaseT.

Головним комерційним аргументом на користь 100BaseT є те, що Fast Ethernet базується на успадкованій технології. Оскільки в Fast Ethernet використовується той же протокол передавання повідомлень, що і в старих версіях Ethernet, а кабельні системи цих стандартів сумісні,

для переходу до 100BaseT від 10BaseT потрібні менші капітальні вкладення, чим для установки інших видів високошвидкісних мереж. Крім того, оскільки 100BaseT є продовженням старого стандарту Ethernet всіма інструментальними засобами і процедурами аналізу роботи мережі, а також всім програмним забезпеченням, що працює на старих мережах Ethernet, вони повинні в даному стандарті зберегти працездатність.

Передавальні середовища. Для 100Base-T Ethernet використовуються кабелі, що містять чотири неекрановані скручені пари. Одна пара слугує для передавання даних, одна – для вирішення конфліктів; дві пари, що залишилися, не використовуються. Очевидно, що передавання даних при всіх чотирьох парах дасть виграш учетверо. Заміна стандартного «манчестерського» кодування ефективнішим – 5B6B NRZ – дає виграш ще майже вдвічі (за рахунок передавання двох бітів даних за один такт). Таким чином, при лише невеликому підвищенні несучої частоти (близько 20%), продуктивність лінії зв'язку підвищується вдесятеро. При роботі з екранованими кабелями, характерними для мереж Token Ring, використовуються дві скручені пари, але при вдвічі більшій частоті (завдяки тому, що кабель екранований). При передаванні таким кабелем кожна пара використовується як фіксований однонаправлений канал. Однією парою передаються вхідні дані, іншою – вихідні. Стандартне віддалення вузлів, на якому гарантуються параметри передавання – 100 метрів для пар третьої й четвертої категорії і 200 метрів для п'ятої.

Допускається використання оптоволоконних пар. Завдяки такому носієві відстань, що покривається, збільшується до двох кілометрів, як і у випадку екранованого кабелю використовується двонаправлене з'єднання.

Хаби 100VG можуть з'єднуватися каскадом, що забезпечує максимальну відстань між вузлами в одному сегменті на неекранованих кабелях до 2,5 кілометрів.

Передбачуваний стандарт IEEE-802.12 підтримує три типи форматів кадрів передавання даних: IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) і спеціальний формат кадрів тестування з'єднань IEEE 802.3.

Стандарт обмежує допустиму організацію мереж, забороняючи використання різних форматів кадрів у рамках одного сегменту мережі. Кожен сегмент може підтримувати тільки один логічний стандарт, а для побудови гетерогенних мереж необхідне застосування спеціальних мостів.

Порядок передавання даних для форматів Ethernet і Token Ring однаковий (першим передається байт старшого розряду, останнім – молодшого). Розрізняється лише порядок бітів в байтах: у форматі Ethernet першими передаються молодші біти, а в Token Ring – старші.

Кадр Ethernet (IEEE 802.3) повинен містити наступні поля:

- DA – адреса одержувача пакет (6 байт);
- SA – адреса відправника (6 байт);
- L – показник довжини даних (2 байти);
- дані користувача й заповнювачі;
- FCS – контрольна послідовність.

Кадр Token Ring (IEEE 802.5) містить більше число полів. Деякі з них протоколом 100VG-AnyLAN не використовуються, а збережені лише для того, щоб забезпечити сумісність даних з сегментами 4 і 16 Мбіт/с (при обміні через відповідні мости):

- AC – поле контролю доступу (1 байт, не використовується);
- FC – поле контролю кадру (1 байт, не використовується);
- DA – адреса одержувача (6 байт);
- SA – адреса відправника (6 байт);
- RI – інформаційне поле маршрутизатора (0-30 байт);
- поле інформації;
- FCS – контрольна послідовність (4 байти).

Три види FAST ETHERNET

Разом зі збереженням протоколу CSMA/CD, іншим важливим рішенням було спроектувати 100BaseT так, щоб у ньому можна було застосовувати кабелі різних типів: як ті, що використовуються в старих версіях Ethernet, так і новіші моделі. Стандарт визначає три модифікації для забезпечення роботи з різними видами кабелів Fast Ethernet: 100BaseTX, 100BaseT4 і

100BaseFX. Модифікації 100BaseTX і 100BaseT4 розраховані на кабель типу «скручена пара», а 100BaseFX був розроблений для оптично-волоконного кабелю.

Стандарт 100BaseTX вимагає застосування двох пар UTP або STP. Одна пара служить для передавання, інша – для приймання. Цим вимогам відповідають два основні кабельні стандарти: EIA/TIA-568 UTP категорії 5 і STP типу 1 компанії IBM. У 100BaseTX привабливе забезпечення повнодуплексного режиму при роботі з мережевими серверами, а також використання всього двох з чотирьох пар восьмижильного кабелю – дві інші пари залишаються вільними і можуть бути використані надалі для розширення можливостей мережі.

Стандарт 100BaseT4 відрізняється м'якшими вимогами до використовуваного кабелю. Причиною тому та обставина, що в 100BaseT4 використовуються всі чотири пари восьмижильного кабелю: одна для передавання, інша для приймання, а дві, що залишилися, працюють як на передавання, так і на приймання. Таким чином, в 100BaseT4 і приймання, і передавання даних може здійснюватися за трьома парами. Розкладаючи 100 Мбіт/с на три пари, 100BaseT4 зменшує частоту сигналу, тому для його передавання досить і менш високоякісного кабелю. Для реалізації мереж 100BaseT4 підійдуть кабелі UTP категорій 3 і 5, так само як і UTP категорії 5 і STP типу 1.

Мережі Gigabit Ethernet.

Питання «Gigabit Ethernet – це Ethernet чи ні?» зовсім не довільне, і, хоча Gigabit Ethernet Alliance відповідає на нього ствердно на тій підставі, що ця технологія використовує той же формат кадрів, той же метод доступу до середовища передавання CSMA/CD, ті ж механізми контролю потоків і ті ж об'єкти, що управляють, все ж таки Gigabit Ethernet відрізняється від Fast Ethernet більше, ніж Fast Ethernet від Ethernet. (До того ж, наприклад, Hewlett-Packard вважає, що він має більше схожості з 100VG-AnyLAN, ніж з Fast Ethernet.) Зокрема, якщо для Ethernet була характерна різноманітність підтримуваних середовищ передавання, що давало привід говорити про те, що він може працювати хоч з колючим дротом, то в Gigabit Ethernet волоконно-оптичні кабелі стають домінуючим середовищем передавання.

Основні труднощі при використанні Gigabit Ethernet пов'язані з виникненням диференціальної затримки сигналів (differential mode delay, DMD) в багатомодових волоконних кабелях. Ця затримка з'являється при використанні деяких комбінацій багатомодового волокна і лазерних діодів, що використовуються для прискорення передавання даних волоконним кабелем. У результаті виникають порушення синхронізації (свого роду тремтіння) сигналу, що обмежують максимальну відстань (табл. 2.2), на яку можуть передаватися дані за Gigabit Ethernet.

Таблиця 2.2

Стандарти й додатки

Інтерфейс фізичного рівня	**Тип кабелю**	**Максимальна протяжність (у дужках діаметр волокна)**	**Типові застосування**
1000BASESX	Багатомодовий кабель з короткохвильовим лазером (850 нм)	220 м (62,5 мкм); 500 м (50 мкм)	Короткі магістралі
1000BASELX	Багатомодовий і одномодовий кабель із довгохвильовим лазером (1300 нм)	Багатомодовий: 550 м (62,5 мкм); 550 м (50 мкм) Одномодовий: 5 км. (9 мкм)	Короткі магістралі Територіальні магістралі
1000BASECX	Короткий мідний кабель (STP/коаксиальний)	25 м	Міжмережеві з'єднання, устаткування в монтажній шафі
1000BASET	4-парний неекранований категорії 5	100 м	Горизонтальні траси

FDDI - розподілений волоконно-оптичний інтерфейс передавання даних

Однією з сучасних мережевих архітектур являється архітектура FDDI (Fiber Distributed Data Interface), яка визначає:

- двохкільцеву топологію на основі оптоволокна;

- з маркерним методом доступу;
- із швидкістю передавання 100 Мбіт/с при загальній довжині кілець до 200 км.

Ця архітектура забезпечує сумісність із Token Ring, оскільки у них однакові формати кадрів. Проте є і відмінності. У мереж FDDI комп'ютер:

- захоплює маркер на певний інтервал часу;
- за цей інтервал передає стільки кадрів, скільки встигне;
- завершує передавання або після закінчення виділеного інтервалу часу, або через відсутність передаваних кадрів.

Оскільки комп'ютер, завершивши передачу, відразу звільняє маркер, можуть залишитися декілька кадрів, що одночасно циркулюють кільцем. Цим пояснюється вища продуктивність FDDI, ніж Token Ring, яка дозволяє циркулювати в кільці тільки одному кадру.

FDDI заснована на технології сумісного використання мережі. Це означає, що передавати дані одночасно можуть декілька комп'ютерів. Хоча FDDI працює із швидкістю 100 Мбіт/с, технологія сумісного використання може стати причиною її перевантаження. Так, якщо 10 комп'ютерів почнуть передавати дані із швидкістю 10 Мбіт/с кожен, загальний потік дорівнюватиме 100 Мбіт/с. А при передаванні відеоінформації або даних мультимедіа середовище передавання виявиться потенційно вузьким місцем системи.

FDDI використовує передачу маркера в подвійному кільці. Трафік мережі складається з двох схожих потоків, які рухаються в протилежних напрямах за двома кільцями: основному і додатковому. Зазвичай, дані передаються за основним кільцем. Якщо в основному відбувається збій, мережа автоматично реконфігурується і дані починають передаватися за другим кільцем в іншому напрямі. Однією з переваг FDDI є надмірність: одне кільце є резервним. При відмові кільця або розриві кабелю мережа автоматично переконфігується і передавання продовжиться. Існують обмеження:

- довжина кабелю об'єднаних кілець до 200 км.;
- загальна кількість комп'ютерів до 1000 штук;
- через кожних 2 км необхідно установлювати репітер.

Оскільки друге кільце призначене для захисту від збоїв, то для високонадійного передавання ці показники треба ділити на два (500 комп'ютерів при довжині кожного кільця 100 км.). Комп'ютери можуть підключатися доодного або обох кілець: станції класу А підключені до обох кілець; станції класу В тільки до основного. Якщо відбувається збій мережі, станції класу А беруть участь в переконфігурації, а станції класу В – не беруть участь.

Фізично FDDI має топологію «зірка». При цьому окремі комп'ютери можуть мати з'єднання «крапка-крапка» з концентратором. Таке рішення дозволяє використовувати інтелектуальні концентратори для мережевого управління і пошуку несправностей.

Сфери застосування FDDI

1. FDDI забезпечує високошвидкісний зв'язок між мережами різних типів і може використовуватися в мережах міського масштабу.
2. Використовується для з'єднання великих або міні-комп'ютерів в традиційних комп'ютерних залах, обслуговуючи дуже інтенсивне передавання файлів.
3. Виступає як магістральна мережа, до якої підключаються ЛОМ малої продуктивності.
4. Локальні мережі, де потрібна висока швидкість передавання даних. Це мережі, що складаються з інженерних РС і комп'ютерів, де ведеться відеообробка, працюють системи автоматизованого проектування, управління виробництвом.
5. Будь-яка установа, що потребує високошвидкісної обробки. Навіть у офісах комерційних фірм створення графіки або мультимедіа для презентацій та інших документів нерідко викликає перевантаження мережі.

Підхід на основі віртуальних мереж

Одна із причин, із-за якої віртуальні мережі набувають популярності, полягає в тому, що сегменти рідко бувають статичними: у силу виробничих міркувань, а також через кадрові зміни сегменти знаходяться в стані постійної видозміни. Конфігурування цих змін вручну, наприклад, переведення людей з однієї групи в іншу або надання доступу членам однієї групи до ресурсів іншої, досить трудомістке заняття. Як правило, для цього потрібно додаткове встаткування, приміром, маршрутизатори й брандмауери, а значить моніторинг і обслуговування додаткових пристроїв і без того складної мережі. Тому віртуальні мережі стають найкращим засобом сегментування, особливо у великих мережах. Існує декілька засобів

побудови віртуальних мереж:

- Угруповування портів.
- Угруповування MAC-адрес.
- Використання міток у додатковому полі кадру – приватні протоколи й специфікації IEEE 802.1 Q/p.
- Специфікація LANE для ATM-комутаторів.

Технологія Інтранет – підхід до управління інформацією

Щоб інформація була корисною для споживача, вона повинна доставлятися до нього за запитом саме тоді, коли в ній виникла необхідність, і бути актуальною. Крім того, постачальник повинен зберігати можливість управління інформацією, він повинен не тільки створювати її, але і вчасно оновлювати і видаляти. Людині зручніше працювати за принципом «я отримую інформацію в потрібному об'ємі саме тоді, коли вона мені необхідна».

Централізовані комп'ютерні системи, що домінували ще 30 років тому, дозволяли користувачам порівняно легко знаходити інформацію в оперативному режимі, але за однієї умови – інформація повинна була концентруватися в одному місці, у рамках однієї програмної системи. Інформація не могла бути територіально розподіленою й різнорідною – такою інформацією централізовані системи управляти не могли. Крім того, вони були украй дорогі й складні в управлінні.

Мережі персональних комп'ютерів істотно дешевші централізованих систем, вони залишають за постачальником необхідну свободу управління інформацією, проте, споживачам доводиться шукати необхідні дані на безлічі машин, користуючись великим числом додатків із різними й далеко не завжди вдалими інтерфейсами. У таких системах відсутній універсальний підхід до споживання інформації, і працювати рядовому користувачеві в такому різнорідному прикладному середовищі украй незручно.

Системи Інтранет та задачі, які вони вирішують.

Наступним етапом в розвитку технологій, які були розроблені в Інтернет, насамперед Web-технології, стало їх застосування до корпоративних інформаційних систем.

Цей етап цікавий тим, що саме він забезпечує розвиток і фінансування Інтернет- і Інтранет-технологій. Про це часто забувають, і це не дивно – адже максимальний зовнішній ефект досягається при спілкуванні з Web-серверами, які працюють в Інтернет, доступні широким колам користувачів, і саме до них прикована основна увага. При цьому забувається, що дійсних фінансових вигод ні компанії-розробники таких серверів, ні навіть компанії, які будують свої власні Web-сервери, сьогодні не отримують. Справжнє фінансування цих технологій відбувається за рахунок їх застосування для корпоративних мереж. Це саме те, за що платять гроші великі компанії.

Сам термін "Інтранет" з'явився весною 1995 року. Спочатку це слово мало що означало для переважної більшості людей, багато хто з них, прочитавши його, подумав би, що це друкарська помилка. Після того, як це слово завоювало право на життя, виникло питання: "Що під цим розуміється?" - адже після того, як термін з'явився, його стали використовувати всі. Багато компаній "раптом" виявили, що давно цим займаються і є "провідними виробниками" в цій області. Зараз практично неможливо знайти фірму, яка б не говорила, що вона знаходиться в авангарді даного напряму.

При цьому глибина розуміння й значення, яке люди вкладають у поняття Інтранет, дуже сильно розрізняються. Сказати, що **Інтранет – це застосування технології Інтернет у рамках корпоративних систем –** це означає, насправді, не сказати практично нічого.

Дивно, що сам по собі феномен Інтранет не можна пояснити появою нової інформаційної технології. Тут криються глибші причини. Які ж?

Відомо, проте, що корпоративні системи зазвичай є украй консервативними, вони виключно неохоче приймають нові технології, логіка їх існування така, що вони прагнуть зберегти статус-кво. Проте технологія Інтранет стрімко просувається на ринок корпоративних систем.

Цей факт свідчить про те, що насправді бізнес-потреба в технології Інтранет уже була, уже давно були потрібні принципово нові підходи до управління інформацією. Саме тому ринок вбирає сьогодні технологію Інтранет, як губка вбирає воду. Сучасна організація, що живе в умовах динамічного бізнесу, швидких і частих змін, переросла рамки паперової технології – те-

хнології, на якій більшість організацій власне й працюють, не дивлячись на велику кількість комп'ютерів.

У наявності конфлікт – паперова технологія не витримує нових інформаційних потреб сучасної організації, вона не адекватна її актуальним завданням. Необхідні свіжі ідеї й концепції. Ринок корпоративних інформаційних систем чекає їх. У концентрованому вигляді вони знаходять своє віддзеркалення в технології Інтранет.

Для нас важливі три ключові сторони Інтранет. По-перше, нові методи управління інформацією і їх вплив на бізнес-процеси в сучасній організації. По-друге, організаційно-методологічна й адміністративна сторона нової технології управління інформацією. По-третє, питання архітектури, системно-технічної інфраструктури і технологічних засобів побудови систем Інтранет.

Спочатку коротко торкнемося найістотнішої сторони – бізнесу. Що ж так привертає великі компанії до застосування технології Інтранет для побудови корпоративних інформаційних систем?

Бізнес і Інтранет

Вище вже говорилося, що інформація є ключовим чинником успішного бізнесу, взагалі успішного ведення справ. Навряд чи хто візьметься оспорювати цю тезу. Взагалі кажучи, Інтранет несе із собою нову філософію управління інформацією всередині організації. Зараз же ми звернемо увагу на економічні аспекти технології Інтранет.

Відзначимо перш за все, що впровадження технології Інтранет дає відчутний економічний ефект у діяльності організації. Зміни пов'язані насамперед із різким поліпшенням якості споживання інформації, що безпосередньо впливає на продуктивність праці співробітників організації. Для інформаційної системи ключовими стають нові поняття: публікація інформації, споживачі інформації, надання інформації. Результат застосування Інтранет – різке скорочення паперових архівів, легкість і простота публікації інформації, універсальний і природний доступ до інформації за допомогою навігаторів, істотне скорочення витрат на адміністрування додатків на робочих місцях користувачів, негайна актуалізація будь-яких змін в інформаційному сховищі організації, зсув акцентів від створення інформації до її ефективного споживання.

Ключовими якостями Інтранет, безпосередньо пов'язаними з економічними аспектами діяльності сучасної організації, є:

- простота й природність технології;
- низький ризик і швидка віддача інвестицій;
- інтеграційний і "каталітичний" характер технології;
- ефективне управління й комунікації в організації.

Простота й природність технології

Програма перегляду, яка розміщується на робочому місці користувачів (навігатор), Web-сервер, який виступає як інформаційний концентратор, і стандарти взаємодії між клієнтом і Web-сервером. Це практично все, що необхідне для побудови варіанту системи. На цій основі можна розширювати спектр функцій системи, додаючи такі сервіси, як пошук інформації, як колективна робота з єдиним масивом інформації, і ряд інших.

При створенні систем Інтранет відмічена ще одна унікальна якість нової технології, яка полягає в тому, що ускладнення системи, розширення сервісів, деталізація функцій не вимагає від користувача нарощування спеціальних знань. Він навчається роботі з інформацією один раз, а далі, користуючись у своїй повсякденній роботі засобами навігації інформаційним простором організації, він раз за разом виявляє нові можливості, що полегшують виконання його завдань, – але при цьому інструмент-то залишається старим, надійним і випробуваним! Зрозуміло, це психологічно виключно важливо. Людина починає по-іншому відноситься до роботи з інформацією – вона починає працювати швидше, ефективніше, бачить реальні результати, залучається до колективної роботи над колосальною цінністю, практично найважливішим, чим володіє організація – її інформаційним сховищем.

Більш того, в організації встановлюється розумна й підтримувана всіма співробітниками дисципліна роботи з інформацією. Інформація важлива в роботі – вона актуальна, достовірна, вона доступна – і доступна безперервно, у будь-який час, як тільки вона знадобиться. Близькість інформації до споживача, "інформація на кінчиках пальців" – ось у чому одна із причин колосального успіху технології Інтранет.

Низький ризик і швидка віддача інвестицій

Особливості впровадження Web-технології вельми нетипові для нової революційної технології. Мова йде про простоту і дуже невисоку вартість створення систем Інтранет. Вартість початкових вкладень виявляється дуже невеликою, при цьому концептуальна простота спрощує і впровадження.

Унікальність Web-технології полягає в тому, що вона дозволяє почати з малого, зробивши дуже невеликі попередні витрати. У них входить тільки вартість навігаторів і Web-сервера – оскільки організувати Web-сервер можна практично на будь-якій техніці, що вже є у розпорядженні організації. Далі можна послідовно розвивати й удосконалювати в рамках Web-сервера необхідні організації сервіси, рухатися в бажаному напрямі, на кожному маленькому кроці отримувати конкретні видимі результати, і коректувати курс, якщо які-небудь з сервісів реалізовані невірно, незручно, не в повному об'ємі і так далі

Одна з колосальних проблем традиційних інформаційних систем полягає в тому, що, починаючи сьогодні планувати появу систем, ми можемо чекати появу перших результатів рік-півтора. Необхідно протягом тривалого часу рухатися вибраним шляхом, щоб продемонструвати перші результати. При цьому завжди виникає багато питань, чи достатні швидко ми йдемо, чи відповідає наше просування графіку робіт і, найголовніше, чи той результат ми хочемо отримати. Адже ситуація в організації може змінитися, і завдання, які здавалися важливими рік тому, зараз могли втратити актуальність, зате на перший план могли вийти нові, про існування яких ми раніше й не підозрювали.

Істотною властивістю впровадження Інтранет є швидка віддача. Це не означає, що дуже швидко ми починаємо отримувати ВСІ результати. Чудес не буває. Але дуже швидко ми починаємо отримувати проміжні, проте негайно корисні й використовувані результати. Правильність вибраного шляху може бути перевірена нашим керівництвом або нами самими дуже швидко. Ухваливши рішення й почавши процес, через декілька тижнів, максимум через місяць, ми демонструємо перші результати. Користувачі дають свої зауваження, і вже через півтора місяці перші компоненти системи починають з'являтися в реальній експлуатації.

Це різко спрощує впровадження технології, оскільки користувач відразу бачить віддачу, бачить користь від впровадження технології, і тому охоче починає взаємодіяти з розробниками і допомагати у впровадженні системи. Психологічний ефект "швидко досяжних цілей", "участі в загальній справі" неможливо переоцінити. Більш того, мабуть, це і є єдиний реальний спосіб впровадження нових технологій при побудові інформаційної системи сучасної організації.

Інтеграційна технологія

Ця якість означає можливість ефективного об'єднання програмних рішень напрацьованих раніше, створюваних зараз і проектованих на основі різнорідного апаратного забезпечення в загальне інформаційне середовище з єдиними правилами створення й споживання інформації, з єдиним уніфікованим доступом до інформації.

На практиці Інтранет дозволяє створити інформаційну систему організації на основі вже існуючої технічної інфраструктури. Причина полягає як у максимально узагальненому підході Інтранет до споживання інформації, так і в максимально гнучких технічних методах і підходах, які лежать в основі Інтранет. Сила Web-технології – в еволюційному характері її впровадження, який дозволяє досягти практично стовідсоткового збереження зроблених раніше інвестицій. Усе складне й дороге господарство – мережі, комп'ютери, бази даних, прикладні системи – все зберігається і йде в справу.

При впровадженні Web-технології ніхто не говорить: "Ми допоможемо перейти з вашої старої системи на нову, у нас є хороший шлях". Такі розповіді багато хто чув, інші намагалися діяти за запропонованою схемою, і результат один – ніхто не хоче повторення. Колосальна перевага Інтранет у тому, що ті технології, які сьогодні існують і експлуатуються, комп'ютери, фактично вся інфраструктура не підлягає заміні. Її потрібно адаптувати, але адаптація не означає ні зміни платформи, ні якихось додаткових великих вкладень в інфраструктуру.

Фактично необхідні мінімальні додаткові інвестиції для того, щоб змусити раніше зроблені вкладення грати абсолютно нову роль. Можна отримати абсолютно новий рівень віддачі від існуючих вкладень, причому зробити це швидко і ефективно. Web-технологія грає роль своєрідного "каталізатора інвестицій".

Каталізатор інвестицій

Повільне повернення інвестицій в інформатизацію сучасної організації є однією із головних проблем, що стоять перед її керівництвом. За час існування в організації накопичується безліч комп'ютерів і програм, ефективному використанню яких перешкоджає складний за своєю природою (а тому повільний) цикл розробки й впровадження прикладного програмного забезпечення. Засоби, витрачені на придбання комп'ютерів і програм, часто лежать мертвим вантажем, не приносячи ніякої користі. Тривала відсутність результатів інформатизації приводить до того, що керівництво організації починає скептично відноситися до самої можливості створення інформаційної системи, що ефективно діє. Створюється в певному значенні тупикова ситуація, коли попередні вкладення (деколи величезні) в інформатизацію привели до дуже скромних результатів, а традиційні методи створення інформаційних систем очевидно себе вичерпали (зрозуміло, у рамках даної конкретної організації).

Природним і розумним вирішенням ситуації було б виключно швидке отримання конкретних результатів при дуже невеликих витратах. Якраз таку можливість надає технологія Інтранет. Будучи застосовною практично в будь-яких умовах, володіючи унікальною інтеграційною якістю, ця технологія при украй малих витратах і в гранично стислі терміни дозволяє отримати конкретний, видимий, ефективний для щоденної роботи організації результат, зрозумілий як для її керівництва, так і для рядових співробітників. Отриманий результат визначає загальний напрям розвитку й удосконалення інформаційної системи організації, зокрема, дозволяє систематизувати й упорядкувати подальші інвестиції в інформатизацію. Саме тому ми розглядаємо технологію Інтранет як каталізатор інвестицій, як вирішення проблеми, украй актуальної для вітчизняних організацій.

Ефективне управління організацією

Ця якість актуальна перш за все для керівника організації. Для нього інформаційна система представляє перш за все інструмент, що допомагає в ефективному управлінні очолюваної ним організації. Відомо, що ефективне управління вимагає, окрім інших умов, повного володіння в потрібний термін інформацією, що адекватно відображає стан організації.

Традиційні підходи до побудови інформаційних систем припускають створення додатків під назвою "автоматизоване робоче місце керівника", що реалізовують обмежений набір функцій управління документами, контролю виконання й так далі - тобто ставлять керівника організації у вельми жорсткі рамки. Як правило, такі застосування мають масу недоліків, вони складні, вельми незручні у використанні, вимагають навчання й реально на практиці керівниками не використовуються.

Причина неуспіху такого підходу – функціональна обмеженість і неприродний інтерфейс. Керівник сучасної організації – людина зайнята і вона не може витрачати час на освоєння складнощів роботи з тим або іншим застосуванням. З іншого боку, керівникові все ж таки необхідно мати адекватну і всеосяжну інформацію про діяльність організації, щоб у будь-який момент часу представляти, що ж все-таки в ній відбувається («тримати руку на пульсі»). Для вирішення цього завдання ідеально підходить технологія Інтранет. Не потрібно практично ніяких знань про специфіку роботи додатку, достатньо торкання курсором "миші" потрібних посилань і натиснення однієї кнопки.

У той же час спектр інформації, що надається керівникові, практично нічим не обмежений. Він не обмежений можливостями навігатора (оскільки навігатор лише "вікно" до інформації). Він ніяк не обмежений технічними можливостями Web-сервера. Уся інформація, що генерується в даній організації, може стати доступною для керівника (зрозуміло, у концентрованому й стислому вигляді). Для цього потрібно тільки правильно спроектувати і підготувати зміст інформаційного сервера.

Ефективні комунікації між співробітниками організації

Ключ до розуміння життєвості принципів Інтранет – це природність сприйняття співробітниками організації такого способу отримання інформації. Дані виходять саме в той момент, коли вони необхідні, у найзручнішому вигляді. Актуальна інформація завжди знаходиться "під рукою", нею можна скористатися в будь-який час, як тільки це буде потрібно. Люди дістають доступ до найціннішого, що має організація – її інформаційного сховища, вони працюють швидше й ефективніше. Не потрібно дзвонити по телефонах, бігати по кабінетах у пошуках документів, відволікати колег від роботи, чекати, поки те або інше розпорядження надійде у від-

діл – достатньо лише запустити навігатора й "перейти" за посиланням у необхідну точку інформаційного сховища.

Інтранет має властивість руйнувати комунікаційні бар'єри в організації. Відомо, що в будь-якій організації існує проблема: декілька співробітників, що сидять у різних кімнатах, і що працюють у вельми близьких напрямах і свідомо не приховують того, що вони роблять - і не підозрюючи про те, що колега поряд працює над тією ж проблемою, і потребує інформації, якою даний співробітник уже володіє. Керівництво організації всіляко прагне подолати це незнання, але існують комунікаційні бар'єри, які пов'язані зі структурою організації, зі способами її роботи, які приводять до того, що інформація розповсюджується дуже погано або поволі й із великими спотвореннями. Руйнування комунікаційних бар'єрів – це не просто позитивний гуманітарний або психологічний чинник. Це чинник реального бізнесу, що поза сумнівом впливає на ефективність роботи організації.

У цілому, Інтранет зачіпає величезні пласти в управлінні інформацією і в оптимізації бізнес-процесів в сучасній організації. Тут ми лише коротко зупинилися на найпривабливіших якостях Інтранет.

Перспективи систем Інтранет

На закінчення декілька слів про те, до чого сьогодні йде ця технологія. У цілому тенденції розвитку систем Інтранет такі:

- інтелектуальний мережевий пошук;
- висока інтерактивність навігаторів за рахунок застосування Java-технології;
- мережеві комп'ютери;
- перетворення інтерфейсу навігатора на універсальний інтерфейс із комп'ютером.

Як уже говорилося вище, щоб полегшити й спростити пошук інформації в системах Інтранет, необхідні інтелектуальні системи мережевого пошуку. Як правило, дані надходять із різних джерел, з різних комп'ютерів, розташованих у різних місцях мережі, і питання пошуку інформації за всіма цими джерелами надзвичайно актуальне.

Розвиток технології Java означає на практиці, що від статичних екранів, характерних для існуючої Web-технології, ми вже зараз переходимо до динамічних систем, коли на екрані ми отримуватимемо той інтерфейс і в тій динаміці, з якою ми звикли працювати на ПК.

Концепція універсального клієнта привела природним чином до появи такого засобу, як мережевий комп'ютер. Фактично це нова версія терміналу, комп'ютер, який забезпечуватиме доступ до інформаційної системи згідно невеликому набору стандартних протоколів, характерних для мережі Інтернет. На ньому виконуватиметься лише одна програма - програма-навігатор.

Комунікаційні утиліти для роботи в мережі

До складу операційної системи Windows включений ряд комунікаційних утиліт, які дозволяють визначити значення параметрів IP- конфігурації (ipconfig), перевірити працездатність з'єднання з віддаленим вузлом (ping), прослідкувати маршрут проходження пакетів до віддаленого вузла (tracert).

Для їх запуску достатньо перейти в режим командного рядка **Пуск-Программы-Стандартные-Командная строка** й ввести із клавіатури у відповідь на запрошення ім'я утиліти з відповідними параметрами.

Утиліта IPCONFIG

Утиліта ipconfig є одним з основних інструментів користувача, яка показує значення параметрів IP-конфігурації (звідси і її назва, рис. 2.4).

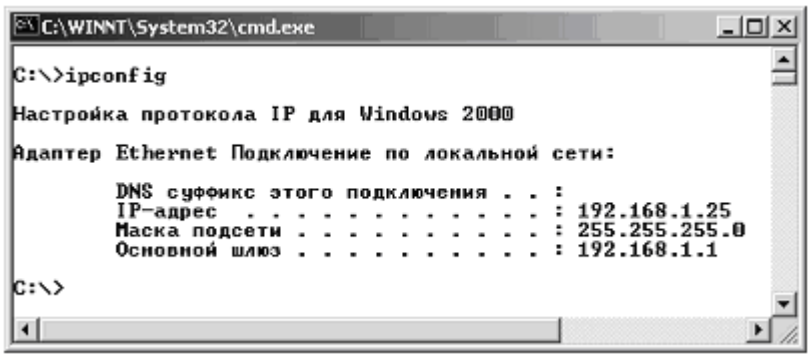


Рис. 2.4. Відомості про IP-конфігурацію, що відображаються утилітою ipconfig

У випадку виклику утиліти без додаткових ключів (Рис. 2.4) на екран виводяться:

- IP-адреса локального DNS-сервера (сервера імен);
- IP-адреса самого хоста й маска підмережі;
- IP-адреса сервера-шлюза до Internet.

До складу операційних систем Windows 95, Windows 98, Windows Millennium Edition поряд з утилітою ipconfig входить також її графічний аналог, який працює в стандартному вікні Windows, - winipcfg.

Windows 2000 та Windows XP не мають такого аналога, але в них для перегляду відомостей про IP-конфігурацію можна скористуватися іншою утилітою – "Сетевые подключения". Її запуск здійснюється за допомогою команди **Пуск-Программы-Стандартные-Связь-Сетевые подключения**. У вікні, що відкриється, треба клацнути правою кнопкою миші по з'єднанню, вибрати з контекстного меню команду **Состояние** й у вікні стану з'єднання перейти на вкладку **Поддержка**.

IP-адреси використовуються для ідентифікації комп'ютерів у мережі.

IP-адреса завжди має довжину 32 біти й складається із чотирьох частин, які називаються октетами (octet). Чотири частини об'єднуються в запис, у якому кожний октет відокремлюється крапкою, наприклад, 198.68.191.10.

За своєю структурою кожна 32-бітова IP-адреса ділиться на дві частини – префікс і суфікс, які складають дворівневу ієрархію. Префікс означає фізичну мережу, до якої підключений комп'ютер, а суфікс – окремий комп'ютер у цій мережі. Яка частина адреси відноситься до префікса, а яка до суфікса, визначається значеннями перших чотирьох бітів і відповідно до цього вони поділяються на три основних класи A, B і C. Для забезпечення максимальної гнучкості IP-адреси виділяються організаціям у залежності від кількості мереж і комп'ютерів в організації у відповідності із цими класами.

Мережі *класу A* належать найбільшим світовим постачальникам послуг Internet. Їх усього 126, а кожен із них може мати майже 17 мільйонів комп'ютерів.

Мережі *класу B* – мережі середнього масштабу. Їх може бути трохи більше 16 тисяч, а в кожній із них 65 534 хостів. Такі мережі мають найбільші університети та інші великі організації.

Мережі *класу C* – мережі дрібних постачальників, кількість яких може перевищувати 2 мільйони, а число комп'ютерів у кожній мережі – до 254. Саме до цього класу мереж відносяться мережі переважної більшості провайдерів Internet.

Якщо довільну IP-адресу символічно позначити як набір октетів w.x.y.z, то в узагальненому вигляді структуру IP-адрес для основних класів A, B і C можна представити у вигляді (табл. 2.3).

Таблиця 2.3

Структура IP-адрес у мережах класів A, B і C.

Клас мережі	Значення першого октету (w)	Октет номеру мережі	Октет номеру хосту	Кількість мереж	Кількість хостів в мережі
A	1-126	w	x.y.z	126	16 777 214
B	128-191	w.x	y.z	16 384	65 534
C	192-223	w.x.y	z	2 097 151	254

Наведена таблиця дозволяє за відомою IP-адресою комп'ютера швидко визначити клас мережі, її номер та номер комп'ютера в мережі. Наприклад, комп'ютер з IP-адресою 221.132.3.123 знаходиться в мережі класу C з ідентифікатором мережі 221.132.3 і має в цій мережі ідентифікатор 123.

Для того, щоб відділити префікс від суфікса в IP-адресі застосовується спеціальне 32-бітне число, яке називається маскою мережі. За своєю структурою маска представляє собою такий же набір із чотирьох октетів, що й звичайна IP-адреса. Нижче (табл. 2.4) наведені маски підмереж, які використовуються за замовчуванням для мереж класів A, B і C.

Таблиця 2.4

Значення масок підмереж (за замовчуванням)

Клас мережі	Значення маски
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Маски підмереж застосовується також для логічного поділу великих мереж на підмережі меншого масштабу.

Для зручності користувачів у Internet кожному комп'ютеру поряд з IP-адресою присвоюється власне символьне ім'я. Цю функцію в Internet виконує доменна служба імен – DNS (Domain Name System). Вона являє собою розподілену базу даних, у якій підтримується ієрархічна система символьних імен. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним іменем вузла.

База даних про відповідність символьних імен і IP- адрес не зберігається на кожному комп'ютері, а розподілена за великою кількістю DNS-серверів, що розташовані на різних вузлах Internet. Кожного разу, коли в прикладній програмі виникає необхідність перетворити ім'я в IP-адресу, вона стає клієнтом служби імен. Клієнт сервера DNS знає IP-адресу сервера DNS свого адміністративного домену, і направляє йому запит, у якому повідомляє відоме символьне ім'я, і просить повернути відповідну IP-адресу. Якщо дані про запитану відповідність вдається відшукати в базі даного DNS-сервера, то він відразу посилає відповідь клієнту. Якщо ж сервер DNS не може знайти відповіді на запит, він тимчасово стає клієнтом для іншого сервера DNS, а потім – наступного сервера імен і т.д., поки не знайде такий сервер, який зможе дати відповідь на запит.

Утиліта PING

Це службова програма, що перевіряє зв'язок із віддаленим комп'ютером. Для цього використовуються пакети відповіді-запиту й відповіді-відповіді спеціального протоколу міжмережевих керуючих повідомлень ICMP (Control Message Protocol).

Формат команди:

ping [-<Sw>] [<ім'я_кінцевого_комп'ютера>],

де -<Sw> - комбінація додаткових параметрів, призначення окремих з яких наведено нижче (Табл. 2.5), <ім'я_кінцевого_комп'ютера> - IP-адреса або доменне ім'я віддаленого хоста.

Таблиця 2.5

Призначення окремих параметрів команди ping.

Параметр	Призначення
-a	Повертає доменне ім'я хоста з вказаною IP-адресою.
-n *лічильник*	Задає число повідомлень, що відправляються з відлунням-запитом. За замовчуванням — 4.
-w *інтервал*	Визначає в мілісекундах час очікування повідомлення з відлунням-відповіддю у відповідь на повідомлення з відлунням-запитом. Якщо повідомлення з відлунням-відповіддю не отримано в межах заданого інтервалу, то видається повідомлення про помилку "Время ожидания запроса истекло". Інтервал за замовченням дорівнює 4000 (4 секунди).

За замовчуванням ping посилає на віддалений хост чотири повідомлення з відлуннямзапитом. У разі справності хоста після кожного передавання виводиться відповідне повідом-

лення з відлунням-відповіддю (рис. 2.5). Якщо ж хост не відповідає, то видається повідомлення з текстом про помилку "Время ожидания запроса истекло"(рис. 2.6).

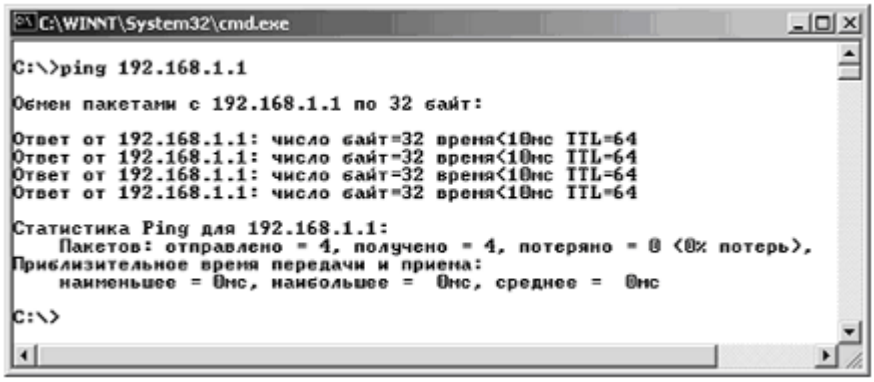


Рис. 2.5. Приклад відповіді від діючого хоста.

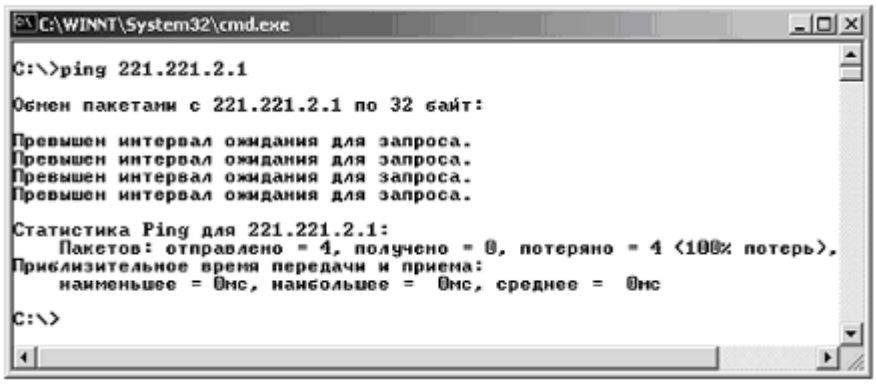


Рис. 2.6. Приклад відсутності відповіді від хосту.

Крім своєї основної функції – тестування з'єднання з віддаленим хостом, ping дозволяє перевірити правильність функціонування DNS-серверів: якщо деякий вузол "відгукується" на IP-адресу, але "не відгукується" на доменне ім'я, то або DNS-сервер непрацездатний, або він неправильно вказаний у конфігурації.

Утиліти IPCONFIG і PING

Для тестування з'єднання Microsoft рекомендує таку процедуру перевірки:

1) Запустіть утиліту ipconfig і визначте такі параметри, як IP-адреса локального комп'ютера (IP_adress_of_Local_host) і маска підмережі, адреса шлюзу за замовченням (IP_adress_of_default_gateway), адреса DNS- сервера (IP_adress_of_DNS_server). Якщо вказані співпадаючі IP-адреси, то маска підмережі буде вказана як 0.0.0.0.

2) Зверніться за IP-адресою "замикання на себе": ping 127.0.0.1.

3) Перевірте відгук власного комп'ютера: ping IP_adress_of_Local_host .

4) Запитайте відгук шлюзу за замовчуванням: ping IP_adress_of_default_gateway. Якщо команда не була успішно виконана, слід перевірити правильність IP-адреси основного шлюзу й працездатність цього шлюзу (маршрутизатора).

5) Зверніться за адресою віддаленого вузла: ping IP_adress_of_remote_host. Якщо команда не була успішно виконана, слід перевірити правильність IP-адреси віддаленого вузла, працездатність цього вузла, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і вилученим вузлом.

Зверніться за адресою DNS-сервера: ping IP_adress_of_DNS_server. Якщо команда не була успішно виконана, слід перевірити правильність IP-адреси DNS-сервера, працездатність DNS-сервера, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і DNS-сервером.

Утиліта TRACERT

Утиліта дозволяє прослідкувати маршрут проходження текстового пакета з даними до віддаленого вузла. З її допомогою можна визначити, на яких ланках маршруту затримка пакетів максимальна.

Шлях до точки призначення визначається за допомогою посилання в точку призначення відлуння-повідомлень протоколу ICMP. Виведений шлях – це список найближчих маршрутизаторів, що знаходяться на шляху між вузлом джерела й пунктом призначення.

Формат команди:

Tracert [-<Sw>] [<ім’я_кінцевого_комп’ютера>],

де -<Sw> - комбінація додаткових параметрів, призначення яких наведено нижче (табл. 2.6), <ім’я_кінцевого_комп’ютера> - IP-адреса або доменне ім’я віддаленого вузла.

Таблиця 2.6

Параметри команди tracert

Параметр	Призначення
-d	Забороняє визначення доменних імен проміжних маршрутизаторів, що збільшує швидкість виводу результатів.
-h *максимальне_число_переходів*	Задає максимальну кількість переходів при пошуку на шляху до кінцевого об'єкта. Значення за замовченням дорівнює 30.
-j *список_вузлів*	Вказує для повідомлень з відлуням-запитом використання параметра вільної маршрутизації в заголовку IP з набором проміжних місць призначення, зазначених у *списку_вузлів*. При вільній маршрутизації успішні проміжні місця призначення можуть бути розділені одним чи декількома маршрутизаторами. Максимальне число адрес чи і імен у списку — 9.
-w *інтервал*	Визначає в мілісекундах час очікування повідомлення відлуння-відповіді на повідомлення відлуння-запиту. Якщо повідомлення не отримане протягом заданого часу, виводиться зірочка (*). Таймаут за замовченням 4000 (4 секунди).

Приклад визначення маршруту слідування пакетів за допомогою команди tracert показаний нижче (рис. 2.7).

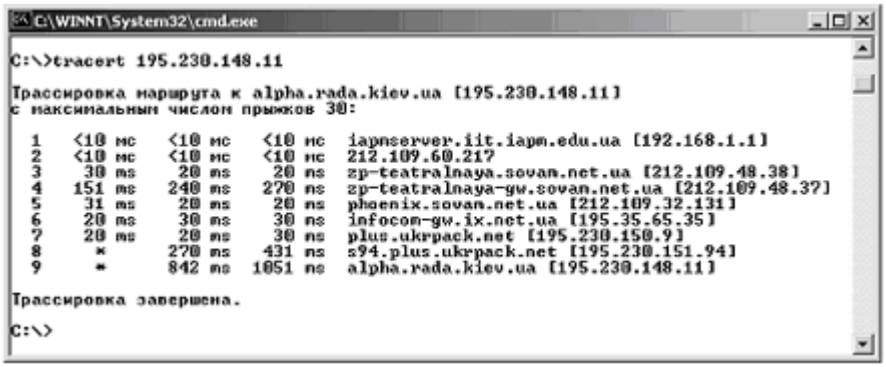


Рис. 2.7. Лістинг застосування утиліти tracert .

Деякі маршрутизатори не видимі для команди tracert. У цьому випадку перехід відображається рядом зірочок (*).

Спрощена методика ТСО

Спрощена методика теоретично-статистичного обрахунку (ТСО) витрат на інформаційні технології (ІТ) дає можливість порівнювати витрати на різних часових відрізках (наприклад, поточний рік і минулий, або поточний квартал і попередній), оцінюючи зміни. Найголовніше, що дає ця методика – розуміння структури витрат на ІТ, а отже, і можливостей скорочення цих витрат. Основний її недолік полягає в тому, що за нею неможливо порівнювати різні варіанти побудови системи.

Складові витрат

Прямі витрати можна отримати за даними бухгалтерії, визначивши загальні витрати на заробітну плату, закупівлю устаткування й програмного забезпечення. Також за даними бухгалтерії визначається сума амортизації, що нараховується, на основні фонди, що відносяться до інформаційних систем (ІС).

Непрямі витрати отримати завжди складніше. Фактично неможливо визначити, яку частину робочого часу користувачі витрачають на усунення збоїв або проблем на власних комп’ютерах або комп’ютерах колег, поки не змусити всіх у компанії вести деталізований лист обліку робочого часу (а його ведення – саме по собі завдання витратне за часом!). Для розраху-

нку багатьох статей непрямих витрат використовуються усереднені показники за галуззю, які надають і постійно оновлюють консалтингові компанії.

Статистична інформація

Перед початком збору детальної інформації необхідно знати три параметри.

1. *Кількість ПК в організації.* За відсутності хорошої системи обліку встаткування (яка є важливою частиною системи обліку основних засобів) достатньо складно виконати повний розрахунок, але дуже важливо зібрати інформацію акуратно. В облік потрібно брати тільки ті комп'ютери, які доступні кінцевим користувачам, і не включати комп'ютери, які використовуються як сервери. Указана кількість повинна включати й ноутбуки, які використовуються користувачами, а також усі робочі комп'ютери співробітників відділу IT.

2. *Кількість користувачів в організації.* Це може бути число, відмінне від попереднього, оскільки іноді користувачі мають декілька комп'ютерів, або декількома користувачами використовується один.

3. *Середня зарплата користувача.* Відповідь на це питання точно можна отримати за даними бухгалтерії. Середня цифра повинна розраховуватися за всім персоналом (виробничому й управлінському). Зовсім не обов'язково мати точні до копійки цифри, хоча підрахунок повинен бути максимально акуратним.

Прямі витрати на устаткування і програмне забезпечення

У вартість покупки встаткування й програмного забезпечення входять усі витрати, пов'язані із закупівлею клієнтських робочих місць, серверів, мережевого й периферійного встаткування, а також будь-якого пов'язаного із цим устаткуванням програмного забезпечення. Витрати на встаткування й ПЗ не включають витрати на оплату праці обслуговуючого персоналу. Дуже важливо, щоб у процесі накопичення такої інформації брали участь і служба закупівель, і бухгалтерія. Ідеальною була б ситуація, коли така інформація міститься в єдиній системі обліку й доступна співробітникам служби IT.

В *устаткування* включаються: настільні і переносні ПК; сервери; периферійні пристрої (принтери, сканери і ін.); оперативна пам'ять; пристрої зберігання інформації; пристрої CD-ROM; джерела безперебійного живлення; карти розширення всіх видів; мережеве комунікаційне устаткування (хаби, комутатори і т. д.); кабельна система.

У *програмне забезпечення* включаються: нове ПЗ і оновлення для всіх типів робочих станцій, серверів і телекомунікаційного встаткування; операційні системи; (текстові процесори, електронні таблиці й т. д.). Не включається ПЗ, розроблене самостійно – воно буде враховано далі.

Середні витрати на закупівлю встаткування в рік. Використання статистики за 12 минулих місяців дає хороший показник, проте, слід пам'ятати, що більшість компаній, що роблять великі закупівлі техніки, в основному розглядають такі закупівлі як капітальні вкладення, а не витрати поточного періоду (тоді вони враховуються в амортизації).

Середні витрати на ПЗ у рік. Використання витрат за останніх 12 місяців дає хороший показник. За аналогією з устаткуванням, капітальні витрати не включаються в цю вартість, а враховуються в амортизаційних відрахуваннях.

Щорічна сума амортизації капітальних вкладень в устаткування й ПЗ. Сума амортизації розраховується бухгалтерією для основних фондів і нематеріальних активів. В основному - за прискореним методом в розрахунку за три роки.

Деякі види основних засобів амортизуються за триваліші періоди.

Щорічні витрати на комплектуючі матеріали. Включають щорічні витрати на комплектуючі й витратні матеріали за всією організацією (дискети, CD, стрічки, тонер і картриджі).

Річні витрати на оренду встаткування й ПЗ. Сюди включаються всі витрати на оренду встаткування й програмного забезпечення.

Управління й персонал

Інформація про витрати на оплату праці повинна бути якомога точнішою й включати накладні витрати, премії, податки й інші платежі. Бажано отримувати інформацію з автоматизованих систем, у яких виконуються відповідні розрахунки.

Річні витрати на оплату персоналу за категоріями (включаючи керівництво). Якщо в організації є декілька офісів, усі вони повинні бути враховані. Якщо в інших службах, наприклад, відділі закупівель, є співробітники, які витрачають частину свого часу на роботу для слу-

жби IT, пропорційна частина з їх оплати повинна бути відбита у відповідній категорії цього розділу.

У конкретному випадку цей склад може змінюватися з урахуванням специфіки підприємства й вибиратися з наступного списку: служба технічної підтримки; мережеві адміністратори; системні адміністратори; тренери/фахівці з навчання; персонал служби закупівель; служба підтримки користувачів; управління системами.

Для обліку непередбачених витрат пропонується збільшувати витрати на 30%.

Витрати на відрядження за рік. Зазвичай співробітники служби IT не працюють на одному місці постійно, а виїжджають для виконання робіт в інші підрозділи.

Консультаційні послуги третіх фірм і інші пов'язані із цим витрати. У цю категорію потрапляють витрати, пов'язані з консалтинговими послугами, які використовуються для вирішення окремих завдань.

Витрати на завдання, делеговані іншим організаціям. Часто організація не реалізує всі завдання самостійно, а використовує ASP. В Україні це, наприклад, система Ліга, сервіси додатків електронної комерції, такі як 1Е (Банкомсвязь) і eDisty (Квазармікро).

Витрати на навчання персоналу питанням IT у рік. Витрати на внутрішнє навчання користувачів уже враховані і не включаються в цю категорію. Але якщо були витрати на навчання сторонніми організаціям – їх потрібно включити сюди.

Вартість обслуговування техніки за контрактами у рік. Якщо які-небудь роботи з обслуговування техніки доручаються стороннім організаціям, ці витрати повинні бути враховані в даному розділі. Якщо контракт на супровід був сплачений одного разу на декілька років уперед, то його потрібно враховувати в цьому розділі за частинами, як амортизацію капітальних вкладень.

Розвиток

Витрати на розвиток включатимуть щорічну оплату праці й витрат на виробництво й підтримку всіх застосувань. Існує дві великі групи додатків:

Бізнес додатки, які використовуються, головним чином, користувачами, ведучими основний бізнес компанії (додатки для бухгалтерського обліку, обробки рахунків, продажів, заробітної плати, складського обліку, управління персоналом).

Інфраструктурні застосування не впливають безпосередньо на бізнес, але використовуються для підтримки системної інфраструктури (додатки для управління системами, комунікаційне ПЗ, СУБД і комплекти програм для офісної діяльності).

Залежно від організації підрозділу розробки частина персоналу може відноситися до декількох категорій одночасно, тоді їх витрати повинні ділитися пропорційно часу їх роботи як кожна категорія.

Щорічні витрати на оплату праці за напрямами розробки. Інформація про оплату праці повинна бути гранично точною, такою, що містить повну суму компенсації, включаючи премії, податки й підвищення оплати протягом періоду розрахунку. Можна виділити чотири групи:

- проектування – персонал, залучений у збір вимог користувачів, визначення специфікацій, створення архітектури й прототипів проекту;
- розробка – персонал, залучений у створення кодів програм;
- тестування – персонал, що відповідає за якість і тестування;
- документація – персонал, залучений у контроль конфігурації й технічний опис додатків.

Щорічні витрати на заробітну плату за супроводом наявних систем. Ідентична категорії розробки "нових" застосувань і охоплює персонал, залучений в обслуговування існуючих застосувань.

Щорічні витрати на оплату послуг консультантів або сервісних організацій у частині розвитку. Ця категорія повинна включати будь-які оплати стороннім організаціям або приватним особам за проектування, розробку, тестування, або документування роботи в зв'язку з новими або існуючими проектами.

Зв'язок

Ця категорія охоплює всі річні витрати на голосові лінії зв'язку й лінії передавання даних, а також їх використання.

Щорічні витрати на оренду виділених ліній і каналів зв'язку. Сюди входять щомісячні витрати, що повторюються, на комутовані й виділені канали (наприклад, модемні 56k, ISDN, T1 і T3 потоки).

Щорічні витрати на віддалений доступ. Включає витрати на оплату віддаленого доступу до локальної мережі, витрати на Web-хостинг, платежі провайдерам Internet.

Річна вартість корпоративних мереж передавання даних. Включає будь-які витрати, пов'язані з користуванням мережами передавання даних на великі відстані (WAN).

Непрямі витрати

Сюди відносяться такі пов'язані з IT витрати, які не входять до бюджетів і не вимірюються більшістю відділів IT. Найвагомішою частиною зазвичай є супровід користувачем свого комп'ютера й ПЗ, а також допомогу колегам. Це включає самостійне налагодження систем при виникненні помилок, резервне копіювання й відновлення цінної інформації, операції з файлами й каталогами, позапланове навчання в робочий час і програмування малих (або великих) застосувань.

При спробі понизити прямі витрати багато організацій просто урізають IT бюджети, не розуміючи, що в результаті спостерігатиметься зростання непрямих витрат – користувачі витрачатимуть більше часу на підтримку себе, друзів і колег. Не існує точного способу зміряти, скільки часу користувач витратив на виконання завдань, пов'язаних з IT, без детального урахування часу або статистично вірних спостережень. Для тих, хто не має можливості і ресурсів проводити багатогодинні вимірювання, існують середні галузеві показники за кожною категорією.

Витрати користувача на IT

Кількість годин на самонавчання роботі з комп'ютером і ПЗ одного користувача. При ознайомленні нового користувача з корпоративною комп'ютерною системою витрачається час на його навчання. Аналогічно, коли нове застосування вводиться в організації, усі користувачі потребують тренінгу або знайомства із програмою. Ці й інші витрати на навчання включаються в цю категорію. Дослідження показують, що 40 годин у рік – достатньо обґрунтоване значення. Якщо необхідно, можна використовувати інше значення, ближче до реалій конкретного підприємства.

Кількість годин, що витрачаються одним користувачем на обслуговування файлів, комп'ютера й програм, написання скриптів і програм. Це найскладніше число для підрахунку без детального вивчення й спостереження. Дослідження показують, що 40 годин у рік - достатньо точне значення.

Простої за період

Кількість годин простою в місяць у зв'язку із плановими/позаплановими зупинками в роботі мережі/системи. Є показником річних втрат продуктивності, коли користувачі не можуть виконувати свою роботу унаслідок недоступності їх комп'ютерів або програм.

Причин може бути багато, наприклад, наступні:

- очікування вирішення проблеми службою підтримки;
- планована або позапланова зупинка системи;
- недоступність однієї або декількох програм;
- проблеми сервера, що приводять до недоступності інформації.

Середнє значення в даний час визначається як 2 години в місяць на користувача (якщо власна статистика дає інші цифри – можна використовувати їх).

Після того як на всі питання дана відповідь, розрахунок показує усереднену річну сукупну вартість володіння комп'ютером (для порівняння, у даний час середнє значення по США складає близько $10 000 на комп'ютер).

Контрольні питання

1. Поняття корпоративних мереж.
2. Що входить до корпоративних мереж?
3. Які функції єдиної інформаційної мережі підприємства?
4. Охарактеризуйте топології обчислювальних мереж.
5. Велика мережа з топологією типу «зірка»
6. В чому полягає сегментація мереж?
7. Яке устаткування забезпечує сегментацію мереж? Дайте його коротку характеристику.
8. Яке призначення утиліт ipconfig, ping, tracert?
9. Які дані виводяться на екран у випадку виклику утиліти ipconfig без додаткових ключів?

10. Які Ви знаєте графічні аналоги утиліти ipconfig?
11. Що таке IP-адреса? Поняття префіксу та суфіксу.
12. Яка структура IP-адрес у мережах класів A, B і C?
13. Яке значення масок підмереж?
14. Яке призначення доменної служби імен – DNS (Domain Name System)?
15. Яке призначення окремих параметрів команди ping?
16. Охарактеризуйте параметри команди tracert .
17. Охарактеризуйте використання пакетів IEEE 802.3.
18. Охарактеризуйте мережу стандарту IEEE 802.5 (Token Ring).
19. Охарактеризуйте оптично-волоконний розподілений інтерфейс FDDI.
20. Які Ви знаєте мережеві технології? Дайте коротку характеристику.
21. Охарактеризуйте порівняльні й техніко-економічні характеристики мережевих технологій.
22. Призначення концентраторів, повторювачів, мостів, шлюзів, маршрутизаторів, комутаторів, брандмауерів.
23. Охарактеризуйте модель STM.
24. Охарактеризуйте технологію Asynchronous Transfer Mode (ATM).
25. Охарактеризуйте технологію 100VG-AnyLAN.
26. Охарактеризуйте технологію Fast Ethernet.
27. Охарактеризуйте мережі Gigabit Ethernet.
28. Що тке система Intranet? Її призначення та характеристикию.
29. Охарактеризуйте срощену методику TCO.
30. Охарактеризуйте пистрої з’єднання та комутації мереж.

РОЗДІЛ 3
ГЛОБАЛЬНА МЕРЕЖА INTERNET

Internet – глобальна комп'ютерна мережа, що охоплює весь світ. Сьогодні Internet має близько 15 мільйонів абонентів в більш ніж 150 країнах світу. Щомісячно розмір мережі збільшується на 7-10%. Internet утворює начебто ядро, що забезпечує зв'язок різних інформаційних мереж, що належать різним установам у всьому світі.

Якщо раніше мережа використовувалася виключно як середовище передавання файлів і повідомлень електронної пошти, то сьогодні вирішуються складніші завдання розподіленого доступу до ресурсів.

Компанії спокушають швидкість, дешевий глобальний зв'язок, зручність для проведення спільних робіт, доступні програми, унікальна база даних мережі Internet. Вони розглядають глобальну мережу як доповнення до своїх власних локальних мереж.

Фактично Internet складається з безлічі локальних і глобальних мереж, що належать різним компаніям і підприємствам, зв'язаних між собою різними лініями зв'язку. Internet можна уявити собі у вигляді мозаїки складеної з невеликих мереж різної величини, які активно взаємодіють одна з іншою, пересилаючи файли, повідомлення і тому подібне.

При низькій вартості послуг (часто це тільки фіксована щомісячна плата за використовувані лінії або телефону) користувачі можуть дістати доступ до комерційних і некомерційних інформаційних служб США, Канади, Австралії і багатьох європейських країн. В архівах вільного доступу мережі Internet можна знайти інформацію практично з усіх сфер людської діяльності, починаючи з нових наукових відкриттів до прогнозу погоди на завтра.

Крім того, Internet надає унікальні можливості дешевого, надійного і конфіденційного глобального зв'язку зі всім світом. Це виявляється дуже зручним для фірм тих, що мають свої філії у всьому світі, транснаціональних корпорацій і структур управління. Зазвичай, використання інфраструктури Internet для міжнародного зв'язку обходиться значно дешевше за прямий комп'ютерний зв'язок через супутниковий канал або через телефон.

Електронна пошта – найпоширеніша послуга мережі Internet. У даний час свою адресу за електронною поштою мають приблизно 20 мільйонів чоловік. Надсилання листа електронною поштою обходиться значно дешевше за надсилання звичайного листа. Крім того, повідомлення, надіслане електронною поштою дійде до адресата за декілька годин, тоді як звичайний лист може добиратися до адресата декілька днів, а то і тижнів.

У даний час Internet відчуває період підйому, багато в чому завдяки активній підтримці з боку урядів європейських країн і США, яка дещо знизилась завдяки впливові сучасної світової економічної кризи. Щорічно в США виділяється близько 1-2 мільйонів доларів на створення нової мережевої інфраструктури. Дослідження в області мережевих комунікацій фінансуються також урядами Великобританії, Швеції, Фінляндії, Німеччини.

Проте, державне фінансування – лише невелика частина коштів, що надходять, оскільки все помітнішою стає "комерціалізація" мережі (80-90% засобів поступає з приватного сектора).

Історія мережі Internet

У 1961 році Defence Advanced Research Agency (DARPA) за завданням міністерства оборони США приступило до проекту зі створення експериментальної мережі передавання пакетів. Ця мережа, названа ARPANET, призначалася спочатку для вивчення методів забезпечення надійного зв'язку між комп'ютерами різних типів. Багато методів передавання даних через модеми було розроблено в ARPANET. Тоді ж були розроблені й протоколи передавання даних у мережі – TCP/IP. TCP/IP – це безліч комунікаційних протоколів, які визначають, як комп'ютери різних типів можуть спілкуватися між собою.

Експеримент із ARPANET був настільки успішний, що багато організацій захотіли увійти до неї, з метою використання для щоденного передавання даних. І в 1975 році ARPANET перетворилася з експериментальної мережі в робочу мережу. Відповідальність за адміністрування мережі узяло на себе Defence Communication Agency (DCA), в даний час зване Defence Information Systems Agency (DISA). Але розвиток ARPANET на цьому не зупинився. Протоколи TCP/IP продовжували розвиватися і удосконалюватися.

У 1983 році вийшов перший стандарт для протоколів TCP/IP, що увійшов в Military Standarts (MIL STD), тобто у військові стандарти, і всі, хто працював в мережі, зобов'язані були перейти до цих нових протоколів. Для полегшення цього переходу DARPA звернулася із пропозицією до керівників фірми Berkley Software Design упровадити протоколи TCP/IP в Berkeley (BSD) UNIX. Із цього й почався союз UNIX і TCP/IP.

Через деякий час TCP/IP був адаптований в звичайний, тобто в загальнодоступний стандарт, і термін Internet увійшов до загального вживання. У 1983 році з ARPANET виділилася MILNET, яка почала відноситися до Defence Data Network (DDN) міністерства оборони США. Термін Internet почав використовуватися для позначення єдиної мережі: MILNET плюс ARPANET. І хоча в 1991 році ARPANET припинила своє існування, мережа Internet існує, її розміри набагато перевищують первинні, оскільки вона об'єднала безліч мереж у всьому світі. (рис. 3.1) ілюструє зростання числа хостів, підключених до мережі Internet з 4 комп'ютерів в 1969 році до 8,3 мільйонів в 1994 році. *Хостом* у мережі Internet називаються комп'ютери, що працюють в багатозадачній операційній системі (Unix, VMS), підтримують протоколи TCP\IP і надають користувачам які-небудь мережеві послуги.

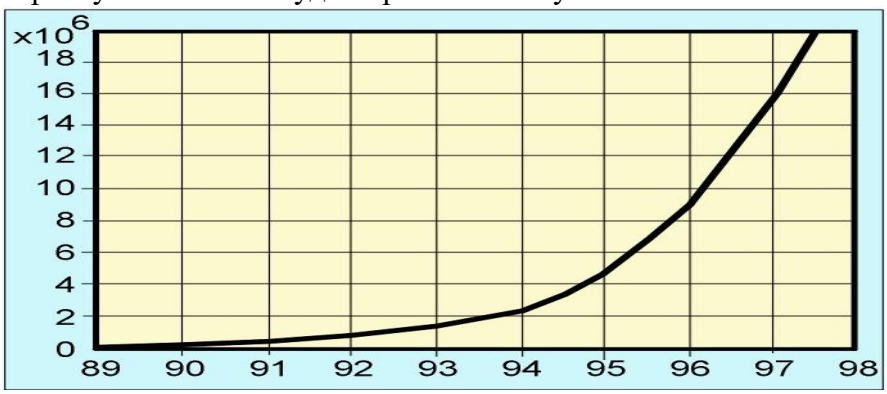


Рис. 3.1. Кількість хостів, підключених до Internet .

Протоколи мережі Internet

Основне, що відрізняє Internet від інших мереж – це її протоколи – TCP/IP. Взагалі, термін TCP/IP зазвичай означає все, що пов'язане з протоколами взаємодії між комп'ютерами в Internet. Він охоплює ціле сімейство протоколів, прикладні програми, і навіть саму мережу. TCP/IP – це технологія міжмережевої взаємодії, технологія internet. Мережа, яка використовує технологію internet, називається "internet". Якщо мова йде про глобальні мережі, що об'єднують безліч мереж з технологією internet, то її називають Internet.

Свою назву протокол TCP/IP отримав від двох комунікаційних протоколів (або протоколів зв'язку). Це Transmission Control Protocol (TCP) і Internet Protocol (IP). Не дивлячись на те, що в мережі Internet використовується велике число інших протоколів, мережу Internet часто називають TCP/IP-мережею, оскільки ці два протоколи, безумовно, є найважливішими.

Основні протоколи TCP/IP

Прикладний рівень: HTTP, DHCP, IRC, SNMP, DNS, NNTP, XMPP, SIP, BitTorrent, IPP, NTP, SNTP .

Транспортний рівень: TCP UDP, SCTP, DCCP, RTP, RUDP.

Мережевий рівень: IPv4 , IPv6, ARP, RARP, ICMP, IGMP.

Канальний рівень: Ethernet, 802.11 WiFi, Token ring, FDDI, PPP, HDLC, SLIP, ATM, DTM, X.25, Frame Relay, SMDS.

Фізичний рівень: Ethernet , RS-232, EIA-422, RS-449 , EIA-485.

Електронна пошта: SMTP.

Передавання файлів: FTP, TFTP, SFTP.

Віддалений доступ: rlogin, Telnet, SSH.

Рівень уявлення: XDR.

Як і у всякій іншій мережі в Internet існує 7 рівнів взаємодії між комп'ютерами: фізичний, логічний, мережевий, транспортний, рівень сеансів зв'язку, представницький і прикладний рівень. Відповідно кожному рівню взаємодії відповідає набір протоколів (тобто правил взаємодії).

Протоколи фізичного рівня визначають вигляд і характеристики ліній зв'язку між комп'ютерами. У Internet використовуються практично всі відомі в даний час способи зв'язку від простого дроту (скручена пара) до волоконно-оптичних ліній зв'язку (ВОЛЗ).

Для кожного типу ліній зв'язку розроблений відповідний протокол логічного рівня, що займається управлінням передаванням інформації каналом. До протоколів логічного рівня для телефонних ліній відносяться протоколи SLIP (Serial Line Interface Protocol) і PPP (Point to Point Protocol). Для зв'язку кабелем локальної мережі – це пакетні драйвери плат ЛОМ.

Протоколи мережевого рівня відповідають за передавання даних між пристроями в різних мережах, тобто займаються маршрутизацією пакетів в мережі. До протоколів мережевого рівня належать IP (Internet Protocol) і ARP (Address Resolution Protocol).

Протоколи транспортного рівня управляють передаванням даних з однієї програми в іншу. До протоколів транспортного рівня належать TCP (Transmission Control Protocol) і UDP (User Datagram Protocol).

Протоколи рівня сеансів зв'язку відповідають за встановлення, підтримку й знищення відповідних каналів. У Internet цим займаються вже згадані TCP і UDP протоколи, а також протокол UUCP (Unix to Unix Copy Protocol).

Протоколи представницького рівня займаються обслуговуванням прикладних програм. До програм представницького рівня належать програми, що запускаються, наприклад, на Unix-сервері, для надання різних послуг абонентам. До таких програм відносяться: telnet-сервер, FTP-сервер, Gopher-сервер, NFS-сервер, NNTP (Net News Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP2 і POP3 (Post Office Protocol) і так далі.

До протоколів прикладного рівня відносяться мережеві послуги й програми їх надання.

Послуги, які надаються мережею

Усі послуги, що надаються мережею Internet, можна умовно поділити на дві категорії: обмін інформацією між абонентами мережі й використання баз даних мережі.

До послуг зв'язку між абонентами належать:

Telnet – віддалений доступ. Дає можливість абонентові працювати на будь-якій ЕОМ мережі Internet як на своїй власній. Тобто запускати програми, змінювати режим роботи й так далі.

FTP (File Transfer Protocol) – протокол передавання файлів. Дає можливість абонентові обмінюватися двійковими й текстовими файлами з будь-яким комп'ютером мережі. Установивши зв'язок із віддаленим комп'ютером, користувач може скопіювати файл із віддаленого комп'ютера на свій, або скопіювати файл зі свого комп'ютера на віддалений.

NFS (Network File System) – розподілена файлова система. Дає можливість абонентові користуватися файловою системою віддаленого комп'ютера, як своєю власною.

Електронна пошта – обмін поштовими повідомленнями з будь-яким абонентом мережі Internet. Існує можливість відправлення як текстових, так і двійкових файлів. На розмір поштового повідомлення в мережі Internet накладається наступне обмеження – розмір поштового повідомлення не повинен перевищувати 64 Кб.

Новини – отримання мережевих новин, електронні дошки оголошень мережі та можливість розміщення інформації на дошки оголошень мережі. Електронні дошки оголошень мережі Internet формуються за тематиками. Користувач може на власний вибір підписатися на будь-які групи новин.

Rsh (Remote Shell) – віддалений доступ. Аналог Telnet, але працює тільки в тому випадку, якщо на віддаленому комп'ютері працює ОС UNIX.

Rexec (Remote Execution) – виконання однієї команди на віддаленій UNIX-машині.

Lpr – мережевий друк. Відправлення файлу на друк на віддаленому (мережевому) принтері.

Lpq – мережевий друк. Показує файли, що стоять у черзі на друк на мережевому принтері.

Ping – перевірка доступності віддаленої ЕОМ, що знаходиться в мережі.

Talk – дає можливість відкриття "розмови" із користувачем віддаленої ЕОМ. При цьому на екрані одночасно видно текст, що вводиться, і відповідь віддаленого користувача.

Iptunnel – надає можливість доступу до сервера ЛОМ NetWare, з яким немає безпосереднього зв'язку за ЛОМ, а є лише зв'язок за мережею Internet.

Whois – адресна книга мережі Internet. За запитом абонент може отримати інформацію про приналежність віддаленого комп'ютера, про користувачів.

Finger – отримання інформації про користувачів віддаленого комп'ютера.

Окрім вище перелічених послуг, мережа Internet надає також наступні специфічні послуги:

Webster – мережева версія тлумачного словника англійської мови.

Факс-сервіс – надає можливість користувачеві відправляти повідомлення за факсимільним зв'язком, користуючись факс-сервером мережі.

Електронний перекладач – проводить переклад тексту з однієї мови на іншу. Звернення до електронних перекладачів відбувається за допомогою електронної пошти.

Шлюзи – дають можливість абонентові відправляти повідомлення в мережі, що не працюють із протоколами TCP\IP (FidoNet, Goldnet, AT50).

До систем автоматизованого пошуку інформації в мережі Internet належать наступні системи.

Gopher – найпоширеніший засіб пошуку інформації в мережі Internet, що дозволяє знаходити інформацію за ключовими словами й фразами. Робота із системою Gopher нагадує проглядання змісту, при цьому користувачеві пропонується пройти крізь ряд вкладених меню й вибрати потрібну тему. У Internet в даний час понад 2000 Gopher-систем, частина з яких є вузькоспеціалізованою, а частина містить більш різносторонню інформацію.

Gopher дозволяє отримати інформацію без вказівки імен і адрес авторів, завдяки чому користувач не витрачає багато часу і нервів. Він просто повідомить систему Gopher, що саме йому потрібно, і система знаходить відповідні дані. Gopher-серверів понад дві тисячі, тому з їх допомогою не завжди просто знайти необхідну інформацію. У разі виниклих утруднень можна скористатися службою VERONICA. VERONICA здійснює пошук більш ніж в 500 системах Gopher, звільняючи користувача від необхідності проглядати їх уручну.

WAIS – ще потужніший засіб отримання інформації, ніж Gopher, оскільки він здійснює пошук ключових слів у всіх текстах документів. Запити посилаються в WAIS на спрощеній англійській мові. Це значно легше, ніж формулювати їх на мові алгебри логіки, і це робить WAIS привабливішою для користувачів-непрофесіоналів.

При роботі з WAIS користувачам не потрібно витрачати багато часу, щоб знайти необхідні їм матеріали.

У мережі Internet існує понад 200 WAIS-бібліотек. Але оскільки інформація представляється переважно співробітниками академічних організацій на добровільних засадах, велика частина матеріалів відноситься до області досліджень і комп'ютерних наук.

WWW – система для роботи з гіпертекстом. Потенційно вона є найбільш потужним засобом пошуку. Гіпертекст сполучає різні документи на основі заздалегідь заданого набору слів. Наприклад, коли в тексті зустрічається нове слово або поняття, система, що працює з гіпертекстом, дає можливість перейти до іншого документа, у якому це слово, або поняття, розглядається детальніше.

WWW часто використовується як інтерфейс до баз даних WAIS, але відсутність гіпертекстових зв'язків обмежує можливості WWW до простого перегляду.

Користувач зі свого боку може задіяти можливість WWW працювати з гіпертекстом для зв'язку між своїми даними і даними WAIS і WWW так, щоб власні записи користувача як би інтегрувалися в інформацію для загального доступу. Насправді цього, звичайно, не відбувається, але сприймається саме так.

Практично всі послуги мережі побудовані на принципі клієнт-сервер. *Сервером* у мережі Internet називається комп'ютер, здатний надавати клієнтам (у міру надходження від них запитів) деякі мережеві послуги. Взаємодія клієнт-сервер будується зазвичай, таким чином. Із приходом запитів від клієнтів сервер запускає різні програми надання мережевих послуг. У міру виконання запущених програм сервер відповідає на запити клієнтів.

Усе програмне забезпечення мережі також можна поділити на клієнтське й серверне. При цьому програмне забезпечення сервера займається наданням мережевих послуг, а клієнтське програмне забезпечення забезпечує передавання запитів серверу й отримання відповідей від нього.

Доменна система імен.

Цифрові адреси – і це стало зрозуміло дуже скоро – хороші при спілкуванні комп'ютерів, а для людей – імена. Незручно говорити, використовуючи цифрові адреси, і ще важче запам'ятовувати їх. Тому комп'ютерам в Internet привласнені імена. Усі прикладні програми Internet дозволяють використовувати імена систем замість числових адрес комп'ютерів.

Звичайно, використання імен має свої недоліки. По-перше, потрібно стежити, щоб одне й те ж ім'я не було випадково привласнене двом комп'ютерам. Крім того, необхідно забезпечити перетворення імен у числові адреси, адже імена хороші для людей, а комп'ютери все-таки віддають перевагу числам. Можливо вказати програмі ім'я, але в неї повинен бути спосіб пошуку цього імені й перетворення його в адресу.

На етапі становлення, коли Internet була маленькою спільністю, використовувати імена було легко. Центр мережевої інформації (NIC) створював спеціальну службу реєстрації. Користувач посилав заповнений бланк (звичайно, електронними засобами), і NIC вносив до свого списку імен і адрес. Цей файл, званий *hosts* (список вузлових комп'ютерів), регулярно розсилався на всі комп'ютери мережі. Як імена використовувалися прості слова, кожне з яких обов'язково було унікальним. Коли вказати ім'я, комп'ютер шукав його в цьому файлі й підставляв відповідну адресу.

Коли Internet розрослася, на жаль, розмір цього файлу теж збільшився. Почали виникати значні затримки при реєстрації імен, пошук унікальних імен ускладнився. Крім того, на розсилання цього великого файлу на всі вказані в ньому комп'ютери йшло багато мережевого часу. Стало очевидно, що такі темпи зростання вимагають наявності розподіленої інтерактивної системи. Ця система називається «доменною системою імен» (Domain Name System, DNS).

Структура доменної системи

Internet-адреси складаються із чотирьох чисел, кожне з яких не перевищує 256. При записі числа відділяються одне від іншого крапками, наприклад:

192.112.36.5

128.174.5.6

Доменна система імен є методом призначення імен шляхом покладання на різні групи користувачів відповідальності за підмножини імен. Кожен рівень у цій системі називається *доменом*. Домени відділяються один від одного крапками:

ux.cso.uiuc.edu

nic.ddn.mil

yoyodyne.com

В імені може бути будь-яка кількість доменів, але більше п'яти зустрічається рідко. Кожен подальший домен в імені (якщо дивитися зліва направо) більше попереднього. В імені **ux.cso.uiuc.edu** елемент **ux** – ім'я реального комп'ютера з IP-адресою. Ім'я цього комп'ютера створене групою **cso**, яка є не що інше, як відділ, у якому знаходиться цей комп'ютер. Відділ **cso** є відділом університету штату Іліонйс (**uiuc**). **uiuc** входить до національної групи учбових закладів (**edu**). Таким чином, домен **edu** включає всі комп'ютери учбових закладів США; домен **uiuc.edu –** всі комп'ютери університету штату Іліонйс і так далі.

Кожна група може створювати і змінювати всі імена, що знаходяться під її контролем. Якщо **uiuc** вирішить створити нову групу й назвати її **ncsa**, вона може ні в кого не питати дозволу. Усе, що потрібно зробити – це додати нове ім'я у свою частину усесвітньої бази даних, і рано чи пізно той, кому потрібно, дізнається про це ім'я (ncsa.**uius.edu)**. Аналогічним чином **cso** може купити новий комп'ютер, привласнити йому ім'я й включити в мережу, не питаючи ні в кого дозволу. Якщо всі групи, починаючи з **edu** і нижче, дотримуватимуть правил і забезпечуватимуть унікальність імен, то ніякі дві системи в Internet не матимуть однакового імені. У мережі можуть бути два комп'ютери з ім'ям fred**,** але лише за умови, що вони знаходяться в різних доменах (наприклад, fred.**cso.uiuc.edu і fred**.**ora.com)**.

Легко дізнатися звідки беруться домени й імена в організації типу університету або підприємства. Але звідки беруться домени «верхнього рівня» типу **edu**? Вони були створені, коли була винайдена доменна система. Спочатку було шість організаційних доменів вищого рівня (табл. 3.1).

Таблиця 3.1.

Первинні домени верхнього рівня.

Домен	Використання
com	Комерційні організації
edu	Учбові заклади (університети, середні школи і так далі)
gov	Урядові установи (окрім військових)
mil	Військові установи (армія, флот і так далі)
org	Інші організації
net	Мережеві ресурси

Коли Internet стала міжнародною мережею, виникла необхідність надати зарубіжним країнам можливість контролю за іменами систем, що знаходяться в них. Для цієї мети створений набір доменів, які складаються з двох букв і відповідають доменам вищого рівня для цих країн. Оскільки **ca** – код Канади, то комп'ютер на території Канади може мати таке ім'я:

hockey.guelph.ca

Загальне число кодів країн – 300; комп'ютерні мережі існують приблизно в 170 із них.

Остаточний план розширення системи привласнення імен ресурсів в Internet був нарешті оголошений комітетом IAHC (International Ad Hoc Committee). Згідно з новим рішенням, до доменів вищого рівня, що включають сьогодні **com, net, org,** додадуться:

- **firm** – для ділових ресурсів Мережі;
- **store** – для торгівлі;
- **web** – для організацій, що мають відношення до регулювання діяльності в WWW;
- **arts** – для ресурсів гуманітарної освіти;
- **rec –** ігри й розваги;
- **info** – надання інформаційних послуг;
- **nom** – для індивідуальних ресурсів, а також тих, хто шукає свої шляхи реалізації.

Насправді Internet не просто мережа – це структура, що об'єднує звичайні мережі. Internet – це «мережа мереж». Що включає Internet? Питання непросте. Відповідь на нього змінюється із часом. Спочатку відповідь була б достатньо проста: всі мережі, що використовують протокол IP, які кооперуються для формування єдиної мережі своїх користувачів. Це включало б різні відомчі мережі, безліч регіональних мереж, мережі учбових закладів і деякі зарубіжні мережі (за межами США).

Трохи пізніше привабливість Internet усвідомили і деякі не-IP-мережі. Вони захотіли надати її послуги своїм клієнтам і розробили методи підключення цих мереж (наприклад, Bitnet, DECnet і так далі) до Internet. Спочатку ці підключення, названі шлюзами, служили тільки для передавання електронної пошти. Проте, деякі з них розробили способи передавання і інших послуг. Чи є ці мережі частиною Internet? І так, і ні. Усе залежить від того, чи хочуть вони того самі.

Адміністративний устрій Internet

Internet за організацією багато в чому нагадує церкву. Це організація з повністю добровільною участю. Управляється вона чимось на зразок ради старійшин, проте, у Internet немає патріарха, президента або Папи. Складові мережі можуть мати своїх президентів або аналогічних вождів, але це зовсім інша справа; у Internet немає єдиної авторитарної фігури. Вища влада, де б Internet не була, залишається за ISOC (Internet Society). ISOC – товариство з добровільним членством. Його мета – сприяти глобальному обміну інформацією через Internet. Воно призначає раду старійшин, яка відповідає за технічну політику, підтримку і управління Internet. Рада старійшин є групою запрошених добровольців, званою IAB (Рада з архітектури Internet.). IAB

регулярно збирається, щоб «благословити» стандарти і розподілити ресурси, такі, наприклад, як адреси. Internet працює, оскільки є стандартні способи спілкування між комп'ютерами і прикладними програмами. Це дозволяє комп'ютерам різного типу зв'язуватися без особливих проблем. IAB відповідальна за стандарти; вона вирішує, коли стандарт необхідний і яким йому слід бути. Коли потрібний стандарт, рада розглядає проблему, приймає стандарт і за мережею оповіщає про нього світ. IAB також стежить за різними номерами (і іншими речами), які повинні залишатися унікальними. Наприклад, кожен комп'ютер в Internet має свою унікальну 32-розрядну двійкову адресу; ніякий інший комп'ютер не має такої ж. Як привласнюється ця адреси? IAB піклується про такого роду проблеми. Вона не привласнює адресу особисто, але розробляє правила, як ці адреси привласнювати.

Користувачі Internet висловлюють свої скарги і пропозиції на зустрічах IETF (Оперативного інженерного загону Internet). IETF – це інша добровільна організація; також збирається регулярно, щоб обговорити поточні експлуатаційні і назріваючі технічні проблеми. При обговоренні достатньо важливої проблеми IETF створює робочу групу для її подальшого дослідження. (На практиці важлива зазвичай означає, що для робочої групи знаходиться достатня кількість добровольців). Відвідувати зустрічі IETF і працювати в робочих групах можуть всі; головне, щоб люди працювали, справа-то добровільна. Робочі групи мають різні функції: це може бути випуск документації, вироблення стратегії дій при виникненні проблем, стратегічні дослідження, розробка нових стандартів і протоколів, доопрацювання тих, що вже існують (наприклад, зміна значень окремих полів). Робоча група зазвичай випускає доповідь. Залежно від виду рекомендації, це може бути просто документацією й бути доступною для будь-якого охочого, і може бути прийняте добровільно як здорова ідея, або ж це може бути послано в IAB і бути оголошено стандартом.

Якщо якась мережа приймає учення Internet, приєднується до неї і вважає себе її частиною, тоді вона і є частиною Internet. Можливо їй багато що здасться безрозсудним, дивним, сумнівним – вона може поділитися своїми сумнівами з IETF. Деякі скарги-пропозиції можуть виявитися цілком розумними і, можливо, Internet відповідно зміниться. Щось може показатися просто справою смаку або традиції, тоді ці заперечення будуть відхилені. Якщо мережа робить що-небудь, що може нашкодити Internet, вона може бути виключена із співтовариства до тих пір, поки вона не виправиться.

Зараз Internet складається із понад 15 тисяч об'єднаних між собою мереж.

Огляд рівнів мережі Internet.

Рівень 0 – пов'язаний із фізичним середовищем – передавачем сигналу й насправді не включається в цю схему, але дуже корисний для розуміння. Цей почесний рівень представляє посередників, що сполучають кінцеві пристрої: кабелі, радіолінії й так далі Кабелів існує велика кількість різних видів і типів: екрановані й неекрановані скручені пари, коаксіальні, на основі оптичних волокон і так далі Оскільки цей рівень не включений у схему, він нічого й не описує, тільки вказує на середовище.

Рівень 1 – фізичний. Включає фізичні аспекти передавання двійкової інформації за лініями зв'язку. Детально описує, наприклад, напругу, частоти, природу передавального середовища. Цьому рівню ставиться в обов'язок підтримка зв'язку й приймання-передавання бітового потоку.

Рівень 2 – канальний зв'язок даних. Забезпечує безпомилкове передавання блоків даних (званих кадрами (frame)) через рівень 1, який при передаванні може спотворювати дані. Цей рівень повинен визначати початок і кінець кадру в бітовому потоці, формувати з даних, що передаються фізичним рівнем, кадри або послідовності, включати процедуру перевірки наявності помилок і їх виправлення. Цей рівень (і лише він) оперує такими елементами, як бітові послідовності, методи кодування, маркери. Він несе відповідальність за правильне передавання даних (пакетів) на ділянках між безпосередньо зв'язаними елементами мережі. Забезпечує управління доступом до середовища передавання. Із-за його складності, канальний рівень підрозділяється на два підрівні: MAC (Medium Access Control) – управління доступом до середовища і LLC (Logical Link Control) – управління логічним зв'язком (каналом). Рівень MAC управляє доступом до мережі (з передаванням маркера в мережах Token Ring або розпізнаванням конфліктів (зіткнень передач) в мережах Ethernet) і управлінням мережею. Рівень LLC, що діє над рівнем MAC, і є власне той рівень, який посилає і отримує повідомлення з даними.

Рівень 3 – мережевий. Цей рівень використовує можливості, що надаються йому рівнем 2, для забезпечення зв'язку двох будь-яких, необов'язково суміжних, крапок у мережі. Цей рівень здійснює передавання повідомлень мережею, яка може мати багато ліній зв'язку, або безліччю спільно працюючих мереж, що вимагає маршрутизації, тобто визначення шляху, яким слід пересилати дані. Маршрутизація проводиться на цьому ж рівні. Виконує обробку адрес, а також і демультиплексування.

Основною функцією програмного забезпечення на цьому рівні є вибірка інформації із джерела, перетворення її в пакети й правильне передавання в місце призначення.

Є два принципово різних способи роботи мережевого рівня. Перший – це *метод віртуальних каналів*. Він полягає в тому, що канал зв'язку встановлюється при виклику (початку сеансу зв'язку), за ним передається інформація, і після закінчення передавання канал закривається (знищується). Передавання пакетів відбувається із збереженням початкової послідовності, навіть якщо пакети пересилаються за різними фізичними маршрутами, тобто віртуальний канал динамічно перенаправляється. При цьому пакети даних не включають адресу пункту призначення, оскільки вона визначається під час установлення зв'язку.

Другий – *метод дейтаграм*. Дейтаграми – незалежні, вони включають усю необхідну для їх пересилання інформацію. У той час, як перший метод надає наступному рівню (рівню 4) надійний канал передавання даних, що вільний від спотворень (помилок) і правильно доставляє пакети в пункт призначення, другий метод вимагає від наступного рівня роботи над помилками і перевірки доставки потрібному адресатові.

Рівень 4 – транспортний. Регламентує пересилання пакетів повідомлень між процесами, що виконуються на комп'ютерах мережі. Завершує організацію передавання даних: контролює потік даних, що проходить за маршрутом, визначеним третім рівнем: правильність передавання блоків даних, правильність доставки в потрібний пункт призначення, їх комплектність, збереження, порядок проходження. Збирає інформацію із блоків в її колишній вигляд. Або ж оперує з дейтаграмами, тобто чекає відгук-підтвердження прийому з пункту призначення, перевіряє правильність доставки і адресації, повторює надсилання дейтаграми, якщо не прийшов відгук. У рамках транспортного протоколу передбачено п'ять класів якості транспортування і відповідні процедури управління. Цей же рівень повинен включати розвинену й надійну схему адресації для забезпечення зв'язку через безліч мереж і шлюзів. Іншими словами, завданням даного рівня є забезпечити передавання інформації з будь-якої крапки в іншу у всій мережі.

Транспортний рівень приховує від усіх вищих рівнів будь-які деталі й проблеми передавання даних, забезпечує стандартну взаємодію нижчого рівня із прийманням-передавання інформації незалежно від конкретної технічної реалізації цього передаванн.

Рівень 5 – сеансовий. Координує взаємодію користувачів, що зв'язуються: установлює їх зв'язок, оперує ним, відновлює аварійно закінчені сеанси. Цей же рівень відповідальний за картографію мережі – він перетворює регіональні (доменні) комп'ютерні імена в числові адреси і навпаки. Він координує не комп'ютери й пристрої, а процеси в мережі, підтримує їх взаємодію – управляє сеансами зв'язку між процесами прикладного рівня.

Рівень 6 – рівень представлення даних. Цей рівень має справу з синтаксисом і семантикою інформації, що передається, тобто тут встановлюється взаєморозуміння двох комп'ютерів щодо того, як вони представляють і розуміють після отримання інформацію, яка передається. Тут вирішуються, наприклад, такі завдання, як перекодування текстової інформації і зображень, стискування і розпаковування, підтримка мережевих файлових систем (NFS), абстрактних структур даних і так далі.

Рівень 7 – прикладний. Забезпечує інтерфейс між користувачем і мережею, робить доступними для людини всілякі послуги. На цьому рівні реалізується, принаймні, п'ять прикладних служб: передавання файлів, віддалений термінальний доступ, електронне передавання повідомлень, служба довідника й управління мережею. У конкретній реалізації визначається користувачем (програмістом) згідно його потребам і можливостям його гаманця, інтелекту й фантазії. Має справу, наприклад, з безліччю різних протоколів термінального типу.

Слід розуміти, що переважна більшість сучасних мереж через історичні причини лише в загальних рисах, приблизно, відповідають еталонній моделі ISO OSI.

Пересилання бітів

Пересилання бітів відбувається на фізичному рівні схеми OSI. На жаль, тут усяка спроба короткого і доступного опису приречена на провал. Потрібне введення величезної кількості спеціальних термінів, понять, описів процесів на фізичному рівні і так далі. І потім, існує така велика різноманітність приймачів і передавальних середовищ, що важко навіть і оглянути цей океан технологій. Для розуміння роботи мереж цього й не потрібно. Вважайте, що просто є труба, за якою з кінця в кінець перекачуються біти. Саме біти, без жодного ділення на якінебудь групи (байти, декади і тому подібне).

Пересилання даних

Про організацію блокового, символьного передавання, забезпечення надійності пересилання поговоримо на інших рівнях моделі ISO OSI. Тобто функції канального рівня в Internet розподілені за іншими рівнями, але не вище транспортного. У цьому сенсі Internet не зовсім відповідає стандарту ISO. Тут канальний рівень займається тільки розбиттям бітового потоку на символи і кадри та передаванням отриманих даних на наступний рівень. Забезпеченням надійності передавання він себе не утруднює.

Мережі комутації пакетів

Настав час поговорити про Internet саме як про мережу, а не павутину ліній зв'язку і безліч приймачів. Здавалося б, Internet цілком аналогічна телефонній мережі, і модель телефонної мережі досить адекватно відображає її структуру і роботу. Насправді, обидві вони електронні, обидві дозволяють встановлювати зв'язок і передавати інформацію. І Internet теж складається, насамперед, з виділених телефонних ліній. Але, на жаль, картина ця невірна й приводить до багатьох помилок щодо роботи Internet, до безлічі непорозумінь. Телефонна мережа – це так звана мережа з *комутацією ліній*, тобто коли здійснюється виклик, встановлюється зв'язок і на весь час сеансу зв'язку є фізичне з'єднання з абонентом. При цьому виділяється частина мережі, яка для інших вже не доступна, навіть якщо мовчки дихаєте в трубку, а інші абоненти хотіли б поговорити у дійсно невідкладній справі. Це приводить до нераціонального використання дуже дорогих ресурсів – ліній мережі. Internet же є мережею з *комутацією пакетів*, що принципово відрізняється від мережі з комутацією каналів.

Для Internet більше підходить модель звичайної державної поштової служби. Пошта є мережею пакетного зв'язку. Немає ніякої виділеної частини цієї мережі. Ваше послання перемішується з посланнями інших користувачів, кидається в контейнер, пересилається в інше поштове відділення, де знову сортується. Хоча технології сильно різняться, пошта є прекрасним і наочним прикладом мережі з комутацією пакетів. Модель пошти дивно точно відображає суть роботи і структури Internet. (див. розділ 1, перемикання з'єднань).

Технології мережі Internet

TELNET

У теперішній час у багатьох, особливо у користувачів, що недавно підключилися до мережі, може виникнути враження, що Усесвітня павутина WWW, в яку вони заходять, використовуючи популярні програми, такі як Netscape Navigator або Microsoft Internet Explorer, – це і є Інтернет. Дійсно, значна частина інформаційних джерел мережі Інтернет доступна через WWW, проте у багатьох випадках все ж таки буває необхідне підключення до комп'ютерів, включених в мережу Інтернет, в режимі віддаленого терміналу, використовуючи один з базових і найстаріших інтернетівських протоколів – telnet.

Доступ за протоколом telnet означає, що комп'ютер на якийсь час стає терміналом віддаленої машини, таким чином, стає можливим виконувати на віддаленій машині такі дії, як редагування файлів, трансляцію, виконання прикладних програм і навіть системне адміністрування. Зрозуміло, для всього цього необхідно бути зареєстрованим користувачем цієї машини з відповідними повноваженнями, і мати уявлення про операційну систему цієї машини (переважна більшість машин, що допускають підключення в режимі віддаленого терміналу, працюють під управлінням тієї або іншої версії операційної системи UNIX). Крім того, в мережі до цих пір існує немало інформаційних джерел, доступ до яких організований тільки за протоколом telnet (в цьому випадку влаштовується гостьовий вхід, без реєстрації, але з обмеженими можливостями).

Слід розуміти, що в роботі за протоколом telnet, так само як і за іншими інтернетівськими протоколами, беруть участь 2 програми – клієнтська програма на тій машині, яка стає від-

даленим терміналом, і серверна, яка постійно працює на віддаленій машині у фоновому режимі або автоматично запускається за запитом на підключення. При цьому ПК повинен мати свою власну IP-адресу, тобто він повинен бути або підключена в режимі інфолінія або знаходитися в локальній мережі, підключеній до Internet.

Telnet – це програма, що дає можливість використовувати всі засоби Internet для зв'язку з базами даних, каталогами бібліотек та інших інформаційних ресурсів світу. Хочете довідатися погоду у Вермонті? Довідатися, як ростуть овочі в Азербайджану? Одержати додаткову інформацію про людину, чиє ім'я мигнуло в сеансі зв'язку? Усе це й багато чого іншого дозволить зробити Telnet.

На жаль, існує одне велике "але". На відміну від телефонної мережі, Internet не універсальний – не всі мають доступ до будь-яких його послуг. Майже всі коледжі й університети забезпечують доступ до telnet. Те ж вірно й у відношенні платних загальнодоступних систем. Але безкоштовні системи (Free-Net) не дають доступу до кожної системи telnet. А якщо працювати із загальнодоступною підсистемою UUCP або Usenet, то доступу до telnet у не буде. Основною причиною цього є ціна. Зв'язок з Internet легко може коштувати 1000 доларів США або більше при оренді високошвидкісної телефонної лінії. Проте доступ до деяких баз даних і бібліотек файлів можна одержати за електронною поштою; трохи пізніше ми покажемо, як це зробити.

Здебільшого підсистеми telnet прості у використанні й мають апарат оперативних підказок. Велика частина таких підсистем працює найкраще при емуляції термінала VT100. Один із прикладів – free-пакет NCSA Telnet для DOS або WinQVT для Windows.

Послуги, які надаються Telnet

1. Визначає мережевий віртуальний термінал (NVT – network virtual terminal), який забезпечує стандартний інтерфейс для віддаленої системи.
2. Включає механізм, який дозволяє клієнтові і серверу погоджувати опції обміну.
3. Забезпечує симетрію з'єднання, дозволяючи будь-якій програмі (наприклад, FTP) виступати в якості клієнта.

Протокол Telnet дозволяє обслуговуючій машині розглядати всі віддалені термінали як стандартні «мережеві віртуальні термінали» рядкового типу, що працюють в кодах ASCII, а також забезпечує можливість узгодження складніших функцій (наприклад, локальний або віддалений контроль, сторінковий режим, висота і ширина екрану і т. д.). На прикладному рівні над Telnet знаходиться або програма підтримки реального терміналу, або прикладний процес в обслуговуючій машині, до якого здійснюється доступ з терміналу. Формат NVT достатньо простий. Для даних використовуються 7-бітові коди ASCII. 8-бітові ж октети зарезервовані для командних послідовностей.

Утиліта Telnet взаємодіє з іншою ЕОМ через протокол Telnet. Якщо команда Telnet вводиться без аргументів, то ЕОМ переходить в командний режим, надрукувавши запрошення telnet>. У цьому режимі вона сприймає і виконує команди, описані нижче.

Встановлення зв'язку з віддаленим об'єктом

При введенні Telnet з аргументами програма здійснить зв'язок вашої ЕОМ з віддаленим комп'ютером, ім'я або адресу якого введено як одного з аргументів. Для встановлення з'єднання зазвичай потрібно ввести пароль, але він вводиться відкритим текстом, що робить процедуру потенційно небезпечною.

Після того, як Telnet зв'язок встановлений, починаються переговори про використання опції (табл. 3.2). Кожна з договірних сторін може послати інший один з чотирьох запитів will, do, wont і dont(табл. 3.3).

Далі Telnet переходить в режим введення. У цьому режимі будь-який введений текст пересилається віддаленій ЕОМ. Введення може проводитися посимвольно або порядково. При посимвольному режимі кожен введений символ пересилається негайно, при рядковому режимі відгук на кожне натиснення клавіші проводиться локально, а пересилка виконується лише при натисненні клавіші <Enter>. Деякі опції вимагають додаткових даних, така інформація може бути отримана за допомогою субопцій (RFC-1091). При цьому клієнт посилає трьохбайтову послідовність IAC WILL 24, де 24 – код-ідентифікатор терміналу. Одержувач може відгукнутися послідовністю IAC DO 24, якщо все гаразд. Сервер у свою чергу посилає послідовність IAC SB 24 1 IAC SE, запрошуючи тип терміналу клієнта. Тут код 24 означає, що це субопція для опції типу терміналу (табл. 3.2), а наступна опція 1 є командою «Пришліть код вашого терміналу».

Клієнт, у свою чергу, може відгукнутися, пославши послідовність – IAC SB 24 0 I B M P C IAC SE. Тут байт 0 має значення «Мій термінал має тип». Список кодів терміналів міститься в RFC-1700. Основні параметри Telnet наведені в табл.. 3.3-3.7.

Таблиця 3.2.

Коди опцій Telnet

Код опції в Telnet	Опис	Номер RFC
0	Двійковий обмін	856
1	Відлуння	857
2	Повторне з'єднання	NIC 15391
3	Придушення буферизації введення	858
4	Діалог про розмір повідомлення	NIC 15393
5	Статус	859
6	Тимчасова мітка	860
7	Віддалений доступ і відгук	726
8	Довжина вихідного рядка	nic 20196
9	Розмір вихідної сторінки	nic 20197
10	Режим виведення символів <повернення каретки>	652
11	Виведення горизонтальної табуляції	653
12	Установка положення табуляції при виводі	654
13	Режим виведення команди, зміни сторінки	655
14	Виведення вертикальної табуляції	656
15	Визначає положення вертикальної табуляції	657
16	Режим виведення символу <переклад рядка>	658
17	Розширений набір код ASCII	698
18	Повернення (logout)	727
19	Байт-макро	735
20	Термінал введення даних	732
21	Supdup	736
22	Supdup вивід	747
23	Місце відправлення	779
24	Тип терміналу	930
25	Кінець запису	885
26	Tacacs- ідентифікація користувача	927
27	Позначка виводу	933
28	Код положення терміналу	946
29	Режим 3270	1041
30	X.3 PAD	1053
31	Розмір вікна	1073

Коли зв'язок з віддаленою ЕОМ вже здійснений, перехід в командний режим може бути виконаний за допомогою натиснення клавіши (escape).

У цьому режимі доступні команди:

Табл. 3.3

Команди Telnet

Команда	Опис
open ім'я_ЕОМ [порт]	*open* відкриває зв'язок з ЕОМ, ім.'я якої вказане. Якщо номер порту явно не вказаний, telnet намагається використовувати для зв'язку з сервером номер порту за замовчуванням. Замість імені ЕОМ-сервера може використовуватися його IP-адреса
display [аргумент ...]	Відображає всі, або частину, набору параметрів telnet
close	Закриває сесію Telnet і повертає систему в командний режим
quit	Закриває будь-яку сесію Telnet
mode type	Управляє режимом введення («порядковий» або «посимвольний»). Віддаленій машині посилається запит на перехід у відповідний ре-

	жим. Якщо вона готова (здатна) працювати в потрібному режимі, буде проведено відповідне перемикання
status	Відображає поточний статус telnet. У перелік інформації входить ім'я віддаленої ЕОМ і режим обміну, що діє
? [команда]	Видає довідкову інформацію про команду, назва якої приведена як аргумент
send arguments	Посилає віддаленій ЕОМ один або декілька символьних аргументів. Як аргументи можуть використовуватися: escape, synch, brk, ip, ao, ayt, ecel, ga і ін.
escape	Посилає escape символ (наприклад, `^]')
SYNCH	Посилає synch-послідовність. Ця послідовність дозволяє анулювати все, що було до цього надруковано. Ця послідовність посилається як термінова (важлива) TCP-інформація (може не спрацювати, якщо віддаленою системою є 4.2 BSD). Якщо вона не спрацювала, на термінал буде посланий символ "r"
brk	Посилає Break-послідовність при натисненні клавіші Break (Pause). (Вичерпну інформацію про аргументи можна знайти в описі використовуваного програмного забезпечення або за допомогою команд Help або Man)
set argument value	Привласнює будь-якому числу змінних telnet нові значення. Спеціальне значення "off" вимикає функцію

Таблиця 3.4.

Змінні Telnet

Назва змінної	Призначення
Echo	Визначає, чи відображатиметься на екрані те, що вводиться з клавіатури. При значенні off введення не відображається, наприклад, при введенні пароля
Escape	Задає символ, який використовується як escape. Поява цього символу у вхідному потоці примушує його і подальші символи інтерпретуватися в ЕОМ, де функціонує процес Telnet, як команда
Interrupt	Специфікує символ переривання процесу. Введення його приводить до зупинки процесу користувача, що працює на віддаленій ЕОМ
Quit	Специфікує символ, який використовується користувачем на його клавіатурі, для виконання команд brake або attention
Flushoutput	Визначає символ, який служить для переривання процедури виводу на віддаленій ЕОМ
EOF	Специфікує символ, який використовується для позначення кінця файлу на віддаленій машині

Таблиця 3.5

Послідовності символів, які використовуються спільно з командою send

Послідовність символів	Призначення
?	Відображає довідкову інформацію про команду **send**
escape	Посилає символ escape (без переривання посилання символів для Telnet)
ip	Посилає протокольну послідовність Telnet. Віддалена машина повинна перервати запущений процес
ec	Посилає протокольну ЄС-послідовність Telnet. Віддалена ЕОМ повинна стерти останній надрукований символ
el	Посилає протокольну EL-послідовність Telnet. Віддалена ЕОМ по-

	винна стерти останній надрукований рядок
ao	Посилає протокольну AT-послідовність Telnet. Віддалена ЕОМ повинна направити весь вивід на термінал
brk	Посилає протокольну BRK-послідовність Telnet. Віддалена ЕОМ повинна забезпечити відгук
ayt	Посилає протокольну AYT-послідовність Telnet (Are You There). Віддалена ЕОМ повинна забезпечити відгук

У таблиці 3.6 представлені найменування і коди команд Telnet, які використовуються як клієнтом, так і сервером у поєднанні з префіксним байтом 0xff (IAC – «інтерпретувати як команду»). Якщо потрібно послати код даних, рівний 255, посилається два байти з кодами 255.

Таблиця 3.6.

Коди команд TELNET

Ім'я субкоманди TELNET	Код	Опис
EOF	236	Ознака кінця файлу
SUSP	237	Відкласти виконання поточного процесу
ABORT	238	Відмінити процес
EOR	239	Кінець запису
NOP	241	Ніяких дій
DM	242	Блок даних процедури SYNCH
BRK (Зупинка)	243	brk-символ (break);
IP (Переривання процесу)	244	IP-функція
io (Переривання виводу)	245	AT-функція
AYT (Ви тут?)	246	ayt-функція
ЄС (Стерти символ)	247	ЄС-функція
EL (Стерти рядок)	248	EL-функція
GA (Продовжуйте)	249	GA-функція
SB	250	Початок субопції
SE	240	Завершення узгодження параметрів (кінець субопції)
Will (буде)	251	Початок виконання (опційно)
Won't (не буде)	252	Відмова виконання або продовження виконання (опційно)
Do(виконати)	253	Відображає запит, який інша система виконує (опційно)
Don't (Немає)	254	Вимагає, щоб інша система зупинила виконання (опційно)
IAC	255	Інтерпретується як початок командної послідовності

У таб. 3.7 наведений список комбінацій клавіш, натиснення яких викликає певний результат.

Таблиця 3.7

Комбінації клавіш, що управляють

Комбінація клавіш	Результат, що досягається
Ctrl+E	Echo
Ctrl+]	Escape
Ctrl+?	Erase
Ctrl+O	flushoutput
Ctrl+C	Interrupt (переривання виконання програми)
Ctrl+U	Kill
Ctrl+	Quit
Ctrl+D	EOF

Гіпертекстова технологія WWW, URL, HTML

World Wide Web перекладається українською мовою як "всесвітня павутина". І, за суттю, це дійсно так. WWW є одним з найдосконаліших інструментів для роботи в глобальній світовій мережі Internet. Ця служба з'явилася порівняно недавно і все ще продовжує бурхливо розвиватися.

Початковим розробником технології WWW являється CERN, European Particle Physics Laboratory; але було б помилкою вважати, що Web є інструментом, розробленим фізиками і для фізиків. Плідність і привабливість ідей, покладених в основу проекту, перетворили WWW в систему світового масштабу, що надає інформацію чи не у всіх областях людської діяльності і охоплює приблизно 30 млн. користувачів в 83 країнах світу.

Головна відмінність WWW від решти інструментів для роботи з Internet полягає в тому, що WWW дозволяє працювати практично зі всіма доступними зараз на комп'ютері видами документів: це можуть бути текстові файли, ілюстрації, звукові і відео ролики, і так далі.

Що таке WWW? Це спроба організувати всю інформацію в Internet, плюс будь-яку локальну інформацію за вашим вибором, як набір гіпертекстових документів. Переміщення за мережею проводиться переходом від одного документа до іншого за посиланнями. Усі ці документи написані на спеціально розробленій для цього мові, яка називається HyperText Markup Language (HTML). Він чимось нагадує мову, що використовується для написання текстових документів, тільки HTML простіше. Причому можна використовувати не тільки інформацію, Internet, що надається, але і створювати власні документи. В останньому випадку існує ряд практичних рекомендацій до їх написання.

Уся користь гіпертексту полягає в створенні гіпертекстових документів: якщо зацікавив якийсь пункт у такому документі, то досить перемістити курсор для отримання потрібної інформації. Також в одному документі можливо робити посилання на інші, написані іншими авторами або навіть розташовані на іншому сервері.

Гіпермедіа – це надмножина гіпертексту. У гіпермедіа проводяться операції не тільки над текстом, але й над звуком, зображеннями, анімацією.

Існують WWW-сервери для Unix, Macintosh, MS Windows і VMS, більшість з них розповсюджуються вільно. Установивши WWW-сервер, можливо вирішити два завдання:

1. Надати інформацію зовнішнім споживачам – відомості про вашу фірму, каталоги продуктів і послуг, технічну або наукову інформацію.

2. Надати своїм співробітникам зручний доступ до внутрішніх інформаційних ресурсів організації. Це можуть бути останні розпорядження керівництва, внутрішній телефонний довідник, відповіді на питання, що часто ставляться, для користувачів прикладних систем – технічна документація й усе, що підкаже фантазія адміністратора й користувачів.

Інформація, яка надається користувачам WWW, оформлюється у вигляді файлів на мові HTML. HTML – проста мова розмітки, яка дозволяє позначати фрагменти тексту і задавати посилання на інші документи, виділяти заголовки декількох рівнів, розбивати текст на абзаци, центрувати їх і т. п., перетворюючи простий текст у відформатований гіпермедійний документ. Достатньо легко створити html-файл уручну, проте, є спеціалізовані редактори і перетворювачі файлів з інших форматів.

Для переглядання документів використовуються спеціальні переглядачі, такі як Netscape, Internet Explorer, lynx, www та інші. Mosaic і Netscape зручно використовувати на графічних терміналах. Для роботи на символьних терміналах можна порекомендувати Linux.

Архітектура WWW-технології

Від опису основних компонентів перейдемо до архітектури взаємодії програмного забезпечення в системі World Wide Web. WWW побудована за добре відомою схемою "клієнт-сервер". Програма-клієнт виконує функції інтерфейсу користувача й забезпечує доступ практично до всіх інформаційних ресурсів Internet. У цьому сенсі вона виходить за звичайні рамки роботи клієнта тільки з сервером певного протоколу, як це відбувається, наприклад, в telnet. Досить широко поширена думка, що Mosaic або Netscape, які є WWW-клієнтами, це просто графічний інтерфейс в Internet, є частково вірною. Проте, як вже було відмічено, базові компоненти WWW-технології (HTML і URL) відіграють при доступі до інших ресурсів Mosaic не останню роль, і тому мультипротокольні клієнти повинні бути віднесені саме до World Wide

Web, а не до інших інформаційних технологій Internet. Фактично, клієнт – це інтерпретатор HTML і, як типовий інтерпретатор, клієнт залежно від команд (розмітки) виконує різні функції.

В коло цих функцій входить не тільки розміщення тексту на екрані, але й обмін інформацією з сервером у міру аналізу отриманого HTML-тексту, що найнаочніше відбувається при відображенні вбудованих в текст графічних образів. При аналізі URL-специфікації або за командами сервера клієнт запускає додаткові зовнішні програми для роботи з документами у форматах, відмінних від HTML, наприклад GIF, JPEG, MPEG, Postscript і тому подібне. Взагалі кажучи, для запуску клієнтом програм незалежно від типу документа була розроблена програма Luncher, але останнім часом набагато більшого поширення набув механізм узгодження програм через MIME-типи. Іншу частину програмного комплексу WWW складає сервер протоколу HTTP, бази даних документів у форматі HTML, керовані сервером, і програмне забезпечення, розроблене в стандарті специфікації CGI. До останнього часу (до утворення Netscape) реально використовувалися два HTTP-сервера: сервер CERN і сервер NCSA. Але в даний час число базових серверів розширилося. З'явився дуже непоганий сервер для MS-Windows і Apachie-сервер для Unix-платформ. Існують й інші, але два останніх можна виділити з міркувань доступності використання. Сервер для Windows – це shareware, але без вбудованого самоліквідатора, як в Netscape. Другий сервер – це відповідь на загрозу комерціалізації. Netscape вже не поширює свій сервер Netsite вільно і пройшов слух, що NCSA-сервер також розповсюджуватиметься на комерційній основі. У результаті був розроблений Apachie, який за словами його авторів буде freeware, і реалізує нові доповнення до протоколу HTTP, пов'язані із захистом від несанкціонованого доступу, які запропоновані групою з розробки цього протоколу і реалізуються практично у всіх комерційних серверах.

База даних HTML-документів – це частина файлової системи, яка містить текстові файли у форматі HTML і пов'язану з ними графіку і інші ресурси. Особливу увагу хотілося б звернути на документи, що містять елементи екранних форм. Ці документи реально забезпечують доступ до зовнішнього програмного забезпечення.

Прикладне програмне забезпечення, що працює із сервером, можна розділити на програми-шлюзи та інші. Шлюзи – це програми, що забезпечують взаємодію сервера із серверами інших протоколів, наприклад, ftp, або з розподіленими на мережі серверами Oracle. Інші програми – це програми, що приймають дані від сервера і виконують які-небудь дії: отримання поточної дати, реалізацію графічних посилань, доступ до локальних баз даних або просто розрахунки.

Завершуючи обговорення архітектури World Wide Web хотілося б ще раз підкреслити, що її компоненти існують практично для всіх типів комп'ютерних платформ і вільно доступні в мережі. Будь-хто, хто має доступ в Internet, може створити свій WWW-сервер, або, принаймні, подивитися інформацію з інших серверів.

Основні компоненти технології World Wide Web

До 1989 року гіпертекст представляв нову, багатообіцяючу технологію, яка мала відносно велике число реалізацій, з одного боку, а з іншого боку, робилися спроби побудувати формальні моделі гіпертекстових систем, які носили швидше описовий характер і були навіяні успіхом реляційного підходу опису даних. Ідея Т. Бернерс-Лі полягала в тому, щоб застосувати гіпертекстову модель до інформаційних ресурсів, розподілених у мережі, і зробити це максимально простим способом. Він заклав три наріжні камені системи із чотирьох, що існують нині, розробивши:

- мову гіпертекстової розмітки документів HTML (HyperText Markup Lan-guage);
- універсальний спосіб адресації ресурсів у мережі URL (Universal Resource Locator);
- протокол обміну гіпертекстовою інформацією HTTP (HyperText Transfer Protocol).

Пізніше команда NCSA додала до цих трьом компонентам четвертий:

- універсальний інтерфейс шлюзів CGI (Common Gateway Interface).

Ідея HTML – приклад надзвичайно вдалого вирішення проблеми побудови гіпертекстової системи за допомогою спеціального засобу управління відображенням. На розробку мови гіпертекстової розмітки істотний вплив зробили два чинники: дослідження в області інтерфейсів гіпертекстових систем і бажання забезпечити простий і швидкий спосіб створення гіпертекстової бази даних, розподіленої на мережі.

У 1989 році активно обговорювалася проблема інтерфейсу гіпертекстових систем, тобто способів відображення гіпертекстової інформації й навігації в гіпертекстовій мережі. Значення гіпертекстової технології порівнювали зі значенням книгодрукування. Стверджувалося, що лист паперу й комп'ютерні засоби відображення серйозно відрізняються один від одного, і тому форма представлення інформації теж повинна відрізнятися. Найефективнішою формою організації гіпертексту були визнані контекстні гіпертекстові посилання, а крім того, було визнано ділення на посилання, що асоціюються зі всім документом у цілому й окремими його частинами.

Найпростішим способом створення будь-якого документа є його створення в текстовому редакторові. Досвід створення добре розмічених для подальшого відображення документів в CERN'і був – важко знайти фізика, який не користувався б системою TEX або LaTeX. Крім того, на той час існував стандарт мови розмітки – Standard Generalised Markup Language (SGML).

Слід також взяти до уваги, що згідно своїм пропозиціям Бернерс-Лі припускав об'єднати в єдину систему наявні інформаційні ресурси CERN, і першими демонстраційними системами повинні були стати системи для NEXT і VAX/VMS.

Зазвичай гіпертекстові системи мають спеціальні програмні засоби побудови гіпертекстових зв'язків. Самі гіпертекстові посилання зберігаються в спеціальних форматах або навіть складають спеціальні файли. Такий підхід хороший для локальної системи, але не для розподіленої на безліч різних комп'ютерних платформ. У HTML гіпертекстові посилання вбудовані в тіло документа і зберігаються як його частина. Часто в системах застосовують спеціальні формати зберігання даних для підвищення ефективності доступу. У WWW документи – це звичайні файли ASCII, які можна підготувати в будь-якому текстовому редакторові. Таким чином, проблема створення гіпертекстової бази даних була вирішена надзвичайно просто.

Базою для розробки мови гіпертекстової розмітки була вибрана мова SGML (Standard Generalised Markup Language). Слідуючи академічним традиціям, Бернерс-Лі описав HTML в термінах SGML (які описують мову програмування в термінах форми Бекуса-Наура). Природно, що в HTML були реалізовані всі розмітки, пов'язані з виділенням параграфів, шрифтів, стилів і т. п., оскільки реалізація для NEXT мала на увазі графічний інтерфейс. Важливим компонентом мови став опис вбудованих і асоційованих гіпертекстових посилань, вбудованої графіки і забезпечення можливості пошуку за ключовими словами.

З моменту розробки першої версії мови (HTML 1.0) відбувся досить серйозний розвиток мови. Майже вдвічі збільшилося число елементів розмітки, оформлення документів все більше наближається до оформлення якісних друкарських видань, розвиваються засоби опису не текстових інформаційних ресурсів і способи взаємодії з прикладним програмним забезпеченням. Удосконалюється механізм розробки типових стилів. Фактично, у даний час HTML розвивається у бік створення стандартної мови розробки інтерфейсів як локальних, так і розподілених систем.

Другим наріжним каменем WWW стала універсальна форма адресації інформаційних ресурсів. Universal Resource Identification (URI) є досить стрункою системою, що враховує досвід адресації і ідентифікації e-mail, Gopher, WAIS, telnet, ftp і тому подібне Але реально зі всього, що описане в URI, для організації баз даних в WWW потрібний тільки Universal Resource Locator (URL). Без наявності цієї специфікації вся потужність HTML виявилася б даремною. URL використовується в гіпертекстових посиланнях і забезпечує доступ до розподілених ресурсів мережі. У URL можна адресувати як інші гіпертекстові документи формату HTML, так і, наприклад, ресурси e-mail, telnet, ftp, Gopher, WAIS. Різні інтерфейсні програми по-різному здійснюють доступ до цих ресурсів. Одні, як, наприклад, Netscape, самі здатні підтримувати взаємодію за протоколами, відмінними від базового для WWW протоколу HTTP, інші, як наприклад Chimera, викликають для цієї мети зовнішні програми. Проте, навіть в першому випадку, базовою формою представлення інформації, що відображається, є HTML, а посилання на інші ресурси мають форму URL. Слід зазначити, що програми обробки електронної пошти у форматі MIME також мають можливість відображати документи, представлені у форматі HTML. Для цієї мети в MIME зарезервований тип "text/html".

Третім у нашому списку слідує протокол обміну даними в World Wide Web – HyperText Transfer Protocol. Даний протокол призначений для обміну гіпертекстовими документами й зважає на специфіку такого обміну. Так, у процесі взаємодії клієнт може отримати нову адре-

су ресурсу на мережі (relocation), запитати вбудовану графіку, прийняти і передати параметри і т.п. Управління в HTTP реалізоване у вигляді ASCII-команд. Реально розробник гіпертекстової бази даних працює з елементами протоколу тільки при використанні зовнішніх розрахункових програм або при здійсненні доступу до зовнішніх відносно WWW інформаційних ресурсів, наприклад, баз даних.

Остання складова технології WWW – це вже плід роботи групи NCSA – специфікація Common Gateway Interface. CGI була спеціально розроблена для розширення можливостей WWW за рахунок підключення різного зовнішнього програмного забезпечення. Такий підхід логічно продовжував принцип публічності й простоти розробки й нарощування можливостей WWW. Якщо команда CERN запропонувала простий і швидкий спосіб розробки баз даних, то NCSA розвинула цей принцип на розробку програмних засобів. Треба відмітити, що в загальнодоступній бібліотеці CERN були модулі, що дозволяють підключати свої програми до сервера HTTP, але це вимагало використання цієї бібліотеки. Запропонований і описаний в CGI спосіб підключення не вимагав додаткових бібліотек і буквально приголомшував своєю простотою. Сервер взаємодіяв із програмами через стандартні потоки введення/виводу, що значно спрощує програмування. При реалізації CGI надзвичайно важливе місце зайняли методи доступу, описані в HTTP. І хоча реально використовуються тільки два з них (GET і POST), досвід розвитку HTML показує, що співтовариство WWW чекає розвитку і CGI у міру ускладнення завдань, в яких використовуватиметься WWW-технологія.

Налагодження параметрів підключення до Internet

Налагодження параметрів підключення до Internet, у тому числі через локальну мережу, в операційній системі Windows XP проводиться за допомогою майстра, який викликається з панелі управління (рис. 3.2).

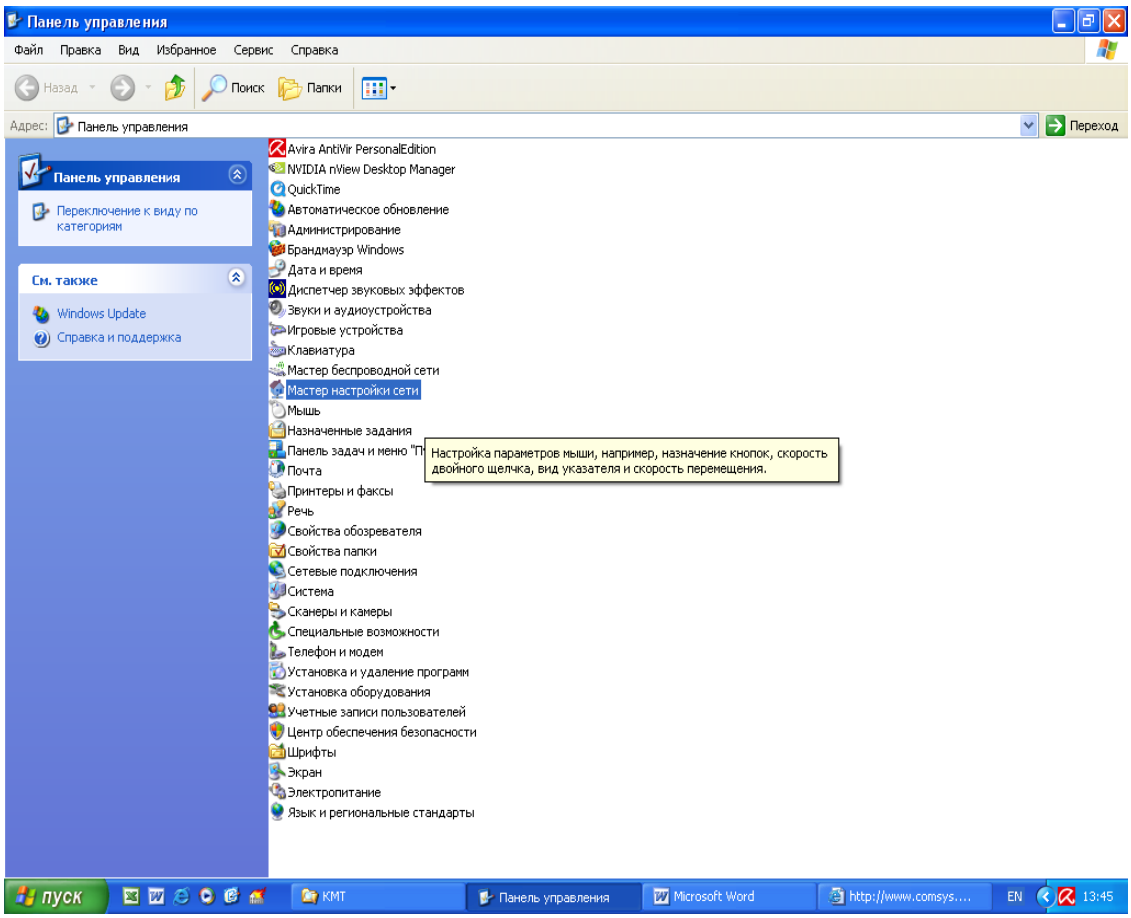


Рис. 3.2. Панель управління

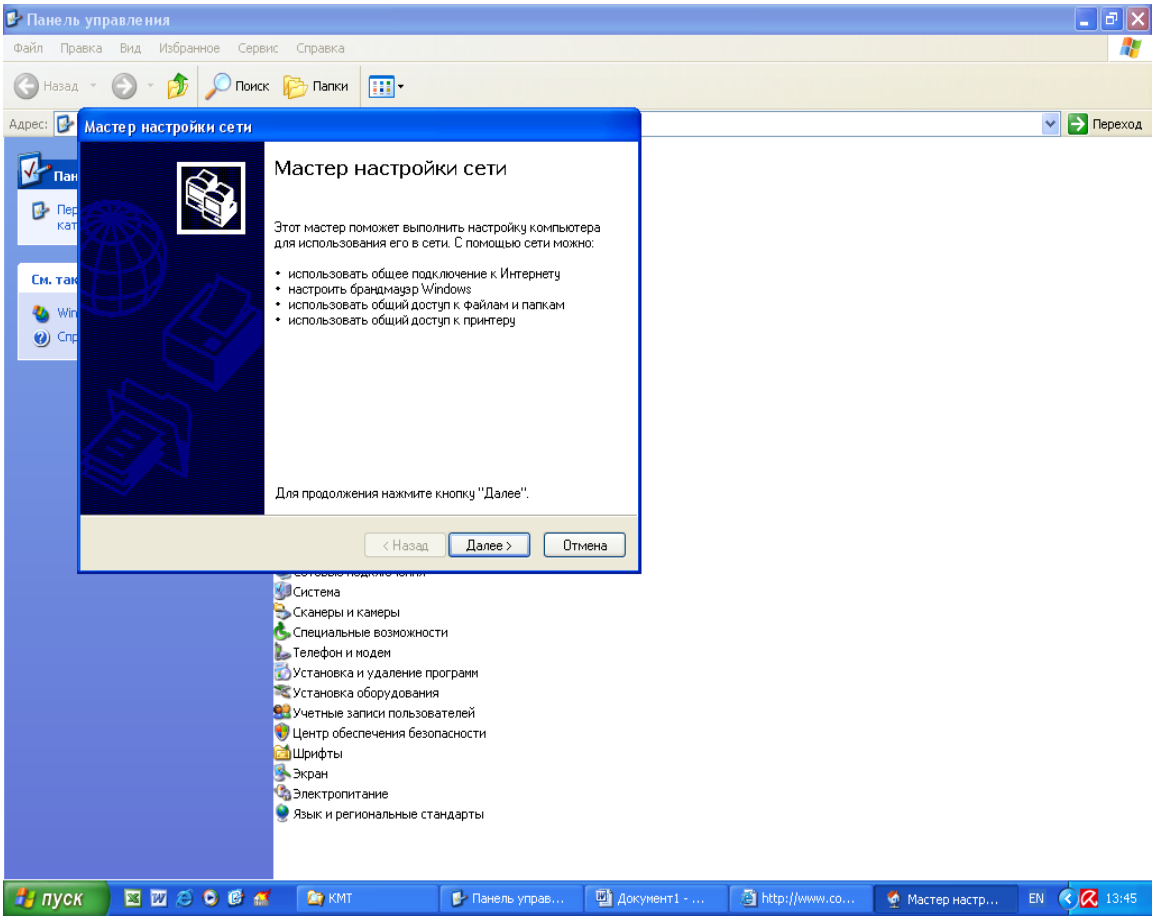


Рис. 3.3. Вікно майстра

В подальшому за допомогою майстра (рис. 3.3) за декілька кроків відбираються параметри підключення до мережі та після їх відбору подається команда **Далее**. Майстер надає довідку про дії, які треба виконувати (рис. 3.4). На рис. 3.5 відбираються параметри підключення до Internet через локальну мережу чи безпосередньо через модем; рис. 3.6 – задається опис та ім'я комп'ютера; рис. 3.7 – задається робоча група, в якій буде знаходитися комп'ютер; рис 3.8 – задається чи забороняється доступ до файлів та каталогів; рис. 3.9 – майстер проводить перевірку заданих параметрів; рис. 3.10 - майстер проводить встановлення параметрів мережі; рис. 3.11, 3.12 – можливе створення копії установки для інших комп'ютерів мережі та завершення роботи майстра. Налагодження параметрів при підключенні через модем показано на рис 3.13-3.18.

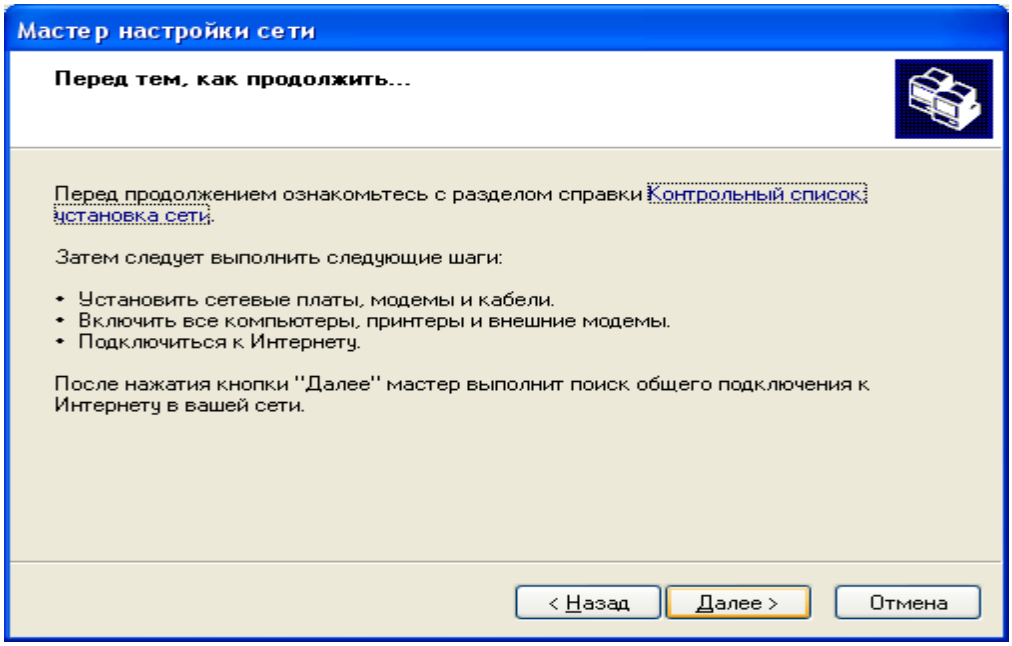


Рис. 3.4. Вікно довідки та попереднього відбору параметрів.

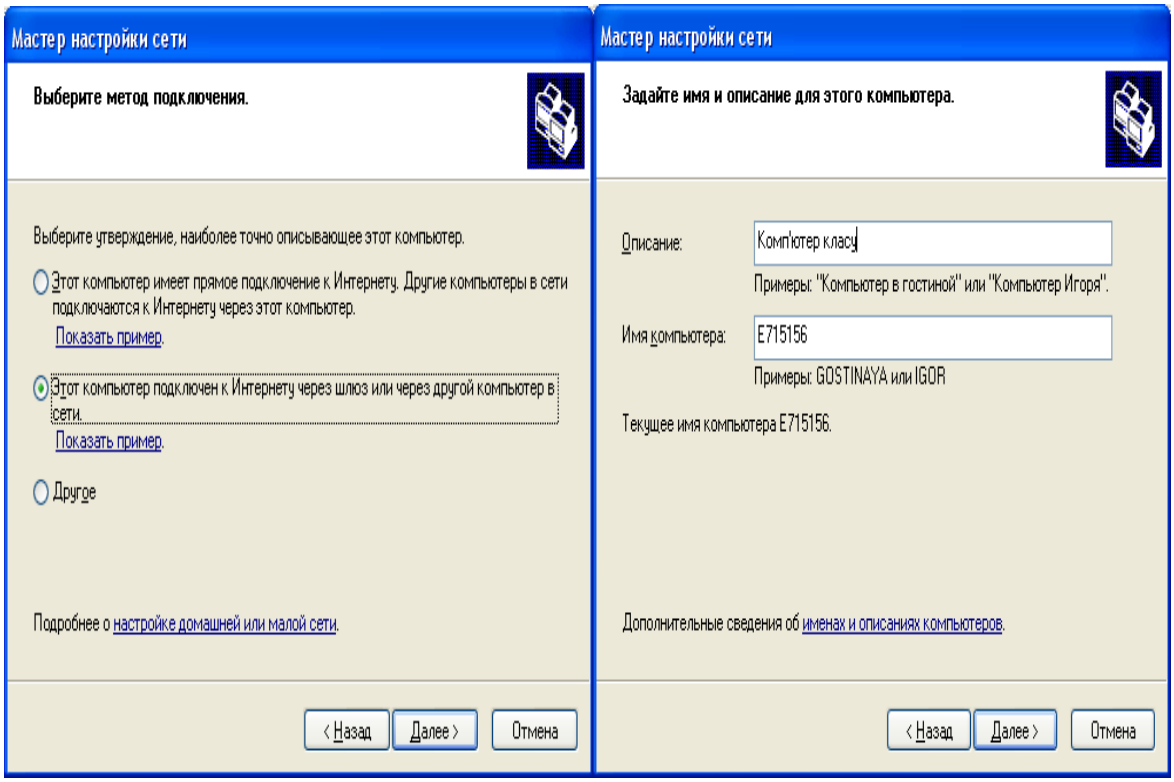


Рис. 3.5. Підключення до Internet через локальну мережу чи модем.

Рис. 3.6. Задання опису та імені комп'ютера

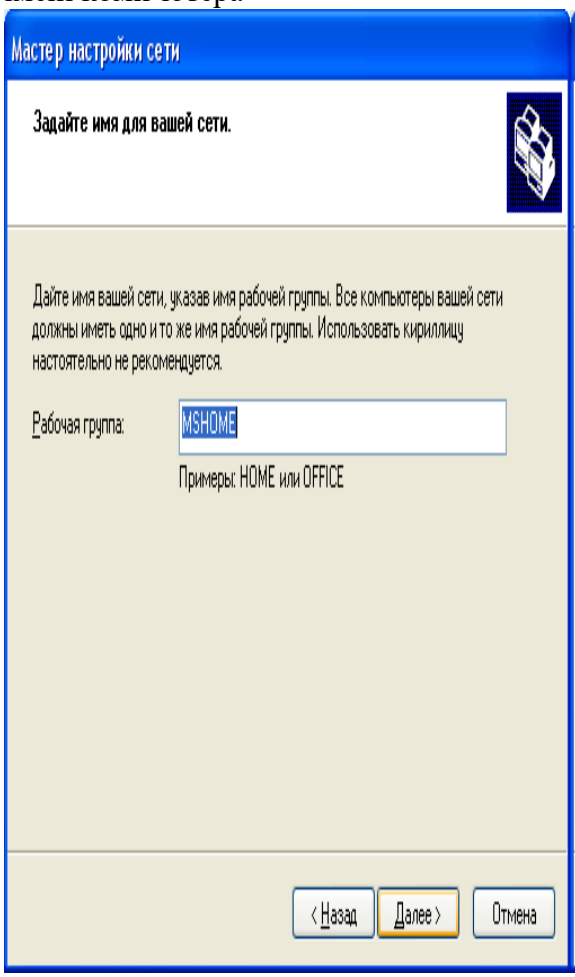


Рис. 3.7. Задання робочої групи

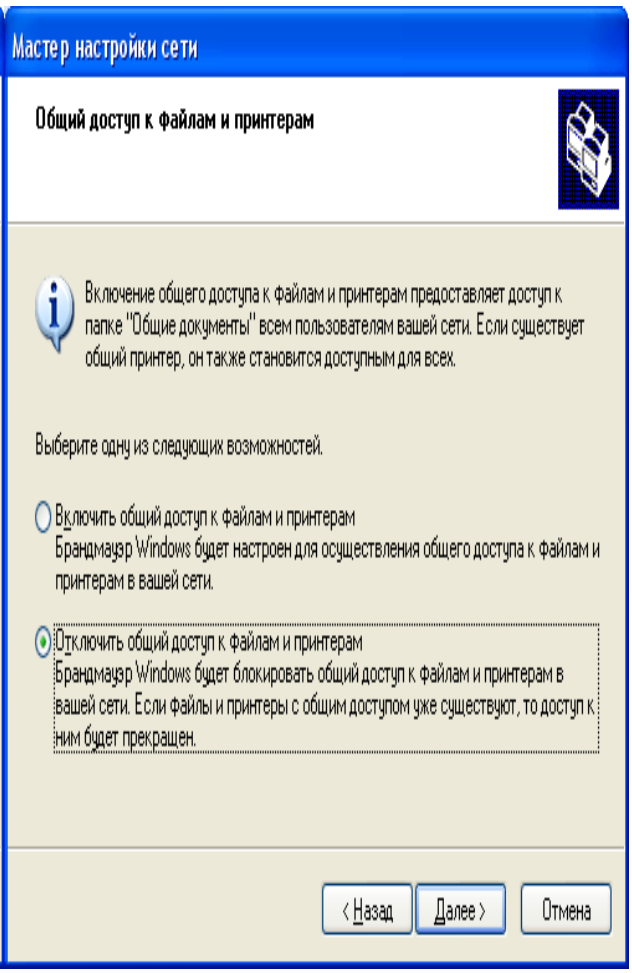


Рис. 3.8. Задання доступу до файлів та каталогів

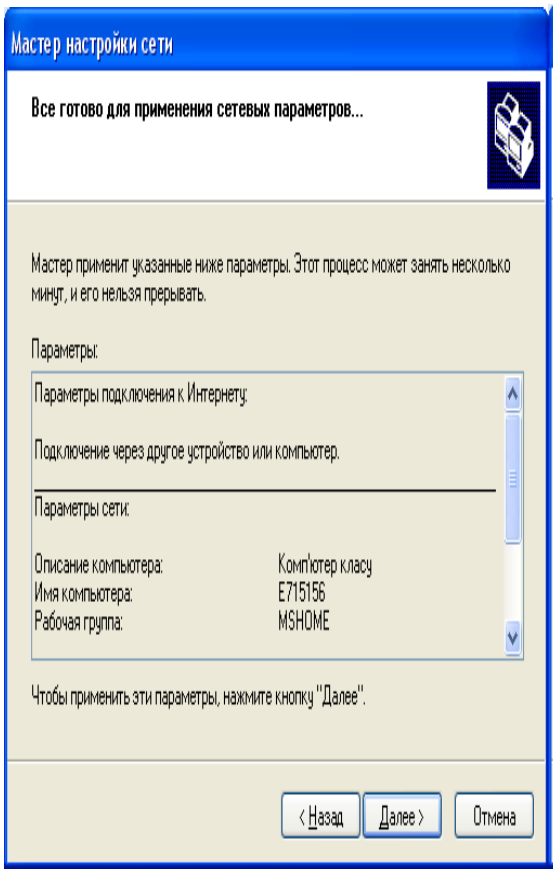


Рис. 3.9. Перевірка заданих параметрів

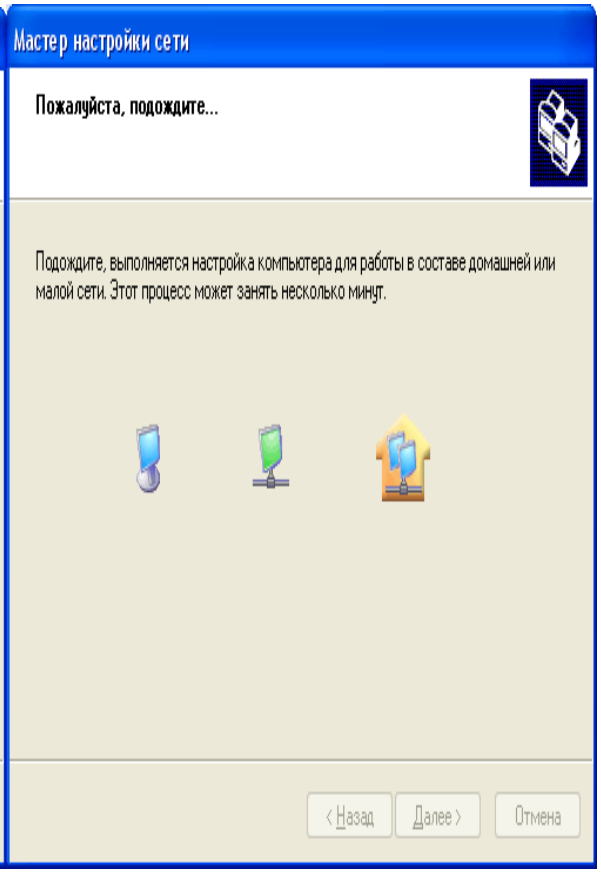


Рис. 3.10. Встановлення параметрів

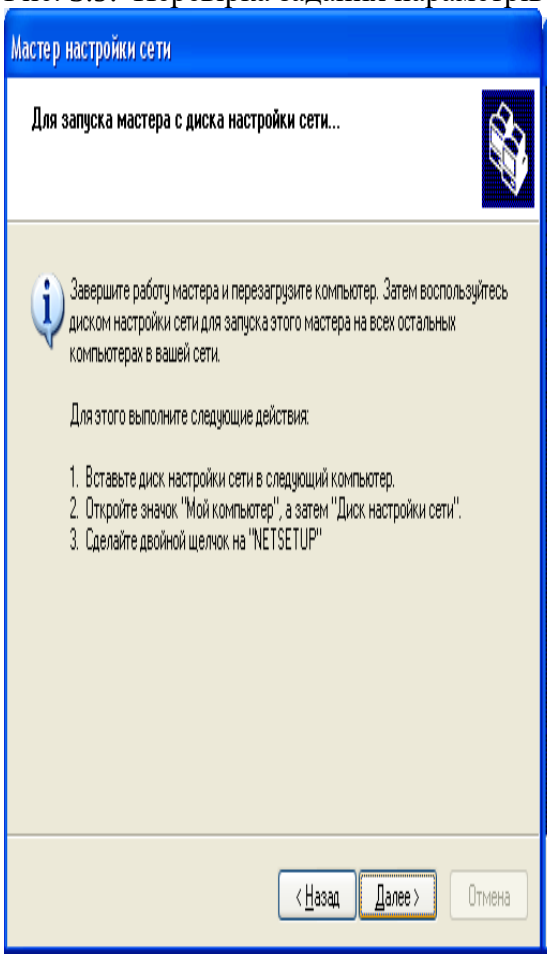


Рис. 3.11. Диск налагодження мережі

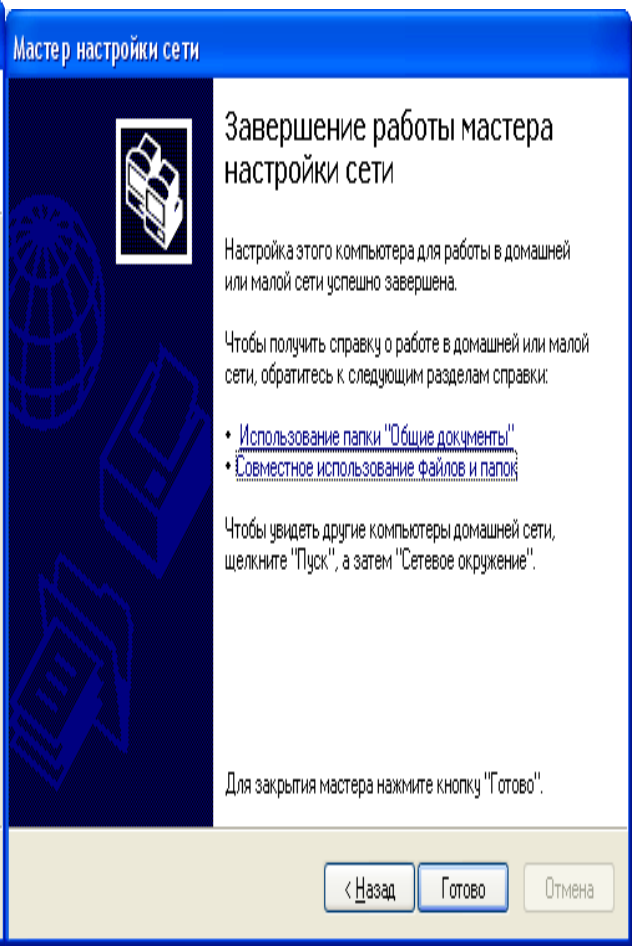


Рис. 3.12. Завершення роботи майстра

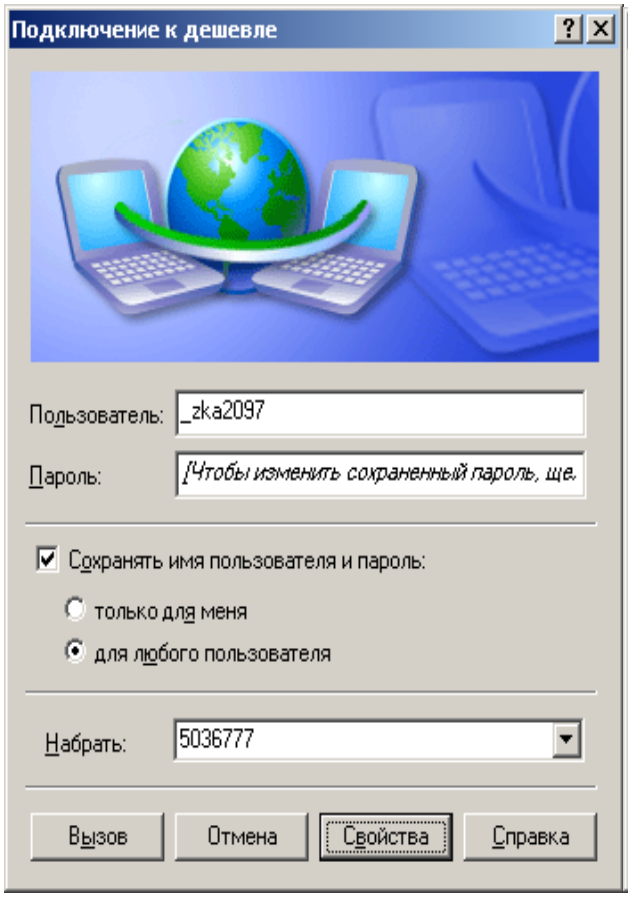


Рис. 3.13. Налагодження зв'язку через модем

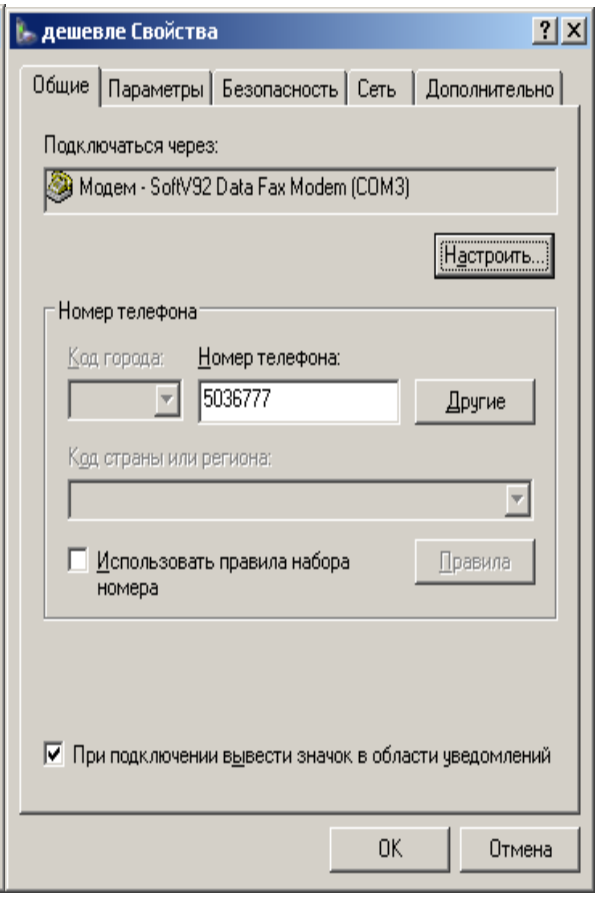


Рис. 3.14. Вікно «Свойства»

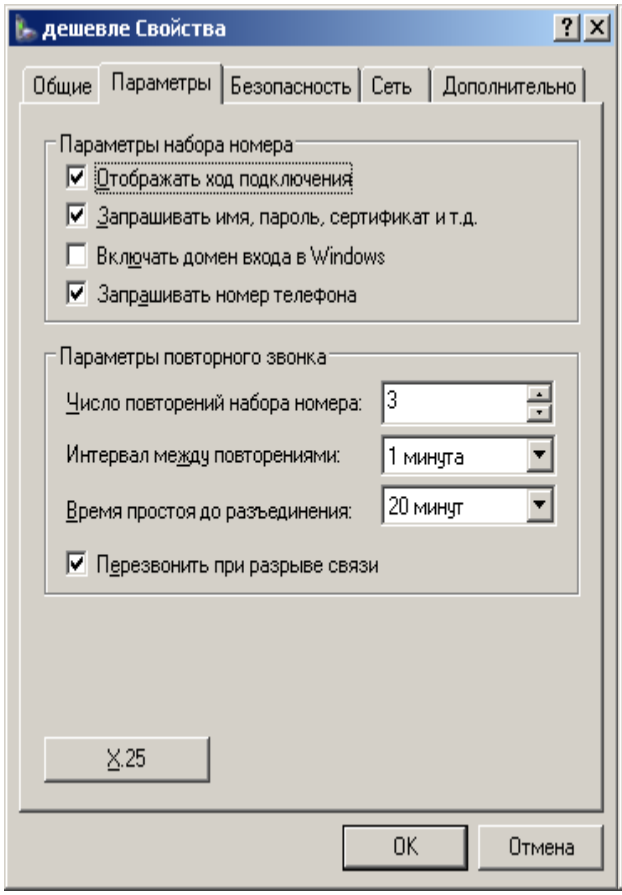


Рис. 3.15. Вкладка параметри

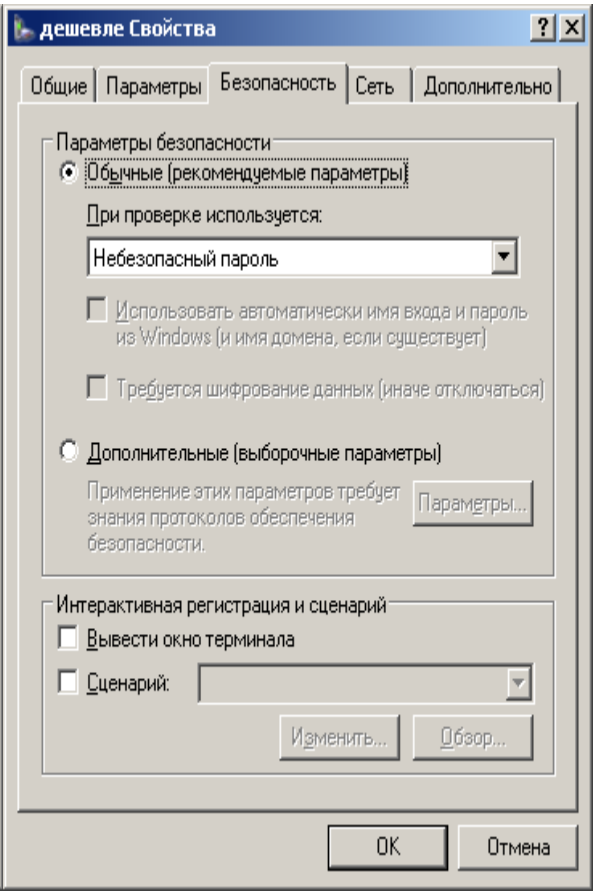


Рис. 3.16. Вкладка безпека

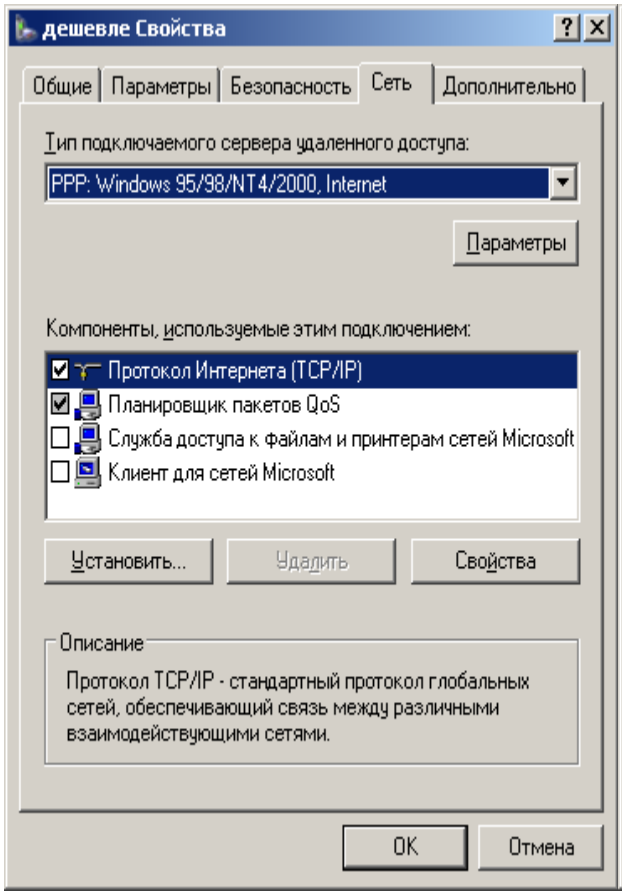


Рис. 3.17. Вкладка мережа

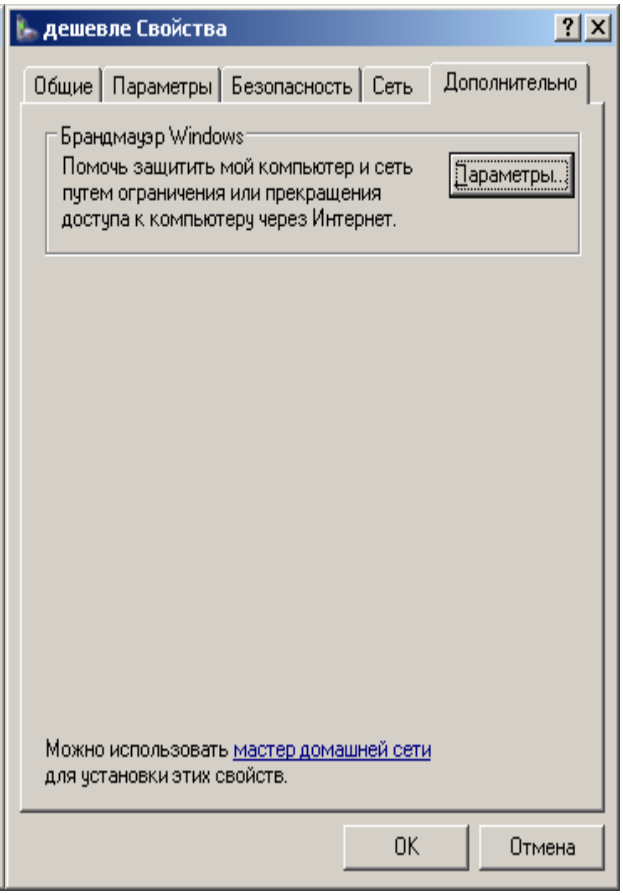


Рис. 3.18. Вкладка додатково

Налагодження віддаленого з'єднання із сервером

В 80-х роках американська фірма Hayes випустила перший модем для комп'ютера IBM PC. Звичайно, ж телефонні лінії розроблялися для передавання на відстань тільки звуків людського голосу.

Взагалі кажучи, природні звуки характеризуються тональністю й інтенсивністю, які безперервно змінюються. Для передавання телефонними лініями вони перетворюються в електричний сигнал із частотою й силою струму, що безперервно й відповідно змінюється. Такий сигнал називається *аналоговим*.

Комп'ютер же, на відміну від модему, розуміє тільки цифровий сигнал, тобто струм тільки двох рівнів. Кожний із них позначає одне із двох зрозумілих комп'ютеру значень: логічні "0" і "1". Щоб передати цифровий сигнал телефонними лініями, йому потрібно надати прийнятний для них аналоговий вигляд.

Саме цією роботою займається модем. Так само він виконує зворотну процедуру, тобто переводить аналоговий сигнал у зрозумілий комп'ютеру цифровий. Слово "модем" походить від скорочення двох термінів: Модулятор/Демодулятор. Модем організовує місток між цифровим сигналом, який видає комп'ютер, і аналоговим сигналом, який, як було сказано вище, розуміє телефонна лінія.

При передаванні даних із комп'ютера в модем, перший видає послідовність нулів і одиниць, а останній перетворює їх в аналоговий сигнал. Потім дані відсилаються в телефонну лінію і їх приймає модем, що стоїть на іншому кінці дроту. Коли модем приймає дані, то він фільтрує корисну інформацію від шумів у лінії. Для цього існують спеціальні протоколи корекції помилок. Самий просунутий із них – MNP10. Окрім цього існують MNP1, MNP2, MNP3, MNP4, MNP5, MNP7. У даний час найпоширенішим є MNP5, оскільки MNP7 і MNP10 встановлюються на спеціальних модемах, які працюють за виділеними лініями, наприклад, у глобальній мережі Internet. Після того як модем відділив корисну інформацію від шумів у лінії, він відбирає дані, які прийняв, від службової інформації. Так відбувається обмін даними при з'єднанні на протоколі Zmodem, Sealink, Ymodem і багатьох інших однонаправлених протоколах.

Звичайно, обидва комп'ютер можуть одночасно приймати й посилати дані. Тому що вони використовують певні угоди про частоти, різні для вхідних і вихідних сигналів.. Для цього існують спеціальні двонаправлені протоколи. Наприклад, Bimodem, Puma, Janus, Zedzap.

MNP-протоколи

MNP (Microsoft Network Protocols) – серія найпоширеніших апаратних протоколів, уперше реалізована на модемах фірми Microsoft. Ці протоколи забезпечують автоматичну корекцію помилок і компресію даних, які передаються. Зараз відомо 10 протоколів:

MNP1. Протокол корекції помилок, що використовує асинхронний напівдуплексний метод передавання даних. Це найпростіший із протоколів MNP.

MNP2. Протокол корекції помилок, що використовує асинхронний дуплексний метод передавання даних.

MNP3. Протокол корекції помилок, що використовує синхронний дуплексний метод передавання даних між модемами (інтерфейс модем-комп'ютер залишається асинхронним). Оскільки при асинхронному передаванні використовується десять біт на байт: вісім біт даних, стартовий біт і стоповий біт, а при синхронній тільки вісім, то в цьому криється можливість прискорити обмін даними на 20%.

MNP4. Протокол, що використовує синхронний метод передавання, забезпечує оптимізацію фази даних, яка дещо покращує неефективність протоколів MNP2 і MNP3. Крім того, при зміні числа помилок на лінії відповідно змінюється й розмір блоків даних, що передаються. При збільшенні числа помилок розмір блоків зменшується, збільшуючи вірогідність успішного проходження окремих блоків. Ефективність цього методу складає близько 20% в порівнянні із простим передаванням даних.

MNP5. Додатково до методів MNP4, MNP5 часто використовує простий метод стиснення інформації, яка передається. Символи, які часто зустрічаються в передаваному блоці, кодуються ланцюжками бітів меншої довжини, ніж символи, що рідко зустрічаються. Додатково кодуються довгі ланцюжки однакових символів. Звичайно, при цьому текстові файли стискаються до 35% своєї початкової довжини. Разом з 20% MNP4 це дає підвищення ефективності до 50%. Відмітимо, що якщо передавати вже стиснені файли, а переважно це так і є, додаткового збільшення ефективності за рахунок стиснення даних модемом не відбувається.

MNP6. Додатково до методів протоколу MNP5 протокол MNP6 автоматично перемикається між дуплексним і напівдуплексним методами передавання залежно від типу інформації. Протокол MNP6 також забезпечує сумісність із протоколом V.29.

MNP7. У порівнянні з ранніми протоколами використовує ефективніший метод стиснення даних.

MNP9. Використовує протокол V.32 і відповідний метод роботи, що забезпечує сумісність з низькошвидкісними модемами.

MNP10. Призначений для забезпечення зв'язку на сильно зашумлених лініях, таких як міжміські лінії, сільські лінії. Це досягається за допомогою наступних методів:

- багатократного повторення спроби встановити зв'язок;
- зміни розміру пакетів відповідно до зміни рівня перешкод на лінії;
- динамічної зміни швидкості передавання відповідно до рівня перешкод лінії.

Усі протоколи MNP сумісні між собою від низу до верху. При встановленні зв'язку відбувається встановлення щонайвищого можливого рівня MNP-протоколу. Якщо ж один із модемів, що зв'язуються, не підтримує протокол MNP, то MNP-модем працює без MNP-протоколу.

Протокол V90

Технологія V.90 дає можливість модемам приймати дані на швидкості до 56 Кбіт/с на звичайних комутованих лініях. V.90 обходить теоретичні обмеження накладені на стандартні, аналогові модеми, використовуючи цифрові канали, які більшість провайдерів Інтернету використовує при підключенні до телефонних мереж.

Звичайно, єдина аналогова частина телефонної мережі – це той шматок мідного кабелю, що сполучає ваш будинок і центральне відділення телефонної компанії. За останні два десятиріччя телефонні компанії проводили заміну аналогових частин їх ліній на цифрові канали. Але найскладніше було змінити невелику ділянку мережі від вашого будинку до телефонної компанії. Вона швидше за все не зазнаватиме змін у кращу сторону ще декілька років.

Усе, що потрібне для переобладнання модемів – це програмний апгрейд (якщо такий передбачений). Програмною модернізацією можна перетворити аналоговий US Robotics Courier V.Everything на V.90 аналоговий модем.

Як уже було відзначено, дані від цифрового V.90 модему посилаються телефонною мережею у вигляді двійкових кодів. Але щоб задовольнити умові x2 цифровий V.90 модем передає дані (8 біт кожного разу) клієнтському аналого-цифровому конвертору з тією ж частотою, що і телефонна мережа (8000 Гц). Це означає, що символьна швидкість модему (Symbol Rate) повинна бути рівна частоті телефонної мережі.

У процесі встановлення з'єднання, V.90 модеми випробовують телефонну лінію на предмет знаходження низхідних аналого-цифрових перетворювачів. Якщо модем знаходить їх, він далі проводить з'єднання на протоколі V.34. Аналогічна ситуація відбувається в тому випадку, якщо модем на іншому кінці лінії не є V.90 модемом.

Задача клієнтського модему полягає в пізнанні 256 потенційних сигналів і відновлення 8000 PCM кодів у секунду. Якби йому це вдалося, швидкість від серверу до клієнта складала б 64 кбіт/с (8000x8 біт у кожному коді). Але, як з'ясувалося, декілька проблем заважають використовуванню такої швидкості.

По-перше, не дивлячись на те, що проблема шуму квантування більш не стоїть, другий набагато менший шум від цифро-аналогового перетворювача все-таки є. Крім того, цей шум здійснюється встаткуванням на вашій станції АТС (від якої йдуть кабелі до вашого будинку). Сам по собі шум виникає через деякі нелінійні спотворення й взаємні наведення.

По-друге, мережеві цифро-аналогові перетворювачі не є лінійними конвертерами, а слідують деякому конвертуючому закону. У результаті коди PCM, які визначають малі сигнали, проходять у цифро-аналоговому встаткуванні, тоді як коди з великими за потужністю сигналами викликаються при перетворенні.

Ці дві проблеми роблять практично неможливим використовування всіх 256 дискретних кодів, оскільки відповідний вихід від цифро-аналогового перетворювача малих сигналів дуже близький до нуля й втрачається на фоні навіть малого шуму. Таким чином, V.90 кодувальник використовує декілька варіантів 256 кодів, які видаляють сигнали, найближчі до шуму. Наприклад, для передавання даних на швидкості 56 кбіт/с використовуються 128-рівневі коди. Використовування меншого числа рівнів дозволяє стабілізувати передавання даних, але на меншій швидкості.

Режими MNP-модемів

MNP-модем забезпечує наступні режими передавання даних:

- Стандартний режим. Забезпечує буферизацію даних, що дозволяє працювати з різними швидкостями передавання даних між комп'ютером і модемом та між двома модемами. У результаті для підвищення ефективності передавання даних можливо встановити швидкість обміну комп'ютер-модем вище, ніж модем-модем. У стандартному режимі роботи модем не виконує апаратної корекції помилок.
- Режим прямого передавання. Даний режим відповідає звичайному модему, що не підтримує MNP-протокол. Буферизація даних не проводиться й апаратна корекція помилок не виконується.
- Режим із корекцією помилок і буферизацією. Це стандартний режим роботи при зв'язку двох MNP-модемів. Якщо віддалений модем не підтримує протокол MNP, зв'язок не встановлюється.
- Режим із корекцією помилок і автоматичною настройкою. Режим використовується, коли наперед не відомо, чи підтримує віддалений модем протокол MNP. На початку сеансу зв'язку після визначення режиму віддаленого модему встановлюється один із трьох інших режимів.

Внутрішні й зовнішні модеми

Модеми внутрішні й зовнішні (існують також спеціальні типи модемів у вигляді PC-карт (PCMCIA), але вони призначені для комп'ютерів типу ноутбуків, і тому вони тут не розглядаються). Внутрішні модеми виконані у вигляді плати розширення, що вставляється в спеціальний слот розширення на материнській платі комп'ютера. Зовнішній модем, на відміну від внутрішнього, виконаний у вигляді окремого пристрою, тобто в окремому корпусі й зі своїм блоком живлення, у той час як внутрішній модем одержує електрику від блоку живлення комп'ютера. Так які ж переваги й недоліки в зовнішніх і внутрішніх модемів?

Внутрішні модеми

Переваги

1. Усі внутрішні моделі модемів без виключення (на відміну від зовнішніх) мають вбудоване FIFO (First Input First Output – першим прийшов, першим прийнятий). FIFO – це мікросхема, що забезпечує буферизацію даних. Звичайний модем при проходженні байта даних через порт кожного разу запрошує переривання у комп'ютера. Комп'ютер за спеціальними IRQ (Interrupt Request) лініями перериває на деякий час роботу модему, а потім знову відновлює її. Це вповільнює роботу комп'ютера в цілому. FIFO же дозволяє використовувати переривання в декілька разів рідше. Це має велике значення при роботі в багатозадачних середовищах, таких як Windows98, OS/2, Windows 2000, UNIX і інших.

2. При використовуванні внутрішнього модему зменшується кількість дротів, натягнутих у найнесподіваніших місцях. Так само внутрішній модем не займає дорогоцінне місце на робочому столі.

3. Внутрішні модеми є послідовним портом комп'ютера й не займають існуючих портів комп'ютера.

4. Внутрішні моделі модемів завжди дешевше зовнішніх.

Недоліки

1. Займають слот розширення на материнській платі комп'ютера. Це дуже незручно на мультимедійних машинах, на яких установлена велика кількість додаткових плат, а також на комп'ютерах, які працюють серверами в мережах.

2. Немає індикаторних лампочок, які при певному навику дозволяють стежити за процесами, які відбуваються в модемі.

3. Якщо модем завис, то відновити працездатність можна тільки клавішею перезавантаження комп'ютера "RESET".

Зовнішні модеми

Переваги

1. Вони не займають слот розширення, і за необхідності їх можна легко відключити й перенести на інший комп'ютер.

2. На передній панелі є індикатори, які допомагають зрозуміти, яку операцію зараз проводить модем.

3. При зависанні модему не потрібно перезавантажувати комп'ютер, достатньо вимкнути й включити живлення.

Недоліки

1. Необхідна мультикарта із вбудованим FIFO. Без FIFO модем, звичайно, працюватиме, але при цьому падатиме швидкість передавання даних.

2. Зовнішній модем займає дорогоцінне місце на робочому столі і йому потрібні додаткові дроти для підключення. Це теж створює деяку незручність.

3. Він займає послідовний порт комп'ютера.

4. Зовнішній модем завжди дорожче аналогічного внутрішнього, оскільки включає корпус з індикаторними лампочками й блок живлення.

Роль індикаторних лампочок

1. MR (Modem Ready)

Показує, що модем включений і готовий до роботи.

2. TR (Terminal Ready)

Цей індикатор горить, коли модем знаходить DTR (Data Terminal Ready), який передається комунікаційною програмою.

3. HS (High Speed)

Цей індикатор спалахує, коли модем працює з максимально можливою для нього швидкістю.

4. CD (Carrier Detect)

Він повинен горіти під час з'єднання модемів і протягом усього сеансу зв'язку, поки один із модемів не "покладе трубку".

5. AA (Auto Answer)

Показує, що модем включений у режим автовідповіді, тобто буде сам відповідати на всі вхідні дзвінки. Якщо модем знаходить Ring (з англ. дзвінок), то цей індикатор мерехтить.

6. OH (Hook)

Цей індикатор еквівалентний знятій трубці телефону. Він горить, коли модем займає лінію.

7. RD (Receive Data)

Мерехтить при прийманні комп'ютером даних.

8. SD (Send Data)

Цей індикатор мигає, коли комп'ютер надсилає дані.

Марки модемів

На сьогоднішній день фактичним стандартом є модем зі швидкістю з'єднання 14400 бод і протоколами передавання даних V32 і V32bis (і поліпшені, наприклад, HST і V32turbo). Орієнтуватися сьогодні варто на цей стандарт. Але й він, як і все в комп'ютерному світі, нестійкий, і поступово відмирає. Звичайно, найкраще брати модем зі швидкістю з'єднання 28800 бод і протоколами передавання даних V34 (і його підмножини V.Fast і V.Everything). Також є поліпшений різновид протоколу V34+. Він дозволяє вести приймання/передавання на швидкостях до 33600 бод. Модеми деяких фірм мають спеціалізовані протоколи для особливих умов експлуатації (зазвичай, на сильно зашумлених лініях. На них ці протоколи поводяться бездоганно). Такими протоколами є HST, розроблений фірмою USRobotics®. Так само існують два протоколи, розроблені Zyxel® . Це Zyx і ZyCell. Zyx – це протокол із можливістю зв'язку з аналогічними моделями на швидкостях 16800 і 19200 бод. А ZyCell – спеціальний протокол для супутникового й настільного зв'язку. Єдиним недоліком таких протоколів є те, що вони зв'язуються на фірмових протоколах тільки з аналогічними моделями.

Тепер можна розглянути деякі марки модемів.

GVC

Ця фірма відома перш за все тим, що виробляє недорогі, але достатньо надійні моделі.

Наприклад, модель GVC 14440 F1114HV – модель, що добре зарекомендувала себе в наших умовах. Вона практично безпомилково "ловить" сигнал BUSY. Це факс-модем, і він має факс класу II. Так само в ньому реалізовано підстроювання рівня сигналу до якості лінії. Однією з його переваг є безшумне герконове реле.

ZyXEL

Декілька років тому це була одна з найпопулярніших і престижних моделей, але на сьогоднішній день фірма сильно здала свої позиції, в основному на фоні досягнень USRobotics. Усі різновиди модемів фірми ZyXEL розбиті на серії.

Серія 1496 – окрім стандартних протоколів V32 і V32bis, має власні протоколи: Zyx і ZyCell. У цих моделях є голосовий режим (VOICE) для того, що б посилати і приймати голосові повідомлення. Так само є режим визначення номера (АОН – автоматичний визначник номера).

Моделі серії 1496 володіють адаптивним факсом, це означає що модем дозволяє автоматично ідентифікувати абонента і перемикатися відповідно на факс, модем або голос.

Так само модеми ZyXEL можуть працювати на виділених чотирьохдротових лініях, розвиваючи при цьому швидкість передавання до 115200 бод.

USRobotics®

Ця фірма випускає декілька серій модемів: USR Sportster, USR Courier, USR WorldPort і інші. Моделі WorldPort призначені для портативних комп'ютерів. Через це вони не набули широкого поширення. Високопродуктивна серія Courier із деяких викладених нижче причин не набула в нашій країні великого поширення. Залишається тільки серія Sportster. Модеми цієї серії охоплюють усю гамму швидкостей від 14400 до 33600 бод. Вони бувають як внутрішніми, так і зовнішніми, і мають безліч модифікацій, що розрізняються як програмно, так і апаратно. Досить зручно, що модеми серії Sportster мають програмно-апаратного апгрейда до дорожчої й набагато функціональнішої серії Courier. Після апгрейда звичайний USR Sportster перетворюється в Courier. При цьому він має таку важливу перевагу як вбудований протокол HST (High Speed Technology). Приклади модемів наведені в додатку 1.

Налагодження віддаленого з'єднання при наявності операційної системи Windows XP та роботі в мережі Інтернет без використання локальної мережі

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настроювання → Панель керування**.
2. Відкрийте піктограму **Мережеві підключення**.
3. Запустіть **Майстра нових підключень** на виконання.
4. У другому вікні майстра виберіть пункт **Підключення до Інтернету.**
5. У третьому вікні майстра виберіть пункт **Увести параметри вручну.**

6. У четвертому вікні майстра виберіть пункт **Під'єднуватись до телефонної лінії, використавши модем.**
7. У п'ятому вікні майстра введіть назву з'єднання, яке створюєте.
8. У шостому вікні майстра вкажіть телефон дозвону.
9. У сьомому вікні майстра вкажіть логін та пароль із підтвердженням (надається провайдером).

Налагодження віддаленого з'єднання при наявності операційної системи Windows XP та роботі в мережі Інтернет із використанням локальної мережі

1. Установіть мережеву карту та її драйвер.
2. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настроювання → Панель керування**.
3. Відкрийте об'єкт **Властивості оглядача.**
4. Відкрийте вкладку **Підключення.**
5. Уведіть команду **Властивості мережі.**
6. Установіть прапорець **Використовувати Проксі-Сервер.**
7. Уведіть адресу Проксі-Сервера **(server)** та його порт (**3128**).
8. Уведіть команду **ОК**.

Пошук інформації в мережі Internet

Основна мета користувача при роботі з мережею Internet – це отримання інформації, оскільки в першу чергу Internet є гігантським інформаційним ресурсом. Завдання пошуку інформації в умовах стрімкого розвитку й постійної зміни мережі і її інформаційного наповнення є нетривіальним.

Випадково знайти потрібну адресу в мережі можна різними способами: просто подорожуючи за вузлами (surfing on the web), дізнатися в знайомих, побачити в рекламі й т.д.

Цілеспрямований пошук явно або неявно вимагає формулювання мети пошуку, розуміння того, що є об'єктом пошуку, обґрунтованого вибору засобу пошуку і ефективної методики.

Мета пошуку

Мета визначає характеристики об'єктів пошуку, об'єм і терміни виконання роботи, перелік засобів пошуку й способи їх застосування. Наприклад, при підготовці до іспиту потрібна методична література, учбові курси, конспекти лекцій, для реферату – аналітичні огляди, для доповіді – графічні матеріали, для презентації – файли мультимедіа, для наукового дослідження – програмне забезпечення і т.д.

Об'єкт пошуку

Як об'єкт пошуку може розглядатися будь-яка інформація, якщо є можливість представлення її в Internet. Це можуть бути телефони й адреси, інформація про товари й послуги, радіо й телетрансляції й багато що інше. Найпоширенішими об'єктами пошуку є:

- Адреса інформаційного ресурсу, зокрема:
  адреса WWW-сервера (http://www.company.ru);
  адреса Web-сторінки (http://www.company.ru/index.html);
  адреса файлу (http://www.company.ru/images/picture.jpg);
  адреса електронної пошти (mailto:user@company.ru);
  адреса FTP-сервера (ftp://ftp.company.ru);
  адреса Gopher-сервера (gopher://gopher.mysite.com);
  стаття UseNet (news:relcom.newusers);
  сеанс Telnet (telnet://mysite.ru).
- Web-сторінка й включені в неї елементи: текст, мультимедіа дані, гіперпосилання, програми (аплети) і т.д.
- Програми, зокрема: демонстраційні й тестові програми, засоби поліпшення (upgrade), оновлення (update) і виправлення помилок (patch) у програмах;
- Повідомлення в телеконференціях;
- Інформація з інтерактивних баз даних, довідників, каталогів, репозиторіїв.

Засоби пошуку

Засобами пошуку є Web-індекси, Web-каталоги, гібридні системи пошуку, метапошукові системи, засоби локального пошуку й утиліти автономного пошуку.

Web-індекси

Даний сервер намагається проглянути всі Web-сторінки, представлені в Internet і врахувати їх уміст у базі даних. Перегляд виконується в автоматичному режимі програмами, які називаються мережевими роботами, павуками або черв'яками (net robot, spider, worm). Кожна знайдена сторінка досліджується спеціальною програмою індексування, яка аналізує заголовок, тему, ключові слова, текст і склад Web-сторінки. Одержана інформація заноситься в базу даних і є основою для виконання пошуку за запитом користувача.

Найвідоміші Web-індекси:

AltaVista (http://www.altavista.com);

HotBot (http://www.hotbot.com);

Google (http://www.google.com.ua).

Web-каталоги

У Web-каталозі посилання на ресурси Internet об'єднані тематично й організовані у вигляді ієрархії категорій. На верхньому рівні ієрархії, зазвичай, знаходяться категорії "бізнес", "наука", "мистецтво" і т.д. Каталоги складаються уручну аналітиками Web-каталогу. Тому для каталогів характерна висока якість відбору інформації і її сортування, але за обхватом інформації й оперативності вони поступаються Web-індексам.

Найвідоміші Web-каталоги – це Yahoo! (http://www.yahoo.com) і Magellan (http://www.magellan.com).

Гібридні пошукові системи

Гібридні пошукові системи мають і індексну базу даних, і структурований тематичний каталог. Прикладами таких систем є:

Lycos (http://www.lycos.com);

Excite (http://www.excite.com);

Infoseek (http://www.infoseek.com);

WebCrawler (http://www.webcrawler.com).

Метапошукові системи

Метапошукові системи забезпечують для кожного запиту одночасний пошук за допомогою декількох пошукових серверів. Такі системи дозволяють задавати тільки прості запити на пошук. Це скорочує час, але одержувані результати, як правило, гірші, ніж при незалежному пошуку на кожному пошуковому сервері з використанням розширених можливостей.

Найзручніші метапошукові системи це:

Accufind (http://www.accufind.com);

Metafind (http://www.metafind.com);

Metasearch (http://www.metasearch.com).

Портали

Слід зазначити тенденцію до перетворення багатьох відомих пошукових серверів у портали Internet (від латинського porta - вхід, ворота). Кожен користувач порталу має можливість набудувати вигляд і зміст вузла-порталу на свій розсуд. При використанні порталу можна обмежити склад тематичних каталогів і баз даних такою інформацією, що цікавить користувача, зберігати пошукові запити і створювати закладки для пошуку.

Засоби локального пошуку

Останнім часом у багато великих Web-вузлів включаються засоби локального пошуку інформації, представленої на вузлі. Це можуть бути довідники, інтерактивні бази даних, архіви публікацій, репозиторії. Застосування подібних засобів актуальне при пошуку вузько спеціалізованої інформації. Наприклад, інформацію про продукцію фірми Sony зручно шукати безпосередньо на вузлі даної фірми (http://www.sony.com).

Автономні утиліти

Утиліти автономного пошуку встановлюються на комп'ютері користувача. Вони забезпечують накопичення пошукових запитів, виконують метапошук, відстежують зміни заданих Web-сторінок. До подібних програм можна віднести WebCompass (http://www.quarterdeck.com) і Copernic (http://www.copernic.com).

Корисними при пошуку можуть опинитися так звані автономні браузери (off-line browsers), що забезпечують завантаження заданих Web-вузлів без участі користувача. У таких програмах можна задавати "глибину" пошуку посилань усередині вузла, тип і граничний розмір копійованих файлів, розклад завантаження. Найбільш популярні: WebWhacker (http://www.ftg.com) і Teleport Pro (http://www.tenmax.com)

Прискорити ручний пошук можна за допомогою засобів аналізу структури Web-вузла. Вони зображають у зручній формі навігаційну карту вузла, на якій показані елементи Web-сторінок з анотаціями і їх зв'язку. Для цієї мети можна застосовувати WebTurbo (http://www.webturbo.com) або PersonalCrawler (http://www.vci.co.il).

Пошукові системи

Пошукові системи, зазвичай, складаються із трьох компонент:

- агент (павук або кроулер), який переміщається мережею й збирає інформацію;
- база даних, яка містить усю інформацію, що збирається павуками;
- пошуковий механізм, який люди використовують як інтерфейс для взаємодії з базою даних.

Spider («павук») – програма, яка завантажує в пошукову машину Web-сторінки. Працює аналогічно браузеру, але не відображає свої дії. Якщо необхідно мати уявлення про те, що саме завантажує в пошукову систему «павук», треба відкрити будь- яку Web-сторінку та вибрати в меню **Вид** браузера пункт **Просмотр HTML**.

Crawler («хропак»,) – программа, яка може знайти на Web-сторінці всі посилання на інші сторінки. Його задача визначити, куда далі повинен іти «павук».

Indexer (індексатор) – програма, яка «розбирає» сторінку на складові частини і аналізує їх.

Як працюють механізми пошуку

Засоби пошуку й структуризації, іноді звані пошуковими механізмами, використовуються для того, щоб допомогти людям знайти інформацію, якої вони потребують. Засоби пошуку типу агентів, павуків, кроулерів і роботів використовуються для збору інформації про документи, що знаходяться в мережі Інтернет. Це спеціальні програми, які займаються пошуком сторінок у мережі, витягують гіпертекстові посилання на цих сторінках і автоматично індексують інформацію, яку вони знаходять для побудови бази даних. Кожен пошуковий механізм має власний набір правил, що визначають, як збирати документи. Деякі слідують за кожним посиланням на кожній знайденій сторінці й потім, у свою чергу, досліджують кожне посилання на кожній із нових сторінок, і так далі. Деякі ігнорують посилання, які ведуть до графічних і звукових файлів, файлів мультиплікації; інші ігнорують посилання до ресурсів типу баз даних WAIS; інші проінструктовані, що потрібно проглядати перш за все найпопулярніші сторінки.

Агенти – «найінтелектуальніші» із пошукових засобів. Вони можуть більше ніж просто шукати: вони можуть виконувати навіть транзакції від імені користувача. Уже зараз вони можуть шукати сайти специфічної тематики і повертати списки сайтів, відсортованих за їх відвідуваністю. Агенти можуть обробляти зміст документів, знаходити й індексувати інші види ресурсів, не тільки сторінки. Вони можуть також бути запрограмовані для отримання інформації з уже існуючих баз даних. Незалежно від інформації, яку агенти індексують, вони передають її назад базі даних пошукового механізму.

Загальний пошук інформації в мережі здійснюють програми, відомі як павуки. *Павуки* повідомляють про зміст знайденого документа, індексують його й отримують підсумкову інформацію. Також вони проглядають заголовки, деякі посилання й посилають проіндексовану інформацію базі даних пошукового механізму.

Кроулери проглядають заголовки й повертають тільки перше посилання.

Роботи можуть бути запрограмовані так, щоб переходити за різними посиланнями різної глибини вкладеності, виконувати індексацію й навіть перевіряти посилання в документі. Із-за їх природи вони можуть застрявати в циклах, тому, проходячи за посиланнями, їм потрібні значні ресурси мережі. Проте, є методи, призначені для того, щоб заборонити роботам пошук за сайтами, власники яких не бажають, щоб вони були проіндексовані.

Агенти витягують і індексують різні види інформації. Деякі, наприклад, індексують кожне окреме слово в документі, що зустрічається, тоді як інші індексують тільки 100 найважливіших слів у кожному, індексують розмір документа й число слів у ньому, назву, заголовки й

підзаголовки й так далі. Вид побудованого індексу визначає, який пошук може бути зроблений пошуковим механізмом і як одержана інформація буде інтерпретована.

Агенти можуть також переміщатися у Інтернеті і знаходити інформацію, після чого поміщати її в базу даних пошукового механізму. Адміністратори пошукових систем можуть визначити, які сайти або типи сайтів агенти повинні відвідати й проіндексувати. Проіндексована інформація відсилається базі даних пошукового механізму так само, як було описано вище.

Люди можуть поміщати інформацію прямо в індекс, заповнюючи особливу форму для того розділу, у який вони хотіли б помістити свою інформацію. Ці дані передаються базі даних.

Коли хто-небудь хоче знайти інформацію, доступну в Інтернет, він відвідує сторінку пошукової системи й заповнює форму, що деталізує інформацію, яка йому необхідна. Тут можуть використовуватися ключові слова, дати й інші критерії. Критерії у формі пошуку повинні відповідати критеріям, що використовуються агентами при індексації інформації, яку вони знайшли в мережі.

База даних відшукує предмет запиту, заснований на інформації, указаній у заповненій формі, і виводить відповідні документи, підготовлені базою даних. Щоб визначити порядок, у якому список документів буде показаний, база даних застосовує алгоритм ранжирування. В ідеальному випадку документи, найбільш релевантні призначеному для користувача запиту, будуть поміщені першими в списку. Різні пошукові системи використовують різні алгоритми ранжирування, проте основні принципи визначення релевантності наступні:

- Кількість слів запиту в текстовому вмісті документа (тобто в html-коді).
- Теги, у яких ці слова розташовуються.
- Місцеположення шуканих слів у документі.
- Питома вага слів, відносно яких визначається релевантність, у загальній кількості слів документа.

Ці принципи застосовуються всіма пошуковими системами. А представлені нижче використовуються деякими, але достатньо відомими (такими як AltaVista, HotBot).

- Час – як довго сторінка знаходиться в базі пошукового сервера. Спочатку здається, що це досить безглуздий принцип. Але, якщо задуматися, як багато існує в Інтернеті сайтів, які живуть максимум місяць. Якщо ж сайт існує досить довго, це означає, що власник вельми досвідчений у даній темі й користувачу більше підійде сайт, який декілька років сповіщає світові про правила поведінки, ніж той, який з'явився неділю тому із цією ж темою.
- Індекс цитованості – як багато посилань на дану сторінку веде з інших сторінок, зареєстрованих у базі пошукача.

База даних виводить ранжируваний так само список документів з HTML і повертає його людині, що зробила запит. Різні пошукові механізми також вибирають різні способи показу одержаного списку – деякі показують тільки посилання; інші виводять посилання з першими декількома пропозиціями, що містяться в документі або заголовок документа разом із посиланням.

Коли клацнути на посиланні до одного з документів, який цікавить, цей документ запрошується в того сервера, на якому він знаходиться.

Робота з браузером Microsoft Internet Explorer

Програма Internet Explorer (завантажувальний файл Iexplore.exe знаходиться в каталозі Program Files\Internet Explorer) призначена для навігації за мережею Internet і виконання дій над її об'єктами. Для запуску цієї програми можна скористатися одним із наведених нижче способів:

а) в меню **Пуск** вибираємо команду **Программы**, потім команду **Internet Explorer**;

б) двічі клацнути основною клавішею маніпулятору "миша" на піктограмі Internet Explorer;

в) в меню **Пуск** вибрати команду **Выполнить**, використовуючи кнопку **Обзор** знайти файл **Iexplore.exe** та клацнути основною клавішею маніпулятору "миша" на кнопці **Ok**.

Після запуску програми відкриється вікно (рис. 3.19).

Вивчення можливостей браузера.

1. Розгляньте вікно браузера та визначте призначення основних його складових: рядку заголовку, головного меню, панелей інструментів, рядку адрес, області перегляду документу, рядку стану, системного меню.

2. Проведіть зміну виду вікна браузера, використавши відповідні команди меню **Вид**, підменю **Панели обозревателя**, команди: **Поиск**, **Избранное**, **Журнал**, **Папки**, **Полезный совет**.

3. Проведіть налагоджування панелей та елементів браузера за допомогою меню **Вид**, підменю **Панели инструментов**, команди: **Обычные кнопки**, **Адресная строка**, **Ссылки**, **Радио**, **Настройка**.

4. Опануйте операцію зміни кодування Web-сторінки, яка переглядається, за допомогою команд меню **Вид**, підменю **Вид кодировки**, та зміни розміру шрифта за допомогою команд підменю **Размер шрифта** в цьому ж меню **Вид**.

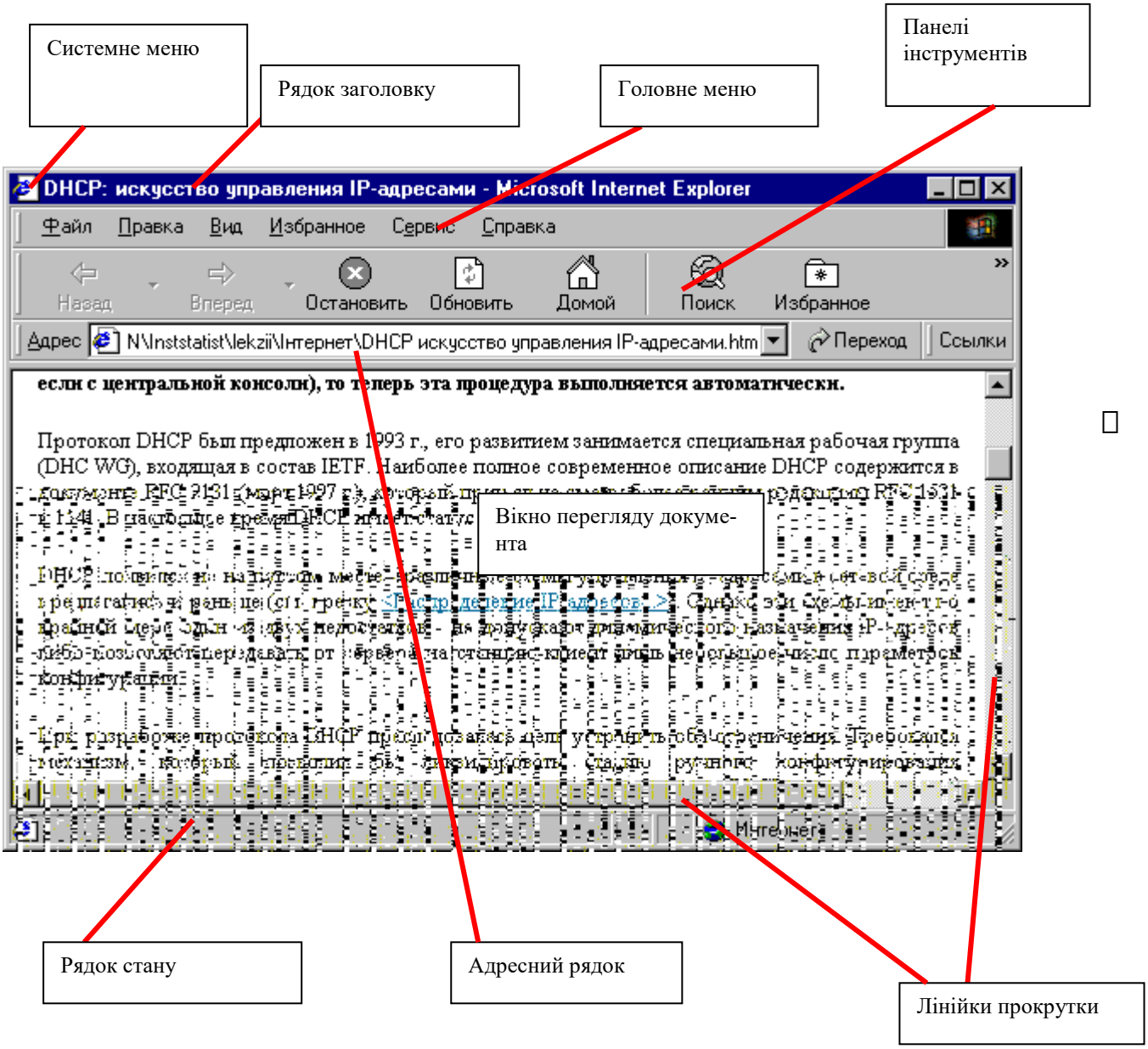


Рис. 3.19. Загальний вигляд вікна Internet Explorer.

5. Перегляньте підручник Microsoft з Internet за адресою http://home.microsoft.com/intl/ru/tutorial. Випробуйте різні режими швидкого переходу між Web-сторінками, використовуючи для цього кнопку **Назад**, список останніх набраних адрес у рядку адрес, **Закладку** в каталозі **Избранное**, **Ярлыки** на робочому столі або в будь-якому іншому каталозі, швидке посилання в підменю **Вид/Параметры/Переходы**…

6. Налагодьте параметри браузера за допомогою підменю **Сервис\Свойства обозревателя**. Встановіть адресу домашньої сторінки http://home.microsoft.com/intl/ru/tutorial/; шрифт Times New Roman; рівень безпеки – попередження перед завантаженням змісту, який не є безпечним; параметри – відображати малюнки; попереджувати при адресації форм, які передаються.

Методика пошуку інформації в мережі Internet

Методика пошуку включає правила формування запиту на пошук, методи звуження області пошуку, управління процесом пошуку, вибір форми представлення результатів.

Запити на пошук описують умови, яким повинні відповідати результати пошуку. У запитах задаються слова або фрази, які будуть шукатися, вони називаються ключовими.

Правила формування запиту:

1. Ім'я власне (повинно починатися із прописної букви): **Слово**.
2. Пошук слова без урахування регістра: **слово**.
3. Ключове слово з будь-яким закінченням: **слово***.
4. Ключове слово з будь-яким закінченням, що складається з одного символа: **слово?**.
5. Неподільна ключова фраза: "**слово1 слово2 ...**".
6. Ключове слово обов'язкове: **+слово**.
7. Ключове слово повинно бути відсутнім: **-слово**.

У запиті можливо задавати логічні вирази, які швидше за все застосовуються при розширеному пошуку (Advanced search). Логічні вирази будуються шляхом застосування ключових слів, круглих дужок і логічних операцій **AND**, **OR**, **NOT** (указані операції можуть позначатися, як **- &**, **|** , **!**)

Приклади логічних виразів:

1. Вираз: **слово1 AND слово2 AND NOT слово3**
   еквівалентний: **+слово1+слово2-слово3.**
2. Вираз: **"фраза" AND (слово1 OR слово2)**
   еквівалентний: **("фраза" AND слово1) OR ("фраза" AND "слово2").**

Деякі пошукові системи підтримують *метакоманди*, повний перелік, яких можна отримати за допомогою довідкової системи. У системі AltaVista метакоманди застосовують для наступних видів пошуку:

1. Пошук Web-сторінок з указівкою заголовків: **title:заголовок**;
2. Пошук у тексті сторінок: **text:слово**;
3. Пошук слова серед посилань на Web-сторінці: **anchor:слово**;
4. Пошук сторінок, які мають посилання на визначену адресу: **link:адрес**;
5. Пошук графічного файлу на Web-сторінці: **image: імя.jpg**;
6. Пошук сторінок з аплетом: **applet: імя апплета**.

Рекомендації щодо формування запитів

В якості ключових слів у запиті треба використовувати слово або словосполучення, яке найточніше характеризує об'єкт пошуку.

Не потрібно використовувати слова, які часто зустрічаються, типу "**Internet**", "**web**", "**програма**", бо можливий результат пошуку може бути дуже великим.

Для областей знань, де термінологія ще не встоялася (наприклад, в області комп'ютерних технологій), можна використовувати слова-синоніми, з'єднуючи їх логічною операцією OR.

При недостатньому числі результатів пошуку можна варіювати ключовими словами "бігати", "біжить", "пробіг" або використовувати символи-джокери "біг*".

Область пошуку

Більшість пошукових систем (Yahoo, AltaVista і інші.) дозволяють перед виконанням запиту уточнити область за тематичним каталогом категорій. Для цього треба спочатку вибрати одну або декілька категорій, а потім виконати запит. Існує можливість вибору мови, місця пошуку (Internet, UseNet, і т.д.), держави або домену. Можливо задати часові межі для дати останнього оновлення інформації про об'єкти, які шукаємо.

Управління процесом пошуку

Зазвичай, процес пошуку являється циклічною процедурою, яка складається з послідовних запитів на уточнення запиту та перегляду інформації, що знайдена. Якщо знайдене посилання, яке максимально задовольняє мету пошуку, то доцільно виконати пошук подібних документів за допомогою кнопки **More like this**.

Стратегія пошуку індивідуальна, але корисно враховувати певні практичні рекомендації.

Починати пошук слід із пошукових серверів, які є спеціальними в даній області (тематиці). Першим об'єктом пошуку можуть бути огляди посилань, які регулярно розробляють користувачі Internet. Має рацію пошук, у першу чергу, документів за часто наведеними питаннями FAQ (Frequently Asked Questions) за якоюсь темою. В таких випадках перший запит на пошук повинен містити фрази типу "**Поиск ...**", "**Обзор ...**" або "**FAQ ...**".

Якщо використання пошукових серверів не приводить до результату, то доцільно використовувати сервери організацій (університетів, видавництв, фірм), які працюють у даній області. За допомогою контактів з указаними організаціями можливо отримати інформацію, яка не представлена в Internet (рекламні матеріали, копії публікацій, безкоштовні CD і т.п.).

Якщо необхідно мати швидкий доступ до Web-сторінок, то посилання на них тримають у каталогах "Избранное", копіюючи адреси сторінок. Виклик Web-сторінки проводиться подвійним натиском основної клавіші маніпулятору "миша" на відповідній адресі.

Результати пошуку

Пошуковий сервер у результаті виконання запиту виводить загальну кількість знайдених об'єктів та список їх анотацій. Кожний об'єкт в анотації описується заголовком або назвою об'єкта, адресою ресурсу, де розташований об'єкт, коротким описом та характеристиками.

Характеристиками є розмір, дата знаходження об'єкта в мережі та ступінь відповідності запиту, виражений у відсотках (%) або в кількості використаних ключових слів.

Можна управляти об'ємом інформації в анотації, порядком анотацій у списку й числом анотацій на сторінці. Якщо список великий, то найважливішим параметром є порядок. Можливі наступні варіанти умов сортування результатів пошуку з використанням заданих ключових слів у документі:

1. ключові слова в заголовку Web-сторінки;
2. ключові слова в списку ключових слів Web-сторінки (тег <META>);
3. довжина й дата документа.

Обмеження доступу

1. Використання властивостей оглядача.

Увести команду **Свойства** з меню **Сервис**, вибрати вкладку **Безопасность** та рівень безпеки, увівши команду **Другой**. У діалоговому вікні встановити відповідні налагодження.

2. Установлення фільтрів.

Увести команду **Свойства** з меню **Сервис**, вибрати вкладку **Содежание** натиснути кнопку **Включить**. Відібрати потрібну категорію, наприклад, **Насилие**, використати повзунок для фільтрації вказаної категорії. Положення повзунка зліва – найменша можливість перегляду й справа – найбільша.

Програма електронної пошти OUTLOOK EXPRESS

Програма виконує функції звичайної пошти. Електронний лист може містити, окрім тексту, графічні й звукові файли (вкладення).

У 1971 році Рей Томлінсон (Ray Tomlinson), програміст із комп'ютерної фірми Bolt Beranek and Newman, розробляє систему електронної пошти й пропонує використовувати значок @ (по-англійськи at).

Налагоджування Outlook Express

Щоб почати настроювання Outlook Express, досить клацнути по значку **Запустити Outlook Express** (рис. 3.20) на панелі задач Windows. Інакше програму Outlook Express можна викликати за допомогою послідовності меню **Пуск→Програми→Internet Explorer→Outlook Express.**

Зауваження. Можливо, за якимись причинами додаток Outlook Express не встановлений на комп'ютері, але це можна легко виправити, вибравши за допомогою послідовності меню

Рис. 3.20. Запуск Outlook Express

Пуск→Настроювання→Панель керування→Установка і видалення програм, закладку **Установка Windows** і встановивши прапорець біля **Microsoft Outlook Express**. Оскільки це стандартна операція установлення нових програмних модулів зі складу Windows, ми не будемо на ній зупинятися.

Власне, початковий процес настроювання Outlook Express, необхідний для функціонування сервісу електронної пошти, гранично простий, – при першому виклику програми Outlook Express ще раз запускається **Майстер підключення до Інтернету**, він запросить необхідні дані про поштові сервери й адресу електронної пошти, яку треба одержати від провайдера.

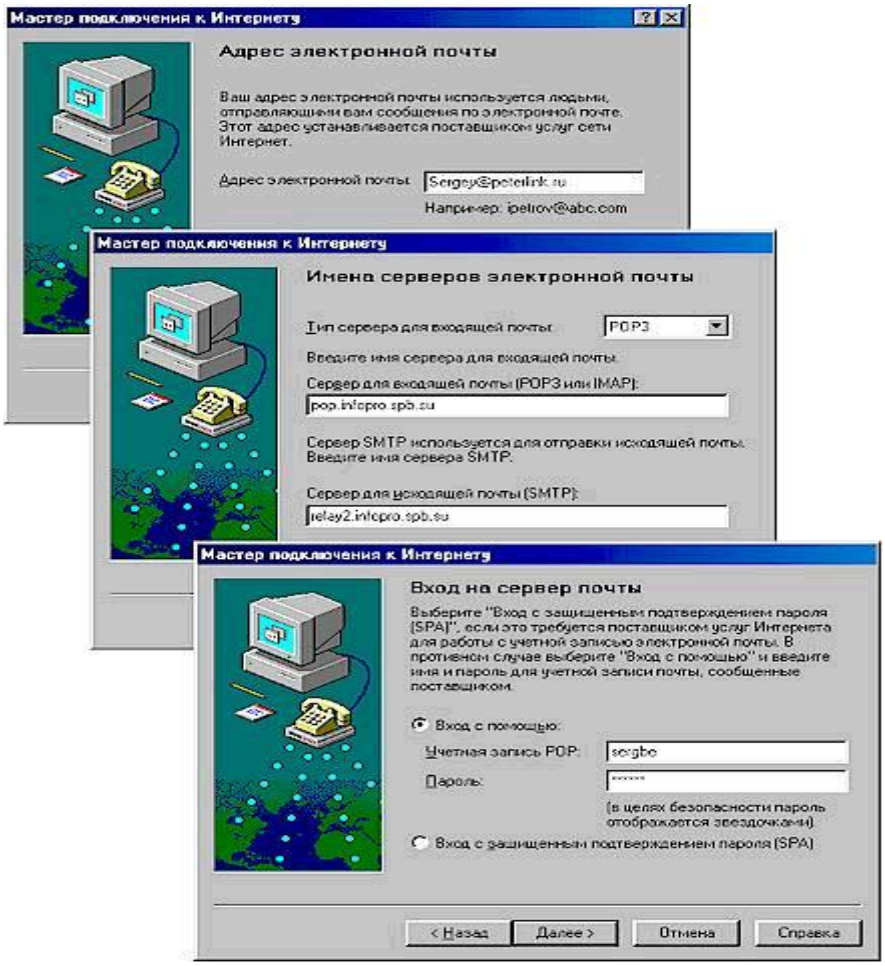


Рис. 3.21. Підключення до Internet

У першому вікні треба буде ввести ім’я абонента електронної пошти, що буде з’являтися в заголовку листів, коли вони прийдуть до адресатів. Зазвичай, користувачі вказують своє дійсне ім’я, але тут можна виявити гнучкість, і якщо поки не планується використовувати свою адресу для ділової кореспонденції, то можна обійтися й псевдонімом. Крім того, можна рекомендувати записувати ім’я латинським шрифтом, щоб уникнути проблем неправильного відображення заголовків із російським шрифтом у ряді програм електронної пошти, так і не створювати зайвих проблем можливим закордонним адресатам. Згодом, до речі, зазначене в цьому вікні ім’я можна буде легко змінити із псевдо
німа на дійсне ім’я й навпаки, якщо в цьому виникне необхідність.

У наступному вікні треба буде ввести адресу електронної пошти. Як правило, адреса E-mail складається з імені й доменного імені провайдера, з’єднаних за допомогою знака @. Приміром, це може бути адреса виду user@peterlink.ua. Коли будете називати свою адресу кому-небудь уголос, то знак @ вимовляється як «ет».

Далі **Майстер** запросить (рис. 3.21) тип сервера вхідної пошти і доменні імена поштових серверів провайдера, призначених, відповідно, для вхідної (**POP3**) і вихідної пошти (**SMTP**). Уведіть ці адреси. У випадку нашого прикладу з Peterlink це будуть адреси pop.infopro.spb.su і relay2.infopro.spb.su, відповідно. Наявність різних поштових серверів пов’язана з тим, що повідомлення електронної пошти пересилаються між вузлами Інтернету (вузлами різних провайдерів) за протоколом SMTP (Simple Mail Transfer Protocol), а на останньому відрізку між вузлом вашого провайдера й вашим комп’ютером – за POP (Post Office Protocol). Уведіть, як показано на рис. 3.21, параметри програми у відповідних полях діалогово-

го вікна отримані від провайдера адреси поштових серверів. Якщо провайдер спеціально не вказав тип сервера вхідної пошти, то, за замовчуванням, залишіть POP3.

Тепер у новому вікні вкажіть параметри облікового запису з'єднання – ім'я користувача й пароль. Це ті ж самі параметри, що звичайно використовуються для підключення до Інтернету. У даному випадку ці параметри потрібні для того, щоб програма Outlook Express могла автоматично додзвонюватися до провайдера й установлювати з'єднання для відправлення й приймання електронних листів. У наступному вікні буде запропоновано ввести «дружнє ім'я» для даного облікового запису пошти. Можете ввести що-небудь типу "Моя пошта на Kyivlink" чи залишити той запис, що пропонується за замовчуванням.

У черговому вікні вкажіть тип з'єднання, для нашого випадку – це з'єднання за модемом, хоча якщо користуєтесь Outlook Express в офісі, то там можна використовувати й підключення через локальну мережу. Ці з'єднання будуть установлюватися автоматично, але можна вибрати й третє значення перемикача, що пропонує вручну з'єднуватися із провайдером перед кожним сеансом роботи з електронної пошти.

Тепер залишилися два останніх вікна – в одному треба вибрати обліковий запис (якщо усього один провайдер, то й вибір, відповідно, буде невеликий), але сьогодні поширена ситуація, коли користувач має облікові записи в декількох провайдерів і ще обліковий запис для модемного доступу до локальної мережі своєї компанії. І, нарешті, залишилося те вікно, де потрібно підтвердити дані, введені в попередніх вікнах, клацнувши по кнопці **Готово** (Finish). Після натискання кнопки **Готово Майстер підключення до Інтернету** завершить процес настроювання Outlook Express.

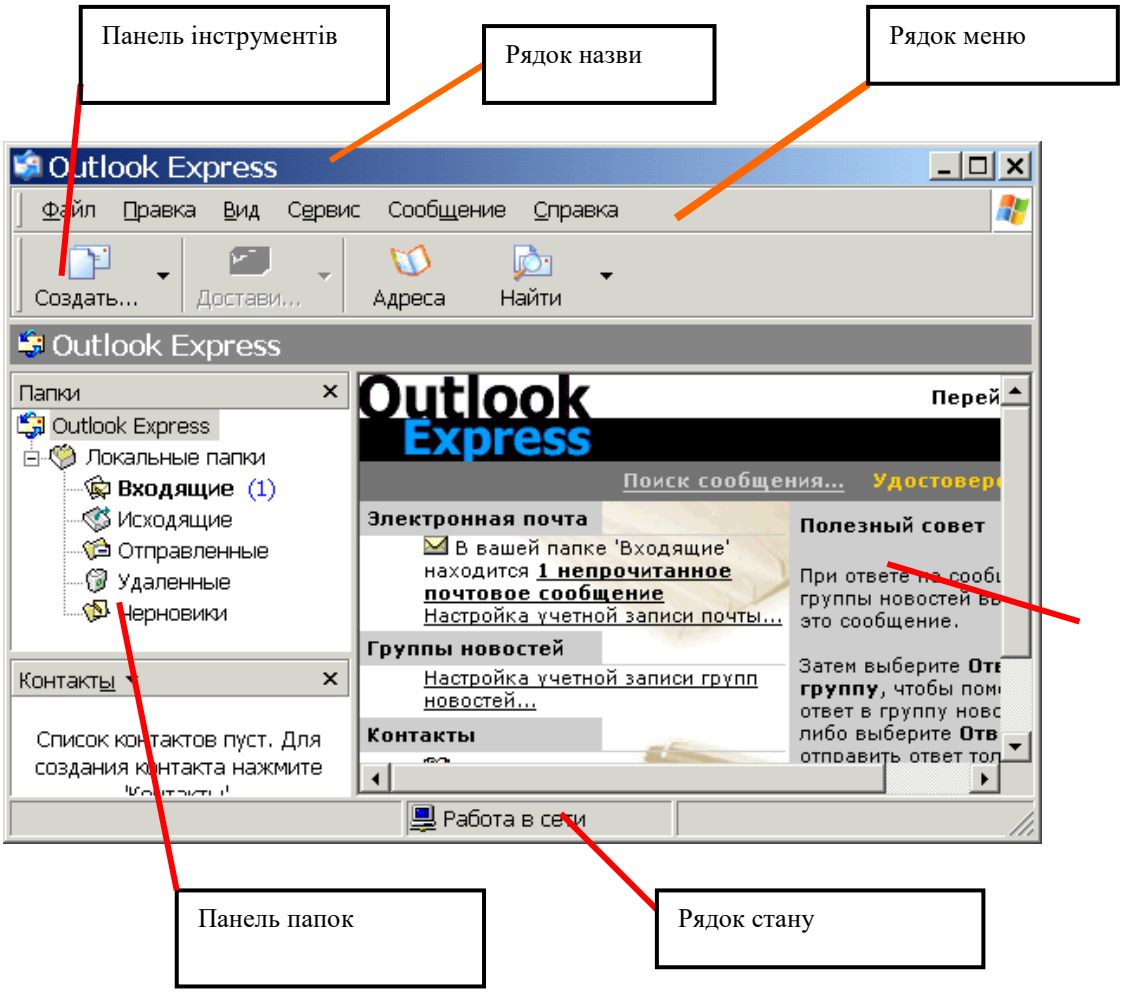


Рис. 3.22. Вікно програми

Інтерфейс користувача пошти Outlook Express

Давайте познайомимося з інтерфейсом Outlook Express, звернувшись до рис. 3.22.

- *Рядок заголовка* (title bar) містить стандартні назви.
- *Елементи вікна* Windows-додатка (кнопки Згорнути, Відновити й Закрити). У цьому рядку також зазначена назва додатка (Outlook Express).

• *Рядок меню* (menu bar) містить заголовки меню, що надають доступ до всіх функцій, необхідних для роботи з Outlook Express. За допомогою меню можна формувати нові повідомлення, відправляти й одержувати пошту, пересилати листа іншим користувачам, набудовувати інтерфейс Outlook Express і т.д. Крім того, в меню є безліч звичайних пунктів, характерних для всіх додатків Windows: друк, довідка й т.д. З рядка меню так само можливо викликати Internet Explorer і завантажувати для перегляду сторінки Web.

• *Панель інструментів* (toolbar) призначена для швидкого доступу до деяких найчастіше використовуваних команд Outlook Express. У залежності від того, у якому режимі працює Outlook Express (пошта чи новини), число кнопок і їхнє призначення автоматично змінюються. Крім того, у початковий момент після завантаження Outlook Express встановлюється в загальний режим (коли ще не обраний потрібний режим – пошта чи новини). У такому загальному режимі кнопки панелі інструментів виконують наступні функції:

• *Створити повідомлення* (Compose message) – відкриває вікно для формування нового листа.

• *Доставити пошту* (Send and Receive) – за допомогою цієї кнопки можливо швидко й легко підключитися до провайдера, щоб перевірити й доставити вхідну пошту, а так само відправити вашу власну.

• *Адресна книга* (Address Book) – відкриває доступ до адресної книги, куди записуються для збереження адреси e-mail ваших друзів, колег із роботи й т.д.

• *З'єднати* (Connect) – натискання на цю кнопку активізує процес з'єднання із провайдером.

• *Розірвати з'єднання* (Hang Up) – розриває з'єднання із провайдером Інтернету.

• Панель *Папки* (Folders) дозволяє вивести на екран списки листів і їхній уміст, що зберігаються в одній з 4-х стандартних папок Outlook Express: Вхідні (Inbox), Вихідні (Outbox), Відправлені (Sent Items), Видалені (Deleted Items) і Чернетки (Drafts). Outlook Express дозволяє завести нові додаткові папки користувача, і вони так само будуть доступні із цієї панелі. Якщо налаштувати доступ до серверів новин, то в цій панелі з'являться й імена відповідних серверів новин.

• *Область перегляду* Outlook Express при роботі з електронною поштою чи новинами розділена на дві частини: угорі можливо бачити список повідомлень електронної пошти з поточної папки, а в нижній частині вікна показується вміст відзначеного листа. Уміст листа можна подивитися й в окремому вікні, якщо зробити подвійне клацання по рядку з обраним листом. Область перегляду може бути розділена горизонтально або вертикально – якщо такий спосіб організації інтерфейсу здасться зручнішим. За замовчуванням усі листи в папках розташовуються відповідно до алфавітного порядку імен відправників, але їх можна відсортувати й інакше, наприклад, за датою надходження листа.

Кілька слів про те, як інтерпретуються значки з різними зображеннями конверта в області перегляду:

• *Відкритий конверт* позначає вже прочитаний лист.

• *Закритий конверт* та жирний шрифт позначають лист, який ще не читали.

• *Скріпка в листах* говорить про те, що в лист вкладений окремий файл (наприклад, документ у форматі Word, графічний файл і т.д.). Якщо виділити такий лист і клацнути по зображенню скріпки в правому куті нижньої частини вікна, то буде показане ім'я файлу. Подвійне клацання по імені вкладеного файлу дозволить переглянути його вміст за допомогою відповідної програми.

• *Рядок стану* (status bar) використовується для двох цілей. Зазвичай, у ньому Outlook Express указує загальну кількість повідомлень у даній папці й окремо – кількість непрочитаних повідомлень. У правій частині рядка стану при перевірці надходження нової пошти з'являється напис, що інформує про надходження чи, навпаки, відсутність нових листів. Крім того, при роботі Outlook Express, там з'являються значки, що характеризують режим роботи цього додатка в даний момент часу (наприклад, закреслений значок мережевого диска означає, що в цей момент немає з'єднання з Інтернетом).

• *Порада*. Щоб зберегти місце на екрані, можна порадити відразу ж відключити дві панелі – найлівіший стовпчик зі значками папок (тому що його вміст повторюється лівіше) і сірий рядок із написом Outlook Express над областю перегляду (він не несе функціонального навантаження). Для цього виберіть у меню *Вид* (View) пункт *Розкладка*. Повторний вибір цього

пункту меню відновлює ці панелі. Можна ще порадити встановити в нижній частині області перегляду Outlook Express прапорець *Переходити в папку «Вхідні» при запуску* (When starting, go directly to my Inbox folder). Тоді відразу після запуску Outlook Express буде переходити до папки «Вхідні», що дозволить швидше приступити до читання нових листів.

Формування нового повідомлення

- Для створення нового повідомлення натисніть на кнопку **Створити повідомлення (Compose Message)** на панелі інструментів Outlook Express, або подати команду **Почтовое сообщение** із підменю **Создать** підменю **Файл**, що викликає окреме вікно. Роботу з новим листом варто почати із заповнення заголовка листа, що має поля: **Кому: (To:), Копія:(Cc:), Схована: (Bcc:) ,Тема: (Subject:)**. Відмітимо, що обов'язковим є заповнення тільки поля **Кому: Кому: (To:)** (рис. 3.23) – так само, як і на звичайному конверті, у цьому полі треба ввести адресу – у даному випадку адресу електронної пошти вашого адресата. Можна не вводити адресу вручну, а вибрати його з адресної книги, якщо занесли його туди заздалегідь.
- **Копія: (Cc:)** – якщо потрібно, щоб аналогічний лист надійшов й іншим адресатам, уведіть потрібні адреси в даному полі, розділяючи їх за допомогою знака «;» (крапка з комою). Абревіатура «Cc» – це скорочення від англійського «канцелярського» терміна Carbon Copy («копірка»). Усі люди, до яких прийшов даний лист, легко зможуть довідатися із заголовка, кому ще надісланий даний лист. Цей рядок також може бути заповнений з адресної книги.

(To:) – інакше лист просто не знайде свого адресата. Розглянемо докладніше елементи заголовка:

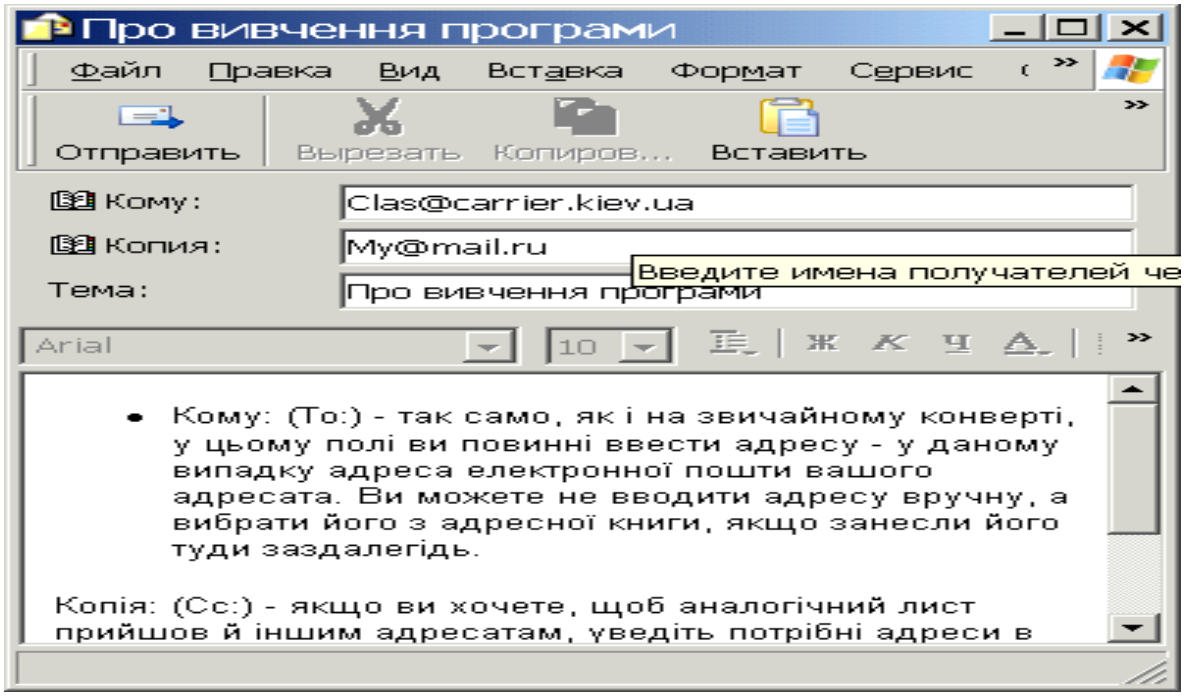


Рис. 3.23. Формування нового повідомлення

- **Схована: (Bcc:)** – якщо потрібно, щоб аналогічний лист прийшов й іншим адресатам, але вони не знали, кому ще відісланий даний лист, то введіть потрібні адреси в даному полі, розділяючи їх за допомогою знака «;» (крапка з комою). Абревіатура «Bcc» – це скорочення від англійського Blind Carbon Copy (що можна було б перекласти як «сліпа копірка»). Цей рядок також може бути заповнений з адресної книги.
- **Тема: (Subject:)** – тут варто вписати кілька слів, що характеризують тему повідомлення. Заголовок краще писати англійською, якщо поштова програма вашого адресата підтримує 8-бітове кодування заголовків і на його машині інстальовані шрифти кирилиці. Крім того, часто ушкоджується тип кодування українських заголовків при пересиланні між різними провайдерами.

Примітка. Зверніть увагу на те, що Outlook Express підказує призначення кожного незаповненого поля за допомогою напису сірого кольору чи пояснення. Після заповнення заголовка листа спочатку можете скористатися кнопкою на панелі інструментів вікна **Перевірити імена (Check Names)**, щоб бути впевненим у правильній відповідності введених адрес того фо-

рмату, що передбачений в Інтернеті для повідомлень E-mail, наприклад, user@host.domain, де user – ім'я адресата, host.domain – доменне ім'я поштового сервера адресата).

Далі вже можна приступати до самого листа, для чого клацніть курсором миші в поле листа й уведіть потрібний текст. При необхідності потрібно «прикріпити» до листа файл будь-якого формату. За традицією, завершує лист вставка підпису, для чого варто натиснути кнопку із зображенням авторучки на панелі інструментів (оригінальний і дотепний підпис – одна із традицій Інтернету). Якщо у Вас ще не створений підпис, то створити його можна, вибравши в меню **Сервіс (Tools)** пункт **Бланк повідомлень (Stationary)** і далі – натиснувши на кнопку **Підпис (Signature)**. Створений у такий спосіб підпис можна потім багаторазово використовувати. Зверніть ще увагу на зображення логотипа Internet Explorer (стилізованої букви е) у правій верхній частині нового повідомлення. Лого є ідентифікатором «важливості» повідомлення, що відправляється. У меню **Сервіс (Tools)** є пункт вибору важливості повідомлень, при натисканні на який буде виведений список можливих опцій важливості повідомлень (**Висока, Звичайна й Низька**). Тепер залишилося лише натиснути на кнопку відправлення листа (крайня ліва кнопка на панелі інструментів цього вікна із зображенням конверта, що летить, і написом **Відправити**) і ваш лист на шляху до адресата. Якщо встановлений прапорець **Відправляти повідомлення негайно** (**Send messages immediately...**) на вкладці **Відправлення** у вікні **Параметри**, то Outlook Express відразу ж з'єднається з провайдером і відправить лист. Якщо ж прапорець знятий, ваші листи будуть тимчасово знаходитись в папці **Вихідні (Outbox)**, де вони будуть накопичуватися перед відправленням. В останньому випадку на екран буде виведене повідомлення про переміщення листа в папку **Вихідні**. Коли завершите створення всіх листів, натисніть на кнопку **Доставити пошту (Send and Receive)** на панелі інструментів основного вікна Outlook Express, і далі процес з'єднання із провайдером відбудеться аналогічно тому, як ми розглянули вище.

Пересилання прикріплених файлів з допомогою електронної пошти

Можливість відправити електронною поштою файли будь-якого формату – дуже корисна властивість E-mail. Можна направити своїм адресатам і документ Word, і файл із потрібним зображенням, звукове чи відео-вітання та інші файли. Єдина умова – не посилати дуже великі файли, якщо немає упевненості в тому, що адресат має виділений канал в Інтернет, а, можливо, працює зі звичайною телефонною лінією. Для таких випадків файл розміром 200-300 Кб вважається межею «пристойності». Також треба мати на увазі, що деякі поштові сервери провайдерів просто повертають назад пошту, якщо її розмір перевищує певну межу (наприклад, більше 1 Мб).

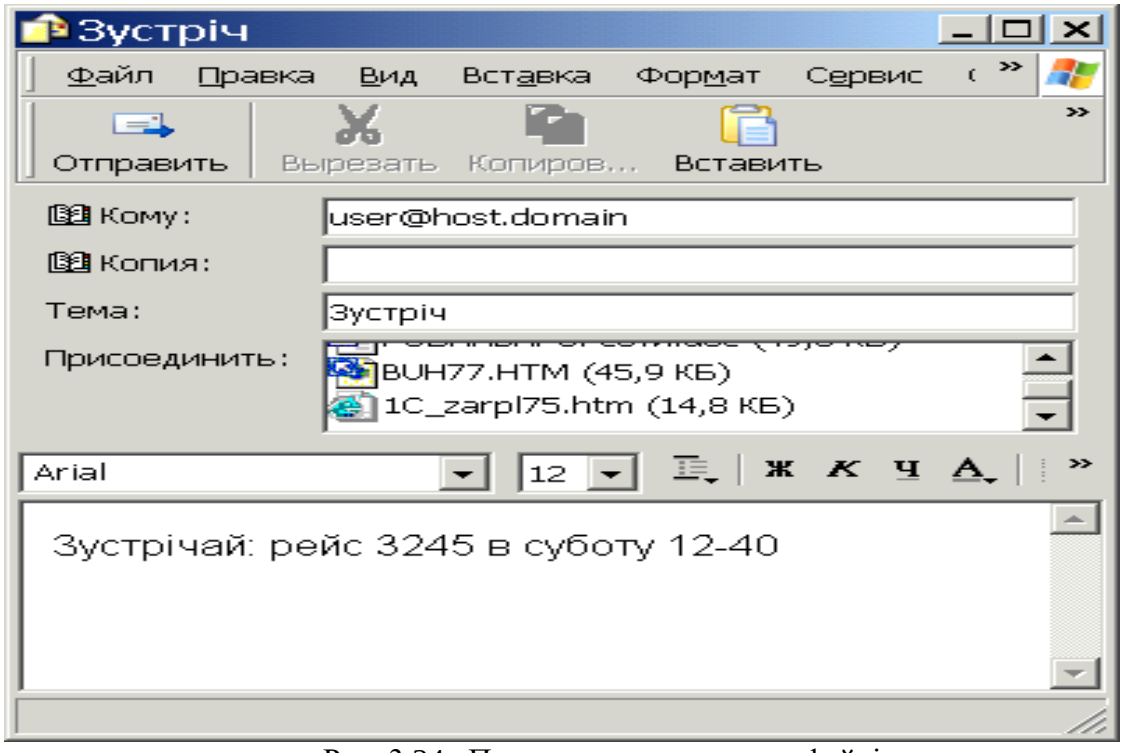


Рис. 3.24. Пересилання вкладених файлів

Отже, для вкладення файлу в лист, необхідно, розмістивши курсор у вікні для введення листа, натиснути кнопку із зображенням скріпки на панелі інструментів, або подати команду **Вложение файла** з підменю **Вставка**. У відповідь на екран буде виведене стандартне діалогове вікно із зображенням файлової структури вашого комп'ютера. Коли знайдете на диску потрібний файл, треба виділити його й натиснути кнопку **Вкласти** (**Attach**). Outlook Express прикріпить файл до електронного листа, і нижче тексту листа з'явиться додаткове вікно з позначкою прикріпленого файлу (рис. 3.24).

Варто нагадати, що аналогічним чином виглядають і листи, які прийшли, і мають вкладені файли. Досить двічі клацнути по значку із вкладеним файлом, як завдяки механізму OLE (Object Linking and Embedding) операційної системи Windows буде запущений відповідний додаток для перегляду цього файлу.

Поштові папки Outlook Express

Хоча назви поштових папок Outlook Express багато в чому говорять самі за себе, але якщо немає досвіду роботи з поштовими програмами, усе-таки варто познайомитися з їхнім призначенням:

- *Вхідні* (Inbox). Сюди, за замовчуванням, надходить уся нова пошта і тут зберігаються всі повідомлення, що прийшли. Згодом можна створити додаткові папки (наприклад, присвячені різним проектам чи листам від постійних адресатів) і налагодити Outlook Express таким чином, щоб при надходженні нових листів уся пошта автоматично розбиралася й складалася в окремі папки.
- *Вихідні* (Outbox). Ця папка призначена для тимчасового збереження листів, що відправляються. Навіщо це потрібно? Уявіть, що відбувається створення декількох листів один за одним. Щоб не з'єднуватися щораз з Інтернетом для відправлення чергового листа, листи тимчасово накопичуються в цій папці. Потім при натисканні на кнопку **Доставити пошту** (**Send and Reseive**) вони разом ідуть на поштовий сервер провайдера й далі – до своїх адресатів. Саме такий режим відправлення листів установлюється в Outlook Express за замовчуванням.
- *Відправлені* (Sent Items). Тут, за замовчуванням, зберігаються копії відправлених повідомлень, тому завжди можна згадати кому, коли і які листи надіслані.
- *Видалені* (Deleted Items). Якщо потрібно видалити непотрібні повідомлення, то вони тимчасово поміщаються на збереження в цю папку (на випадок, якщо не потрібно їх видаляти). Якщо потрібно назовсім видалити повідомлення із цієї папки, клацніть правою клавішею по значку папки й із меню виберіть пункт **Очистити папку** (**Empty folder**).
- *Чернетки* (Drafts). Якщо готується новий лист, але виявилось, що його потрібно дописати лист, то виберіть у меню **Файл** (**File**) пункт **Зберегти** (**Save**). Такий «недописаний» лист тимчасово зберігається в папці **Чернетки** (**Drafts**). Щоб продовжити згодом роботу над листом із цієї папки, просто відкрийте цю папку й двічі клацніть по чернетці листа. Потім, якщо лист готовий, то його можна відправити й він буде поміщено в папку **Вихідні** (**Outbox**). Якщо ж лист, як і раніше, не готовий до відправлення, то його знову можна зберегти в папці чернеток.

Одержання вхідної пошти

Одержання вхідної пошти – це, напевно, найпростіша дія з усього спектра робіт з Outlook Express, уся функціональність якого полягає в тому, що треба встановити з'єднання з поштовим сервером провайдера. Тому досить запустити програму Outlook Express, що за замовчуванням відразу запропонує з'єднатися із сервером провайдера. Якщо з'єднання із провайдером уже встановлено, то досить, вибравши назву з'єднання, натиснути кнопку **ОК**. Інакше з'явиться додаткове вікно, де треба буде ввести ім'я користувача й пароль. У будь-якому випадку підсумок буде один – комп'ютер почне встановлювати з'єднання з поштовим сервером провайдера.

Після того як модем здійснить з'єднання, з'явиться вікно, у якому Outlook Express буде перевіряти наявність листів, що прийшли, і здійснювати їхнє завантаження на комп'ютер. Після завершення цієї дії поштова програма перевірить, чи немає у папці **Вихідні** (**Outbox**) готових листів для відправлення, і якщо є, то у свою чергу, перешле їх на поштовий сервер провайдера, звідки вони вже підуть адресатам.

Порада. Outlook Express дозволяє встановлювати сеанс зв'язку із провайдером тільки на час доставки листів (одержання листів, що прийшли, і відправлення своїх), відразу ж відключаючись від Інтернету після завершення передавання. Щоб увімкнути цю опцію, потрібно встановити прапорець **Розірвати з'єднання за завершенням доставки** (**Disconnect**...) на вкладці

Віддалений зв'язок (**Connection**) вікна властивостей прямо у вікні. Тим самим уникаються нераціональні витрати часу.

Адресна книга Outlook Express

Адресна книга – це збірник адрес e-mail ваших колег за електронним переписуванням, організований за допомогою зручної програмної оболонки. Адресна книга в програмі Outlook Express являє собою запозичену копію адресної книги з корпоративної поштової програми MS Exchange. Крім експорту адрес з MS Exchange, у Outlook Express можна також експортувати адреси з цілого ряду інших поштових програм: MS Internet Mail, Eudora Pro, Eudora Light, а також із цілого ряду поштових клієнтів Netscape різних версій. Заповнювати адресну книгу Outlook Express можна у двох режимах: по-перше, витратити спочатку якийсь час і заздалегідь увести дані про ваших колег, та, по-друге, поповнювати адресну книгу «на льоту», у міру роботи з поштою, просто копіюючи туди адреси листів, що прийшли. Нижче ми розглянемо ці два випадки.

1. Якщо потрібно заповнити адресну книгу заздалегідь, натисніть кнопку **Адресна книга**, або введіть команду **Адресная книга** в меню **Сервис**, що викликає появу головного вікна цього збірника адрес і іншої контактної інформації (рис. 3.25).

Крім імен і адрес E-mail в адресній книзі можна зберігати безліч різної інформації: номери телефонів, пейджерів, особистих і службових сторінок Web, звичайну поштову адресу абонента й ін. Для того щоб внести в адресну книгу нове ім'я, натисніть кнопку **Створити адресу (New Contact),** або введіть команду **Создать контакт** в меню **Файл**. Уведіть у відповідних полях ім'я абонента й адресу його електронної пошти, при бажанні можете заповнити додаткові дані на абонента на інших закладках. Якщо потрібно відредагувати адресу електронної пошти чи інший параметр, то виберіть ім'я в адресній книзі й, натиснувши кнопку **Властивості** (**Properties**), змініть дані на закладках аналогічним чином.

2. Друга можливість: після того як адресна книга заведена й наповнена деякими адресами, надалі книгу можна поповнювати за рахунок адрес із листів, які прийшли. Для цього відкрийте потрібний лист, відзначте ім'я адресата в полі заголовка, натисніть праву клавішу миші і зі спливаючого контекстного меню виберіть пункт **Додати в адресну книгу (Add To Address Book).**

Тепер, коли адресна книга містить дані з адресами e-mail колег із переписки, ми коротенько розглянемо порядок роботи з нею при формуванні нових листів і заповненні поля **Кому**: (**To**:):

- Натисніть кнопку **Створити повідомлення (New Message)** в основному вікні Outlook Express, помістіть курсор у поле **Кому: (To:)** у вікні створення нового повідомлення.
- Клацніть по значку із зображенням відірваного листка папера поруч зі словом **Кому**. Ця дія викликає появу діалогового вікна, де можна легко вибрати одержувачів даного листа.
- Виберіть зі списку абонентів потрібну людину й натисніть кнопку **Кому: (To:)** у середній частині вікна.
- **Прихована копія** (**Bcc**:), якщо необхідно розіслати цей лист ще декільком адресатам.
- Натисніть кнопку **ОК**, і обрані адреси з'являться у відповідних полях заголовка нового листа.
- Тепер можна приступати до заповнення тіла листа і його відправлення, про що ми вже розповіли раніше.

Зауваження. Імена абонентів, введених у поле **Кому**: (**To**:), **Копія**: (**Cc**:), **Прихована**: (Bcc:) за допомогою адресної книги, можуть бути представлені у вікні іменами абонентів, а не їх електронними адресами. Не турбуйтеся, програма Outlook Express сама підставить адреси e-mail при відправленні повідомлення.

- Аналогічним чином додайте абонентів у полях **Копія**: (**Cc**:) чи **Прихована.**

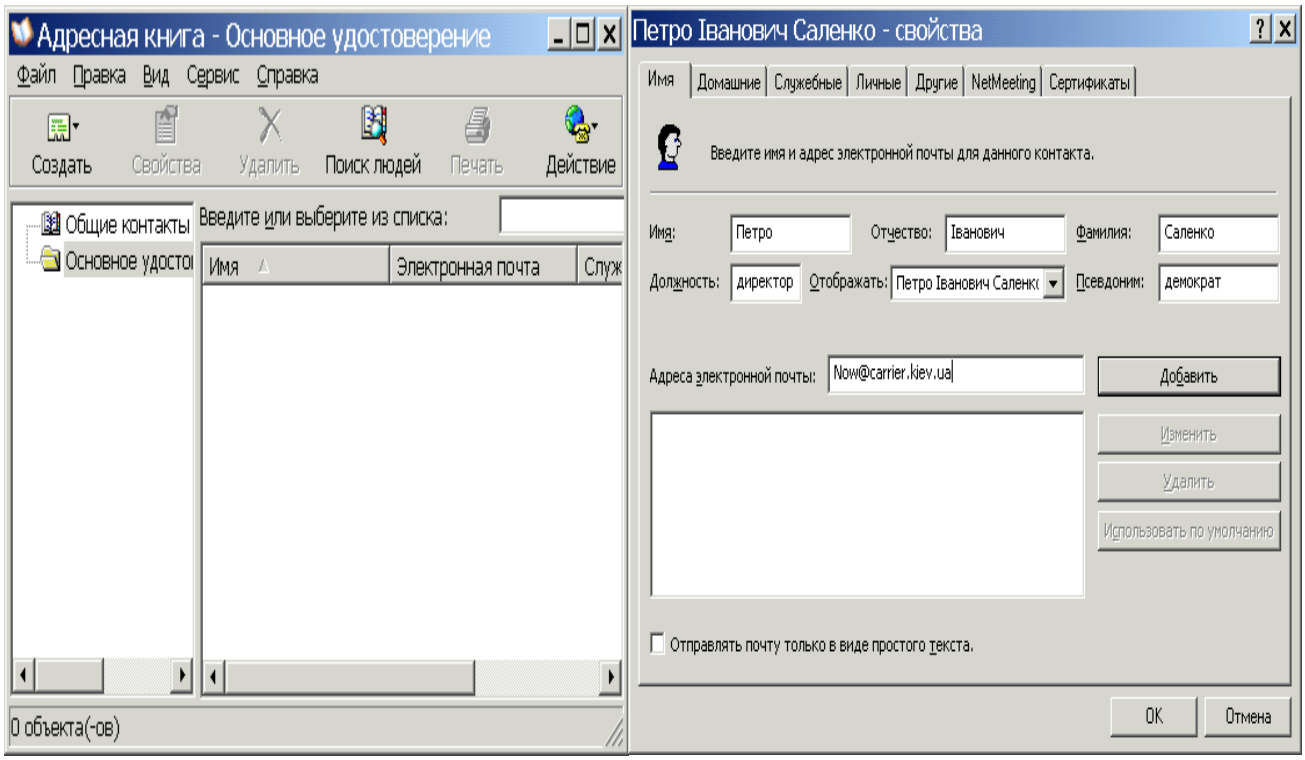


Рис. 3.25. Адресна книга

Ще одна опція, яку можна використовувати в адресній книзі Outlook Express, – це групові імена. Групові імена являють собою ваші особисті списки розсилання й зручні в тому випадку, якщо треба часто розсилати листа постійним групам людей (наприклад, учасникам якого-небудь проекту). Групові імена в Outlook Express створюються натисканням на кнопку **Створити групу** (**New Group**) на панелі значків адресної книги. Потім потрібно вказати ім'я групи, і скласти список людей у цій групі. Після того як створена група, потрібно використовувати ім'я групи в поле **Кому**: чи **Копія**: повідомлення, що відсилається, буде надіслане всім, хто входить у цю групу. Щоб відредагувати список членів групи і їхні адреси e-mail, треба вибрати (відзначити) уже існуючу групу й клацнути по кнопці **Властивості**.

Деякі додаткові можливості програми

1. *Відправлення сторінок на основі бланка повідомлень.* Оскільки Outlook Express уміє відправляти повідомлення у форматі HTML, то для таких повідомлень можна використовувати заздалегідь підготовлений бланк (шаблон HTML-сторінки) із фоновим малюнком. Разом з Outlook Express поставляються більше десятка стандартних бланків, що відповідають різним випадкам життя. Природно, що такий лист варто відправляти тільки тому одержувачу, хто також працює з Outlook Express чи іншою програмою, що вміє показувати повідомлення у форматі HTML. Для вибору бланка в меню **Повідомлення** вибрати пункт **Створити з використанням**.

2. *Пошук потрібного повідомлення в папках Outlook Express*. Якщо не вдається знайти потрібне повідомлення електронної пошти, то можна задіяти функцію пошуку по папках на основі шаблона. Щоб викликати вікно пошуку, натисніть на клавіатурі одночасно клавіші **CTRL+SHIFT+F.**

3. *Сортування повідомлень у папках Outlook Express*. Повідомлення в папках Outlook Express можна легко відсортувати в потрібному порядку (за алфавітом, за датою одержання й т.д.). Для цього виберіть у меню **Вид** пункт **Сортування**, і далі той вид сортування, що вважаєте потрібним.

4. *Робота з новинами*. Програма Outlook Express також може бути настроєна для читання новин. Виконати її налагодження дуже просто. Потрібно вибрати папку у вікні **Тек** (рис. 3.26), далі у діалоговому вікні (рис. 3.27), що з'явилося, вибрати групу новин, а потім клацнути на кнопці **Підписатися**. Можна при бажанні завжди відмовитися від підписки на цю групу новин, якщо в цьому ж вікні клацнути на кнопці **Відмовитися від підписки.**

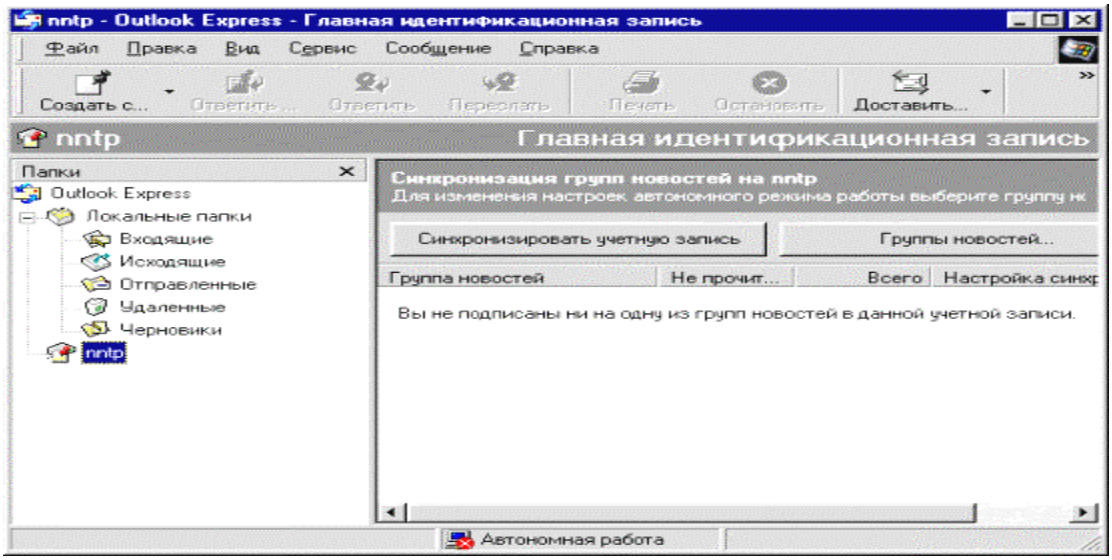


Рис. 3.26. Вікно каталогів

Робота з утилітою обміну файлами FTP.

Протокол FTP (File Transfer Protocol – протокол передавання файлів) призначений для передавання файлів між машинами без установлення дистанційного з'єднання між ними (без використовування Telnet). З його допомогою можна передавати файли, працювати з каталогами й користуватися електронною поштою, але він не дозволяє запускати програми на віддаленій ЕОМ.

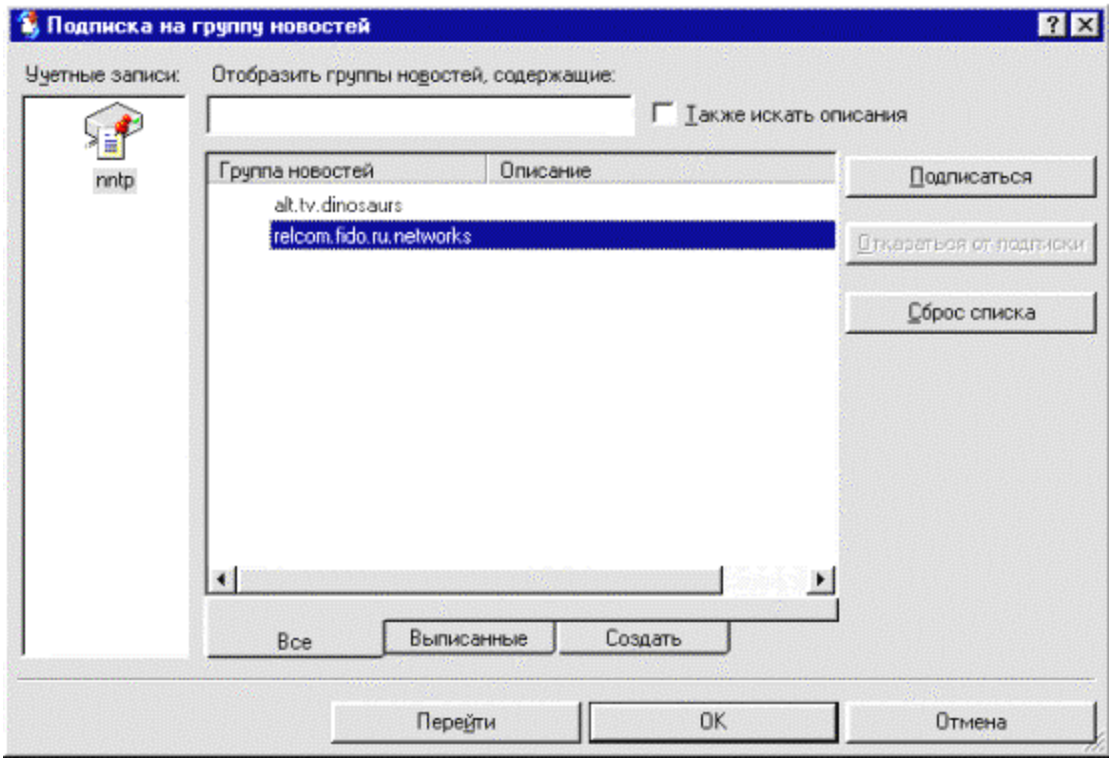


Рис. 3.27. Вікно відбору новин

Для своєї роботи FTP використовує транспортний протокол TCP, але зв'язок по FTP підтримується за допомогою двох з'єднань: за одним з них передаються команди FTP, а за іншим – дані. Тому програмна реалізація FTP припускає роботу двох процесів на кожній із взаємодіючих машин. Перший із них відповідає за передавання команд і називається **протокольним інтерпретатором** (PI – protocol interpreter), а другий – за передавання даних і називається **процесом передавання даних** (DTP – data transfer process). Протокол TCP забезпечує встановлення розірваних з'єднань і надійність передавання даних. На віддаленій ЕОМ (сервері) процесу передавання даних відповідає порт 20, а протокольному інтерпретатору – порт 21.

Також як і протокол Telnet, протокол FTP використовує для своєї роботи спеціальні внутрішні команди. Ці команди можуть використовуватися спеціалізованим програмним забез-

печенням і адміністратором системи, але звичайному користувачу вони, як правило, недоступні. Користувачі для роботи із протоколом FTP використовують сервісні утиліти. В ОС типу UNIX для обслуговування запитів за FTP на віддаленій машині запускається процес ftpd (FTP daemon), в інших ОС для цього можуть використовуватися інші процеси, що надають аналогічний сервіс. На локальній ЕОМ (клієнті) може виконуватися будь-який призначений для користувача додаток, що забезпечує з'єднання за FTP. У даний час розроблена велика кількість програм, що забезпечують роботу із цим протоколом, у тому числі й програми з розвиненим графічним інтерфейсом під ОС і графічні оболонки типу MS Windows 3.11, MS Windows NT, UNIX (X Window). Але широко відома найпростіша утиліта, яка носить ту ж назву, що і протокол – ftp. Вона має тривіальний командний інтерфейс, аналогічний інтерфейсу утиліти telnet.

Загальні принципи роботи з утилітою ftp.

Так як і при роботі з утилітою telnet, при запусканні утиліти ftp вимагається вказати ім'я або IP-адресу віддаленої машини, з якою потрібно встановити з'єднання. Якщо ця адреса не вказана, то ftp переходить у командний режим без установлення з'єднання. Тоді для початку сеансу зв'язку треба скористатися командою *open*. Після того як з'єднання встановлено, необхідно пройти авторизацію доступу, для чого необхідно ввести ім'я й пароль користувача. У більшості систем право доступу мають тільки зареєстровані користувачі, але іноді допускається так званий «анонімний» вхід, який буде розглянутий далі. Як і при роботі з telnet, при роботі з ftp ім'я й права користувача визначаються на віддаленій, а не локальній ЕОМ (в загальному випадку імена користувача на сервері й клієнті можуть бути різні). Для роботи з каталогами користувач повинен мати свої права копіювання і видалення файлів із віддаленої машини, інакше ці команди виконуватися не будуть.

Слід звернути увагу, що й після встановлення з'єднання з віддаленою ЕОМ, усі команди користувача ftp виконуються щодо локальної ЕОМ, на відміну від telnet. Особливо акуратно слід виконувати команди копіювання файлів, щоб не втратити вміст потрібних файлів на машині-клієнті.

Протокол FTP дозволяє передавати файли в декількох форматах, які в загальному випадку системнозалежні. У більшості систем (включаючи UNIX і Windows NT) визначено два режими передавання файлів - текстові й двійкові. Текстовий файл складається з рядків ASCII-символів, розділених кодами закінчення рядка й повернення каретки, при його передаванні виконуються дії перекодування символів. Для двійкових файлів не передбачено ніякого певного формату й ніякого перекодування, їх передавання здійснюється швидше. Типовий сеанс роботи з ftp включає наступні етапи:

- запуск утиліти, установлення з'єднання з віддаленою ЕОМ;
- перехід у необхідний каталог на віддаленій ЕОМ (сервері);
- вибір режиму передавання файлів;
- передавання даних згідно команд користувача;
- завершення роботи, розрив з'єднання.

Ці процедури виконуються послідовно в кожному сеансі. Найпоширеніші команди користувача в утиліті ftp приведені в табл. 3.8.

Таблиця 3.8.

Деякі команди утиліти ftp

Команда	Параметри	Опис
ascii		Перемкнутися в режим передавання текстових файлів
binary		Перемкнутися в режим передавання двійкових файлів
cd	ім'я каталога	Змінити робочий каталог на віддаленій ЕОМ
close		Закрити з'єднання з віддаленою ЕОМ
del	ім'я файлу	Видалити файл на віддаленій ЕОМ
dir	маска файлів	Відобразити вміст поточного каталога серверу
get	ім'я файлу	Одержати файл з віддаленої ЕОМ
hash	on/off	Увімкнути або вимкнути режим знаку "#" для кожного переданого блоку даних при передаванні файлів
help		Одержати підказку
lcd	ім'я каталога	Змінити робочий каталог на локальній ЕОМ
mget	маска файлів	Одержати декілька файлів з віддаленої ЕОМ
mput	маска файлів	Відправити декілька файлів на віддалену ЕОМ

open	адреса ЕОМ	Встановити з'єднання з вказаною ЕОМ
put	ім'я файлу	Передати файл на віддалену ЕОМ
pwd		Вивести ім'я поточного каталога
quote	команда	Передати команду безпосередньо FTP (для введення команд адміністратора)
quit		Завершити роботу з утилітою

Можливості роботи з FTP при анонімному доступі

Протокол FTP широко використовується для обміну даними в мережі Internet. Багато серверів мережі підтримують цей протокол. Оскільки кількість користувачів у цій мережі дуже велика, то задача виділення кожному з них індивідуальних прав доступу представляється абсолютно нереальною. У той же час, велике число серверів прагне надати послуги з обміну даними максимально можливій кількості клієнтів мережі. Наприклад, такі послуги надають серверам сервісних центрів фірм, що займаються розповсюдженням програмного забезпечення, яке вільно використовується й розповсюджується.

У таких випадках для встановлення з'єднання за протоколом FTP використовується метод анонімного доступу. У цьому варіанті як ім'я користувача використовується слово anonymous, а замість пароля – найчастіше слово guest (гість). Іноді для анонімного доступу може використовуватися й інші варіанти пароля: наприклад, слово ftp або адреса електронної пошти користувача (в останньому випадку доступ буде вже не таким анонімним, хоча, звичайно, ніхто не перевірить істинність введених користувачем даних).

При анонімному доступі користувач має, як правило, дуже обмежені права. Найчастіше при анонімному доступі користувач може тільки переміщатися в обмеженому перелікові каталогів і одержувати файли з віддаленої ЕОМ (виконувати команди get і mget).

Нижче наведено короткий перелік команд (табл. 3.9), необхідних для того, щоб переписати необхідний файл або файли при використанні FTP-клієнта з командним рядком. Якщо є бажання дізнатися решту команд, які потрібні для професійної роботи з FTP, то введіть help у Вашому FTP-клієнті. При роботі з графічним клієнтом, що підтримує сучасний інтерфейс, швидше за все, все буде зрозуміло без пояснень. Врахуйте, що в іменах файлів великі і маленькі букви розрізняються.

Таблиця 3.9

Команди необхідні для забезпечення процесу копіювання файлів

open ім'я_сервера – відкрити з'єднання	відкриває з'єднання з сервером. Це ім'я можна вказати відразу при введенні команди, що завантажує клієнта
cd ім'я_директорії – змінити каталог	здійснює перехід в інший робочий каталог на FTP-сервері
dir [ім'я_файла] – видати список файлів	видає список файлів в поточній директорії. Не забувайте, що можна використовувати шаблони групових операцій
get ім'я_файла [ім'я_локального_файла] – переписати файл	переписує файл з віддаленого комп'ютера на локальний. Якщо вказано ім'я локального файлу, то записує його під цим ім'ям, інакше – в каталог
mget [ім'я_файла] – переписати групу файлів	те ж саме, що і get, але дозволяється використовувати шаблони. Перед копіюванням кожного файлу запрошуватиметься підтвердження. Для відміни підтверджень введіть prompt
prompt	відміняє підтвердження в командах mget і mput
put ім'я_файла [ім'я_віддаленого_файла] – записати файл на сервер	переписує файл з локального комп'ютера на віддалений під ім'ям *ім'я_віддаленого_файла*. Якщо воно не вказане, то файл записується в поточний каталог з ім'ям локального файлу. Команда заборонена для анонімних користувачів
mput [ім'я_файла] – записати групу файлів	те ж саме, що і put, але дозволяється використовувати шаблони. Перед записом кожного файлу запрошува-

	тиметься підтвердження
ascii	встановлює ascii-спосіб передавання файлів. Використовується для пересилання файлів-текстів англійською мовою. Проте для надійності краще використовувати binary
binary	встановлює двійковий спосіб пересилання файлів. При цьому файл при передавання не перекодовується і записується в незміненому вигляді. Це найнадійніший спосіб передавання файлів
close	закриває з'єднання з даним сервером і проводить повернення в командний режим. Ця команда автоматично виконується при виході з FTP-клієнта.
quit	вихід з FTP-клієнта
user	реєструє на поточному сервері користувача з новим ім'ям. Використовуйте цю команду, якщо перший раз помилково неправильно ввели ім'я анонімного користувача і не хочете знову перенабирати команду open
lcd [ім'я_каталогу]	здійснює перехід на локальному комп'ютері у вказаний каталог
pwd	виводить на екран поточний каталог на віддаленому комп'ютері
system	виводить на екран тип операційної системи на віддаленому комп'ютері
help [FTP-команда] – допомога	видає коротку інформацію про команди FTP-клієнта або про конкретну команду

Метод анонімного доступу – це основний метод, який використовують для обміну даними за протоколом FTP програми мережі Internet, наприклад, широко поширені програми Internet Explorer і Netscape Navigator. Ці програми мають нагоду тільки одержувати файли з віддалених ЕОМ, у той час, як повний доступ за протоколом FTP дає користувачу також можливість передавати файли на віддалені ЕОМ. Ім'я й пароль для анонімного доступу в цих програмах можна налагоджувати.

Закачування файлів за допомогою програми Teleport Pro

Teleport Pro – це переглядач offline, має можливість віддзеркалювання вузла, автоматизований інструмент в Інтернеті, багатопотоковий web-павук. Він дозволяє повністю завантажити на комп'ютер весь web-вузол (з усіма каталогами, файлами та їх зв'язками), указані файли разом з їх зв'язками, або окремі файли при високих швидкостях виконання.

Програма дозволяє проводити пошук файлів та web-вузлів (можна задати глибину пошуку) за визначеними параметрами (назва, розширення, зміст, розмір, дата створення, тип зв'язків і т.п.).

Для використання teleport Pro, необхідно створити проектний файл, який містить один або більше звернення до файлів в Інтернеті, надати програмі деякі правила, які визначають які зв'язки треба відслідковувати і які файли відновлювати. Далі необхідно посилати павука з його місією за допомогою вибору **Стартової команди** в меню **Файл**, або **Стартової кнопки** на панелі інструментів. Одного разу активізований, teleport-павук прочитає ваш проект запуску адреси і відновить будь-які файли, які знайде там, потім прочитає всі зв'язки на сторінці, прослідує по тих зв'язках, одержить файли на тих сторінках, і т. д.

Teleport Pro використовує спеціальний пошуковий алгоритм, щоб швидко шукати мережеві сторінки, ідентифікувати й класифікувати їх зв'язки, а потім відновлювати всі відповідні типи файлів, які конкретизовані у вікні **Проектних Властивостей**.

Teleport Pro починає роботу із запуску адреси, він пам'ятає, що і де було, тому ніколи не відвідує того ж місця двічі, у межах того ж проектного сеансу. Можливе блокування користувачем відвідування якогось сайту.

Є чотири істотних кроки до запуску teleport Pro на виконання завдання:

1. Створення нового проекту.
2. Збереження проекту.

3. Запуск проекту.
4. Перегляд результатів.

Створення нового проекту

Щоб створити новий проект, треба ввести команду **Новий Проект** із меню **Файл**, або натиснути кнопку на панелі інструментів **Новий Проект** (досвідчений користувач може почати створювати новий проект із нуля, однак при цьому доведеться встановити й проектні властивості вручну).

Майстер нового проекту, який викликається командою **Мастер Нового Проекта** з меню **Файл** (рис. 3.28) за декілька кроків дозволить відібрати вказані властивості та автоматизує процес створення проекту.

Якщо вибрана можливість **Копировать вебсайт на диск проекта**, то на другому кроці роботи майстра (рис. 3.29) треба ввести адресу та ввести глибину пошуку. На третьому кроці (рис. 3.30) вибираються типи файлів та, за необхідності, вводиться пароль (необов'язково). Четвертий крок – заключний, тут підтверджується проект уведенням команди Finish. Після цього у вікні програми (рис. 3.31) з'явиться адреса проекту, якщо проектів декілька – список адрес.

Примітка: під час указаної роботи програма може дослідити тільки типи файлів за адресами HTTP і FTP.

Якщо вибрати команду **Копіювати веб-сайт із структурою каталогів** (рис. 3.32), то на комп'ютері зберігається копія сайту з деревом каталогів, зв'язками і т.п. Уся подальша робота аналогічна вищеописаній.

Команда **Пошук файлів визначеного типу** (рис. 3.33) дозволяє створити проект для проведення пошуку файлів визначеного типу в мережі Internet. Відбір файлів проводиться в третьому вікні майстра. Для вказівки типів файлів, які буде шукати програма, можна використовувати наступні групові імена: наприклад, *.cgi – відповідає будь-якому файлу, що має розширення cgi; bob* – boba.jpg, або навіть bobble; ???.jpg – star005.jpg або starting.jpg, але не star.jpg або starry.jpg.

Команда **Дослідити посилання із сайту** використовується в тому випадку, якщо необхідно створити проект для дослідження видів файлів, які містяться на сайтах, куди є посилання із сайту, який досліджується. При цьому проводиться зберігання не змісту файлів, а посилання на них, тобто ярликів. Це дозволяє економити час обстеження сайтів.

Команда **Отримати декілька файлів з адрес** дозволяє створити проект для дослідження наявності потрібних файлів за списком адрес.

Команда **Пошук за ключовими словами** дозволяє створити проект для пошуку та збереження інформації за ключовими словами, які вносяться в третьому вікні майстра проекту (рис. 3.33).

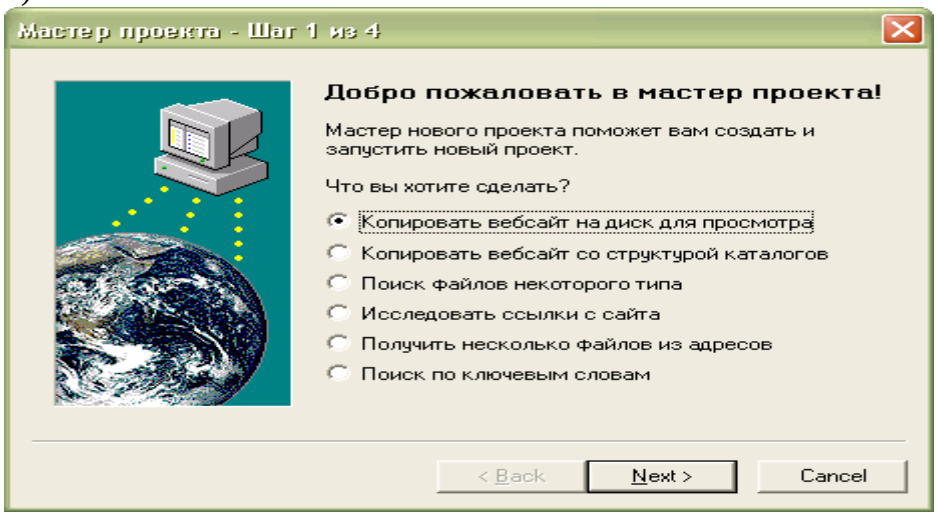


Рис. 3.28. Вікно майстра створення проекту.

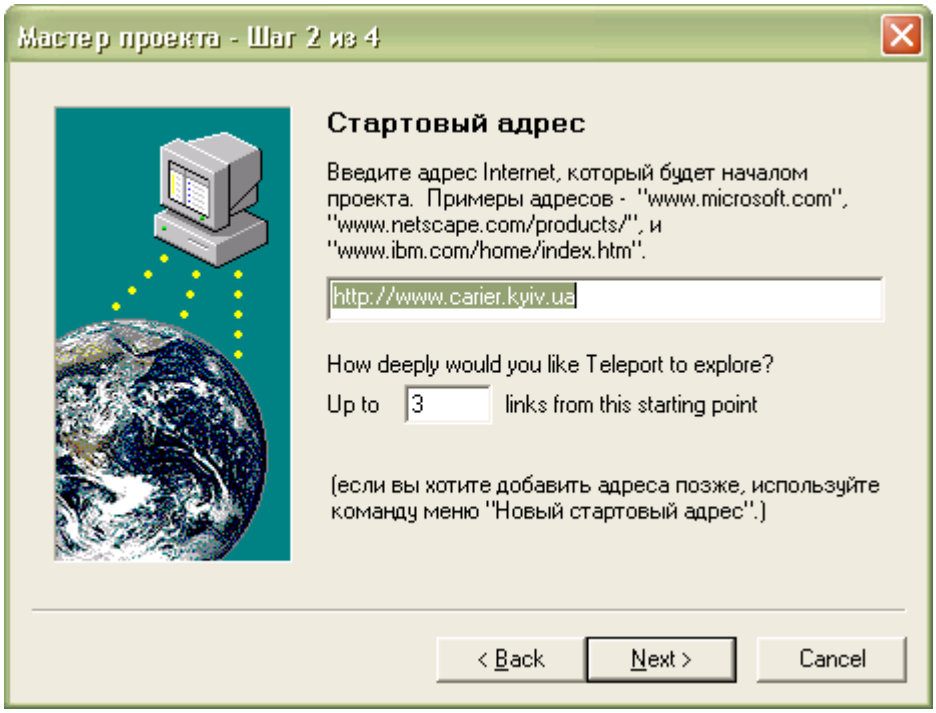


Рис. 3.29. Вікно введення адреси.

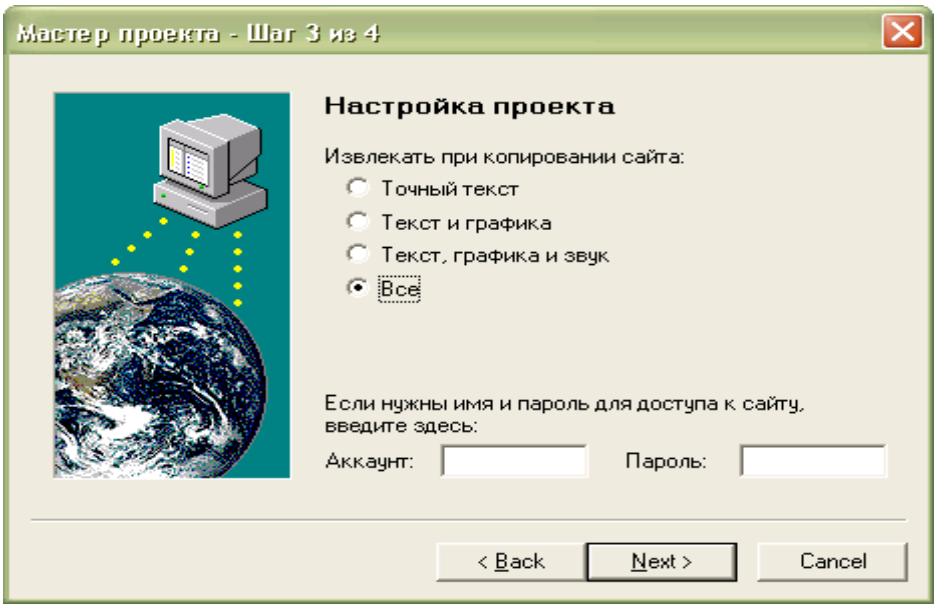


Рис. 3.30. Вікно третього кроку роботи майстра.

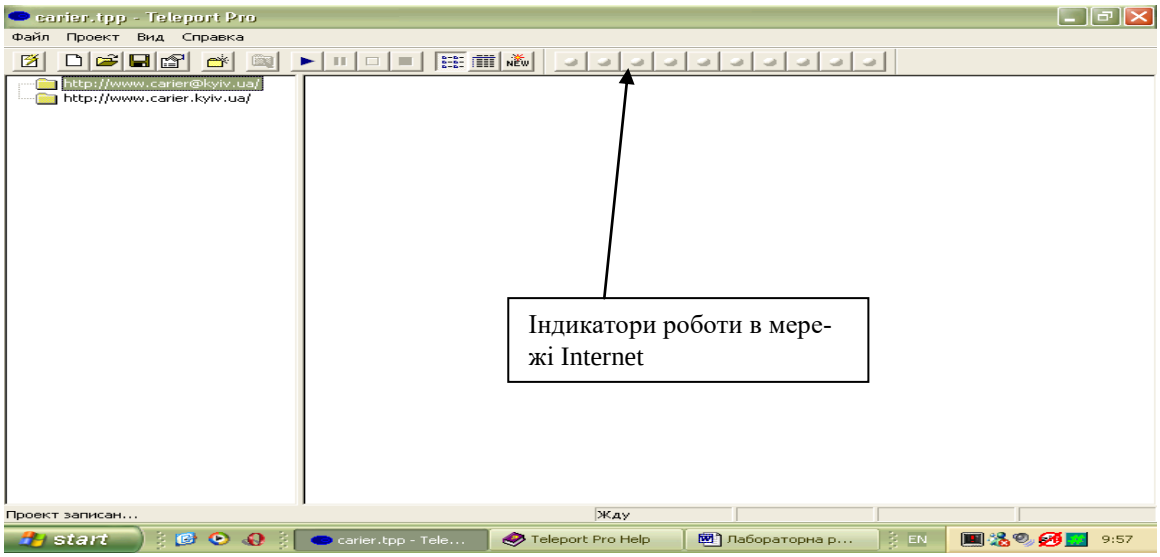


Рис. 3.31. Вікно програми зі списком адрес.

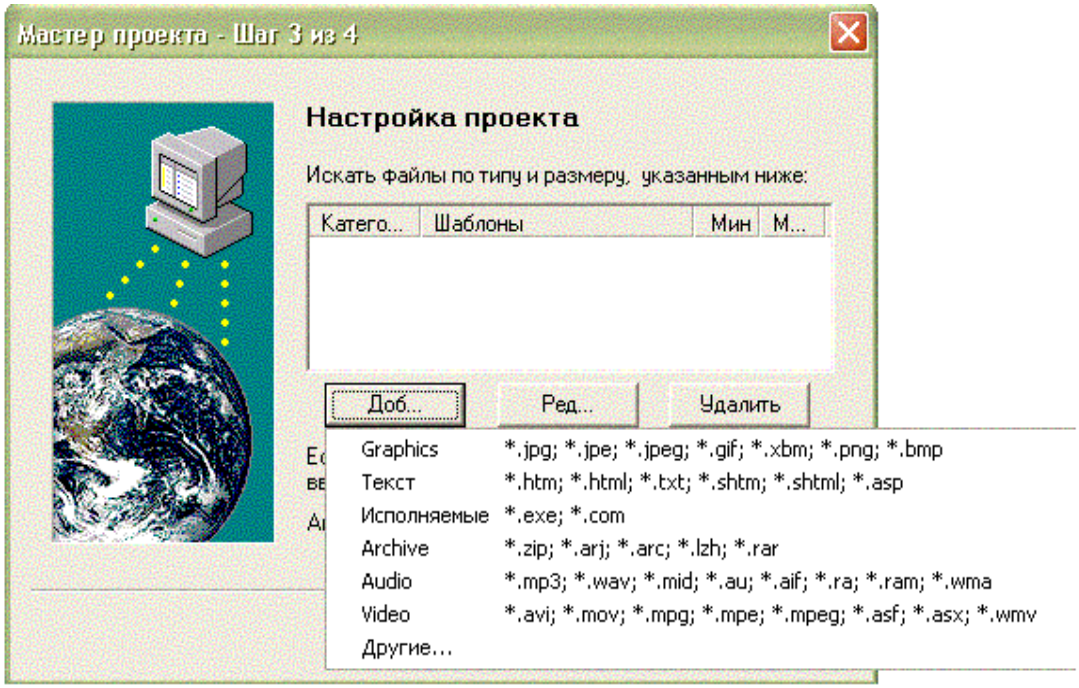


Рис. 3.32. Вікно відбору типів файлів.

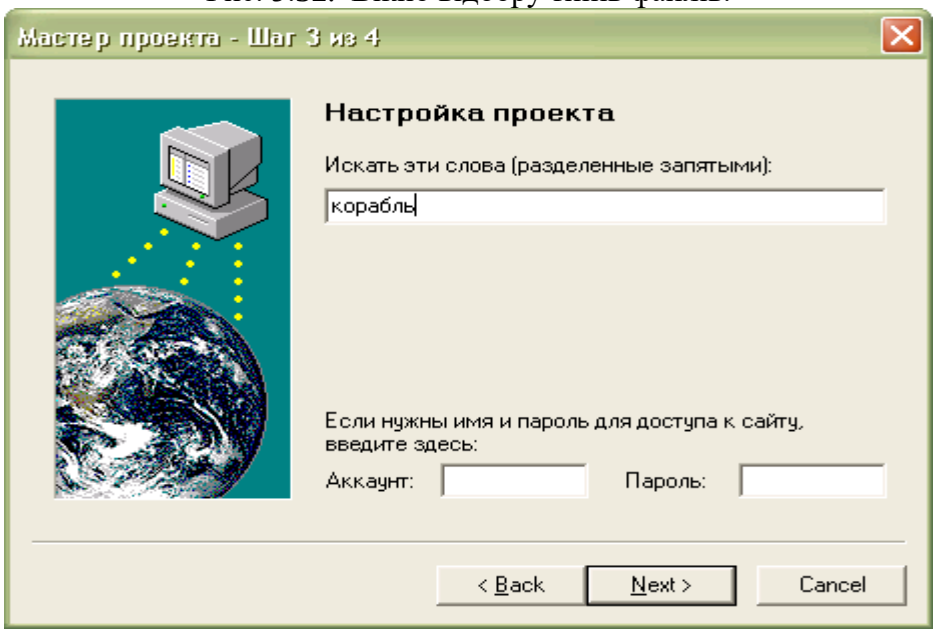


Рис. 3.33. Вікно введення ключових слів.

Збереження проекту

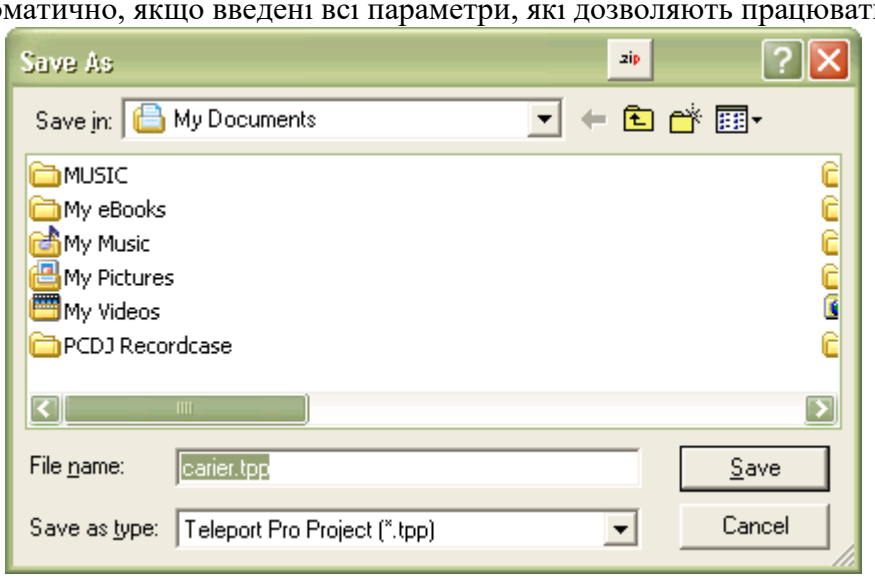
При завершенні роботи з **майстром створення проекту** автоматично після введення команди Finish з'являється діалогове вікно збереження проекту (рис. 3.34). Треба звернути увагу на те, що розширення файлу, у якому буде зберігатися вміст проекту – .tpp.

Якщо майстер не використовувався при побудові проекту, то для його збереження необхідно вибрати команду **Сохранить проект**, або **Сохранить проект как** із меню **Файл**. Потім указати диск та теку, де будете зберігати проект. Програма може при збереженні файлів в одній теці їх перейменовувати, щоб не допустити колізії при однакових іменах. Найшвидше збереження файлів буде при зберіганні «плоскої» копії веб-вузла, тобто без урахування зв'язків та глибини.

Запуск проекту

Запуск проекту проводиться командою **Старт** із меню **Проект**, або натискуванням стартової кнопки на панелі інструментів. Після введення команди програма автоматично з'єднується за вказаною адресою через мережу Internet (з'єднання з Internet запускається про-

грамою автоматично, якщо введені всі параметри, які дозволяють працювати в мережі).



3.34. Вікно збереження проекту

Індикатори програми (рис. 3.35) сигналізують про роботу в мережі. Після цього можна перевести роботу програми у фоновий режим (мінімізувавши вікно).

Примітка: типовий проект Klingon, звичайно, проведе закачування близько 150 файлів, що становить близько одного мегабайта, при швидкості з'єднання 28.8 Кб/с протягом 5 хвилин.

Перегляд результатів

Після того як проект почав працювати або закінчив роботу можна переглянути результати в проектному вікні. У лівій панелі програми показана карта проекту (список сторінок, який дослідила програма), а у правій панелі – список файлів, які закачані.

Можна переглянути повний список файлів або всю їх деталізацію.

Закачані файли зберігаються в теці, яка створюється teleport Pro і одержує те ж ім'я,що і проект. Перегляд теки можна провести із провідника Windows. З файлами в теці можна виконувати всі дії, притаманні Windows (копіювати, переміщати, перейменовувати, видаляти й т.п.).

Налагоджування параметрів проекту

Налагодити додаткові параметри проекту можна при використанні кнопки  **властивості проекту** на панелі інструментів. Після введення команди з'явиться діалогове вікно (рис. 3.35).

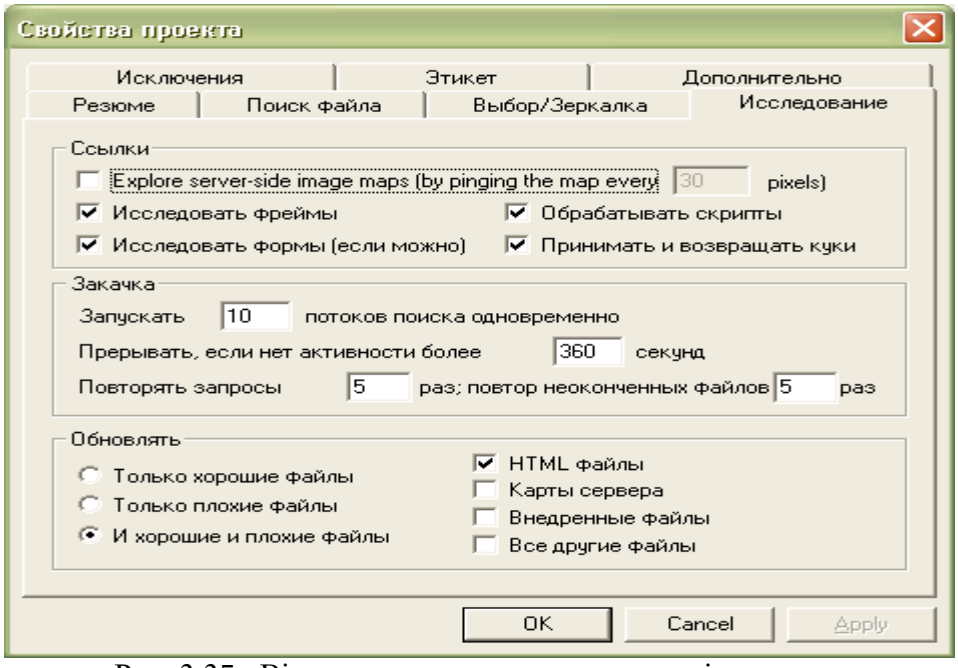


Рис. 3.35. Вікно налагоджування параметрів проекту

Примітка: встановлення мінімального або максимального розміру файлу для закачування до нуля, указує на те, що розмір не обмежений для закачування. Teleport Pro фільтрує файли за розміром, якщо сервер передає їх розміри, якщо сервер цього не робить, то програма закачує файл до розміру обмеження, а потім припиняє його закачування.

Teleport Pro знайде ключові слова, навіть якщо вони приховані всередині кодів HTML або коментарів.

Увага!! Якщо ввести у вкладці **Исключения** типи файлів, які не потрібно переглядати програмі (ключові слова у файлах, розширення, адреси сайтів), то ніякі інші налагодження не вкажуть програмі на можливість пошуку вказаних файлів.

Увага!! Teleport тільки намагається відновити (або модифікувати) ті файли, які відповідають поточним установкам **Проектних властивостей** і правилам дослідження. Іншими словами, якщо в попередньому проектному сеансі направити teleport, щоб відновити графіки і текстові файли; а потім змінити пошукові установки, щоб відновити тільки текстові файли, виконуючи проект, програма буде шукати тільки текстові файли, тому що графічні файли більше не відповідають пошуковим установкам проекту.

Команди **Пауза** й **Прервать** меню **Проект** дозволяють провести до кінця закачування тих файлів, закачування яких уже почалося. Відновлення закачування файлів почнеться в будь-якому випадку (після зупинки процесу) із місця зупинки.

Можливе встановлення виконання проектів один за одним через певні проміжки часу.

Teleport Pro може автоматично під'єднуватися і від'єднуватись від Інтернету, як вимагається для виконання й завершення створених teleport-проектів. Можливий запуск до 10 ліній запитів одночасно.

Teleport може прийняти й передати cookies, які є малим набором даних для ідентифікації та обробки клієнтів, такі як браузери або teleport. Вимкнення вказаного параметра забезпечить у якійсь мірі конфіденційність, але при цьому teleport не зможе обробляти деякі сервери, які вимагають ідентифікації користувача до передавання даних.

У програмі передбачено автозбереження за умовчанням через кожні 5 хвилин.

Можливо встановити автоматичне з'єднання, роз'єднання, і повторне підключення до послуг, використовуючи команду **Соединения** меню **Файл** (рис. 3.36).

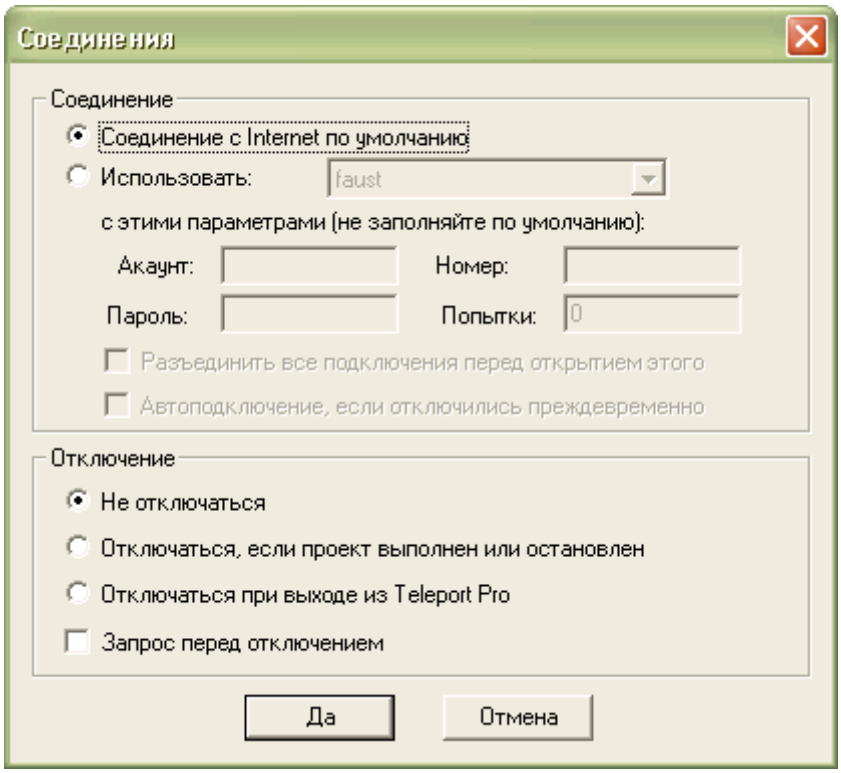


Рис. 3.36. Вікно встановлення автоматичного підключення до Internet

Закачування файлів за допомогою програми FlashGet

Програма FlashGet створена, щоб вирішити дві із найбільших проблем при завантаженні файлів у мережах: швидкість й можливість управління завантаженими файлами.

Це особливо актуально, коли встановлений зв'язок із віддаленим комп'ютером із малим трафіком, або якщо під час завантаження файлу перервано зв'язок. FlashGet може розділити завантажені файли на секції (до десяти частин), завантажуючи кожну секцію одночасно, для зростання швидкості завантаженні до 100-500 %.

Можливе створення списку файлів, які необхідно завантажити на комп'ютер без допомоги користувача. Програма дозволяє здійснити автоматичний пошук найшвидшого сервера, доступного для найшвидшого можливого завантаження. FlashGet автоматично набирає номер телефону, припиняє роботу комп'ютера при відсутності користувача.

Користувач програми може управляти лімітом швидкості завантаження файлів на комп'ютер, із тим аби завантаження файлів не заважало вашому перегляду Інтернету.

При установленні програми використовується архіватор, наприклад, WinZip, після розархівації дистрибутиву запускається на виконання файл SETUP.EXE. Після чого працює майстер установлення, який дозволить відібрати потрібні характеристики за декілька кроків установки, при цьому необхідно мати права адміністратора. За умовчанням усі установки завантаження файлів записуються у файл default.jcd. Видалення вказаного файлу може привести до некоректної роботи програми. Ключі, які відповідають за інтеграцію програми з операційною системою, знаходяться у файлі UNREG.INF. Після встановлення програми вона автоматично бере на себе функції закачування файлів. Якщо цього не сталося, то необхідно налагодити параметри програми командою **Опції** (рис. 3.37) із підменю **Опції/Дозвон**, вкладка **Спостереження**, крім параметрів програми.

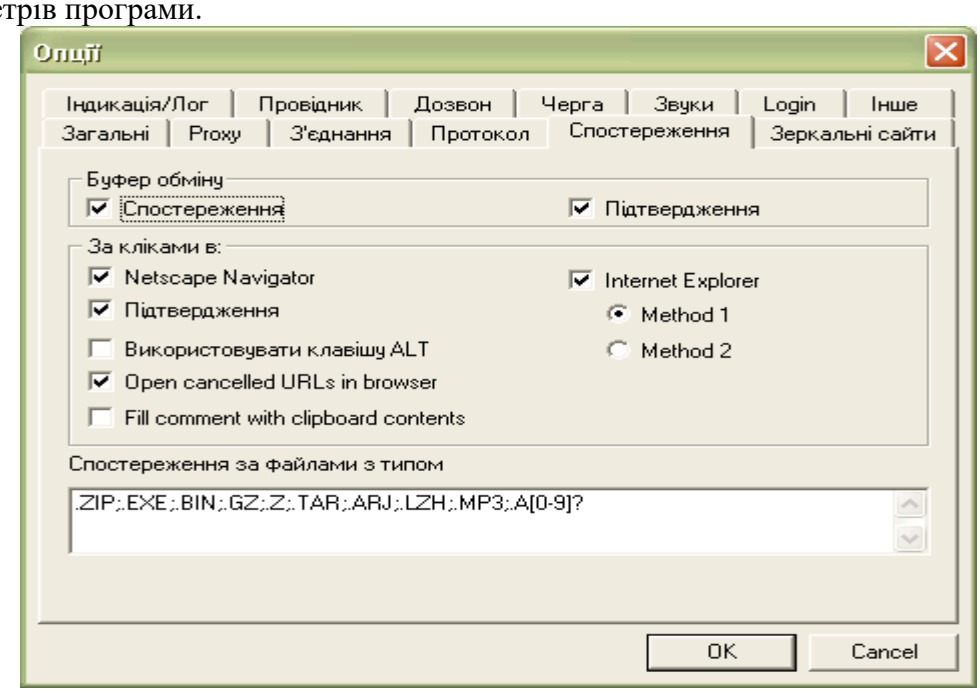


Рис. 3.37. Вікно налагодження параметрів програми

Крім того, можливо відібрати можливі варіанти завантаження файлів, використовуючи відповідні вкладки. Використавши вкладку **Інше**, можна встановити процес закачування файлів подвійним клацанням маніпулятором типу «миш» на терміналі монітору (рис. 3.38).

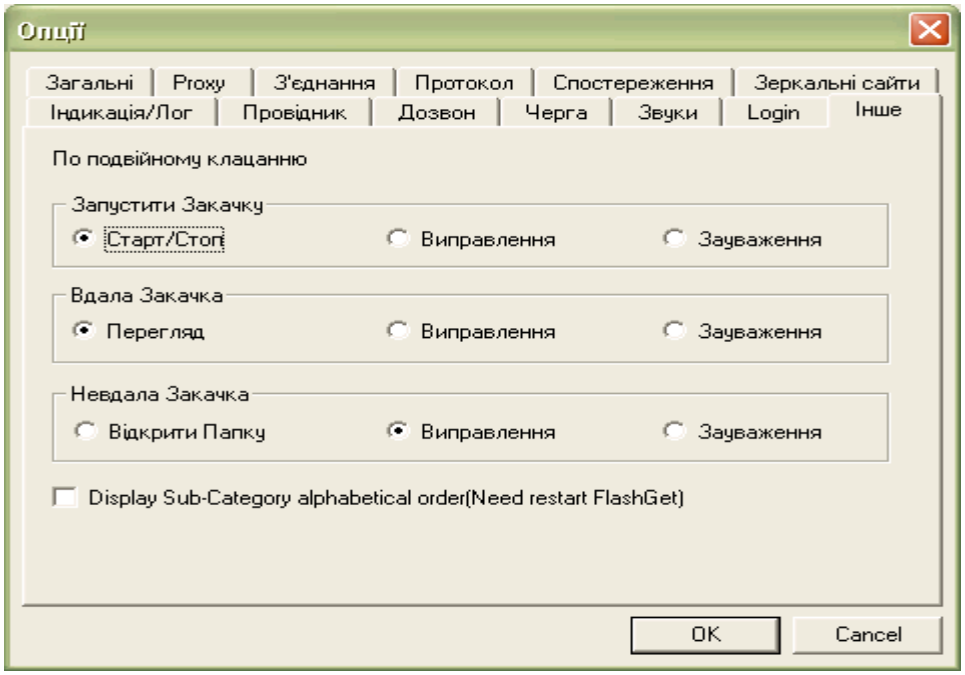


Рис. 3.38. Вікно встановлення закачування файлів

Використання контекстно-залежного меню (рис. 3.39) із відбором команди **Завантажте все** в програмі Internet Explorer надає можливість FlashGet завантажити файл з усіма зв'язками у межах сторінки. Команда **Завантажити** дозволить завантажити тільки виділений файл. Можна використати буксування файлів, які необхідно закачати, у каталог **Закачані**, (рис. 3.40) в потрібну категорію, або копіювати вказаний файл (файли), при цьому автоматично файли додаються у список файлів для подальшого автоматичного закачування. У даному випадку FlashGet підтримує багаторазові зв'язки від IE. У процесі відбору параметрів можна змінити параметри закачування, вибравши з контекстно-залежного меню команду **Властивості**.

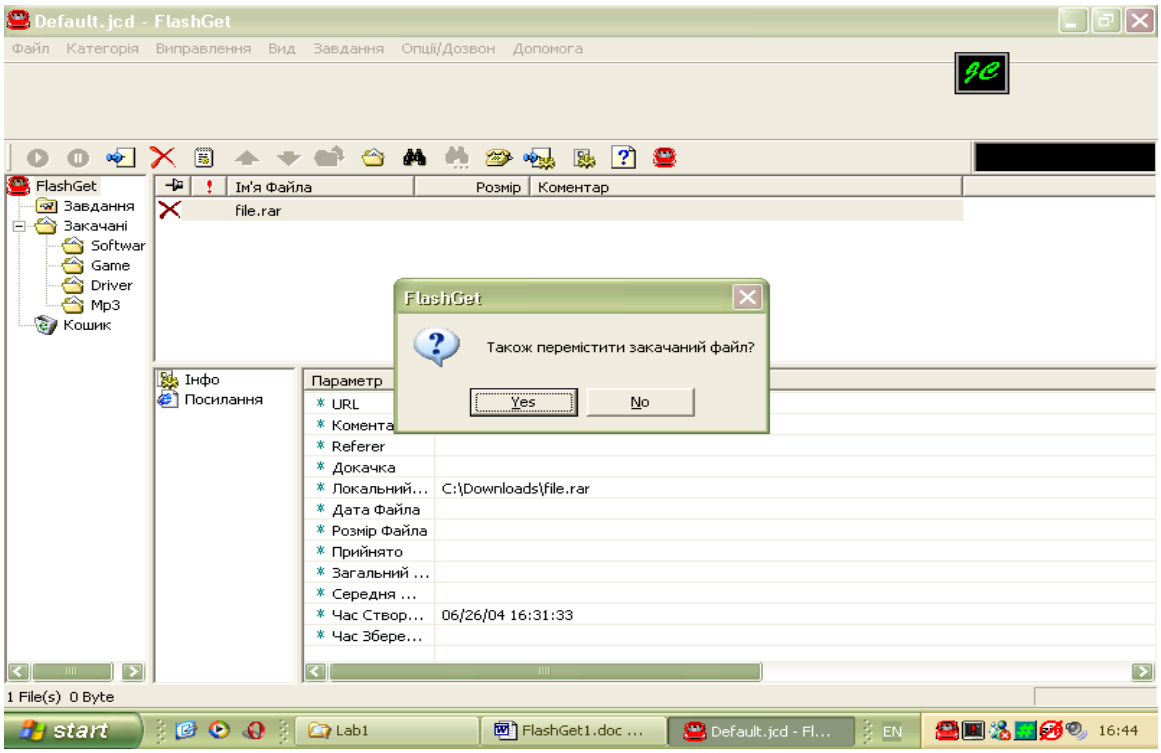


Рис. 3.39. Вікно відбору параметрів запуску процесу завантаження файлів

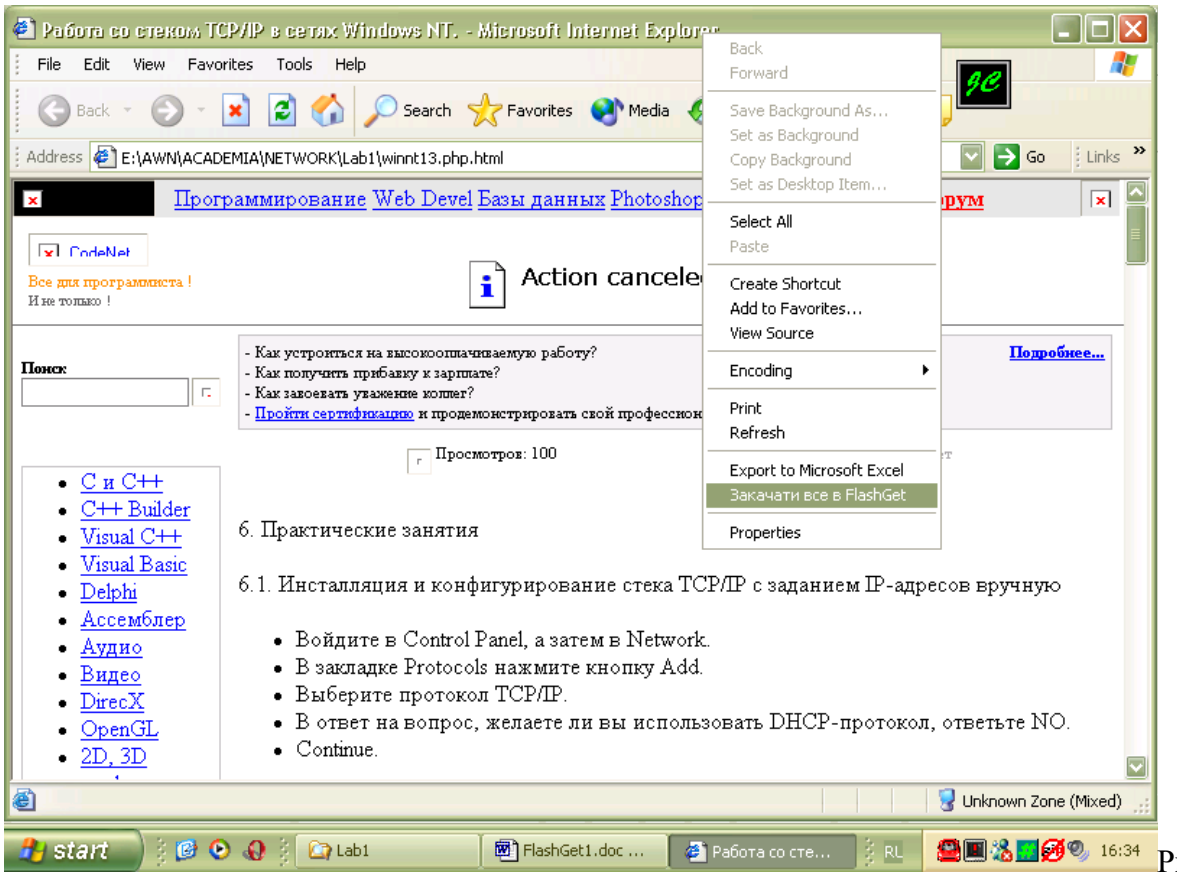


Рис. 3.40. Вікно відбору файлів для завантаження.

Файл можна при закачуванні розбити на десять частин (рис. 3.41), але на практиці достатньо мати їх три-п’ять, при цьому на більш повільних серверах треба вибирати більше частин, що може дати економію часу при закачуванні файлу.

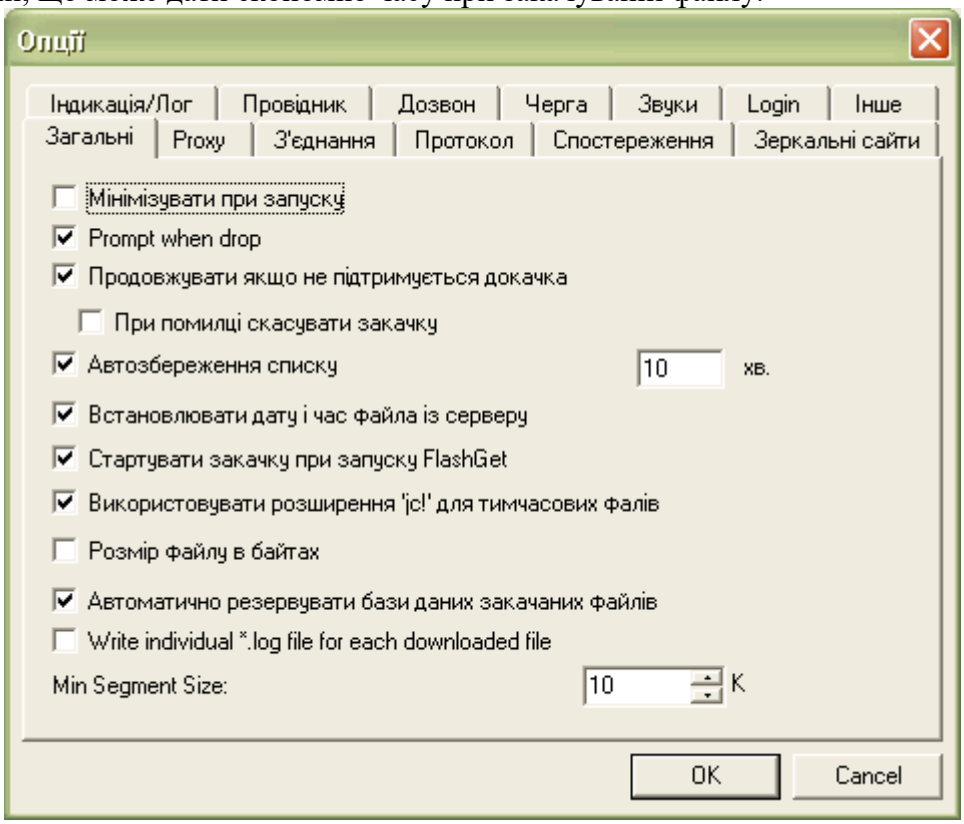


Рис. 3.41. Вікно встановлення поділу файлу для закачування на декілька частин.

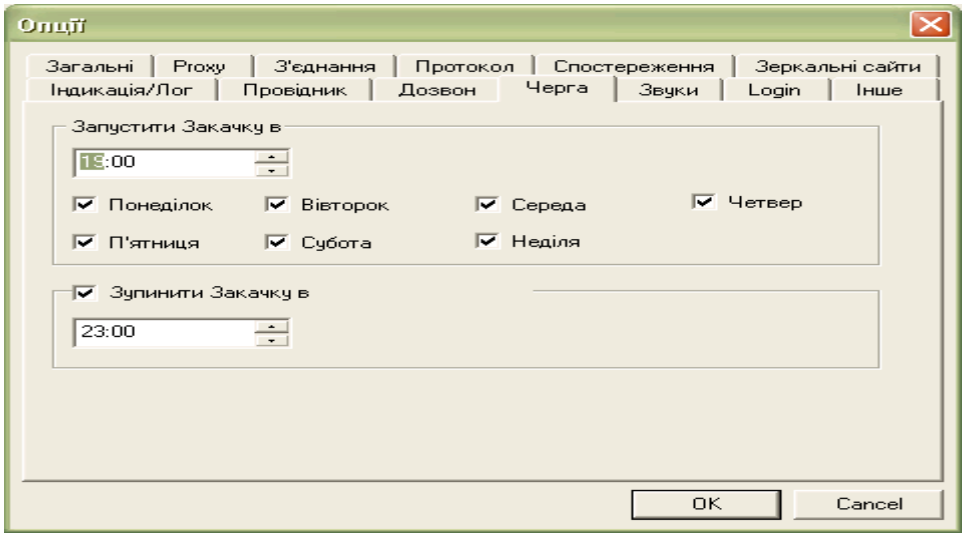


Рис. 3.42. Вікно встановлення часу закачування.

З метою економії часу та грошей треба планувати завантаження файлів у не пікові часи роботи мережі, а у часи коли завантаження дешевше, для цього використовується вікно (рис. 3.42) вкладка – **Черга**. З указаною метою використовується вкладка **Дзеркальні сайти,** яка дозволяє перемкнути закачування файлів на більш доступний сервер.

Деякі сервери вимагають перевірки логіну та паролю перед закачуванням файлів. Вони установлюються через вкладку **Login**, команда **Додати**. При використанні проксі-сервера можна налагодити параметри через вкладку **Proxy** команду **Додати**.

Важливо перевірити закачані файли на наявність вірусів, закладок і т. п. Для цього через вкладку **Провідник** установлюються відповідні параметри (рис. 3.43).

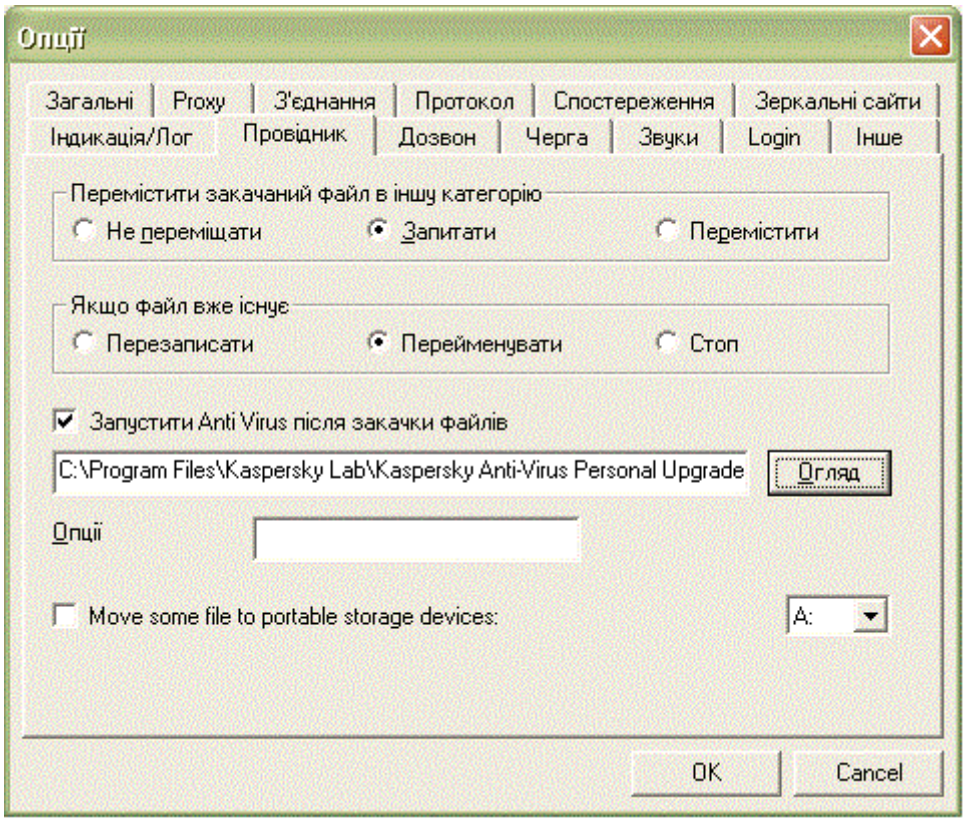


Рис. 3.43. Вікно встановлення автоматичного запуску антивірусної програми.

Головне меню програми FlashGet

Підменю Файл

Новий файл – створюється новий файл даних завантаження.

Відкрити – відкрити існуючий файл даних завантаження.

Збереження – зберегти файл поточних даних. Кожний файл, збережений у категорії MP3, буде переміщений на c:\download\mp3.

Зберегти як – зберегти файл поточних даних із новим ім’ям.

Додати попередній файл – додати завантажені файли (finished/unfinished) до списку роботи.
Імпортувати інформацію – додають пакетні завдання, які не були завантажені або розподілені за категоріями FlashGet.
Експортна інформація – це список вашої поточної бази даних, який указує на те, які файли були завантажені.
Експортуйте – експортує завантажений файл(и) і інформацію завантаження.
Вихід з FlashGet.

Підменю Категорія

Нова категорія – створюється нова категорію завантаження. FlashGet дозволяє створювати необмежену кількість категорій. Якщо завантажується велика кількість файлів, то створення нових категорій необхідне.
Перемістити в – перемістити вибрану категорію/категорії в іншу категорію.
Видалити – видаляє вибрану категорію/категорії. При видаленні категорії, усі файли будуть також видалені.
Властивості – зміна властивостей вибраної категорії.

Підменю Виправлення

Вставте URL – створення нових даних для закачування файлу.
Виділіть усі – виділяється кожна робота в поточній категорії**.**
Інвертувати виділення – зміна вибраних елементів на невибрані, а невибраних елементів на вибрані**.**
Знайти – здійснюється пошук елементів завантаження за іменем, URL або коментарем.

Підменю Вид

Детально – показати вікно завантаження детально (нижнє вікно, що графічно показує завантаження файлу в FlashGet і ділення його на частини).
Кошик – приховує або показує зону кошику FlashGet.
Панель інструментів – налагоджує вигляд панелі інструментів**.**
Колонки – дозволяє налагодити потрібні колонки програми.
Мова – дозволяє вибрати мову спілкування.

Підменю Завдання

Нова закачка – створюється нове завантаження файлу (файлів).
Додати завдання – використовується завантаження пакету. Додають завантаження пакету, якщо там було багато файлів для завантаження й вони мають зразок у їх іменах. Наприклад: file01.zip до file10.zip.
Старт – запуск.
Призупинити – зупинка**,** пауза.
Перемістити в – перемістити вибраний файл(и) в іншу категорію.
Видалити – видалити вибраний файл(и).
Властивості – властивості файлу.
Перемістити вгору (униз) – вибраний файл(и) пересувається вище, або нижче.
Перевірити на відновлення – здійснюється перевірка: був оновлений завантажений файл чи ні.
Повторити закачку – завантажують файл знову.

Підменю Опції/Дозвон

Дозвон – дозволяє відібрати параметри дозвону до віддаленого комп'ютера.
Виключити живлення за завершенням – дозволяє виключити живлення комп'ютера після завершення роботи програми.
Розірвати з'єднання за завершенням – дозволяє розірвати з'єднання з віддаленим комп'ютером після завершення роботи програми.
Повторити з'єднання, якщо припинилося – дозволяє повторити з'єднання з віддаленим комп'ютером після його розриву.
Обмеження трафіку – дозволяє обмежити трафік закачування файлу.
Зберегти за умовчанням – дозволяє зберегти за умовчанням параметри програми.
Опції – дозволяє налагодити параметри програми.

Пірінгова мережа обміну файлами

Одна із сфер застосування технології пірінгових мереж – це обмін файлами. Виглядає це так: користувачі мережі викладають які-небудь файли в теку, файли із якої доступні для скачування іншим клієнтам. Архітектура BitTorrent передбачає наявність у файлу, що викладається в мережу, єдиного власника, який і зацікавлений в його розповсюдженні. Інший користувач мережі посилає запит на пошук певного файлу. Програма шукає у клієнтів мережі файли, відповідні до запиту, і показує результат. Після цього користувач може викачати файли із знайдених джерел. Сучасні файлообмінні мережі дозволяють викачувати один файл відразу з декількох джерел (так швидше і надійніше). Щоб переконатися, що цей файл у всіх джерелах однаковий, проводиться порівняння не тільки за назвою файлу, але і за контрольними сумами або хешами типу MD4, TTH, SHA-1. Під час скачування файлу користувачем (і після його закінчення) цей файл у даного користувача можуть викачувати і інші клієнти мережі, внаслідок чого особливо популярні файли можуть у результаті бути доступними для скачування з сотень джерел одночасно.

Зазвичай у таких мережах обмінюються фільмами і музикою, що є одвічним головним болем відеовидавничих і звукозаписних компаній, яким таке положення справ дуже не до душі. Проблем їм додає той факт, що припинити розповсюдження файлу в децентралізованій пірінговій мережі технічно майже неможливо – для цього потрібно буде фізично відключити від мережі всі машини, на яких знаходиться цей файл, а таких машин може бути дуже і дуже багато – залежно від популярності файлу їх кількість може досягати сотень тисяч. Останнім часом відеовидавці і звукозаписні компанії почали подавати до суду на окремих користувачів таких мереж, звинувачуючи їх в незаконному розповсюдженні музики і відео.

С самого початку творець BitTorrent програміст Брем Коен (Bram Cohen) заклав в нього декілька принципових відмінностей від інших пірінгових мереж: націленість на розповсюдження великих за розміром файлів і не зовсім децентралізована структура мережі. Первинний власник файлу генерує серію хеш-кодів, згодом використовувану клієнтами BitTorrent для перевірки його цілісності. Клієнт пірінгової мережі, щоб отримати файл, повинен завантажити набір даних з розширенням .torrent. У ньому міститься інформація про ім’я файлу, його розмір, хеш-коди сегментів (за замовчуванням розміром 256 КВ) і адресу розповсюджувача, у якого, у свою чергу, повинен бути запущений tracker-сервер для відстежування кількості завантажень файлу в мережі peer-to-peer. Архітектура BitTorrent припускає пірінговий обмін з використанням центрального tracker-сервера для обліку статистики. У міру того як файл частинами надходить з комп’ютера первинного власника в мережу, користувачі починають завантажувати його фрагменти один у одного. В той же час протокол BitTorrent вимагає фіксації кожного такого завантаження на tracker-сервері, навіть якщо сервер розповсюджувача не бере участь у транзакції.

Файли передаються частинами, кожен torrent, отримуючи ці частини, в той же час віддає (закачує) їх іншим клієнтам, що знижує навантаження і залежність від кожного клієнта-джерела і забезпечує надлишковість даних.

Протокол був створений на мові Python 4 квітня 2001 року. Запуск першої версії відбувся 2 липня 2001 року.

Існує множина програм-клієнтів для обміну файлами за протоколом BitTorrent.

Роздача може містити як один файл, так і декілька, наприклад, вміст теки.

Для кожної роздачі створюється файл метаданих з розширенням .torrent, який містить наступну інформацію:

- URL трекера;
- загальну інформацію про файли (ім’я, довжину і ін.) в даній роздачі;
- контрольні суми (точніше хеш-суми SHA1) сегментів файлів, які роздаються;
- Passkey користувача, якщо він зареєстрований на даному трекері. Довжина ключа встановлюється трекером.
- (Необов’язково) хеш-суми файлів цілком;
- (необов’язково) альтернативні джерела, що працюють не за протоколом BitTorrent. Найбільш поширена підтримка так званих web-сидів (протокол HTTP), але допустимими також є magnet URI.

Трекер (англ. tracker – система відстежування). Працює за протоколом HTTP. Трекер потрібний для того, щоб клієнти могли знайти один одного. Фактично, на трекері зберігаються дані про вхідні порти клієнтів, унікальним чином ідентифікуючи об'єкти, що беруть участь в закачуваннях. За стандартом, імена файлів на трекері не зберігаються, і дізнатися їх за хеш-сумами не можна. Проте на практиці трекер часто окрім своєї основної функції виконує і функцію невеликого веб-сервера. Такий сервер зберігає файли метаданих і опис поширюваних файлів, надає статистику закачувань за різними файлами, показує поточну кількість підключених користувачів і ін.

Розмір сегменту регулюється при створенні торрента і, як правило, вибирається розмір, відповідний ступеню двійки. При виборі розміру необхідно дотримувати баланс, пов'язаний з механізмом роботи протоколу. Розмір сегменту найчастіше лежить в діапазоні від 128 Кб до 2-4 Мб, хоча на дуже великих роздачах (близько сотні гігабайт) можуть використовуватися сегменти розміром 32-64 Мб.

Якщо роздача складається з декількох файлів, то в процесі хешування вони прочитуються підряд і розглядаються як безперервний потік даних. Тому найчастіше сегмент, що містить кінець одного файлу, також містить і початок наступного. Разом з тим для того, щоб переконатися в правильності викачаного сегменту, необхідно мати його всього цілком. Саме тому, не дивлячись на те, що більшість клієнтів підтримує скачування не всіх файлів в роздачі, а тільки деяких, майже завжди буде викачаний також і початковий і/або кінцева частина файлів, не вибраних для скачування.

Оскільки хеш-кодування в .torrent-файлі включають імена і структуру тек роздачі, то перейменування файлів із збереженням можливості їх роздавати в загальному випадку неможливе. Проте, деякі клієнти підтримують зміну структури, наприклад, створення або перейменування тек і перейменування або переміщення файлів.

Файл метаданих є словником у bencode форматі. Файли метаданих можуть розповсюджуватися через будь-які канали зв'язку: вони (або посилання на них) можуть розміщуватися на домашніх сторінках користувачів мережі, розсилатися, публікуватися в блогах або стрічках новин RSS. Також є можливість отримати info частину публічного файлу метаданих безпосередньо від інших учасників роздачі завдяки розширенню протоколу "Extension for Peers to Send Metadata Files". Це дозволяє обійтися публікацією тільки магнет-посилання. Отримавши якимнебудь чином файл з метаданими, клієнт може починати скачування.

Принцип роботи протоколу

Принцип роботи BitTorrent: навантаження на розповсюджувача файлу зменшується завдяки тому, що клієнти починають обмінюватися даними відразу ж, навіть якщо файл не докачаний ними до кінця.

Перед початком скачування клієнт під'єднується до трекеру за адресою, вказаною в торрент-файлі, повідомляє йому свою адресу і хеш-кодування-суму торрент-файла, на що у відповідь клієнт отримує адреси інших клієнтів, що викачують або роздають цей же файл. Далі клієнт періодично інформує трекер про хід процесу і отримує оновлений список адрес. Цей процес називається оголошенням.

Клієнти з'єднуються один з одним і обмінюються сегментами файлів без безпосередньої участі трекера, який лише зберігає інформацію, отриману від клієнтів, які підключені до обміну, список самих клієнтів і іншу статистичну інформацію. Для ефективної роботи мережі BitTorrent необхідно, щоб якомога більше клієнтів були здатні приймати вхідні з'єднання. Неправильне налагодження NAT або брандмауера можуть цьому перешкодити.

При з'єднанні клієнти відразу обмінюються інформацією про сегменти, що є у них. Клієнт, який бажає викачати сегмент, посилає запит і, якщо другий клієнт готовий віддавати, – отримує цей сегмент. Після цього клієнт перевіряє контрольну суму сегменту. Якщо вона співпала з тією, що записана в торрент-файлі, то сегмент вважається успішно викачаним, і клієнт оповіщає всіх про наявність у нього цього сегменту. Якщо ж контрольні суми розрізняються, то сегмент починає викачуватися наново. Таким чином, об'єм службової інформації (розмір торрент-файла і розмір повідомлень із списком сегментів) безпосередньо залежить від кількості, а значить, і розміру сегментів. Тому при виборі сегменту необхідно дотримувати баланс: з одного боку, при великому розмірі сегменту об'єм службової інформації буде менший, але у разі помилки перевірки контрольної суми доведеться викачувати ще раз більше інформації. З іншого

боку, при малому розмірі помилки не такі критичні, оскільки необхідно наново викачати менший об'єм, зате розмір торрент-файла і повідомлень про наявні сегменти стає більшим.

Алгоритм обміну даними

Кожен клієнт має можливість тимчасово блокувати віддачу іншому клієнтові. Це робиться для ефективнішого використання каналу віддачі. Крім того, при виборі кого розблоковувати, перевага віддається користувачам, які самі передали цьому клієнтові багато сегментів. Таким чином, користувачі з хорошими швидкостями віддачі заохочують один одного за принципом «ти – мені, я – тобі».

Обмін сегментами ведеться за цим принципом симетрично в двох напрямах. Клієнти повідомляють один одного про сегменти, що є у них, при підключенні і потім при отриманні нових сегментів, і тому кожен клієнт може зберігати інформацію про те, які сегменти є у інших підключених користувачів. Порядок обміну вибирається так, щоб спочатку клієнти обмінювалися найбільш рідкісними сегментами: таким чином підвищується доступність файлів в роздачі. В той же час вибір сегменту серед найрідкісніших випадковий, і тому можна уникнути ситуації, коли всі клієнти починають викачувати один і той же самий рідкісний сегмент, що негативно б відбилося на продуктивності.

Обмін даними починається, коли обидві сторони в нім зацікавлені, тобто, кожна із сторін має сегменти, яких немає у іншої. Кількість переданих сегментів підраховується, і якщо одна із сторін виявляє, що передає в середньому більше, ніж приймає, вона блокує на деякий час віддачу іншій стороні. Сегменти діляться на блоки розміром 16-64 кілобайт, і кожен клієнт запрошує саме ці блоки. Одночасно можуть запрошуватися блоки з різних сегментів. Більш того, деякі клієнти підтримують скачування блоків одного сегменту у різних користувачів. В цьому випадку описані вище алгоритми і механізми обміну застосовні і до рівня блоків.

Режим End game

Коли скачування майже завершене, клієнт входить в особливий режим, званий end game. У цьому режимі він запрошує сегменти, що залишилися, у всіх підключених користувачів, це дозволяє уникнути уповільнення або повного «зависання» майже завершеного закачування із-за декількох повільних клієнтів.

Специфікація протоколу не визначає, коли саме клієнт повинен увійти до режиму end game, проте існує набір загальноприйнятих практик. Деякі клієнти входять в цей режим, коли не залишилося незапитаних блоків, інші – поки кількість блоків, що залишилися, менше кількості тих, що передаються і не більше 20. Існує думка, що краще підтримувати кількість очікуваних блоків низьким (1 або 2) для мінімізації надмірності, це при випадковому запиті зменшить шанс отримати дублікати одного і того ж блоку.

Режим сиду

При отриманні повного файлу клієнт переходить в спеціальний режим роботи, в якому він тільки віддає дані (стає сидом). Далі сид періодично інформує трекер про зміни в стані закачувань і оновлює списки IP-адрес.

Робота без трекера

У нових версіях протоколу були розроблені безтрекерні системи, які вирішують деякі з попередніх проблем. Відмова трекера в таких системах не приводить до автоматичної відмови всієї мережі.

Починаючи з версії 4.2.0 офіційного клієнта, в нім реалізована функція безтрекерної роботи, що базується на DHT Kademlia. У таких системах трекер доступний децентралізовано, на клієнтах, у формі розподіленої хеш-таблиці.

На даний момент не всі клієнти використовують сумісний один з одним протокол. Сумісні між собою Transmission і офіційний клієнт BitTorrent. Vuze (Azureus) також має режим безтрекерної роботи, але його реалізація відрізняється від офіційної, унаслідок чого він не може працювати через DHT з вище переліченими клієнтами. Проте, для Vuze існує підтримка стандартного DHT через плагін Mainline DHT.

Робота без трекера також можлива при використанні мультипротокольних клієнтів, підтримуючих BitTorrent. Shareaza через мережу Gnutella2 обмінюється хеш-кодуваннями і адресами користувачів інших підтримуваних мереж, зокрема BitTorrent.

Робота без торрент-клієнта

Для того, щоб брати і роздавати файли в торрент-мережах, не обов'язково користуватися спеціальними програмами. Існують декілька сервісів, які дозволяють викачувати файли, використовуючи тільки браузер.

Програми-клієнти

Кросплатформенна:

- µTorrent – клієнт BitTorrent для Windows, відрізняється малим розміром і високою швидкістю роботи;
- aria2 – підтримує HTTP, FTP, BitTorrent; файли Metalink 3.0.

Використання протоколу BitTorrent на прикладі Azureus (Vuze):

- Vuze (стара назва – Azureus) – підтримує Tor і I2P. Потрібно врахувати, що використовувана ним бібліотека Eclipse Standard Widget Toolkit використовує системнозалежні модулі і повинна компілюватися для кожної платформи окремо.
- BitTyrant (en) – модифікований варіант клієнта Azureus 2.5.
- BitTornado – кросплатформенний клієнт, написаний на мові Python.
- Deluge – кросплатформенний клієнт, написаний на мові Python; використовує GTK;
- FoxTorrent – розширення для браузера, що реалізовує функції клієнта BitTorrent;
- LeechCraft – кросплатформенний клієнт, існує плагін для підтримки BitTorrent;
- mlDonkey – кросплатформенний клієнт;
- Браузер Opera повністю підтримує закачування торрентів, починаючи з версії 9.0.
- TorrentFlux (en) – працює на віддаленому сервері як PHP-, дозволяючи не тримати свій комп'ютер включеним постійно, але при цьому роздає торренти.
- ABC – ще один Bittorrent Client, оснований на BitTornado.

GNU/Linux, UNIX:

- BTPD – консольний клієнт для /GNU+Linux, написаний на C++; працює в режимі демона;
- CTorrent – консольний клієнт для /GNU+Linux, що припинив розвиток в 2004 р.;
- KTorrent – використовує бібліотеку Qt; працює в середовищі KDE;
- KGet;
- rTorrent – консольний клієнт для /GNU+Linux, написаний на C++; використовує бібліотеки ncurses і libTorrent;
- Transmission – клієнт для GNU/Linux, що використовує GTK. Також може працювати в консольному режимі і в режимі демона;
- Bitflu – консольний клієнт для /GNU+Linux, написаний на Perl; працює в режимі, з підтримкою chroot оточення. Керується через telnet;
- qBittorrent – bittorrent клієнт для Unix/GNU +, можливі інші системи, написаний на C++ /Qt4, що використовує бібліотеку libtorrent. Розповсюджується під ліцензією GNU GPL;
- FatRat.

Windows:

- мTorrent;
- BitComet;
- BitSpirit;
- FlashGet;
- GetRight;
- Shareaza – підтримує роботу з декількома файлообмінними мережами, у тому числі і BitTorrent;
- Free Download Manager.

Mac OS:

- µTorrent;
- XTorrent;
- Transmission;
- BitRocket;
- Tomato Torrent;
- Acquisition.

Програма BitComet

Після установки BitComet відкривається вікно (рис. 3.44):

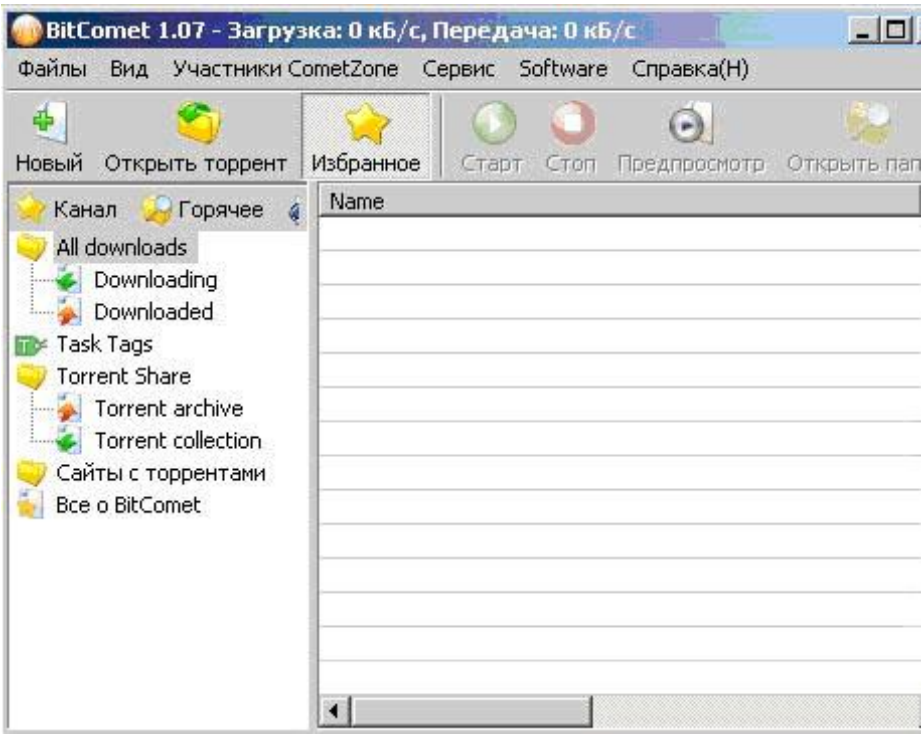


Рис. 3.44 Вікно BitComet

Заходимо у верхню вкладку «Файли», вибираємо «Створити Торрент.» (рис. 3.45).

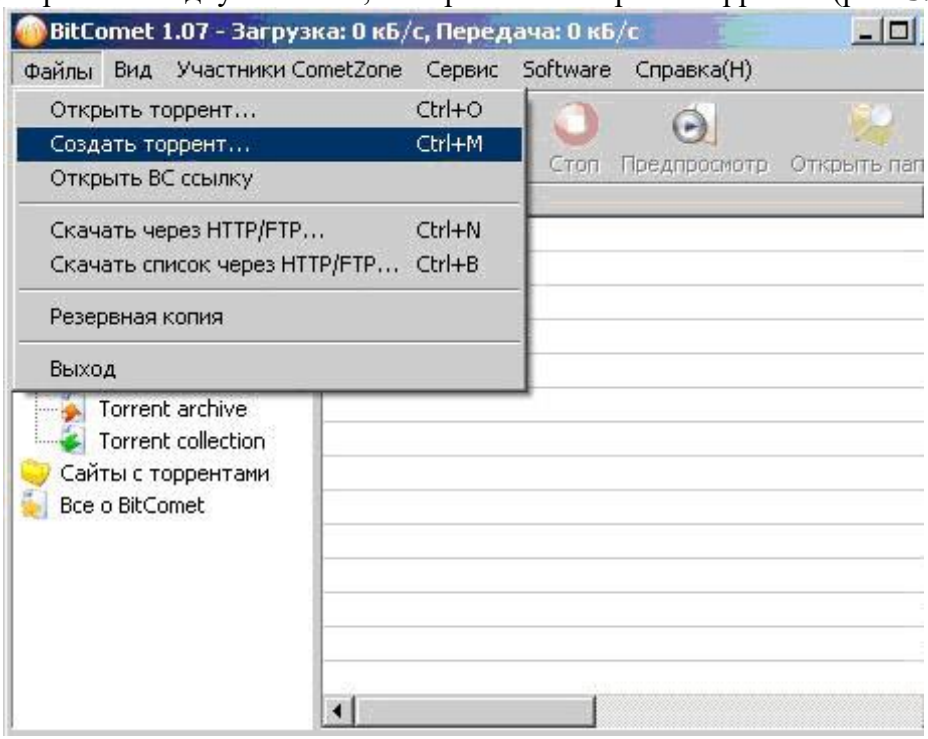


Рис. 3.45 Вікно команди створення Торрент

Відкривається діалогове вікно створення торрент-файла (рис.3.46), на зображення нанесені пояснення.

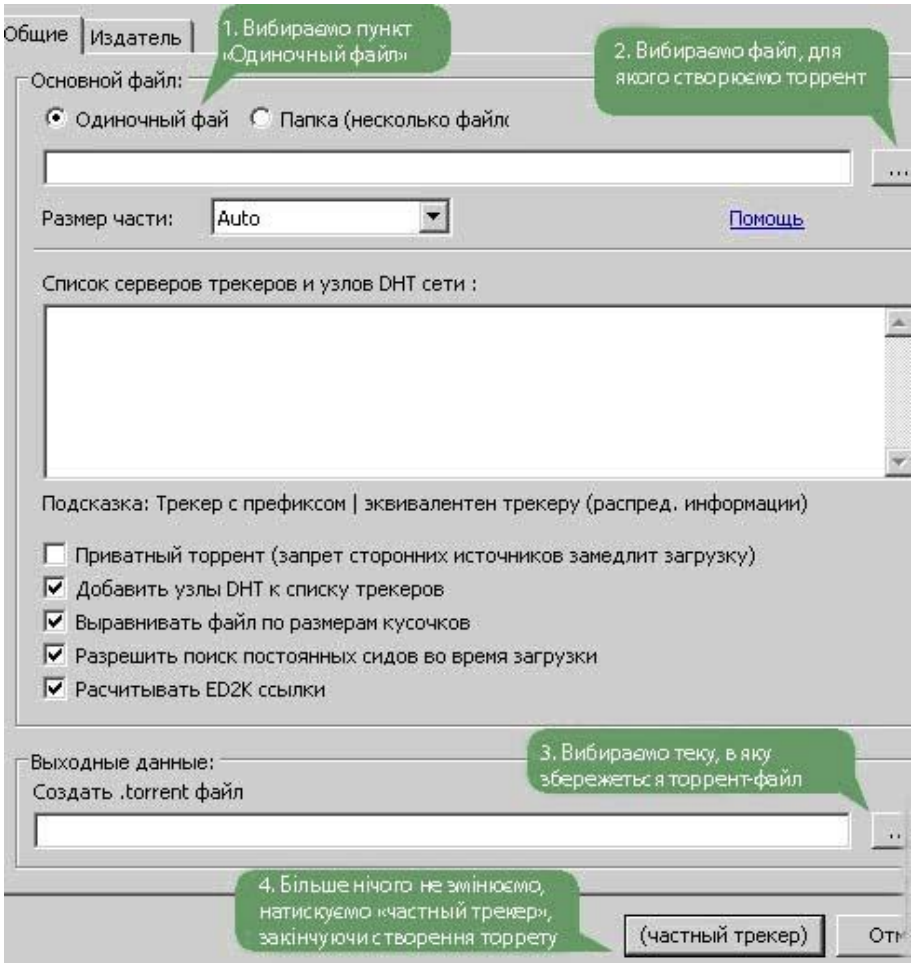


Рис. 3.46 Вікно створення торренту

Коли торрент-файл створився, видаляється завдання (рис. 3.47).

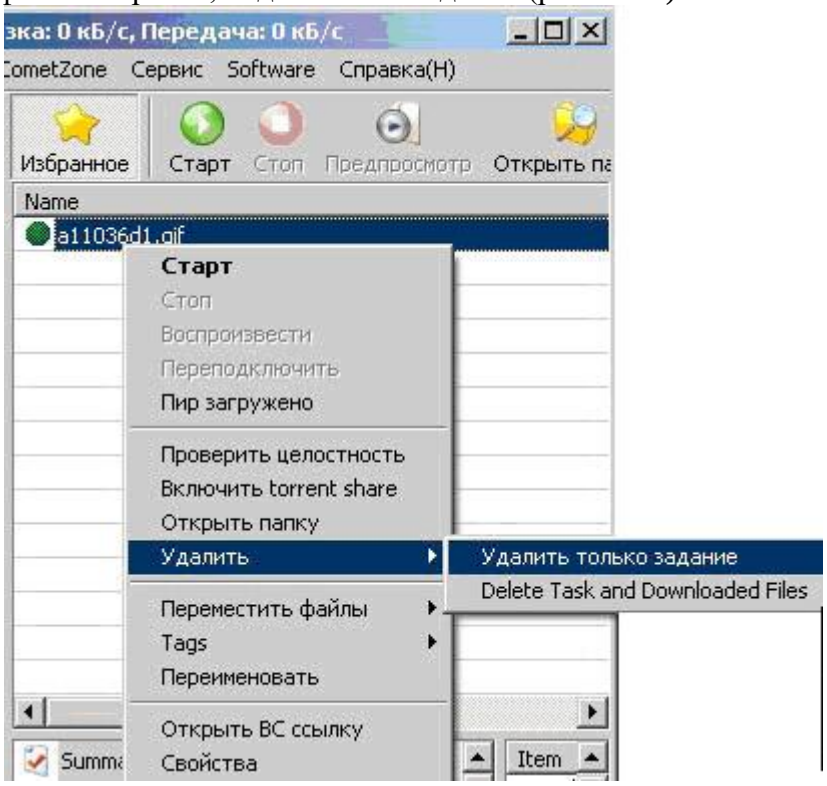


Рис.3.47 Видалення завдання.

Далі викладаємо створений файл торрент на трекер, оформляємо роздачу.

На різних торрент-трекерах оформлення роздач здійснюється по-різному, як правило, це просто і описано в правилах користування торрента.

Опишемо на прикладі Torrents.ru. Створюємо нову тему з описом файлу, який викладатимемо (як описувати, розказано в правилах Торрента) і прикріплюємо Торрент-файл (рис. 3.48):

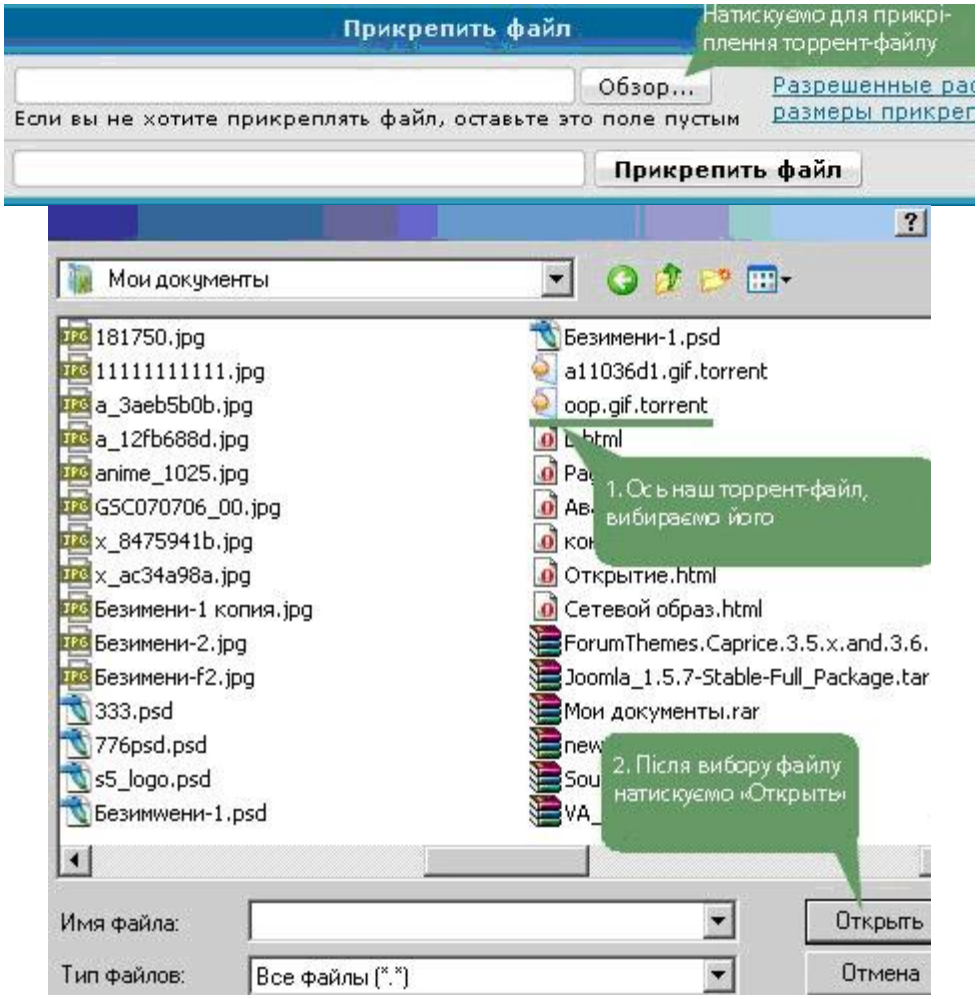


Рис. 3.48 Створення нової теми

Тепер викладений торрент-файл слід поставити на закачування в ту теку, де знаходиться оригінальний файл (рис. 3.49).

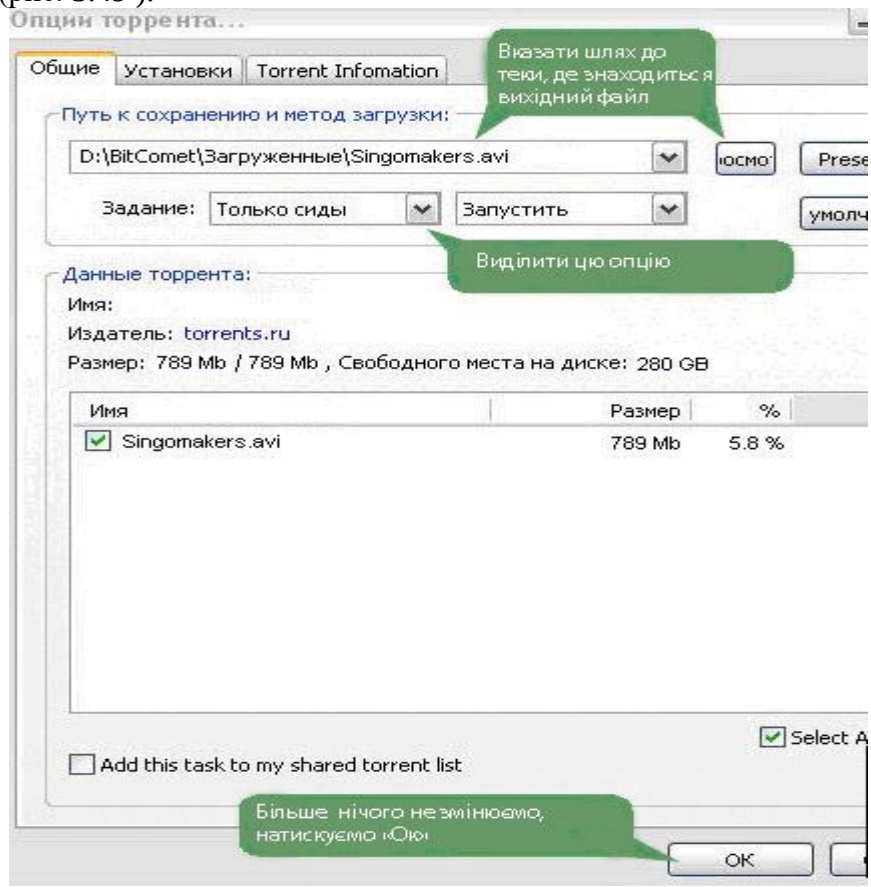


Рис. 3.49Постановка файлу на закачування

Далі програма і трекер перевірять наявність файлу.

Програма µTorrent

Викачуємо останню версію µTorrent на офіційному сайті. Там же, в розділі «Download», викачуємо файл «Language Pack» – це доповнення програми для підтримки російськомовного інтерфейсу. Файл русифікації «utorrent.lng» близько 400 кб, зберігаємо його в теку з програмою, там, де знаходиться файл запуску програми – utorrent.exe.

Після встановлення відкривається стартове вікно програми (рис. 3.50):

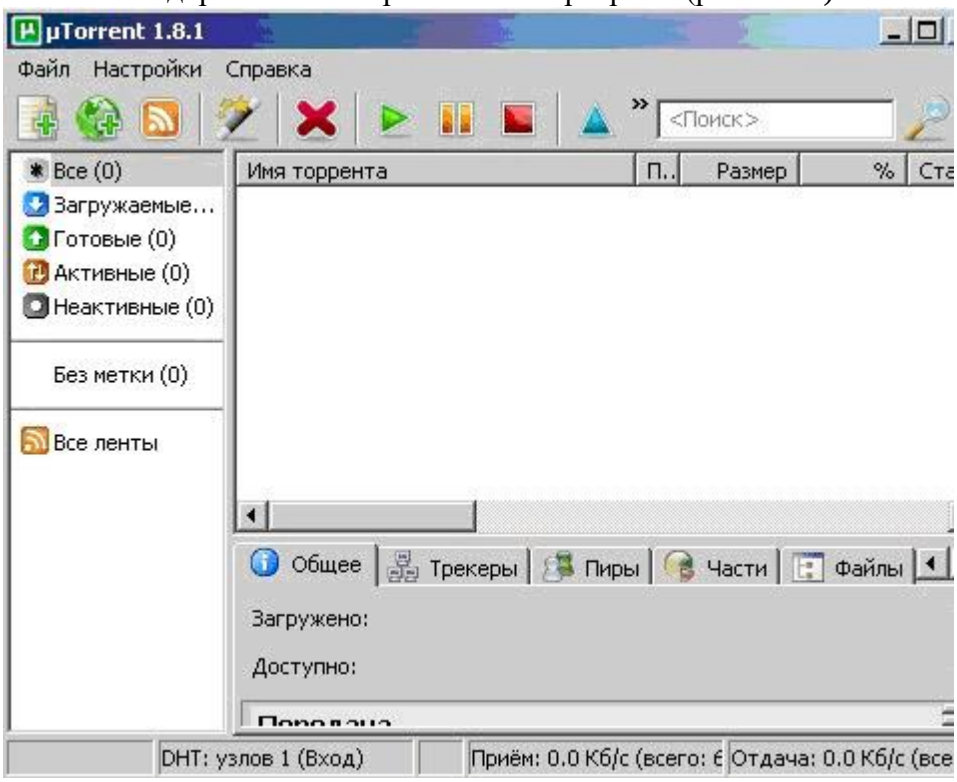


Рис. 3.50 Стартове вікно програми

Отже, створюємо торрент-файл, для цього входимо у верхнє меню «Файл» у вкладку «Створити новий торрент.» (рис. 3.51).

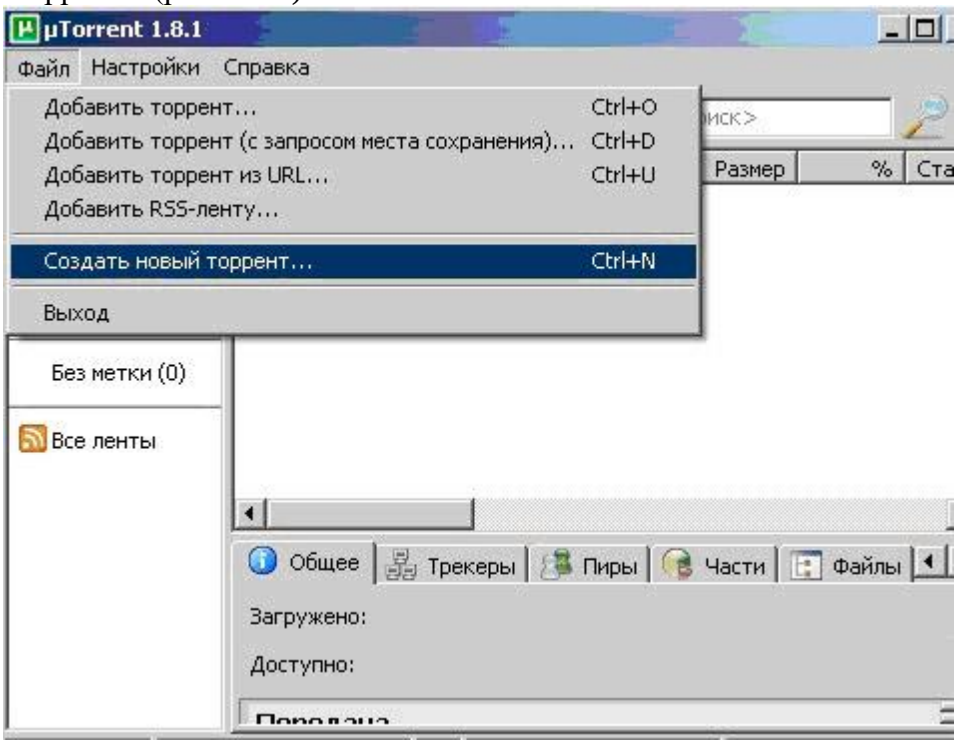


Рис. 3.51 Вікно команди створення торрент-файлу.

Відкрилося вікно створення торрент-файлу. Вибираємо файл або групу файлів для створення торрент-файлу. Натискаємо «Створити і зберегти» (рис. 3.52).

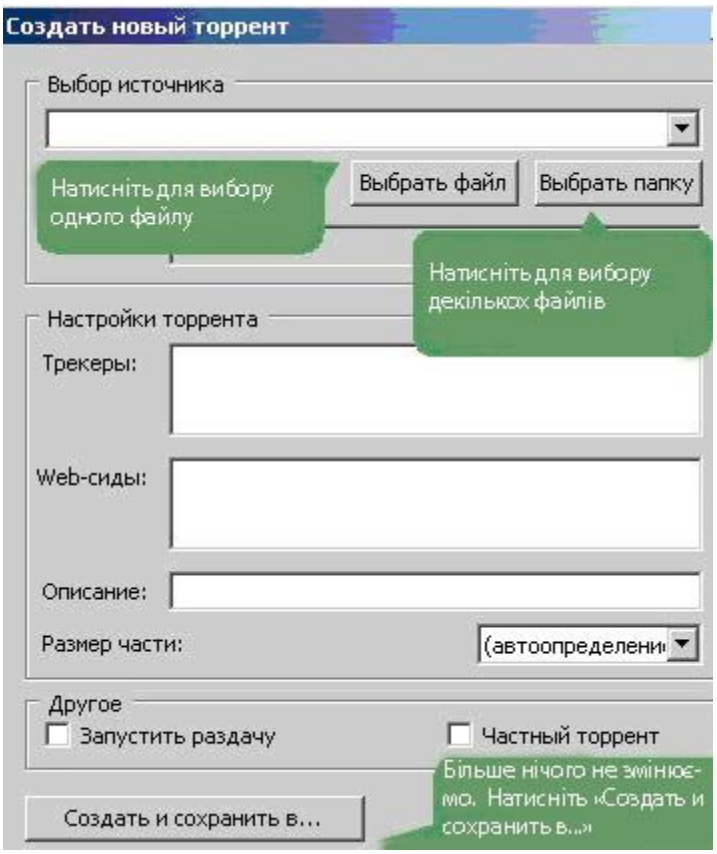


Рис. 3.52Вікно створення торрент-файлу

Необхідно підтвердити, що є бажання продовжити створення торрент-файлу без вказівки трекера. Все, торрент-файл збережений у Вас на комп'ютері. Далі викладаєте його на будь-якому трекері і користувачі зможуть викачувати Ваш файл(и).

Якщо Ви хочете викачати що-небудь з трекера, то просто викачайте відповідний торрент-файл, автоматично відкриється діалогове вікно µTorrent, там слід вказати деякі параметри закачування (рис. 3.53):

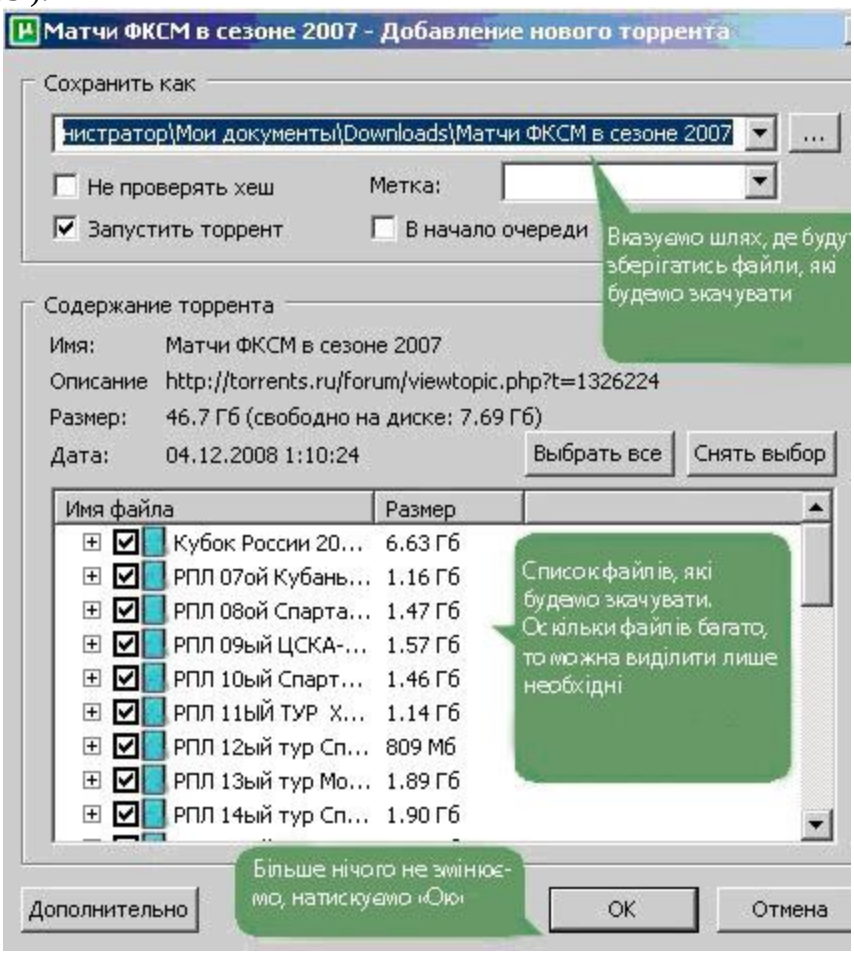


Рис. 3.53Відбір параметрів закачування файлів

Після підтвердження параметрів, які відібрання, програма тут же почне викачувати необхідний файл (рис.3.54).

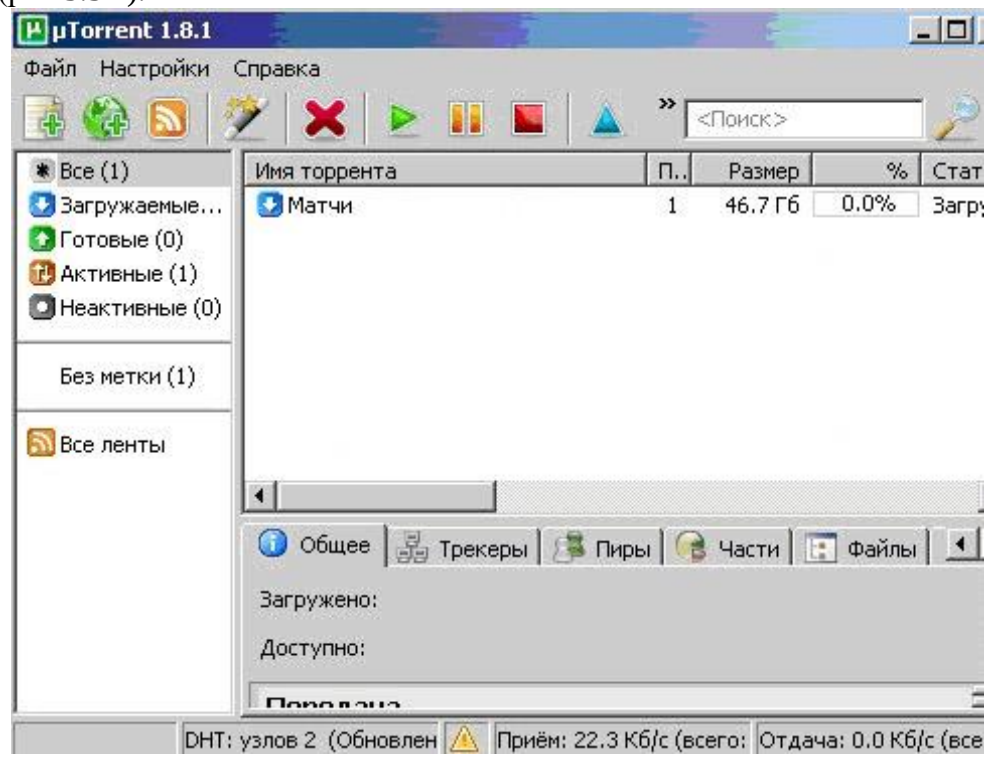


Рис. 3.54 Вікно закачування файлу

Захист інформації в глобальній мережі Internet

Internet і інформаційна безпека несумісні за самою природою Internet. Мережа Internet народилася як чисто корпоративна мережа, проте, в даний час за допомогою єдиного стека протоколів TCP/IP і єдиного адресного простору, вона об'єднує не тільки корпоративні і відомчі мережі (освітні, державні, комерційні, військові і так далі), які є, за визначенням, мережами з обмеженим доступом, але і рядових користувачів, які мають можливість отримати прямий доступ в Internet зі своїх домашніх комп'ютерів.

Як відомо, чим простіше доступ у мережу, тим гірше її інформаційна безпека, тому з повною упевненістю можна сказати, що початкова простота доступу в Internet – гірша за крадіжку, оскільки користувач може навіть і не дізнатися, що у нього були скопійовані файли і програми, не говорячи вже про можливість їх псування і коригування.

Що ж спричинює бурхливе зростання Internet, яке характеризується щорічним подвоєнням числа користувачів? Відповідь проста – дешевизна та зручність отримання інформації, тобто дешевизна програмного забезпечення (TCP/IP), яке в даний час включене в Windows, легкість і дешевизна доступу в Internet (або за допомогою IP-адреси, або за допомогою провайдера) і до всіх світових інформаційних ресурсів.

Платою за користування Internet є загальне зниження інформаційної безпеки, тому для запобігання несанкціонованому доступу до своїх комп'ютерів всі корпоративні і відомчі мережі, а також підприємства, що використовують технологію intranet, ставлять фільтри (fire-wall) між внутрішньою мережею і Internet, що фактично означає вихід з єдиного адресного простору. Ще більшу безпеку дасть відхід від протоколу TCP/IP і доступ в Internet через шлюзи.

Цей перехід можна здійснювати одночасно із процесом побудови усесвітньої інформаційної мережі загального користування, на базі використання мережевих комп'ютерів, які за допомогою мережевої карти і кабельного модему забезпечують високошвидкісний доступ до локального Web-серверу через мережу кабельного телебачення.

Для вирішення цих і інших питань при переході до нової архітектури Internet потрібно передбачити наступне:

По-перше, ліквідовувати фізичний зв'язок між майбутньою Internet (яка перетвориться на Усесвітню інформаційну мережу загального користування) і корпоративними й відомчими мережами, зберігши між ними лише інформаційний зв'язок через систему World Wide Web.

По-друге, замінити маршрутизатори на комутатори, виключивши обробку у вузлах IP-протоколу й замінивши його на режим трансляції кадрів Ethernet, при якому процес комутації зводиться до простої операції порівняння MAC-адрес.

По-третє, перейти в новий єдиний адресний простір на базі фізичних адрес доступу до середовища передавання (MAC-рівень), прив'язаних до географічного розташування мережі, і що дозволяє в рамках 48-біт створити адреси понад 64 трильйонів незалежних вузлів.

Безпека даних є однією з головних проблем в Internet. З'являються все нові і нові страшні історії про те, як комп'ютерні зломщики, використовуючі все більш витончені прийоми, проникають в чужі бази даних. Зрозуміло, усе це не сприяє популярності Internet в ділових колах. Одна тільки думка про те, що які-небудь хулігани або, що ще гірше, конкуренти, зможуть дістати доступ до архівів комерційних даних, примушує керівництво корпорацій відмовлятися від використання відкритих інформаційних систем. Фахівці стверджують, що подібні побоювання безпідставні, оскільки у компаній, що мають доступ і до відкритих, і до приватних мереж, практично рівні шанси стати жертвами комп'ютерного терору.

Кожна організація, що має справу з якими б то не було цінностями, рано чи пізно стикається з посяганням на них. Передбачливі починають планувати захист заздалегідь, ті, які сумнівалися, – після першого великого "проколу". Так або інакше, постає питання про те що, як і від кого захищати.

Зазвичай перша реакція на погрозу – бажання заховати цінності в недоступне місце і приставити до них охорону. Це відносно нескладно, якщо мова йде про такі цінності, які довго не знадобляться: прибрали і забули. Куди складніше, якщо необхідно постійно працювати з ними. Кожне звернення до сховища за цінностями зажадає виконання особливої процедури, відніме час і створить додаткові незручності. Така дилема безпеки: доводиться робити вибір між захищеністю вашого майна і його доступністю, а значить, і можливістю корисного використання.

Усе це справедливо й відносно інформації. Наприклад, база даних, що містить конфіденційні відомості, лише тоді повністю захищена від посягань, коли вона знаходиться на дисках, знятих із комп'ютера й прибраних у місце, що охороняється. Як тільки ці диски встановлені в комп'ютер і почали використовуватись, з'являється відразу декілька каналів, за якими зловмисник, у принципі, має можливість дістати доступ до ваших таємниць без вашого відома. Іншими словами, ваша інформація або недоступна для всіх, або не захищена на сто відсотків.

Може здатися, що із цієї ситуації немає виходу, але інформаційна безпека схожа на безпеку мореплавання: і те, і інше можливе лише з урахуванням деякої допустимої міри ризику.

В області інформації дилема безпеки формулюється, таким чином: слід вибирати між захищеністю системи і її відкритістю. Правильніше, втім, говорити не про вибір, а про баланс, оскільки система, що не володіє властивістю відкритості, не може бути використана.

У банківській сфері проблема безпеки інформації ускладнюється двома чинниками: по-перше, майже всі цінності, з якими має справу банк (окрім готівки і ще дечого), існують лише у вигляді тієї або іншої інформації. По-друге, банк не може існувати без зв'язків із зовнішнім світом: без клієнтів, кореспондентів і тому подібне При цьому за зовнішніми зв'язками обов'язково передається та сама інформація, що виражає собою цінності, з якими працює банк (або відомості про ці цінності і їх рух, які іноді коштують дорожче за самі цінності). Ззовні приходять документи, за якими банк перекладає гроші з одного рахунку на інший. Зовні банк передає розпорядження про рух засобів за кореспондентськими рахунками, так що відкритість банку задана apriori.

Варто відзначити, що ці міркування справедливі у відношенні не тільки до автоматизованих систем, але й до систем, що побудовані на традиційному паперовому документообігу й не використовують інших зв'язків, окрім кур'єрської пошти. Автоматизація додала головного болю службам безпеки, а нові тенденції розвитку сфери банківських послуг, цілком засновані на інформаційних технологіях, посилюють проблему.

Засоби захисту інформації.

Зараз навряд чи комусь треба доводити, що при підключенні до Internet піддається ризику безпека локальної мережі і конфіденційність інформації, що міститься в ній. За даними CERT Coordination Center в 1995 році було зареєстровано 2421 інцидентів – зломів локальних мереж і серверів. За наслідками опитування, проведеного Computer Security Institute (CSI) серед 500 найбільших організацій, компаній і університетів з 1991 року число незаконних вторгнень зросло на 48.9 %, а втрати, викликані цими атаками, оцінюються в 66 млн. доларів США.

Одним із найпоширеніших механізмів захисту від інтернетівських бандитів – "хакерів"– є застосування міжмережевих екранів – **брандмауерів (firewalls).**

Варто відзначити, що унаслідок непрофесіоналізму адміністраторів і недоліків деяких типів брандмауерів близько 30% зломів здійснюється після установки захисних систем.

Атаки на TCP/IP і захист від них

Атаки на TCP/IP можна розділити на два види: пасивні й активні. При даному типі атак крекери ніяким чином не виявляють себе і не вступають безпосередньо у взаємодію з іншими системами. Фактично все зводиться до спостереження за доступними даними або сесіями зв'язку.

Атака типу дслуховування полягають в перехопленні мережевого потоку і його аналізі. Для здійснення підслуховування крекеру необхідно мати доступ до машини, що розташована на шляху мережевого потоку, який необхідно аналізувати; наприклад, до маршрутизатора або PPP-серверу на базі UNIX. Якщо крекеру вдасться отримати достатні права на цій машині, то за допомогою спеціального програмного забезпечення він зможе проглядати весь трафік, що проходить через заданий інтерфейс.

Другий варіант – крекер дістає доступ до машини, яка розташована в одному сегменті мережі з системою, яка має доступ до мережевого потоку. Наприклад, у мережі "тонкий ethernet" мережева карта може бути переведена в режим, в якому вона отримуватиме всі пакети, що циркулюють мережею, а не тільки адресовані їй конкретно. У даному випадку крекеру не потрібний доступ до UNIX – досить мати PC з DOS або Windows (часта ситуація в університетських мережах) .

Оскільки TCP/IP-трафік, як правило, не шифрується (ми розглянемо виключення нижче), крекер, використовуючи відповідний інструментарій, може перехоплювати TCP/IP-пакети, наприклад, telnet-сесій і витягувати з них імена користувачів і їх паролі.

Слід відмітити, що даний тип атаки неможливо відстежити, не володіючи доступом до системи крекера, оскільки мережевий потік не змінюється. Єдиний надійний захист від підслуховування – шифрування TCP/IP-потоку (наприклад, secure shell) або використання одноразових паролів (наприклад, S/KEY). Інший варіант рішення – використання інтелектуальних світчів і UTP, внаслідок чого кожна машина отримує тільки той трафік, що адресований їй.

Природно, підслуховування може бути й корисно. Так, даний метод використовується великою кількістю програм, що допомагають адміністраторам в аналізі роботи мережі (її завантаженості, працездатності й так далі). Один з яскравих прикладів – загальновідомий tcpdump .

Активні атаки на рівні TCP

При даному типі атак крекер взаємодіє з одержувачем інформації, відправником і/або проміжними системами, можливо, модифікуючи і/або фільтруючи вміст TCP/IP-пакетів. Дані типи атак часто здаються технічно складними в реалізації, проте для хорошого програміста не складає труднощів реалізувати відповідний інструментарій. На жаль, зараз такі програми стали доступні широким масам користувачів.

Активні атаки можна розділити на дві частини. У першому випадку крекер робить певні кроки для перехоплення і модифікації мережевого потоку, або спроб "прикинутися" іншою системою. У другому випадку протокол TCP/IP використовується для того, щоб привести систему-жертву в неробочий стан.

Володіючи достатніми привілеями в Unix (або просто використовуючи DOS або Windows, що не мають системи обмежень користувачів), крекер може уручну формувати IP-пакети і передавати їх за мережею. Природно, поля заголовка пакету можуть бути сформовані довільним чином. Отримавши такий пакет, неможливо з'ясувати звідки реально він був отриманий, оскільки пакети не містять шляхи їх проходження. Звичайно, при установці зворотної адреси, не співпадаючої з поточною IP-адресою, крекер ніколи не отримає відповідь на відісланий пакет. Проте, як ми побачимо, часто це і не потрібно.

Можливість формування довільних IP-пакетів є ключовим пунктом для здійснення активних атак.

Захист інформації при застосуванні особистої системи мережевого захисту McAfee Personal Firewall Plus

Особиста система мережевого захисту встановлює бар'єр між вашим комп'ютером і Інтернетом, (табл. 3.9) за умовчанням проводить моніторинг інтернетівського трафіку на предмет підозрілих дій. Вона може виконувати наступні функції:

- Захищати від потенційних досліджень хакера й нападів.

- Захищати від вірусних вторгнень.
- Контролювати інтернетівську й мережеву діяльність.
- Попереджувати про потенційно ворожі події.
- Забезпечувати детальну інформацію щодо підозрілого інтернетівського трафіку.
- Забезпечувати розширену інтелектуальну обробку доступу. Особиста система мережевого захисту спочатку відзначає, чи розпізнає спробу доступу, як дозволену, або недозволену. Якщо спробу доступу визначено як дозволену, система автоматично дозволяє цей доступ до Інтернету.
- Об'єднувати функціональність Hackerwatch.org, зокрема перевіряє повідомлення, події, одночасно перевіряючи інструменти і здатність поштових повідомлень до подій і інших діалогових повноважень.
- Забезпечувати поліпшене запобігання входженню в мережу або надійне виявлення троянців, закладок і т.п. Блокує потенційну можливість передавання ваших особистих даних.
- Забезпечує поліпшений візуальний розгляд (візуальний слід, який включає легкі для читання графічні карти, що показують джерело ворожих нападів і трафік, перелік IP-адрес від вашого комп'ютера до нападника) вторгнення від Інтернету.

Примітка:Використання Firewall дозволяє деякою мірою уникнути загроз, із використанням евристично-подібної функціональності звести "на нівець" ризик від несанкціонованого сканування портів. Ця програма не дає можливості одержати з портів, що не входять у список дозволених, яку-небудь відповідь, тому що взагалі не пропускає до них подібного роду запити. Але Firewall не зможе допомогти, якщо атака ведеться за допомогою цілком законного доступу – скажімо, у вашій пошті виявиться лист, що містить вірус.

Системні вимоги

- Microsoft Windows 98, 2000, або XP.
- Персональний комп'ютер з 486 або вищий процесор (Рекомендований Pentium).
- 8 МБ вільної пам'яті жорсткого диска для інсталяції.
- Microsoft Internet Explorer 5.01 або вище.

Примітка: Щоб відновити найпізнішу версію Internet Explorer, відвідайте сайт Microsoft Web у http://www.microsoft.com/.

Установка програми

Скопіюйте каталог McAfee Personal Firewall Plus на жорсткий диск свого комп'ютера.

Для установки запустіть на виконання файл McAfeePersonalFirewallPlus.exe та виберіть потрібні параметри в процесі роботи майстра установки. Після установки запустіть файл mpf.reg і погодьтеся на внесення змін до реєстру Windows.

Запуск McAfee SecurityCenter

McAfee SecurityCenter – ваш універсальний обчислювальний центр захисту. Він забезпечує консолідоване представлення стану захисту вашого комп'ютера, і наявність вірусних тривог. Можливо запустити Security Center від значка McAfee у панелі задач (кнопка червоного кольору), використавши допоміжну клавішу маніпулятора типу "миш" (рис. 3.55), або з робочого столу Windows.

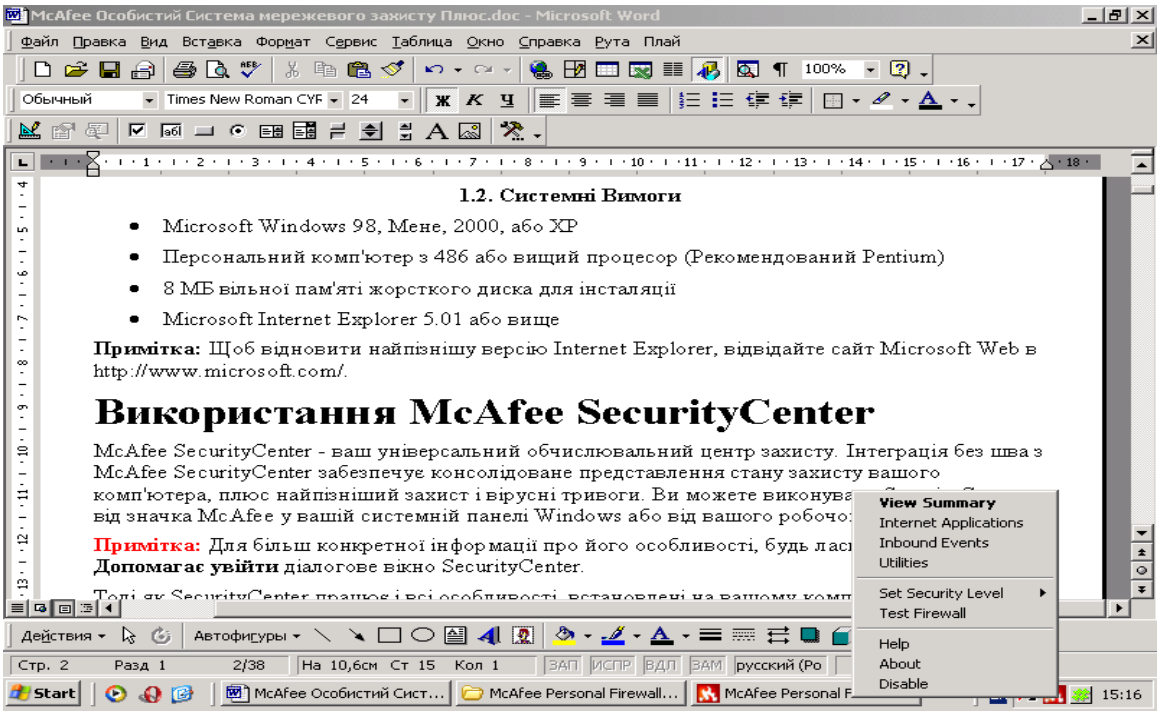


Рис. 3.55. Вікно запуску програми.

Якщо один або більше застосувань, установлених на вашому комп'ютері, McAfee відключені, то колір кнопки змінюється на чорний. Для запуску програми введіть команду View Summary. Перед з'явиться діалогове вікно програми (рис. 3.56).

Конфігурування елементів системи мережевого захисту

Не потрібно, як правило, формувати параметри мережевого захисту, тому що значення, які встановлені за умовчанням забезпечують адекватну безпеку проти вторгнення. Можлива, проте, зміна параметрів налагодження за допомогою помічника встановлення програми.

Помічник установлення дозволяє налагодити:

- вид тривог, які потрібно одержувати;
- захист від вірусів;
- мережевий тип підключення;
- прикладні рекомендаційні параметри налагодження.

Щоб звернутися до **Помічника,** клацніть значок **Security Settings.** Виконуйте команди діалогових вікон.

Установки:

Клацніть правою кнопкою миші кнопку (рис. 3.57) та введіть команду **Утиліти**.

Налагодження параметрів проводиться в діалоговому вікні **Utilities** (рис. 3.58). Установіть рівень захисту, переміщаючи засувку на бажаний рівень. Якщо користувач системи новачок мережевого захисту, прийміть задане за умовчанням врегулювання **Стандарту.** Діапазони рівня захисту змінюються від низького рівня (відкритий) до максимального (сувора ізоляція):

Рис. 3.56. Вікно програми.

Таблиця 3.9

Рівні захисту

Діапазони рівня захисту	Опис
Сувора ізоляція High (Lockdown)	Весь трафік зупинено. Це такий же режим, як і у випадку відключення інтернет-з'єднання. Можливо використовувати це врегулювання, щоб блокувати порти.
Щільний Tight	Через прикладні запити забезпечується тільки вид доступу до Інтернету, який потрібен. Блокується будь-який недозволений доступ.
Стандарт Standard	Рекомендований рівень доступу. Надається прикладний повний доступ. Повний доступ дозволяє застосуванням як посилати дані, так і одержувати непрошені дані на несистемних портах. Використовуйте це врегулювання, якщо користувач – новачок системи мережевого захисту.
Довіра Trusting	Усім підключенням автоматично довірено, коли вони початково намагаються звертатися до Інтернету. Проте, потрібно вибрати параметри, щоб бути повідомленим про нові підключення на вашому комп'ютері із тривогами. Використовуйте це врегулювання, якщо виявлено, що деякі ігри або потокові носії не працюють.
Низька фільтрація Open/No)	Ваша система мережевого захисту фактично відключена. Це врегулювання дозволяє весь трафік пропускати без фільтрації.

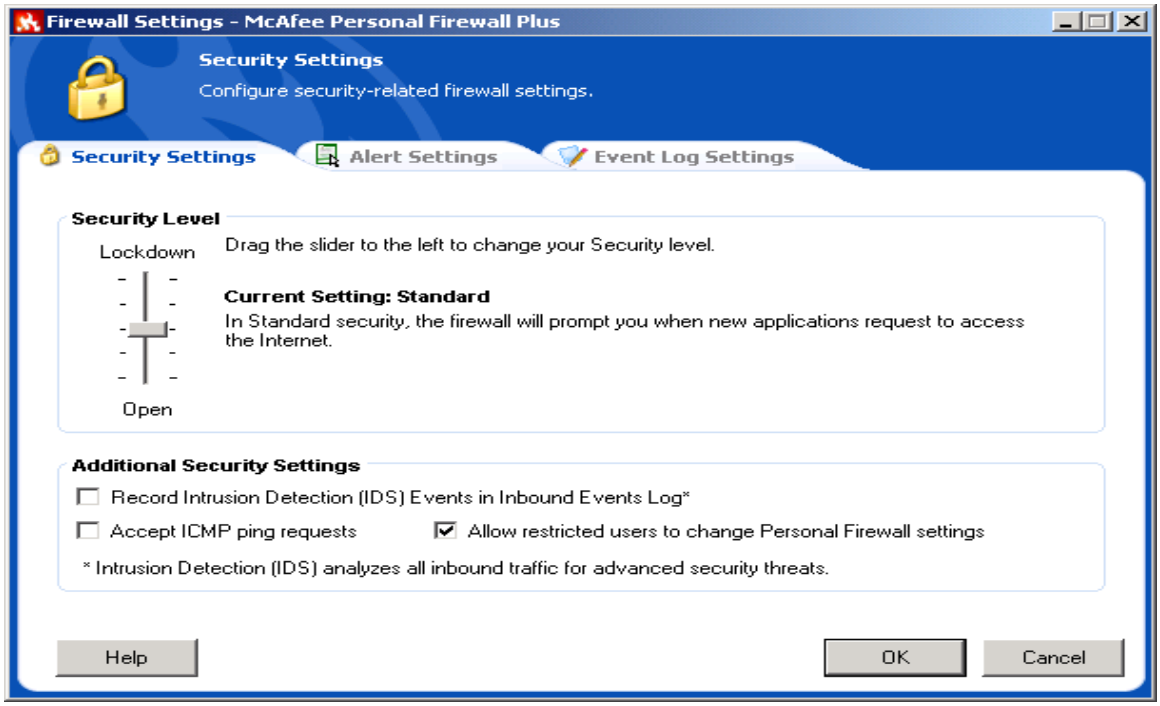


Рис. 3.57. Вікно утиліт.

Примітка: налагодження параметрів можливе, якщо надані права адміністратора системи.

- **Record Intrusion Detection (IDS) Events in Inbound Events Log (система візуального зображення інформації).** Якщо вибрати цей налагоджувальний елемент, події візуального зображення інформації з'являться у файлі реєстрації подій, що відбуваються.
- **Accept ICMP ping requests** (міжмережевий протокол управління повідомленнями, використовується переважно для виконання команд pinging). Якщо вибрати цей налагоджувальний елемент, особиста система мережевого захисту дозволяє всі запити залишати без реєстрації у файлі реєстрації подій, що відбуваються.
- **Allow restricted users to change Personal Firewall settings.** Якщо на комп'ютері операційна система Windows XP і багато користувачів, то необхідно вибрати вказаний параметр для того, щоб дозволити деяким користувачам змінювати параметри налагодження даної програми.

Вкладка Alert Settings.

Виберіть вид тривоги в полі **Alert to Display** для відображення:

- **Show Only Red Alerts** (показувати тільки червоні тривоги) – червоні тривоги містять важливу інформацію, яка вимагає вашої безпосередньої уваги. Наприклад, прикладний доступ запитів до Інтернету й потрібно надати або блокувати доступ.
- **Show Only Red and Green Alerts** (показувати тільки червоні й зелені тривоги) – зелені тривоги інформують про зміни, які були внесені до особистої системи мережевого захисту. Наприклад, зелені тривоги можуть інформувати про підключення, які особиста система мережевого захисту автоматично надала, або про застосування будь-яких нових правил при доступі до Інтернету.
- **Show All Alerts** (показувати усі тривоги) – покази червоних, зелених, і блакитних тривог. Блакитні тривоги містять інформацію, яка не вимагає ніякої відповіді.

Виберіть додаткові налагоджувальні елементи відповіді для тривог, що відображаються:

- **Flash the tray icon when alerts aren't displayed** (спалахнути значку лотка, коли тривоги не відображаються) – при виборі вказаного параметра спалахує значок на панелі задач, коли подія відбувається.
- **Auto-hide non-critical alerts after 10 seconds** (автоматично приховувати некритичні тривоги після 10 секунд) – виконується дія програми, яка вибрана за умовчанням на подію. Якщо не вибрати вказаного параметра, то сигнал тривоги буде на екрані до того часу, доки адміністратор не відреагує на подію. .

- **Animate slide-in alerts** (включені анімовані спливаючі тривоги) – цей перемикач (значення встановлюються за умовчанням) активізує включення ярлика на вашому робочому столі Windows. Щоб одержати стандартні спливаючі тривоги зніміть перемикач.

Виберіть параметри в полі **Smart Recommendations**:

- **Use Smart Recommendations** – особиста система мережевого захисту автоматично дозволяє підключення, що засновані на базі даних розпізнаних застосувань. Завжди буде попередженя про невизначені або потенційно небезпечні програми.
- **Display Smart Recommendations Only** – особиста система мережевого захисту лише рекомендує курс дії.
- **Do not use Smart Recommendations** – не використовувати рекомендації особистої системи мережевого захисту.

Вкладка Event Log Settings

У полі **Inbound Events Logging Settings** виберіть чи повинна реєструвати особиста система мережевого захисту події, що відбуваються. Якщо вибрати реєстрацію подій, особиста система мережевого захисту буде відображати події, що відбуваються, на сторінці Подій основного вікна. За умовчанням, особиста система мережевого захисту реєструє всі типи події. Потрібно змінити типи події для реєстрації. Для цього необхідно ввести команду **Configure**... і у вікні, що з'явиться, відібрати необхідні типи подій, а також указати номери портів показу в представленні подій, що відбуваються, щоб показати початкові й призначені порти події у файлі Подій реєстрації.

Довірені IP-адреси

Список довірених IP-адрес дозволяє отримувати весь трафік від певного комп'ютера на будь-якому порту. Особиста система мережевого захисту не реєструє трафік, або не генерує тривоги події від IP-адреси зі списку довірених IP-адрес. Ваш комп'ютер поводитиметься ніби-то немає ніякої системи мережевого захисту.

Щоб додати IP-адресу до списку "Довірених IP-адрес" необхідно:

Виконати дії за рис. 3.58: на вкладці **Summary** ввести команду **Trusted this IP Addresses**, у діалоговому вікні увести необхідні адреси.

Примітка: при введені адреси, якій довіряють тимчасово, необхідно вказати дату й час закінчення довіри. Після введення команди **OK** IP-адреса з'являється в списку "Довірених IP-адрес".

Системні послуги

У деяких випадках обов'язково необхідно відкрити порти для забезпечення доступу інших комп'ютерів, наприклад, якщо Ваш комп'ютер працює в режимі веб-сервера й т.п. Для цього необхідно на вкладці **Утиліти** ввести команду **System Services** та в діалоговому вікні (рис. 3.59) відібрати потрібні порти доступу, або добавити їх, якщо таких немає в системному списку, ввівши команду **Add**.

Моніторинг трафіку

Моніторинг відображає числові й графічні представлення інтернетівського трафіку, трафіку доступу до Інтернету та доступу від Інтернету. Моніторинг трафіку також показує, які з'єднання зараз використовуються на вашому комп'ютері й IP-адреси, до яких є підключення. Моніторинг трафіку автоматично модифікує свої дані кожних декількох хвилин (рис. 3.60), але можливо уручну модифікувати екран, увівши команду **Refrech**. Для входу в указаний режим необхідно на вкладці **Утиліти** ввести команду **Traffic Monitor**.

Вкладка **Applications** показує інтернетівську діяльність у реальному часі на вашому комп'ютері, швидкості підключення і кількість байтів, які перенесені через Інтернет. **Traffic Analysis** забезпечує візуальне представлення даних, показує норму кілобайт, перенесених за останні 15 хвилин. Із правої сторони графіка нижче розташований перемикач представлення інформації. За його допомогою можна змінити представлення даних та отримати дані за останні 24 години, за поточний або минулий місяць.

Для трафіку, який надходить з Інтернету зелена лінія представляє поточну норму передавання даних, а пунктирна зелена лінія представляє середню норму передавання для вхідного трафіку. Якщо поточна норма передавання й середня норма передавання співпадають за величиною, то пунктирна лінія не з'являється. Для трафіку, який надходить до Інтернету, червоний рядок представляє поточну норму передавання, червона пунктирна лінія представляє середню норму.

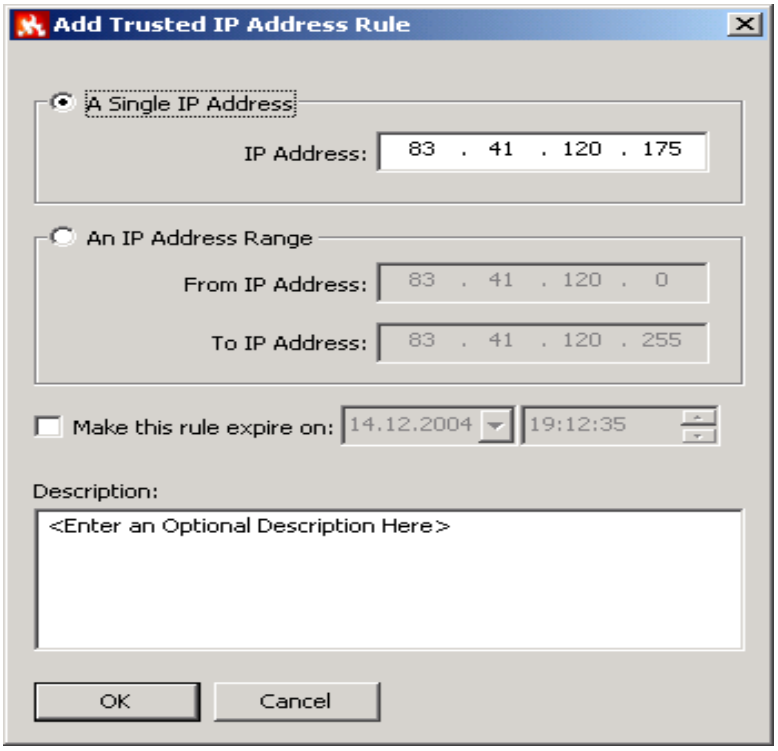


Рис. 3.58. Вікно введення IP-адреси

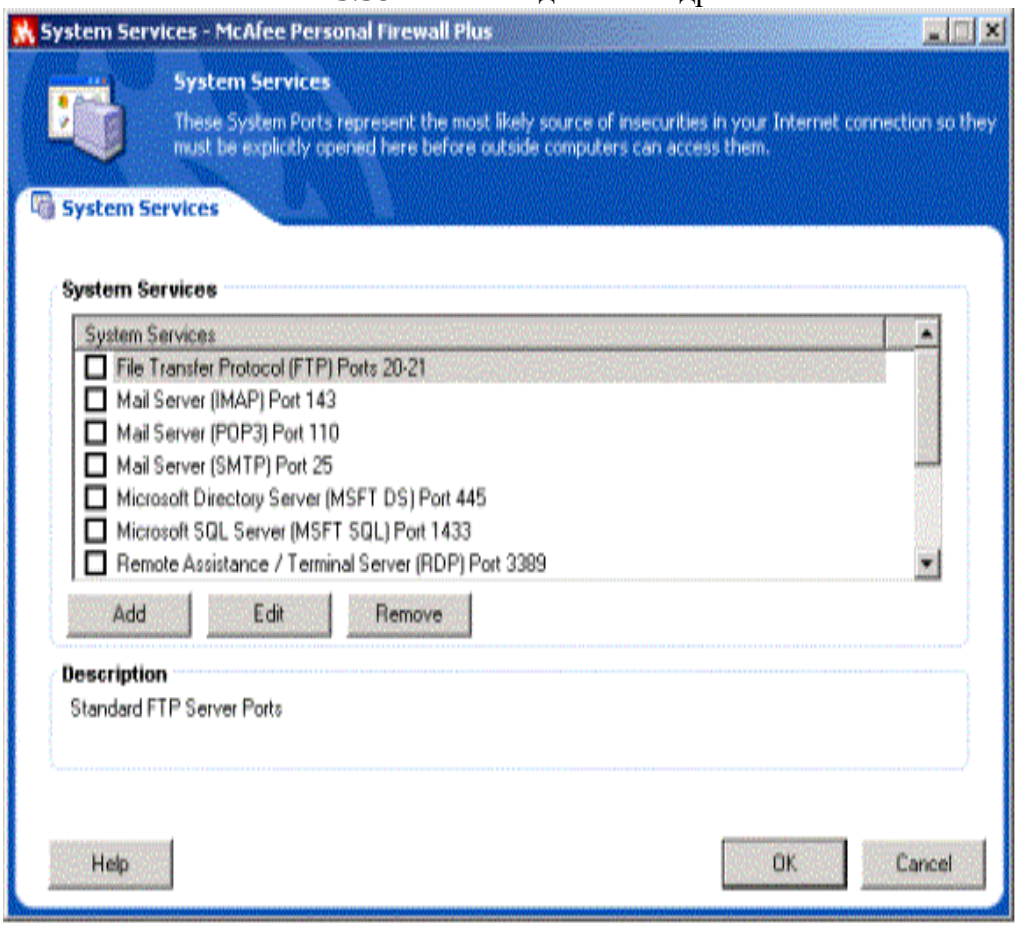


Рис. 3.59. Вікно відбору портів

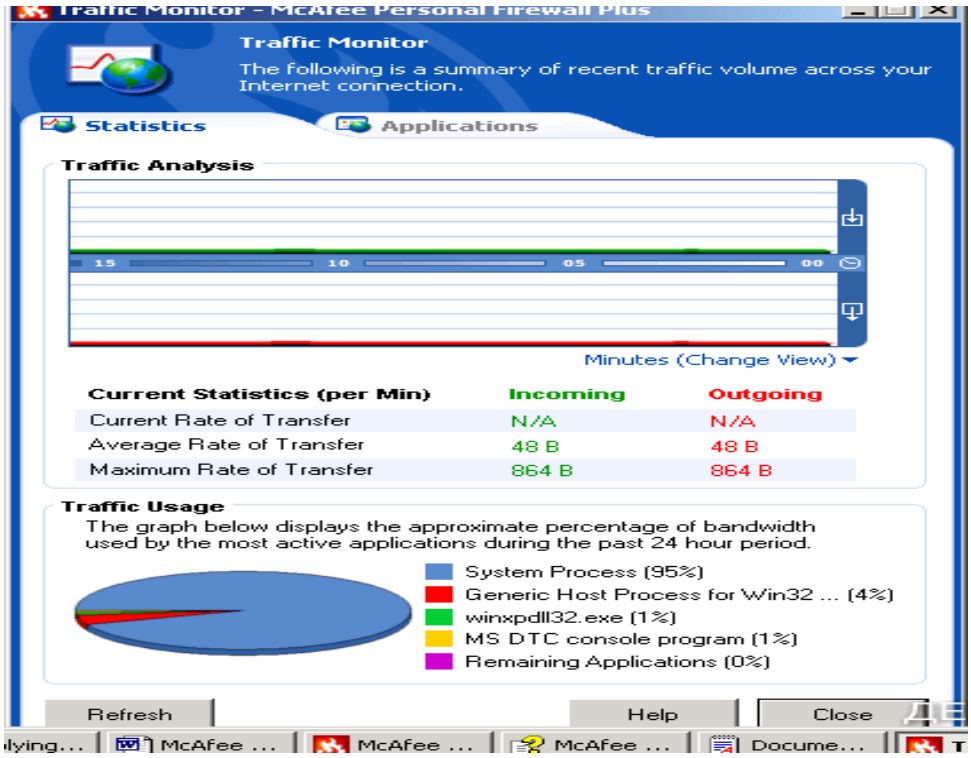


Рис. 3.60. Вікно монітора

Перегляд короткого звіту.

Можна отримати різні сторінки звіту, вибравши потрібну зі списку (рис. 3.61).

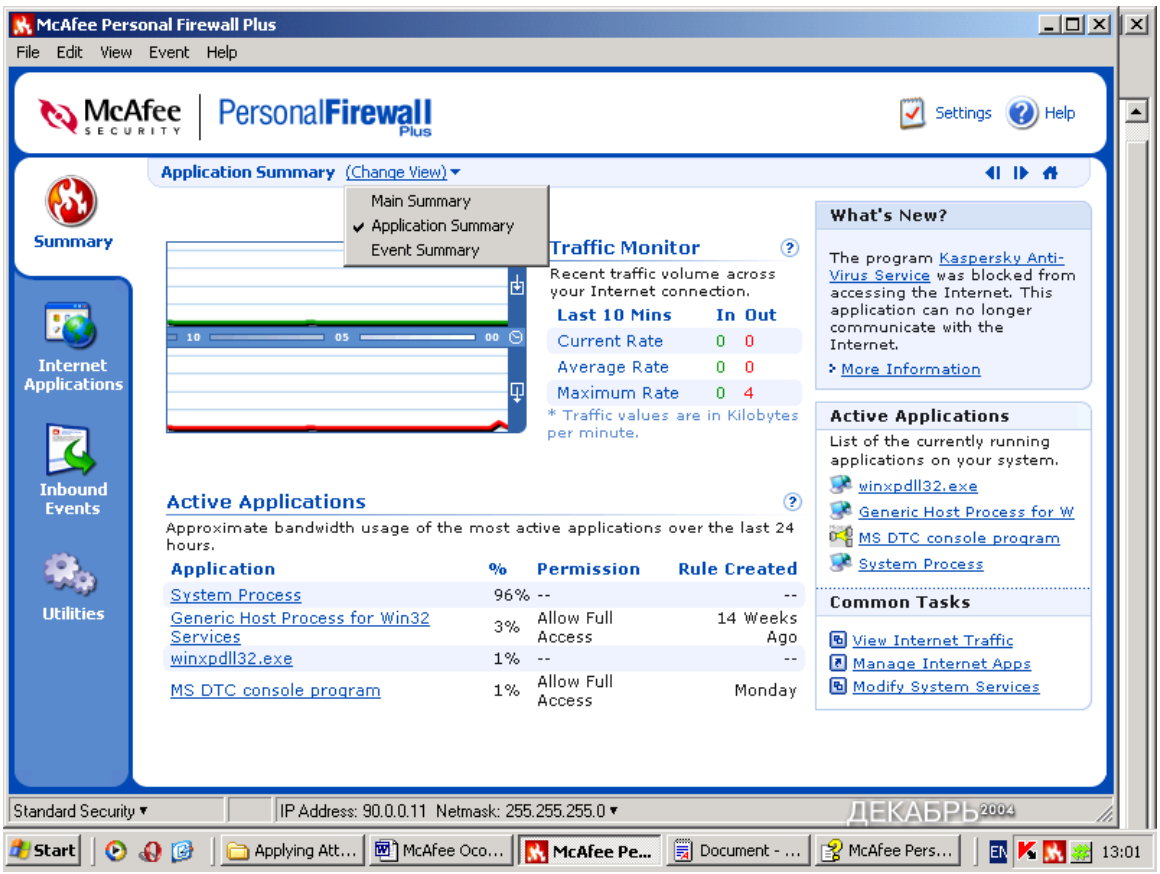


Рис. 3.61. Вікно відбору звітів.

Вкладка Internet Applications.

Вона використовується для того, щоб розглядати список дозволених і блокованих підключень, змінювати параметри підключень, добавляти нові, видаляти старі і т.п. Для дій із підключеннями використовується контекстно-залежне меню (рис. 3.62).

У списку **Дозволів** клацніть правою кнопкою миші рівень дозволу для застосування, і виберіть інший рівень:

- **Allow Full Access –** дозволяє підключення при посиланні й отримуванні даних.
- **Outbound Access Only –** неможливе підключення ззовні.
- **Block This Application** – не дозволяє підключення при посиланні й отримуванні даних.
- **Delete Application Rule –** дозволяє видалити існуюче підключення.

Виберіть команду **New Allowed Application** для створення нового підключення й команду **New Blocked Application** для створення блокованого.

Рис. 3.62. Вікно роботи зі списком дозволів.

Вкладка Inbound Events.

Використовуйте сторінку подій, що відбуваються, щоб розглядати файл подій реєстрації. Він дозволяє створити архів подій та продивитися старі архіви. Можливий перегляд подій за поточний день, останній тиждень, перегляд повного файлу реєстрації, вибір події певних днів, від певних IP-адрес. Для отримання такої інформації необхідно виділити мишкою подію та вибрати відповідну команду у меню **View**.

Можливо експортувати свій файл подій реєстрації, що відбуваються, до текстового файлу. Для цього використовується команда **Exporting Displayed Events** із підменю **Файл.**

Про тривоги.

Для встановлення різних видів тривог необхідно перейти на вкладку **Утиліт** та ввести команду **Alert Settings.** У вікні **Smart Recommendations** відібрати зі списку потрібне значення тривог, за умовчанням установлюється команда **Use Smart Recommendations.** Вона дозволяє отримувати червоні тривоги, які містять важливу інформацію, що вимагає вашої безпосередньої уваги. Розрізняють наступні типи червоних тривог:

- **Internet Application Blocked** – ця тривога з'являється, якщо особиста система мережевого захисту блокує спробу доступу до Інтернету. Наприклад, якщо з'являється тривога програми Trojan, McAfee автоматично блокує цей доступ програми до Інтернету, і рекомендує переглянути комп'ютер на наявність вірусів.
- **Application Wants to Access the Internet** – ця тривога з'являється, коли в результаті Інтернет-пошуків мережа переходить до нової недозволеної IP-адреси. (Стандартний або щільний захист).
- **Application Has Been Modified** – ця тривога з'являється, коли дозвіл доступу до Інтернету, що був наданий раніше, змінився. (Довіра, стандарт, або щільний захист).
- **Application Requests Server Access** – ця тривога з'являється, коли доступ мережі наперед дозволений, а звертання йде як до сервера. (Щільний Захист).

Зелені Тривоги

Зелені тривоги інформують про зміни, які були зроблені до особистої системи мережевого захисту. Наприклад, зелені тривоги можуть інформувати про нові надані доступи до Інтернету, або інформувати про будь-які нові правила застосування.

- **Program Allowed to Access the Internet** – ця тривога з'являється, коли особиста система мережевого захисту автоматично надає інтернетівський доступ для всіх нових або змінених застосувань, а потім повідомляє (Довіра захисту), про нові правила застосування.

Блакитні Тривоги

Блакитні тривоги містять інформацію, але не вимагають ніякої відповіді.

- **Connection Attempt Blocked** – ця тривога з'являється, коли особиста система мережевого захисту блокує небажаний інтернетівський або мережевий трафік. (Довіра, стандарт, або щільний захист)

Блокування спроби підключення до комп'ютера

Наприклад, після отримання сигналу тривоги розгляньте короткий опис події, далі виберіть із цих налагоджувальних елементів:

- Уведіть команду **Trace This Address,** щоб побачити візуальний слід адрес, для цієї події.
- Уведіть команду **Ban This Address ,** щоб блокувати цю адресу для доступу до вашого комп'ютера. Адреса додається до списку "Заборонених IP-адрес".
- Уведіть команду **Trust This Address,** щоб дозволити цій IP-адресі звернутися до вашого комп'ютера.
- Уведіть команду **Continue What I Was Doing,** якщо не потрібно обрати дію після того, як особиста система мережевого захисту вже виконала її.

Розвиток мереж в майбутньому

В майбутньому комп'ютерні мережі, в традиційному сенсі цього слова, тобто мережі, які передають тільки текст і числа зникнуть. Головна тенденція для всіх типів мереж – телефонних, комп'ютерних, телевізійних – конвергенція, тому вже сьогодні комп'ютерні мережі передають невластиві їм спочатку типи трафіку. Це, перш за все, звук в різних видах: у формі інтерактивної взаємодії двох учасників телефонної розмови; у формі мовлення за запитом – передавання пісень або заздалегідь записаних виступів чи інтерв'ю через інтернет; у формі голосової пошти. Передавання зображення вимагає істотно вищої пропускної спроможності і тому поки застосовується набагато в скромніших масштабах, проте, навіть при швидкості доступу 64-128 кбіт/с, можна проглянути в реальному часі телепередачу в невеликому прямокутному віконці на екрані ПК.

Таким чином, телекомунікаційні мережі майбутнього – це мережі, що однаково добре передають пульсуючий трафік даних і потоковий трафік звуку і відео. Мережі майбутнього успадкують кращі риси своїх прабатьків – телефонних і комп'ютерних мереж, а також мереж радіо- і телемовлення, але з використанням загальної транспортної технології, яка повинна забезпечити передавання кожного типу трафіку з потрібною для нього якістю обслуговування (QOS). Така технологія повинна, на загальну думку фахівців, ґрунтуватися на техніці комутації пакетів і широко застосовувати протокол IP, що ріднить мережі майбутнього із нинішніми комп'ютерними мережами, але із значними технологічними новаціями.

У число таких удосконалень, швидше за все, увійдуть термінальні пристрої нового типу, які поєднуватимуть функціональну потужність ПК із простотою в обігу телефону. Прообразом таких пристроїв сьогодні є органайзери, персональні секретарі і мобільні телефони. Відповіддю на різке зростання потреби в надшвидкісному і якісному транспорті стане технологія керованих віртуальних шляхів на основі стандартів DWDM і GMPLS. Ядро нової публічної телекомунікаційної мережі будується на оптичних кабелях з великою кількістю волокон, що забезпечить мультитерабітну пропускну спроможність між вузлами комутації і створить основу для передавання обсягів інформації, що здаються сьогодні немислимими, між абонентами мережі, а також засоби зв'язку супутників.

Низька швидкість доступу, особливо для масових абонентів, являється сьогодні однією з основних перешкод на шляху широкого впровадження нових мультимедійних послуг. Існують декілька шляхів вирішення цієї проблеми – використання існуючих мідних абонентських закін-

чень, що найбільше підходить для масового індивідуального доступу; безпровідного доступу, як фіксованого, так і мобільного; прокладення оптичних абонентських закінчень з використанням економічної пасивної технології PON.

Зміняться і локальні мережі. Замість пасивного кабелю, що сполучає комп'ютери, в них у великій кількості з'явиться різноманітне комунікаційне устаткування – комутатори, маршрутизатори, шлюзи. Завдяки такому обладнанню стане можливою побудова великих корпоративних мереж, що налічують тисячі комп'ютерів і що мають складну структуру. Відродився інтерес до потужних комп'ютерів – в основному через те, що після спаду ейфорії з приводу легкості роботи з персональними комп'ютерами з'ясувалося, що системи, які складаються з сотень серверів, обслуговувати складніше, ніж декілька великих комп'ютерів. Тому на новому витку еволюційної спіралі на підприємства почали повертатися мейнфрейми, але вже як повноправні мережеві вузли, що підтримують технологію Ethernet або Token Ring, а також стек протоколів TCP/IP, що став завдяки Інтернету мережевим стандартом де-факто.

Ось тільки деякі напрями розвитку телекомунікаційних мереж, які виразно видно вже сьогодні.

КОНТРОЛЬНІ ПИТАННЯ

1. Який принцип роботи модемів?
2. Охарактеризуйте поняття MNP- протоколи.
3. Які Ви знаєте режими роботи модемів?
4. Охарактеризуйте внутрішні й зовнішні модеми.
5. Яка роль індикаторних лампочок модему?
6. Які Ви знаєте марки модемів?
7. Який порядок настроювання віддаленого доступу в мережу?
8. Охарактеризуйте протоколи канального рівня: UUCP, SLIP, PPP.
9. Які особливості налагодження з'єднання з Інтернетом при використанні локальної мережі й без неї?
10. Що Ви знаєте про Internet? Історія, призначення, власник, основні характеристики.
11. Що Ви знаєте про World Wide Web? Призначення, основні характеристики.
12. Охарактеризуйте елементи мережі: вузли, лінії зв'язку, комп'ютери, операційні системи.
13. Що Ви знаєте про модеми, швидкість передавання даних?
14. Охарактеризуйте протоколи обміну даними Transmission Control Protocol і Internet Protocol (TCP/IP) у сучасній мережі Internet.
15. Що Ви знаєте про технологію клієнт-сервер у сучасній мережі Internet?
16. Які існують постачальники послуг Internet?
17. Які Ви знаєте сервиси мережі?
18. Які існують IP-адреси комп'ютера?
19. Які принципи формування доменної адреси комп'ютера?
20. Які Ви знаєте домени верхнього рівня в США й інших країнах світу?
21. Які існують буквені доменні адреси й цифрові IP-адреси?
22. Охарактеризуйте таблиці доменних адрес і IP-адрес на серверах DNS (Domain Name Service,).
23. Охарактеризуйте програму- браузер (browser) для різних підсистем мережі Internet (Telnet, FTP, Gopher, WWW).
24. В чому особливість роботи програми-браузера в режимі On-Line (на лінії) і в режимі Off-Line (за межами лінії)?
25. Які Ви знаєте елементи робочого вікна браузера?
26. В чому особливість налагоджування програми-браузера?
27. Охарактеризуйте гіпертекстові посилання для завантаження в браузер повної HTML-сторінки.
28. Які принципи формування структури WEB сторінок?
29. Охарактеризуйте проблеми кодування кирилиці.
30. Охарактеризуйте програми перегляду (браузери) Netscape Navigator і Microsoft Internet Explorer.

31. Як провести виклик із браузера інших засобів перегляду файлів різних форматів різних підсистем мережі Internet (Telnet, FTP, Gopher)?
32. Які Ви знаєте об’єкти пошуку потрібної інформації в Internet?
33. В чому суть технології пошуку інформації в Internet? Виклик у браузер початкової сторінки пошукової системи (тематичного каталогу або автоматичного індексу).
34. В чому суть простого та розширеного пошуку інформації в Internet?
35. Охарактеризуйте використання складних операторів у запитах.
36. Які принципи ранжирування результатів пошуку? Розмітка документа.
37. Порядок запуску програми Outlook Express.
38. Порядок налагоджування програми Outlook Express.
39. Охарактеризуйте користувальницький інтерфейс пошти Outlook Express.
40. Перерахуйте складові вікна програми.
41. Охарактеризуйте призначення складових вікна програми.
42. Яка інтерпретація значків із різними зображеннями конверта в області перегляду?
43. Який порядок формування нового повідомлення?
44. Які Ви знаєте типи “важливості" повідомлення?
45. Як налагодити програму на термінову відправку листів?
46. Як налагодити програму на зберігання листів перед відправкою в папці Вихідні?
47. Який порядок пересилання вкладених файлів за E-mail?
48. Які Ви знаєте типи поштових папок Outlook Express?.
49. Який порядок одержання вхідної пошти?
50. Охарактеризуйте адресну книгу Outlook Express
51. Які Ви знаєте шляхи поповнення адресної книги Outlook Express?
52. Які Ви знаєте додаткові можливості програми Outlook Express?
53. Які Ви знаєте загальні принципи роботи з утилітою FTP?
54. Які дії дозволяє виконати мережева утиліта FTP ?
55. Розкажіть про основні команди утиліти FTP.
56. Як здійснюється з’єднання й взаємодія процесів за протоколом FTP ?
57. Які можливості протоколу FTP використовуються програмами - "браузерами" ?
58. Що таке FTP-сервер ? Для чого використовується анонімне з’єднання із сервером ?
59. Яке призначення програми Telnet?
60. кий порядок включення режиму Telnet?
61. Які Ви знаєте адреси системи Telnet?
62. Який порядок роботи із системою Telnet?
63. Охарактеризуйте систему визначення часу Telnet?.
64. Що таке географічна система Telnet?
65. Що таке системи дошок оголошень Telnet (BBS)?
66. Охарактеризуйте систему конференцій Telnet?
67. Які переваги електронної пошти?
68. Що собою представляє електронна поштова скринька?
69. З яких частин складається адреса електронної пошти, приведіть приклад?
70. Що не рекомендується вказувати в паролі?
71. В якому режимі частіше здійснюється робота з електронною поштою?
72. Як працювати з адресною книгою?
73. Як прикріпити файл до листа, які обмеження накладаються на файли, що прикріплюються?
74. Яке призначення програми Teleport Pro?
75. Сформулюйте поняття проектного файлу.
76. Поясніть процес створення нового проекту.
77. Які типи файлів може дослідити програма Teleport Pro?
78. Поясніть призначення команд майстра створення проектів?
79. Які існують групові імена, що використовуються при пошуку файлів?
80. Які особливості збереження проекту?
81. Як запустити проект на виконання?
82. Як переглянути результати роботи програми?
83. Як налагодити параметри проекту?

84. Як установити програми FlashGet на комп’ютер?
85. Яке призначення програми FlashGet?
86. Як створити список файлів для закачування в FlashGet?
87. Як установити автоматичний запуск програми FlashGet при збереженні файлів із другої програми, наприклад, Internet Explorer?
88. Які методи завантаження файлів у програмі FlashGet?.
89. Як установити розбивання файлу при закачуванні на декілька частин? Для чого це потрібно?
90. Як установити час автоматичного закачування файлів? Для чого це потрібно?
91. Для чого і як налагоджуються параметри PROXY?
92. Як підключити автоматичну перевірку файлів на наявність вірусів?
93. Пірінгові мереж та їх застосування.
94. Порядок роботи з програмами в пірінгвих мережах.
95. Охарактеризуйте складові головного меню програми McAfee Personal Firewall Plus.та її призначення.
96. Які системні вимоги при інсталяції програми?
97. Який порядок запуску McAfee SecurityCenter?
98. Які підходи до конфігурування елементів системи мережевого захисту?
99. Охарактеризуйте конфігурування елементів системи мережевого захисту за допомогою помічника установки.
100. Охарактеризуйте вибір елементів у вікні утиліт.
101. Які типи тривог існують.
102. Охарактеризуйте червоні тривоги, їх призначення.
103. Охарактеризуйте зелені тривоги, їх призначення .
104. Охарактеризуйте блакитні тривоги, їх призначення .
105. Яке призначення вкладки Event Log Settings?
106. Який порядок установлення Ip адрес?
107. Які існують системні послуги?
108. Охарактеризуйте порти та їх відкриття, закриття.
109. Охарактеризуйте моніторинг трафіку.
110. Який порядог роботи зі звітами?
111. Яке призначення вкладки Internet Applications?
112. Яке призначення вкладки Inbound Events?
113. Який порядок бокування спроби підключення до комп’ютера в різних випадках?

РОЗДІЛ 4
БЕЗПРОВІДНІ МЕРЕЖІ

Перша безпровідна мережа ALOHAnet була побудована в Гавайському університеті в 1971 році. З того часу безпровідні мережі використовуються там, де прокладка кабелів утруднена, недоцільна або просто неможлива. Наприклад, в історичних будівлях, промислових приміщеннях із металевою або залізобетонною підлогою, в офісах, отриманих у короткострокову оренду, на складах, виставках, конференціях, і тому подібне.

Існує два типи безпровідних мереж – мережі з крапкою доступу(рис. 4.1) і без неї. Мережа, взаємодія в якій здійснюється безпосередньо між мережевими адаптерами (рис. 4.2) пристроїв, називається Independent Basic Service Set (IBSS) або Ad-Hoc. Переваги Ad-Hoc-мережі полягають у високій мобільності (наприклад, зв'язати пару-трійку КПК за Wi-Fi можно завжди і скрізь) і з порівняно низькою вартостю, яка дорівнює вартості мережевих адаптерів. Мінуси у такої мережі теж є. Наприклад – обмежена відстань між пристроями підключеними до мережі, складність взаємодії з іншими мережами. Всі ці проблеми можна вирішити за допомогою так званої точки безпровідного доступу (Access Point).

Мережа на основі точки доступу називається Infrastructure-мережею, причому, існують різновиди таких мереж – BSS – Basic Service Set – мережа з використанням однієї крапки доступу, і ESS – Extended Service Set – декілька об'єднаних крапок доступу.

Рис. 4.1. Крапка доступу

Крапка доступу може бути оснащена інтерфейсом для підключення її до кабельних сегментів мережі, інтерфейсами для виходу в Інтернет і так далі. В результаті, витративши додаткові кошти на крапку доступу, можна отримаєти безліч переваг.

Рис. 4.2. Адаптер

Комп'ютер, через який інші машини виходять в Інтернет, називається ICS-сервером, а самі комп'ютери, що виходять в мережу, – ICS-клієнтами. ICS розшифровується як Internet Connection Sharing, тобто розділення інтернет-з'єднання. ICS – це програмний механізм, який дозволяє декільком комп'ютерам, сполученим в мережу, виходити в Інтернет, користуючись інтернет-з'єднанням одного з них. У застосуванні до безпровідної Wi-Fi-мережі ICS дозволяє використовувати загальне Інтернет-з'єднання всім комп'ютерам – як звичайним ПК і ноутбукам. Тепер трохи технічних деталей. ICS – це спрощена схема для численного доступу в Інтернет. Вона порівняно проста в налагоджені, але ця простота накладає обмеження на деякі мережеві параметри.

Зокрема, всі IP-адреси комп'ютерів, що входять в ICS-мережу повинні належати діапазону 192.168.0.1 – 192.168.0.254 (при масці підмережі 255.255.255.0), адреса ICS-шлюза повинна бути 192.168.0.1.

Найзручніше налагоджувати ICS, використовуючи автоматичні засоби Windows.

Залежно від технології безпровідні мережі підрозділяють на:

- локальні обчислювальні мережі;
- мобільні обчислювальні мережі.

Проміжним етапом переходу від кабельних мереж до безпровідних є спосіб передавання «крапка-крапка». Ця технологія передбачає обмін даними тільки між комп'ютерами, на відміну від взаємодії між декількома комп'ютерами й периферійними пристроями. Щоб організувати мережу з безпровідною передачею, необхідно до її складу включити додаткові компоненти, такі як:

- одиночні трансивери;
- хост-трансивери.

Їх можна встановлювати як на автономно працюючих комп'ютерах, так і на комп'ютерах, підключених до мережі.

Трансивер – це пристрій для підключення комп'ютера до мережі, тобто пристрій, що здійснює прийом і передачу сигналів. Термін утворений від двох англійських слів передавач-приймач (TRANSmitter-reCEIVER). Якщо в кабельних мережах трансивер в більшості випадках вбудований в мережевий адаптер, то в безпровідних мережах він зазвичай виконаний у вигляді окремого пристрою.

Основна відмінність між різними типами безпровідних мереж – параметри передавання. Локальні мережі і їх розширення використовують передавачі й приймачі, що належать тій організації, у якій функціонує мережа. Для мобільних мереж на базі переносних комп'ютерів як середовище передавання виступають або телефонні компанії, або утримувачі відповідних каналів зв'язку (AT&T, Sprint і т. д.).

У цих випадках мережа реалізується за допомогою мережевих радіо адаптерів (рис. 4.3), забезпечених всенаправленими антенами, які використовують в якості середовища передавання інформації радіохвилі. Така мережа реалізується **топологією "все-у-всьому"** (рис. 4.4) і працездатна при дальності 50–200 м.

Рис. 4.3. Адаптер

На фізичному рівні визначені два широкополосних радіочастотних методи передавання й один - в інфрачервоному діапазоні. Радіочастотні методи працюють в ISM діапазоні 2,4 ГГц і звичайно використовують смугу 83 МГц від 2,400 ГГц до 2,483 ГГц. Технології широкополосного сигналу, використовувані в радіочастотних методах, збільшують надійність, пропускну здатність, дозволяють багатьом незв'язаним один з одним пристроям розділяти одну смугу частот з мінімальними перешкодами один для одного.

Для зв'язку між безпровідною й кабельною частинами мережі використовується спеціальний пристрій, званий крапкою входу (або радіомостом). Можна використовувати й звичайний комп'ютер, у якому встановлено два мережеві адаптери, – безпровідний та кабельний.

Іншою важливою сферою застосування безпровідних мереж є організація зв'язку між віддаленими сегментами локальних мереж за відсутності інфраструктури передавання даних (кабельних мереж загального доступу, високоякісних телефонних ліній і ін.), що типово для нашої країни. У цьому випадку для наведення безпровідних мостів між двома віддаленими сегментами використовуються радіомости з антеною направленого типу (рис. 4.5, 4.6).

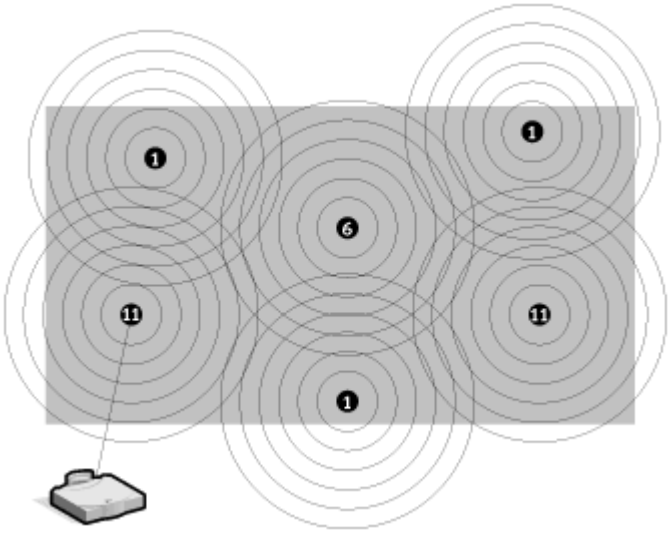


Рис. 4.4. Топологія "все-у-всьому"

Якщо в мережу потрібно об'єднати декілька сегментів, то використовується топологія типу “зірка” (рис. 4.7). При цьому в центральному вузлі встановлюється всенаправлена антена, а віддалених вузлах – направлені. Мережі зіркоподібної топології можуть утворювати мережі різноманітної конфігурації.

Рис. 4.5. Антена

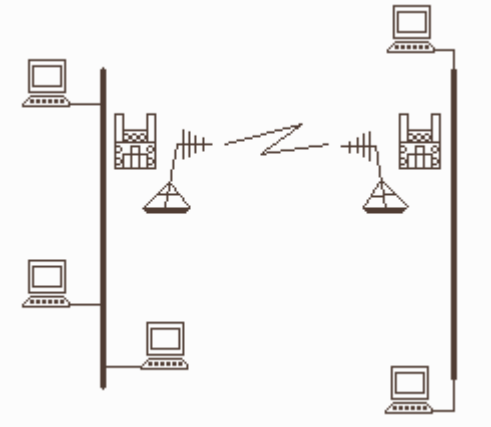


Рис. 4.6. Топологія типу "крапка-крапка"

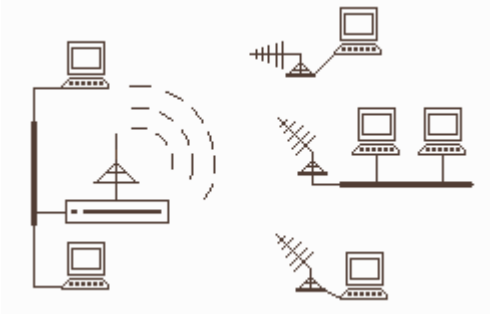


Рис. 4.7. Топологія типу "зірка"

Мережева магістраль із безпровідним доступом дозволяє відмовитися від використання повільних модемів.

Усі *інфрачервоні* безпровідні мережі використовують для передавання даних інфрачервоні промені. У подібних системах необхідно генерувати дуже сильний сигнал, оскільки на нього впливають інші джерела, наприклад, вікна. Цей спосіб забезпечує велику швидкість передавання, оскільки інфрачервоне світло має широкий діапазон частот. Інфрачервоні мережі нормально функціонують на швидкості 10 Мбіт/с. Розрізняють чотири типи інфрачервоних мереж:

1) *Мережі прямої видимості* (між приймачем і передавачем).
2) *Мережі на розсіяному випромінюванні*. Сигнал відбивається від стін і стелі і, урешті-решт, досягає приймача. Дальність – до 30 м. Швидкість передавання невелика, оскільки всі сигнали відбиті.
3) *Мережі на відбитому випромінюванні*. Оптичні трансивери комп'ютерів передають сигнали в певне місце, звідки вони переадресуються іншому комп'ютеру.
4) *Широкосмугові оптичні мережі* надають послуги, відповідні жорстким вимогам мультимедійного середовища й практично не поступаються кабельним системам.

Серед основних переваг інфрачервоних мереж можна відзначити швидкість і зручність використання.

До недоліків використання мереж цього класу можна віднести труднощі при передаванні сигналів на відстань понад 30 м та при наявності перешкод із боку сильних джерел світла, які є в більшості організацій.

Лазерна технологія схожа на інфрачервону тим, що вимагає прямої видимості між приймачем і передавачем. Якщо за якихось причин промінь буде перерваний, урветься й передача.

Безпровідні ЛОМ із радіопередаванням даних

При одно частотному радіопередаванні користувачі настроюють передавачі й приймачі на певну частоту. Цей спосіб схожий на передавання звичайної радіостанції. Пряма видимість необов'язкова; площа передавання близько 4,5 км^2. Сигнал високої частоти, який використовується при цьому методі, не проникає через металеві або залізобетонні перешкоди. Доступ до такого способу зв'язку досягається через постачальника послуг.

При радіопередаванні в розсіяному спектрі сигнали передаються в деякій смузі частот. Доступні частоти розділені на канали (або інтервали).

Адаптери протягом певного проміжку часу налаштовані на один інтервал, після чого перемикаються на інший інтервал. Перемикання всіх комп'ютерів у мережі відбувається синхронно.

Є побудовані за даною технологією мережі, що працюють зі швидкістю до 2 Мбіт/с на відстані до 3,2 км на відкритому просторі й до 120 м усередині будівлі.

Якщо комп'ютери оснастити мережевими адаптерами Xircom CreditCard Netware і ОС Windows 95/98 або Windows NT, Windows XP, то вони можуть без кабелю функціонувати як однорангові мережі.

Мережі WIMAX

Яскравим прикладом безпровідних мереж із радіопередачею даних є мережі WIMAX, які відповідають стандарту IEEE 802.16, використовують LLC (Logical Link Control) рівень (стандарт IEEE 802.2) як і інші LAN і WAN, тому вони можуть прозоро взаємодіяти. На відміну від мереж WiFi (IEEE 802.11x), де доступ до точки доступу клієнтам надається випадковим чином, в мережі WIMAX кожному клієнтові відводиться чітко регламентований проміжок часу. Крім того, WIMAX підтримує комірчасту топологію.

WIMAX — протокол широкосмугового радіозв'язку (Worldwide Interoperability for Microwave Access), розроблений консорціумом (WIMAX Forum) в червні 2001 року, і прийнятим в січні 2003 року під стандартом 802.16. Стандарт IEEE 802.16 дозволяє покрити сигналом площу радіусом до 112.6 кілометрів, без прямої видимості. Пропускна спроможність WIMAX за стандартом складає близько 70 Мбіт/с. Технологія отримала свою назву від WIMAX Forum – організація (заснована в червні 2001 р.), метою якої був розвиток і просування WiMAX.

Основні складові WIMAX мережі:

1. Базові станції.
2. Абонентські станції.
3. Обладнання, що зв'язує ці станції між собою і Інтернетом.

Базова станція WIMAX може розміщуватися на висотному об'єкті: будівлі або вежі.

Приймач WIMAX – антена з приймачем у форм-факторі карти PC Card, карти розширення ПК або зовнішньої карти.

Діапазон частот від 1,5 до 11 ГГц використовується для з'єднання базової станції з абонентською, що дозволяє в ідеальних умовах досягати швидкості передавання 70 Мбіт/с (при цьому не вимагається забезпечення прямої видимості між станцією і приймачем). З'єднання, яке встановлюється між базовими станціями (пряма видимість), використовує діапазон від 10 до 66 ГГц (може досягати до 120 Мбіт/с). Але, все-таки, одна базова станція підключається до провайдера (використовує традиційні кабельні з'єднання. Чим більше підключено базових станцій, тим вища швидкість передавання даних і надійність.

Мета технології WIMAX полягає в тому, щоб надати універсальний безпровідний доступ для широкого спектру пристроїв (робочих станцій, побутової техніки «розумного будинку», портативних пристроїв і мобільних телефонів) і їх логічного об'єднання – локальних мереж. Треба відзначити, що технологія має ряд переваг.

- В порівнянні з кабельними (xDSL, T1), безпровідними або супутниковими системами мережі WIMAX повинні дозволити операторам і сервіс-провайдерам економічно ефективно охопити не тільки нових потенційних користувачів, але і розширити спектр інформаційних і комунікаційних технологій для користувачів, що вже мають фіксований (стаціонарний) доступ.
- Стандарт об'єднує технології рівня оператора зв'язку (для об'єднання багатьох підмереж і надання їм доступу до Інтернет), а також технології «останньої милі» (кінцевого відрізання від крапки входу в мережу провайдера до комп'ютера користувача), що створює універсальність і, як наслідок, підвищує надійність системи.
- Безпровідні технології гнучкіші і, як наслідок, простіші в розгортанні, оскільки в міру необхідності можуть масштабуватися.
- Простота установки як чинник зменшення витрат на розгортання мереж в країнах, що розвиваються, малонаселених або віддалених районах.
- Далекодія є істотним показником системи радіозв'язку. На даний момент більшість безпровідних технологій широкосмугового передавання даних вимагає наявності прямої видимості між об'єктами мережі. WIMAX, завдяки використанню технології OFDM, створює зони покриття в умовах відсутності прямої видимості від клієнтського устаткування до базової станції, при цьому відстані обчислюються кілометрами.

- Технологія WIMAX містить в собі протокол IP, що дозволяє легко і прозоро інтегрувати її в локальні мережі.
- Технологія WIMAX підходить для фіксованих, переміщуваних і рухомих об'єктів мереж на єдиній інфраструктурі.

Стандарт 802.16e-2005 на даний момент надає наступні режими.

• Fixed WIMAX – фіксований доступ;
• Nomadic WIMAX – сеансовий доступ;
• Portable WIMAX – доступ в режимі переміщення;
• Mobile WIMAX – мобільний доступ.

Fixed WIMAX. Фіксований доступ є альтернативою широкосмуговим кабельним технологіям (xDSL, T1 і т.п.). Стандарт використовує діапазон частот 10-66 ГГц. Цей частотний діапазон із-за сильного загасання коротких хвиль вимагає прямої видимості між передавачем і приймачем сигналу. З іншого боку, даний частотний діапазон дозволяє уникнути однієї з головних проблем радіозв'язку – багатопроменевого розповсюдження сигналу. При цьому ширина каналів зв'язку в цьому частотному діапазоні досить велика, що дозволяє досягати швидкостей передавання 120 Мбіт/с. Фіксований режим включався у версію стандарту 802.16d-2004 і вже використовується у ряді країн.

Nomadic WIMAX. Сеансовий (кочівний) доступ додав поняття сесій до вже існуючого Fixed WIMAX. Наявність сесій дозволяє вільно переміщати клієнтське устаткування між сесіями і відновлювати з'єднання вже за допомогою інших веж WIMAX, ніж тих, що використовувалися під час попередньої сесії. Такий режим розроблений в основному для портативних пристроїв, таких як ноутбуки, КПК.

Portable WIMAX. Для режиму Portable WIMAX додана можливість автоматичного перемикання клієнта від однієї базової станції WIMAX до іншої без втрати з'єднання. Проте для даного режиму все ще обмежена швидкість пересування клієнтського устаткування – 40 км/год. Втім, вже у такому вигляді можна використовувати клієнтські пристрої в дорозі. Введення даного режиму зробило доцільним використання технології WIMAX для смартфонів і КПК.

Mobile WIMAX був розроблений в стандарті 802.16e-2005 і дозволив збільшити швидкість переміщення клієнтського устаткування до понад 120 км/год.

Підключення до безпровідної мережі

Якщо при виборі комп'ютера віддати перевагу ноутбуку, то звичайним видом доступу стане підключення безпровідною мережею Wi-Fi. Так, у домашніх умовах безпровідна мережа часто куди простіша і зручніша, ніж звичайна мережа, яка включає багато проводів і розеток.

Спершу приймемо, що комп'ютер вже оснащений Wi-Fi-адаптером (у ноутбуки і КПК вони вбудовані за замовчуванням), а тому у правому нижньому куті екрану напевно вже маячить значок безпровідного підключення. Поки комп'ютер не потрапив у зону дії мережі значок цей виглядає такою сірою і бляклою мишкою – але варто безпровідному адаптеру «зловити хвилю» як він оживе (рис. 4.8) і постарається підключитися до безпровідної мережі у автоматичному режимі (рис. 4.9). Це може і вийти – в тому випадку, якщо незахищена мережа, наприклад, опинилася поруч із загальнодоступною мережею. Але найчастіше втручання користувача все ж таки потрібне: або безпровідних мереж у окрузі декілька, або (що найчастіше і відбувається) мережа захищена і для того, щоб увійти до неї потрібний спеціальний «ключ».

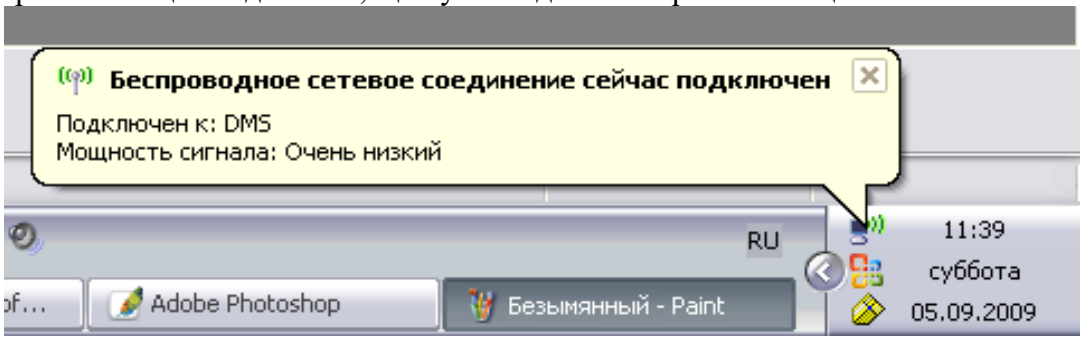


Рис. 4.8. Наявність безпровідних мереж

У будь-якому випадку не зашкодить проглянути повний список доступних у окрузі безпровідних мереж, а вже потім вирішити, що з ними робити. Вивести список на екран можна декількома способами:

Найпростіший – клацнути по значку безпровідного доступу, а потім натиснути кнопку **Безпровідні мережі** .

У Windows Vista підключитися до безпровідної мережі можна з допомогою **Центру управління мережами і загальним доступом** – список доступних безпровідних мереж буде виведений на екран після того, як клацнути по меню **Підключення до мережі.**

Тепер залишається тільки вибрати зі списку потрібну мережу і натиснути кнопку **Підключитися** .

Зазвичай відразу після цього з'явиться вікно з проханням ввести ключ доступу – серед власників безпровідних мереж не так вже багато добрих і безтурботних самаритян, які готові роздавати доступ всім охочим без обмежень. Про те що мережа захищена свідчить і зображення замку на її значку.

Де узяти ключ? Ну, якщо підключитися до мережі офісу або знайомого, то проблем немає –достатньо запитати господаря. З мережами у загальнодоступних місцях – у готелях, аеропортах, вокзалах і так далі – все дещо складніше. Деколи підключення до мережі проходить вдало, але вийти в Інтернет не виходить. У такому разі спробуйте запустити браузер – інколи він відразу ж відкривається на стартовій сторіночці мережі, на якій розміщена докладна інформація про розцінки і способи оплати.

Ввести ключ досить один раз: при успішному підключенні комп'ютер запам'ятовує параметри безпровідної мережі і наступного разу, коли опинитися у зоні її дії сам виконає процедуру входу. Відключитися від безпровідної мережі можна так само, як і від звичайної: клацніть правою кнопкою мишки по значку з'єднання і виберіть команду **Відключитися**. Хоча можна зробити ще простіше – відійти на декілька десятків метрів від зони хот-спота (радіус дії безпровідної мережі невеликий).

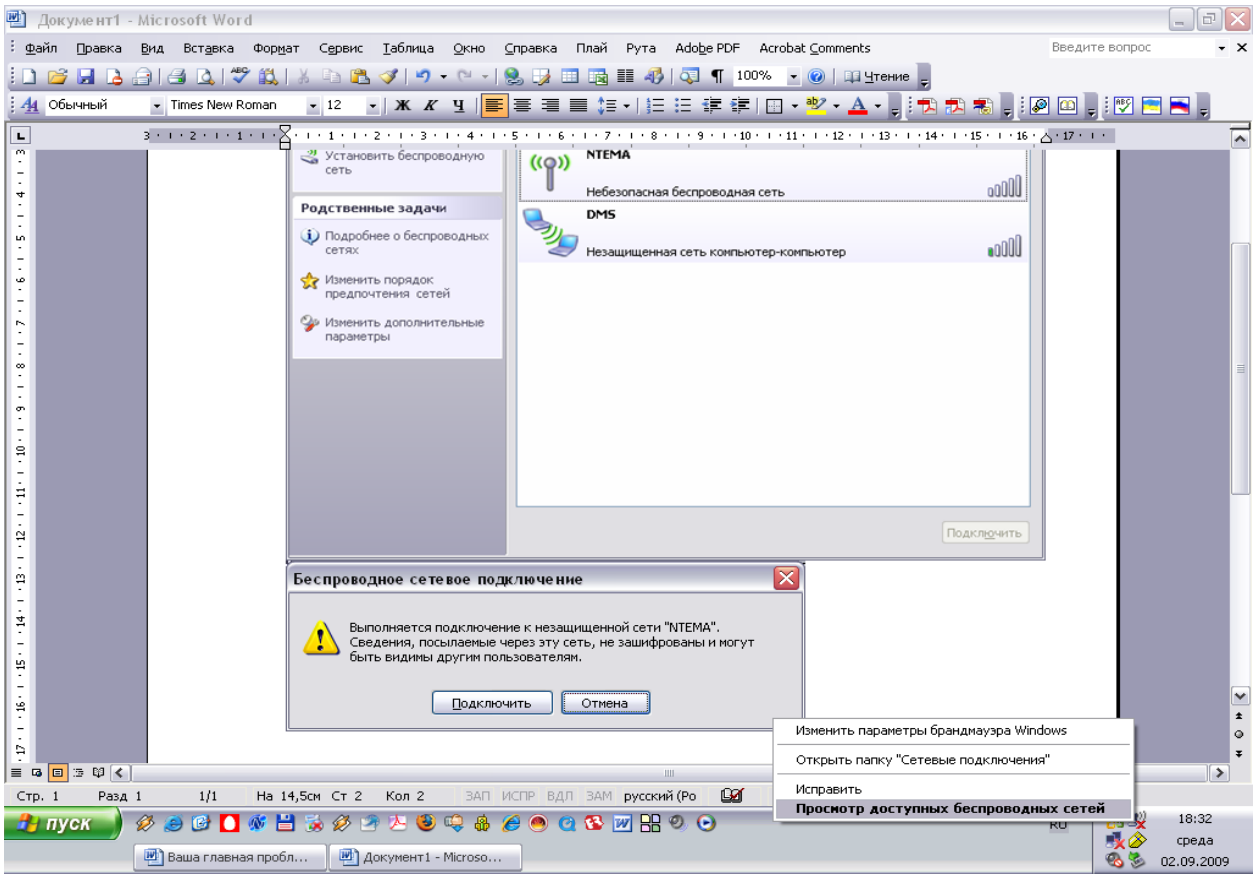


Рис. 4.9. Підключення до безпровідної мережі

Налагодження Wi-Fi-мережі на ПК і ноутбуках

Windows XP SP3 має зручні засоби для роботи з безпровідними мережами. Для автоматичного створення мережі є **Майстер безпровідної мережі**, який доступний в списку задач ме-

режевого оточення. Щоб запустити цей Майстер, треба перейти в **Мережеве оточення** і знайти в списку типових задач пункт **«Встановити безпровідну домашню мережу або мережу малого офісу»**. Після клацання по цьому пункту запуститься Майстер (рис. 4 .10), а далі – залишиться лише уважно читати і виконувати те, що він запропонує (рис. 4.11-4.16).

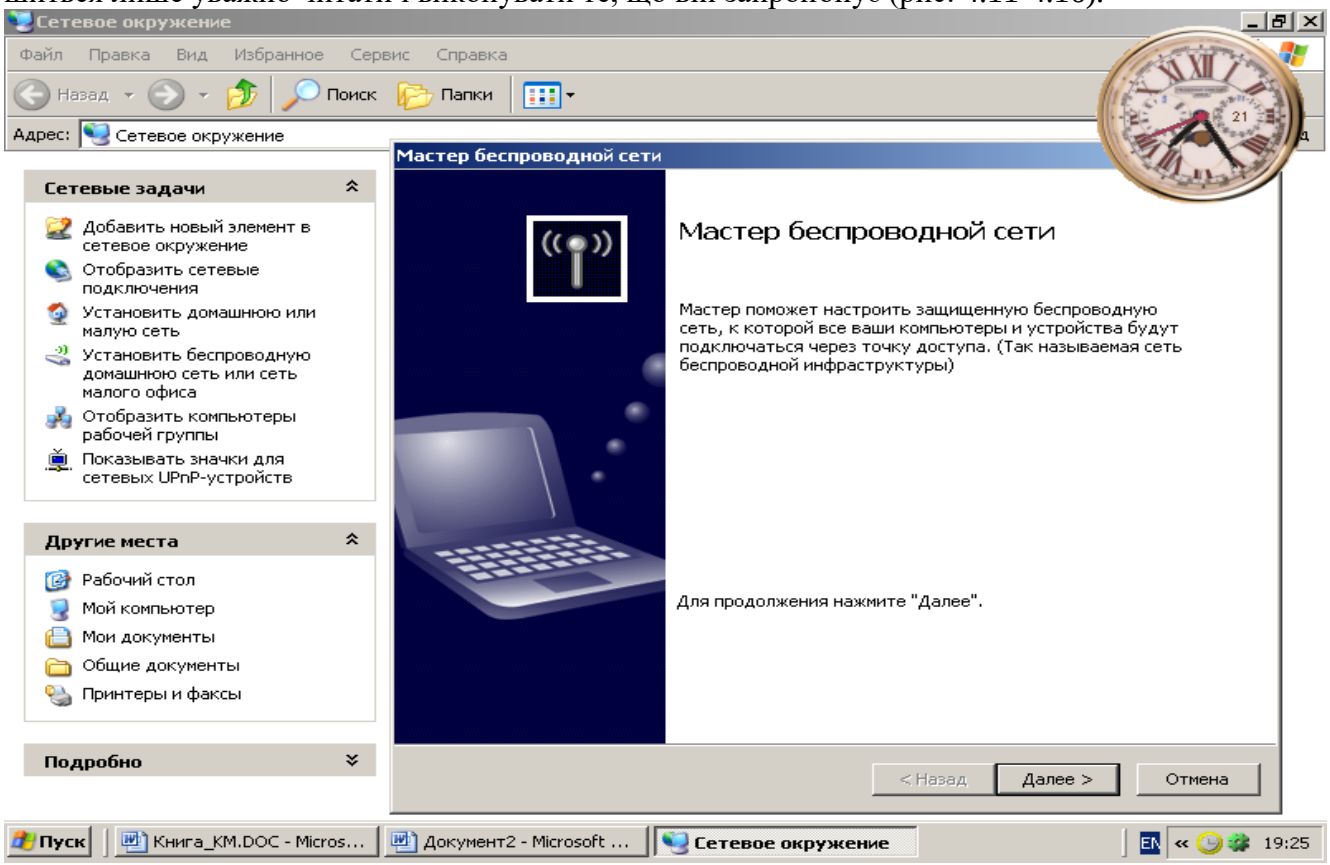


Рис. 4.10. Список типових завдань Мережевого оточення та майстер мережі

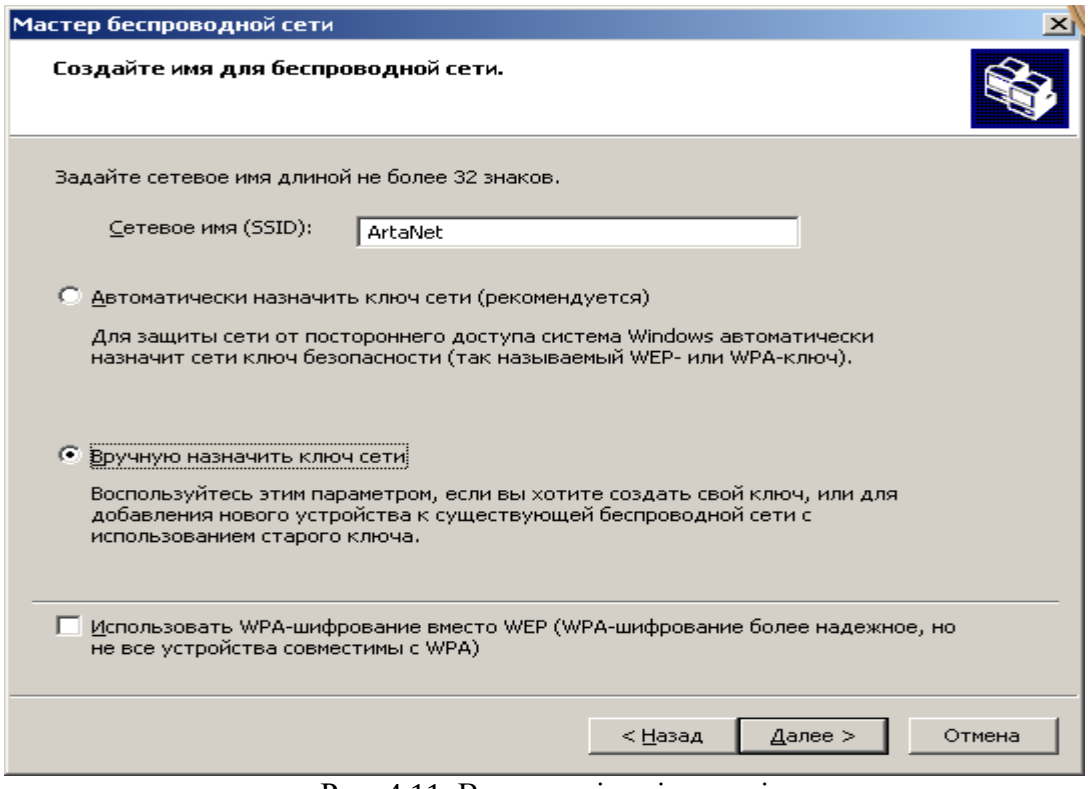


Рис. 4.11. Введення імені мережі

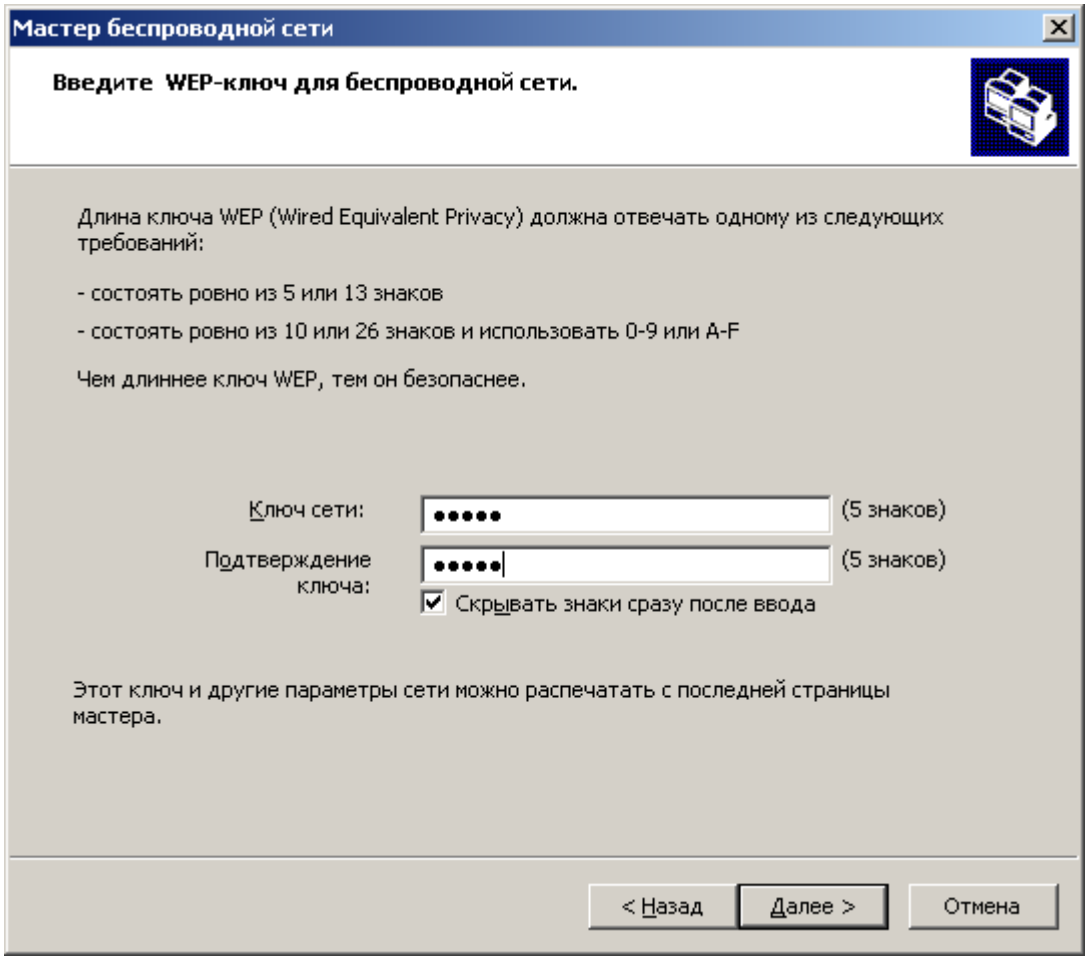


Рис.4.12. Введення ключа мережі

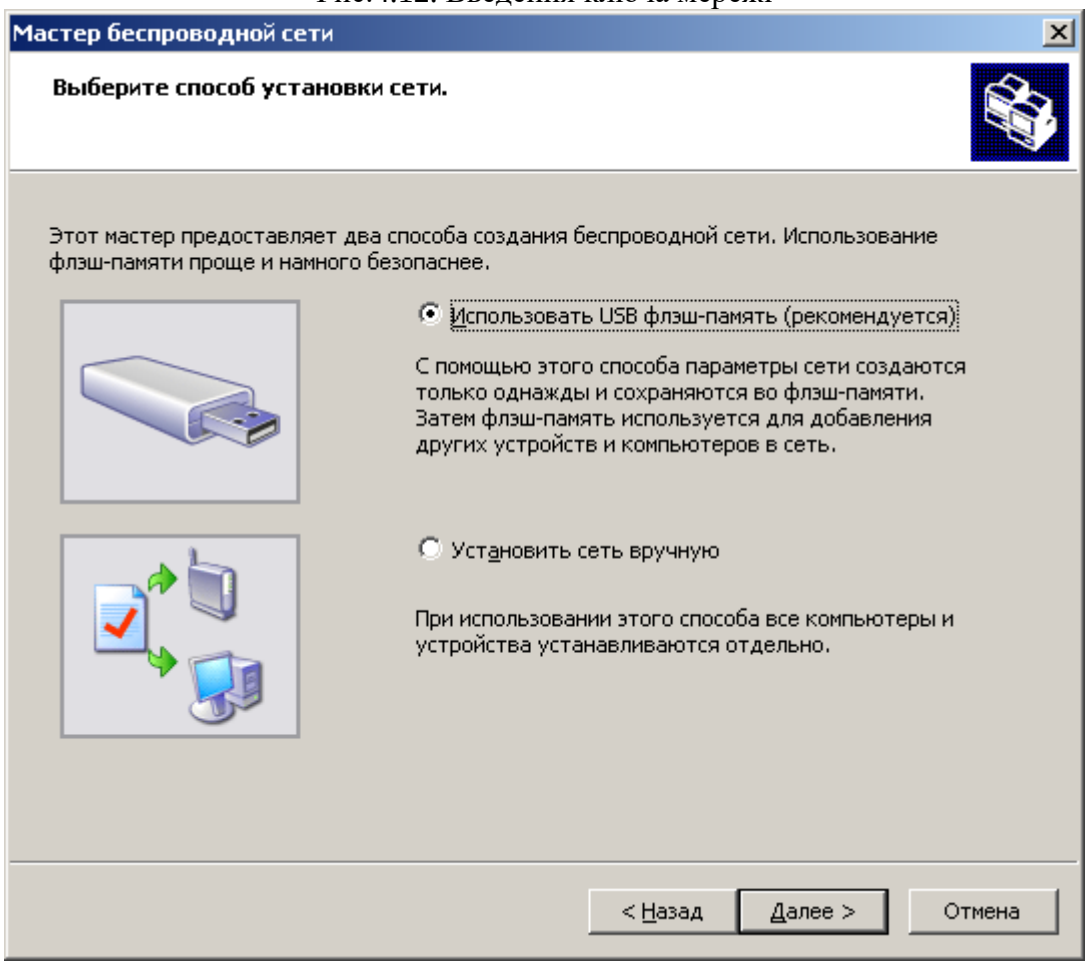


Рис. 4.13. Вибір параметрів мережі

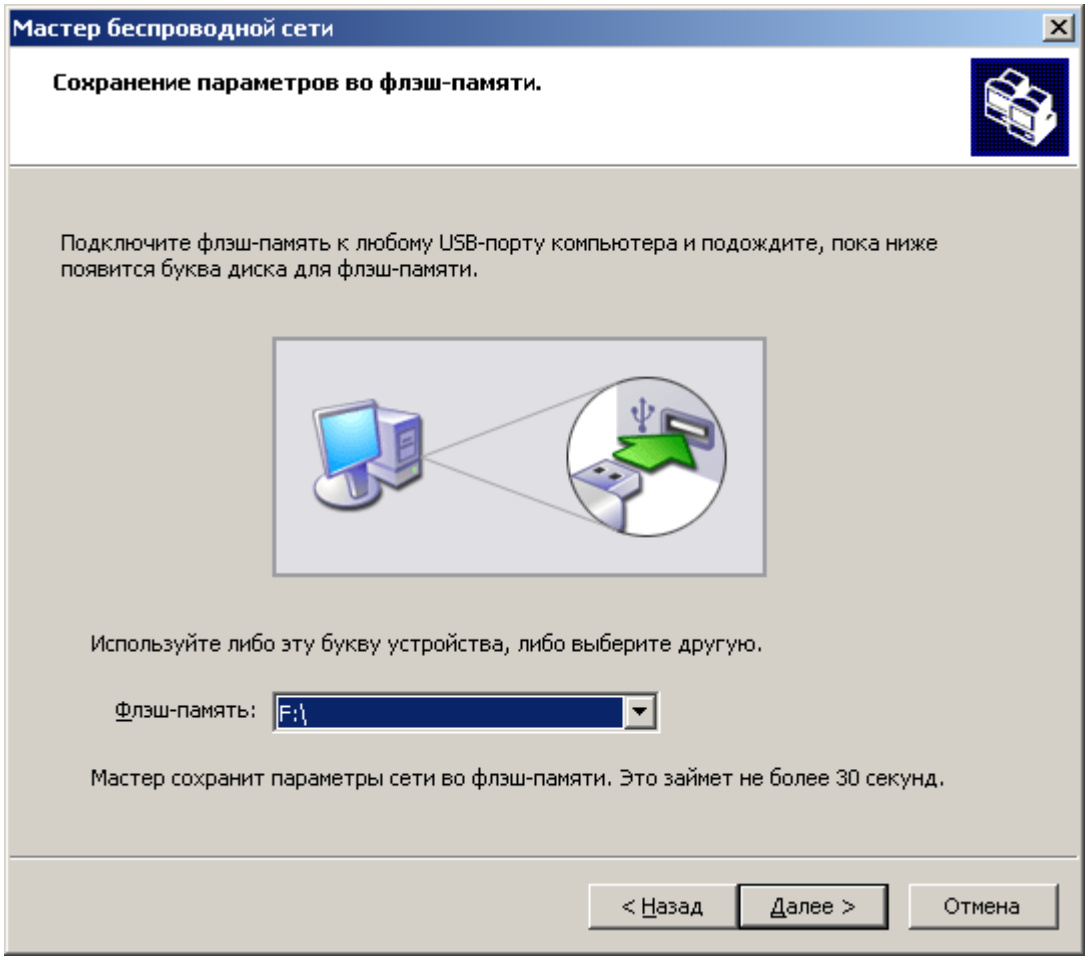


Рис. 4.14. Призначення флеш-пам’яті

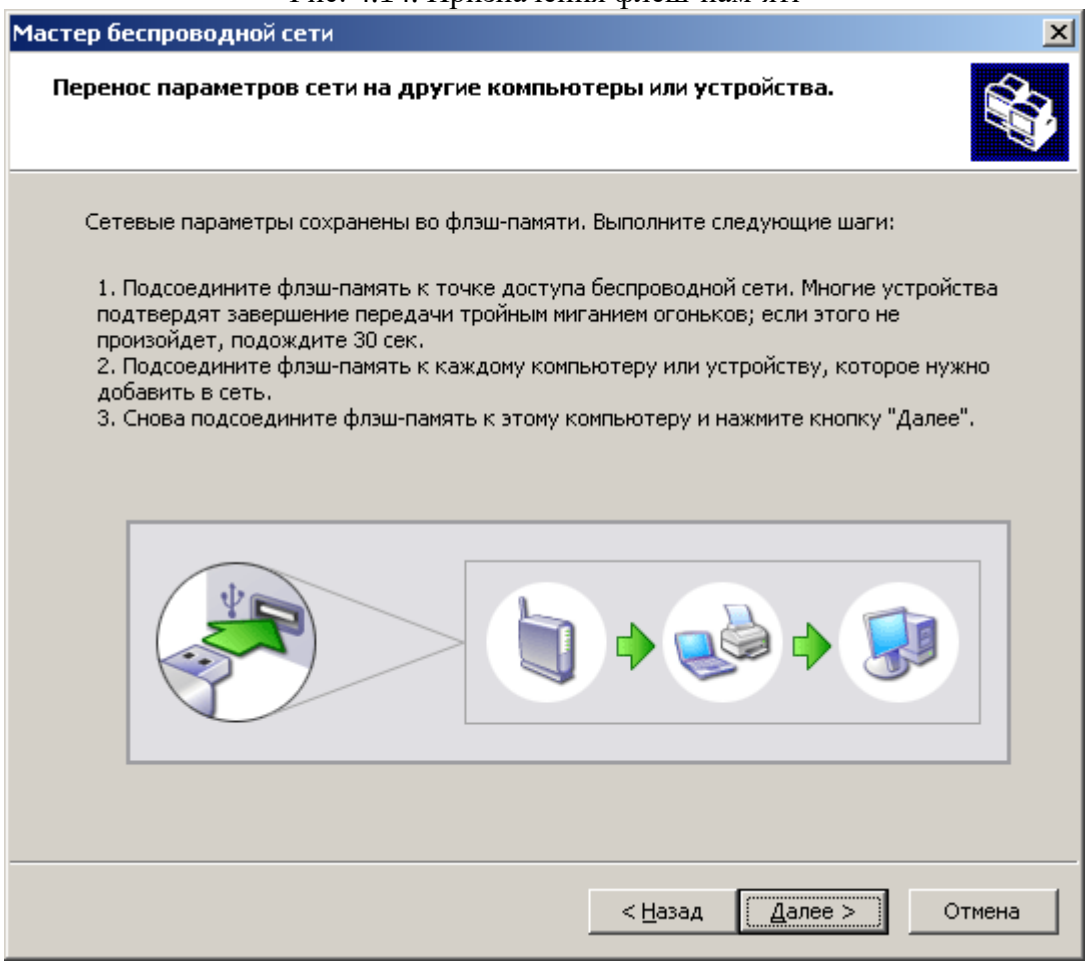


Рис. 4.15. Перенесення параметрів мережі на інші пристрої

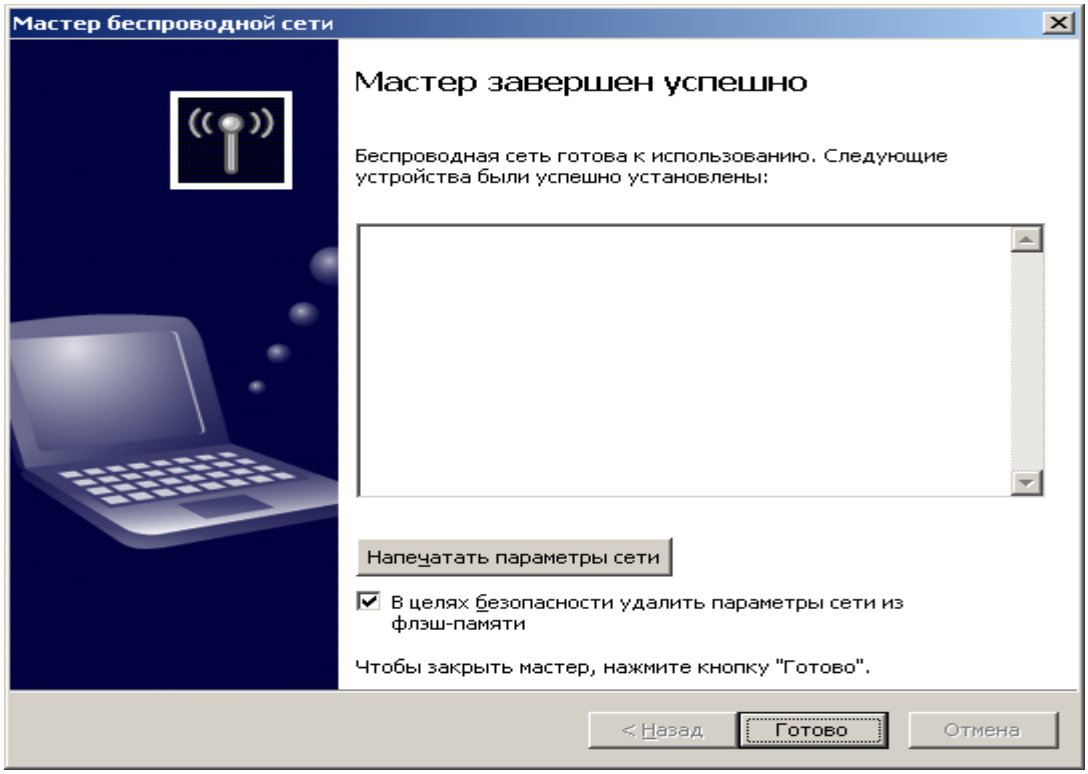


Рис. 4.16. Закінчення роботи майстра

Для того, щоб налагодити Ad-Hoc-мережу, потрібно увійти до **Мережевого оточення** і відкрити **властивості** безпровідного мережевого з'єднання. У властивостях потрібно знайти **вкладку, присвячену безпровідним мережам** (рис. 4.17), – і там створити нову безпровідну мережу, натиснувши на кнопку **Додати** (рис. 4.18). Після цього з'явиться вікно, яке містить параметри безпровідної мережі. Зокрема, потрібно ввести мережеве ім'я (SSID) і вибрати тип ідентифікації в мережі. Якщо зробити мережу відкритою, до неї найлегше підключатися, проте це означатиме, що вона абсолютно незахищена від вторгнень, тому тут найкраще встановити захист, зокрема перевірку достовірності, шифрування даних і ввести ключ мережі (він може бути завдовжки від 5 до 13 символів). У результаті, щоб підключитися до знов створеної мережі, потрібно буде знати SSID і ключ – їх можна порівняти з ім'ям і паролем для доступу в Інтернет по Dial-Up.

Створивши нову мережу, клацніть кнопку **Додатково** в тому ж вікні, де створювали безпровідну мережу і у віконці, що з'явилося, виберіть пункт **Мережа** «компьютер-компьютер» – це потрібно для того, щоб комп'ютер зміг працювати в Ad-Hoc-мережі.

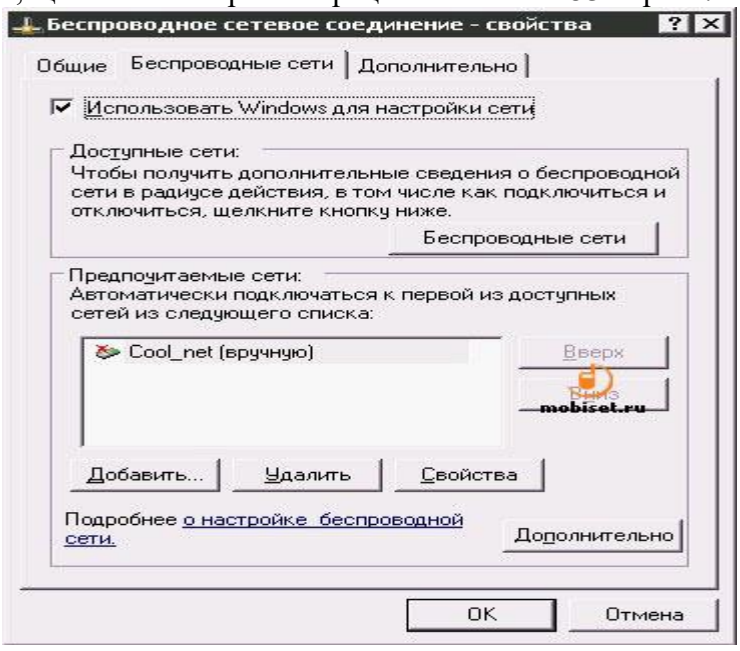


Рис. 4.17. Параметри безпровідної мережі

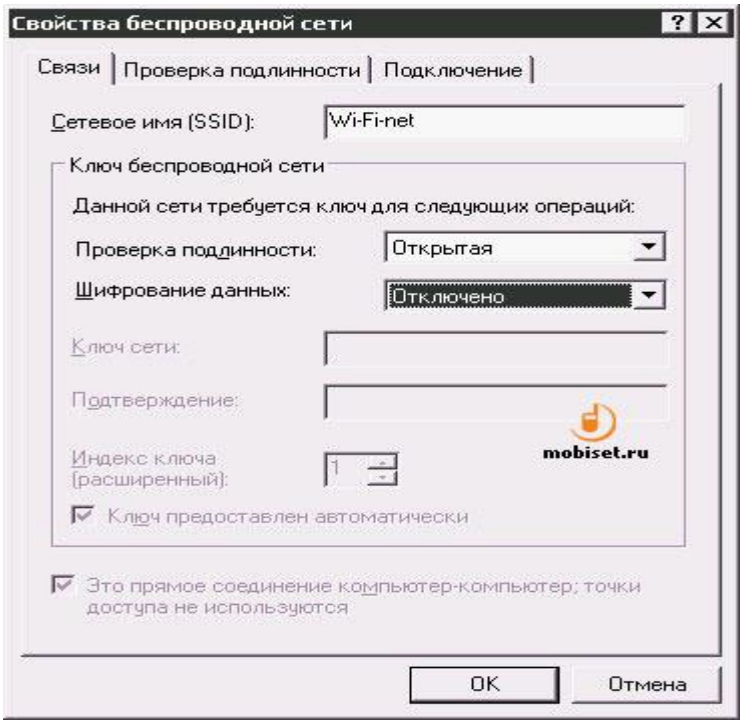


Рис.4.18. Налагодження параметрів безпровідної мережі

Після того, як мережа створена, до неї потрібно буде підключитися. Якщо це відкрита мережа – комп'ютери зможуть підключитися до неї автоматично, якщо ж мережа закрита – знадобиться SSID і ключ. Отже, на одному з комп'ютерів створено мережу – тепер потрібно підключитися до неї з інших комп'ютерів.

Проглянути доступні Wi-Fi-мережі можна, натиснувши кнопку **Безпровідні мережі** у вікні **властивостей безпровідних мереж** (це вікно треба буде відкрити для інших комп'ютерів, які потрібно підключити до Wi-Fi-мережі), – з'явиться вікно (рис. 4.19), що містить інформацію про наявні мережі, – за допомогою цього вікна можна підключатися до мереж і відключатися від них.

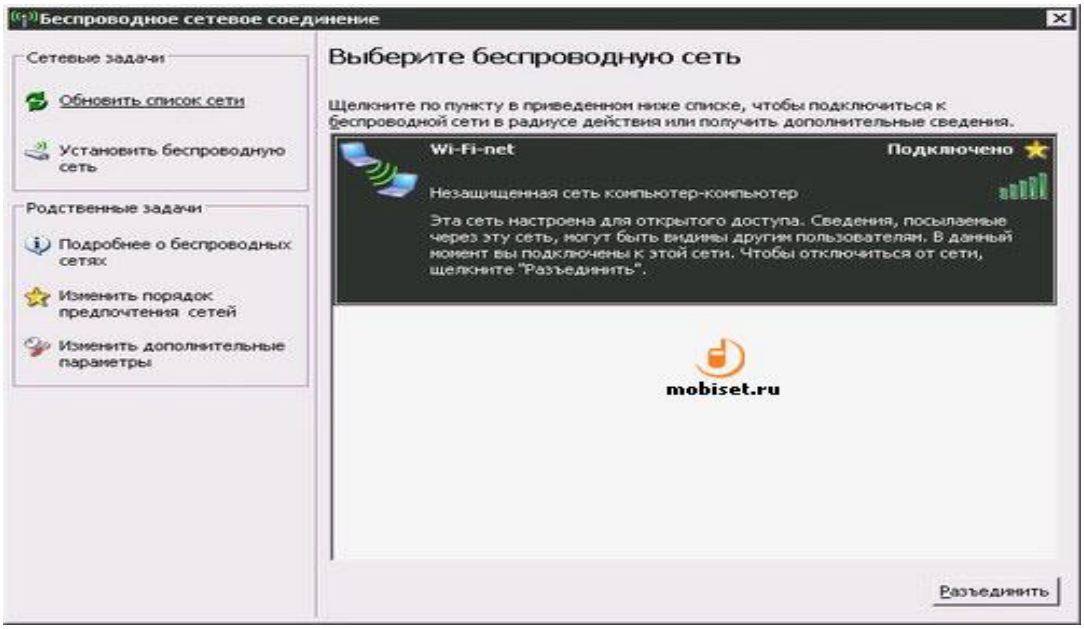


Рис. 4.19. Вікно проглядання безпровідних мереж

Після підключення до створеної Wi-Fi-мережі, треба налагодити мережеві параметри комп'ютерів, які не залежать від апаратної платформи реалізації мережі. Для цього можна скористатися **майстром налагодження мережі** (рис. 4.20) – потрібно буде лише відповідати на його питання, а він все зробить автоматично. Слід зазначити: налагоджуючи сервер (рис. 4.21), треба вказати, що він має власне підключення до Інтернету, а налагоджуючи ICS-клієнтів (рис. 4.22), – вказати, що вони підключатимуться до Інтернету через ресурси іншого ПК. Так

само, налагоджуючи сервер, слід вибрати мережеве з'єднання, через яке буде здійснений вихід в Інтернет.

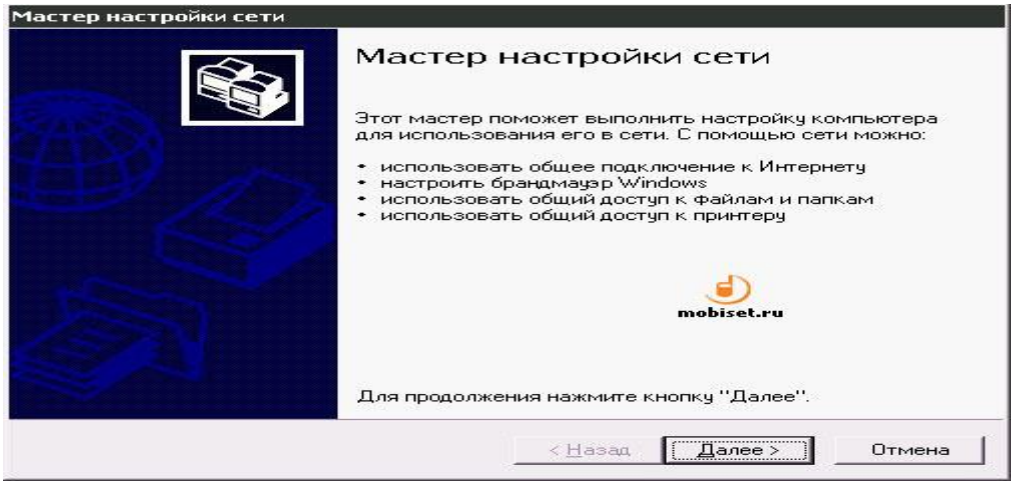


Рис. 4.20. Майстер налагодження локальних мереж

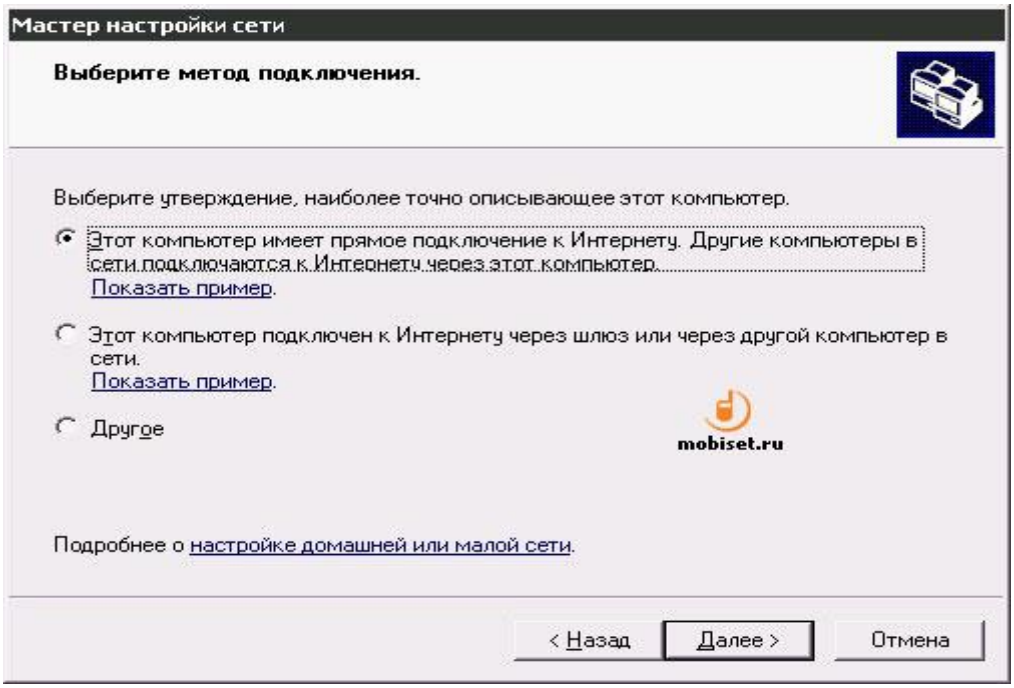


Рис.4.21. Налагодження сервера

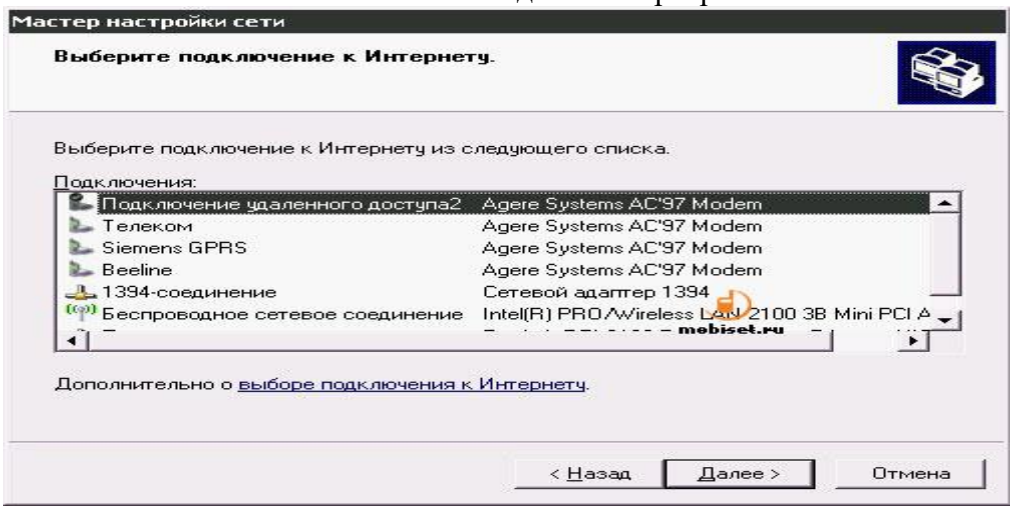


Рис.4.22. Вибір мережевого з'єднання

Для перевірки правильності налагодження прогляньте **властивості** з'єднання (рис. 4.23) і, якщо знадобиться, введіть адреси із вказаного ICS діапазону у вікно властивостей **TCP/IP** (рис. 4.24, 4.25) – його можна відкрити з вікна **властивостей з'єднання**. Так само упевніться, що комп'ютери належать до однієї робочої групи і мають різні імена – це можна зробити у вікні **властивостей Мій комп'ютер** на вкладці **Ім'я комп'ютера**.

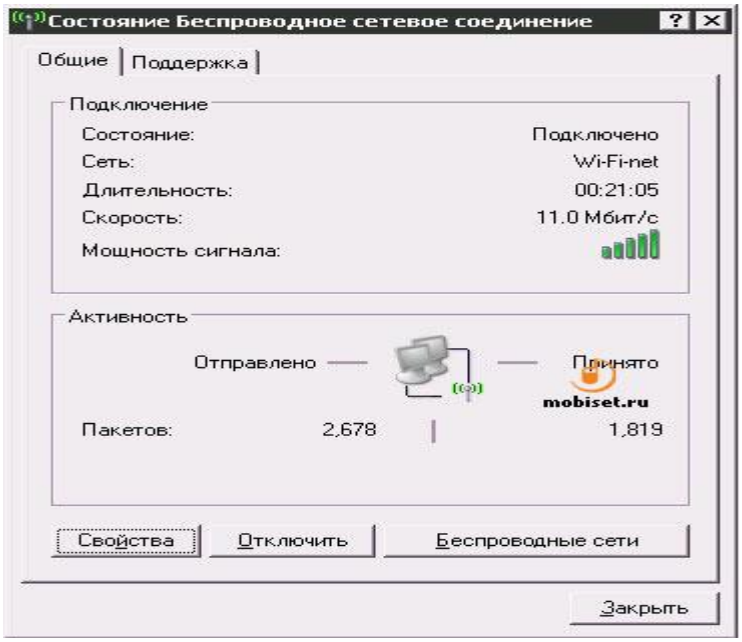


Рис.4.23. Працююче з'єднання

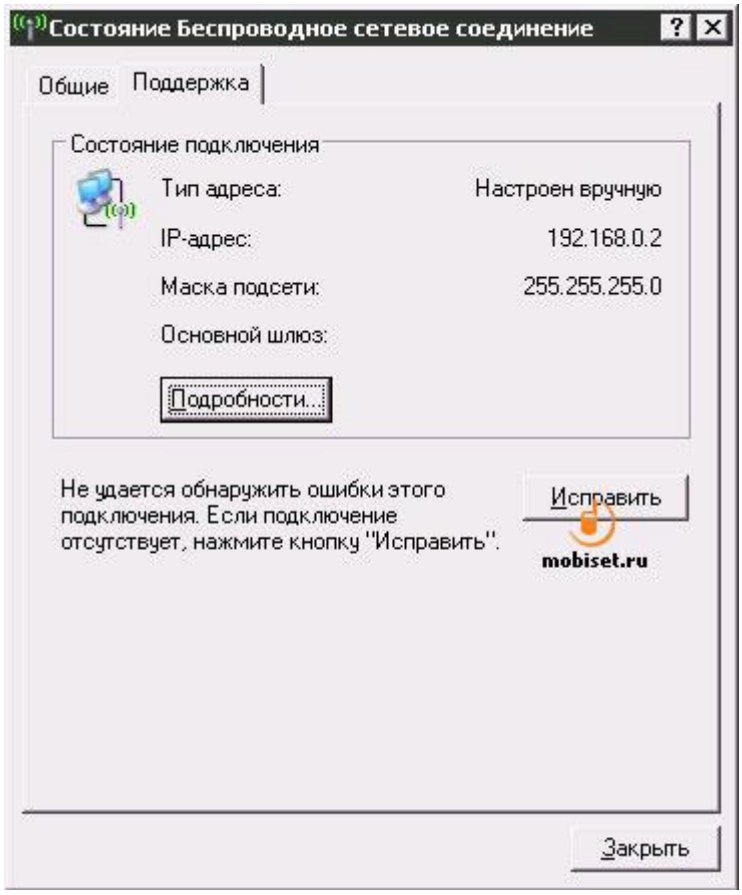


Рис.4.24. Перевірка параметрів TCP/IP

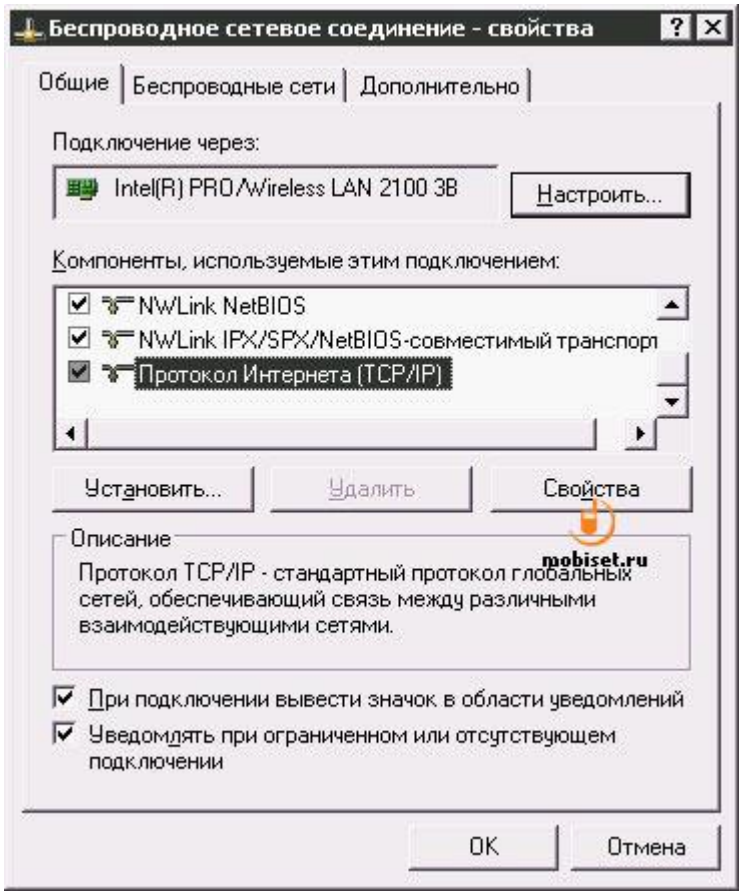


Рис.4.25. Налагодження стека TCP/IP

Після того, як мережа запрацює, наприклад, можна користуватися загальними теками і налагодити Internet Explorer для доступу в Інтернет через ICS. Зокрема, треба увійти до **Панелі управління,** відкрити **Властивості оглядача,** знайти в них вкладку **Підключення** і натиснути на кнопку **Встановити**. З'явиться вікно **Майстра підключення до Інтернету** – у вікні **тип мережевого підключення** встановіть перемикач в положення **Підключення до Інтернету.** Далі – зверніть увагу на вікно для вибору способу підключення – виберіть **Встановити підключення уручну**, і на вікні вибору типу підключення – пункт **Через постійне високошвидкісне з'єднання**.

Налагодження роутера

Роутер (рис. 4.26) – це аналог маршрутизатора в кабельних мережах. Він отримує сигнали від комп'ютерів мережі, підсилює їх та передає далі.

Рис. 4.26. Роутер

Після фізичного підключення комп'ютерів до роутеру потрібно його налагодити, що, як правило, доводиться робити вручну. Зазвичай, це робиться через **«веб-сервер-інтерфейс»** – тобто через звичайний браузер: набравши у його рядку фізичну адресу роутера (вона вказана у документації – як правило це 192.168.0.1 або 192.168.1.1) отримаємо доступ до меню налагодження.

Режим роботи роутера

Будь-який роутер може працювати у декілька режимах, наприклад, *простого «моста» (Bridge)* або *«крапки доступу» (Access Point)* – в різних моделях роутера ці режими можуть називатися по-різному. В тому випадку коли роутер взагалі відмовляється займатися якою-небудь роботою з управління трафіком і тільки пасивно пропускає дані, то всі важливі параметри – мережеві адреси і так далі – треба встановлювати на кожному комп'ютері окремо.

Але існує і інший, основний режим роботи роутера – *Home Gateway* або *Router*: тут маршрутизатор нарешті починає займатися справою – «маршрутизувати» – відправляти пакети даних за призначенням, самостійно роздавати комп'ютерам мережеві адреси і так далі.

Режим *трансляції адрес (NAT).* При використанні системи трансляції адрес (NAT) всі комп'ютери у мережі будуть показні ззовні як один пристрій із однією «зовнішньою» IP адресою. Кожен комп'ютер, що знаходиться в NAT мережі, отримує свою власну «внутрішню» адресу, яка використовується лише для спілкування з його «колегами». Якщо ж режим NAT відключений, то у кожного комп'ютера у локальній мережі буде своя «зовнішня» адреса. На перший погляд, так набагато правильніше і зручніше – навіщо ж зв'язуватися з цією малозрозумілою штукою? Тим паче, що включення NAT деколи спричиняє масу проблем: починають «страйкувати» багато файлообмінних програм (наприклад, eMule), торрент-клієнти. Але це компенсується тими перевагами, які NAT надає: відносною безпекою і можливістю обійти обмеження провайдера! Адже, зазвичай, за кожен підключений до Інтернету комп'ютер стягується додаткова плата – NAT же «маскує» вашу локальну мережу, дозволяючи використовувати одне підключення на всі комп'ютери.

DHCP. Цей режим дозволяє вашому роутеру автоматично роздавати локальні IP-адреси всім комп'ютерам, які підключені до мережі. Активувавши DHCP, все потрібні параметри роутер роздасть комп'ютерам самостійно. Іноді, правда, виникає необхідність закріпити за визначеним комп'ютером яку-небудь конкретну адресу. Для цього треба внести комп'ютер у спеціальний «лист виключень», де потрібна адреса буде прописана заздалегідь. А як роутер відрізнятиме потрібний комп'ютер від інших? Чи означає це, що у комп'ютера вже є якийсь ідентифікатор, з яким ми ще не знайомі? Вірно: цей ідентифікатор називається MAC-адресою, а зберігається він в пам'яті мережевого адаптера.

MAC-адресу комп'ютера можна визначити таким чином: зайдіть на панель, де розташований значок вашого мережевого адаптера (у Windows XP – **Панель Управління/мережеві підключення,** у Windows Vista **– Центр управління мережами і загальним доступом/ Управління мережевими підключеннями)**. Клацніть по значку підключення і викличте інформаційну панель **Стан**. Натисніть кнопку **Властивості**. У рядочку, що з'явився, – **Фізична адреса**: розділена рисками комбінація шести пар букв і цифр – це і є MAC-адреса. Її можна виділити мишкою, скопіювати, використовуючи відповідну команду контекстного меню (клацання правою кнопкою мишки), а вже потім вставити у відповідний розділ налагодження роутера.

Налагодження WAN і LAN. Внутрішніми параметрами мережі (які в режимі DHCP налагоджуються автоматично) завідує розділ LAN, а до меню WAN вносяться налагодження зовнішньої мережі – адреса, сервери доменних імен DNS і так далі.

Wireless . Оскільки у багатьох роутерів сьогодні є не тільки дротяний, але і безпровідною інтерфейс, в меню налагодження обов'язково знайдеться розділ із назвою Wireless. Mode, WiFi або подібне. Що сюди вносити, ми вже знаємо з розділу «Підключення до безпровідної мережі»: вибране нами ім'я-ідентифікатор мережі (SSID) і ключ, який вводитиметься при вході в мережу. Довжина ключа складає від 5 до 13 цифрових або буквених (латинських) символів. Довгий ключ, звичайно, надійніший, хоча запам'ятати його складніше.

Мікрохвильова система включає: два радіотрансивери - один для генерації сигналів, інший для прийому і дві направлені антени. Вони націлені одна на одну, щоб здійснювати прийом сигналів, які передаються трансиверами, і працюють в зоні прямої видимості або між собою, або сьогодні мікрохвильова технологія найпоширеніша в США як спосіб передавання даних на великі відстані. Вона дозволяє організувати взаємодії між будівлями в невеликих компактних системах, наприклад, університетських містечках.

Стандартом 802.11 визначений єдиний підрівень MAC, що взаємодіє із трьома типами протоколів фізичного рівня, відповідних різним технологіям передавання сигналів, - радіоканалами в діапазоні 2,4 ГГц з широкосмуговою модуляцією та прямим розширенням спектру

(DSSS) і зміною частоти (FHSS), а також за допомогою інфрачервоного випромінювання. Специфікаціями стандарту передбачено два значення швидкості передавання даних - 1 і 2 Мбіт/с.

В порівнянні з кабельними ЛОМ Ethernet можливості підрівня MAC розширені за рахунок включення в нього ряду функцій, що зазвичай виконуються протоколами вищого рівня, зокрема, процедур фрагментації і ретрансляції пакетів. Це викликано прагненням підвищити ефективну пропускну спроможність системи через супутник завдяки зниженню витрат на повторну передачу пакетів.

Як основний метод доступу до середовища стандартом 802.11 визначений механізм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance - множинний доступ і запобіганням колізіям).

В основу стандарту 802.11 покладена стільникова архітектура, причому мережа може складатися як з однієї, так і декількох осередків. Кожним осередком керує базова станція, так звана крапка доступу (табл. 4.1), яка разом з робочими станціями користувачів, що знаходяться в межах радіусу її дії, утворює базову зону обслуговування (Basic Service Set, BSS). Крапки доступу багатостільникової мережі взаємодіють між собою через розподільну систему (Distribution System, DS), що є еквівалентом магістрального сегменту кабельних ЛОМ. Вся інфраструктура, що включає крапки доступу і розподільну систему, утворює розширену зону обслуговування (Extended Service Set).

Таблиця 4.1

Можливості сучасних крапок доступу

Тип крапки доступу	**Коротка характеристика**
SSL WEB	веб-сервер управління за SSL
SNMP v3	SNMP-управління з аутентифікацією і шифруванням
Rogue AP Detection	знаходження «чужої» крапки доступу в області покриття
Monitoring Station Statistics	повна інформація про працездатність клієнтів, певна статистика
HTTP(S) File Transfer	завантаження/вивантаження firmware, параметрів через інтернет
Auto Configuration by DHCP Server	завантаження різноманітних налагоджень з DHCP-сервера
Wireless Distribution System	кожна крапка доступу працює з іншими, утворюючи повністю безпровідну інфраструктуру, природно продовжуючи працювати з клієнтами
Multiple RADIUS Server	використання різних Radius-серверів для MAC-аутентифікації і IEEE 802.1X відповідно
Embedded RADIUS Server	вбудований протокол Radius
VLAN Support	підтримка декількох VLAN на кожному з каналів

Стандартом передбачений також варіант безпровідної мережі, з одного осередку, який може бути реалізований і без крапки доступу, при цьому частина її функцій виконується безпосередньо робочими станціями. Для забезпечення переходу мобільних робочих станцій із зони

дії однієї крапки доступу до іншої в багатостільникових системах передбачені спеціальні процедури сканування (активного і пасивного прослуховування ефіру) і приєднання (Association), однак суворих специфікацій з реалізації роумінгу стандарт 802.11 не передбачає.

Стандарт 802.11 визначає два типи устаткування — клієнт, що звичайно являє собою комп'ютер, укомплектований бездротовою мережевою інтерфейсною картою (Network Interface Card, NIC), і крапку доступу (Access point, AP), що виконує роль моста між бездротовою й провідною мережами. Крапка доступу звичайно містить у собі приймально-передаючий пристрій, інтерфейс провідної мережі стандарту (802.3), а також програмне забезпечення, що займається обробкою даних. В якості бездротової станції може виступати ISA, PCI або PC Card мережева карта в протоколі 802.11, або вбудовані рішення, наприклад, телефонна гарнітура стандарту 802.11.

Стандарт IEEE 802.11 визначає два режими роботи мережі – режим "Ad-hoc" і клієнт/сервер (або режим інфраструктури - infrastructure mode). У режимі клієнт/сервер (рис. 4.27) бездротова мережа складається з як мінімум однієї крапки доступу, підключеної до провідної мережі, і деякого набору бездротових оконечних станцій. Така конфігурація зветься базового набору служб (Basic Service Set, BSS). Два або більше BSS, що утворять єдину підмережу, формують розширений набір служб (Extended Service Set, ESS). Тому що більшості бездротових станцій потрібно одержувати доступ до файлових серверів, принтерів, Інтернет, доступним у провідній локальній мережі, вони будуть працювати в режимі клієнт/сервер.

Режим "Ad-hoc" (так званий крапка-крапка, або незалежний базовий набір служб, IBSS) - це проста мережа, у якій зв'язок між численними станціями встановлюється прямо, без використання спеціальної крапки доступу (рис.4.28). Такий режим корисний у тому випадку, якщо інфраструктура бездротової мережі не сформована (наприклад, готель, виставочний зал, аеропорт), або з якихось причин не може бути сформована.

Стандарт IEEE 802.11a - є найбільш "широкосмуговим" із сімейства стандартів 802.11, який передбачає швидкість передавання даних до 54 Мбіт/с (редакцією стандарту, що затверджений в 1999 р., визначено три обов'язкові швидкості - 6, 12 і 24 Мбіт/с і п'ять необов'язкових - 9, 18, 36, 48 і 54 Мбіт/с). На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікаціями 802.11a передбачена робота в діапазоні 5 ГГц. Як метод модуляції сигналу вибрано ортогональне частотне мультиплексування (OFDM). Найістотніша відмінність між цим методом і радіотехнологіями DSSS і FHSS полягає в тому, що OFDM припускає паралельну передачу корисного сигналу одночасно за декількома частотами діапазону, тоді як технології розширення спектру передають сигнали послідовно. В результаті підвищується пропускна спроможність каналу і якість сигналу. До недоліків 802.11a відносяться вища споживана потужність радіопередавачів для частот 5 ГГц, а також менший радіус дії (устаткування для 2,4 ГГц може працювати на відстані до 300 м, а для 5 ГГц - біля 100 м).

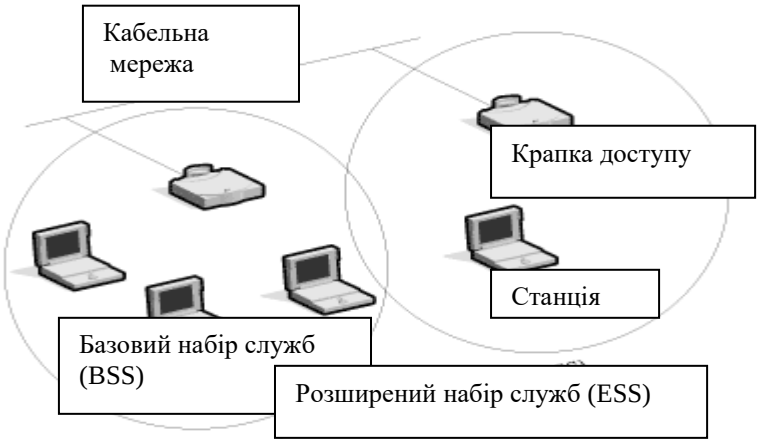


Рис. 4.27. Архітектура мережі "клієнт/сервер".

Рис.4.28. Архітектура мережі " Ad-hoc".

Стандарт IEEE 802.11b завдяки високій швидкості передавання даних (до 11 Мбіт/с), практично еквівалентній продуктивності для кабельних ЛОМ Ethernet, а також орієнтації на "освоєний" діапазон 2,4 ГГц, завоював найбільшу популярність у виробників устаткування для безпровідних мереж. У остаточній редакції стандарт 802.11b, відомий також як Wi-Fi (wireless fidelity), був прийнятий в 1999 р. Як базова радіотехнологія в ньому використовується метод DSSS з 8-розрядними послідовностями Уолша. Оскільки устаткування, що працює на максимальній швидкості 11 Мбіт/с, має менший радіус дії, ніж на нижчих швидкостях, то стандартом 802.11b передбачено автоматичне пониження швидкості при погіршенні якості сигналу. Як і у разі базового стандарту 802.11, чіткі механізми роумінгу специфікаціями 802.11b не визначені. В таб. 4.2 приведено деякі характеристики безпровідних мереж.

Таблиця 4.2

Порівняльні характеристики мереж

Технологія	**Стандарт**	**Використання**	**Пропускна спроможність**	**Радіус дії**	**Частоти**
UWB	802.15.3a	WPAN	110–480 Мбіт/с	до 10 метрів	7,5 ГГц
Wi-Fi	802.11a	WLAN	до 5 Мбіт/с	до 100 метрів	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбіт/с	до 100 метрів	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбіт/с	до 100 метрів	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 600 Мбіт/с	до 100 метрів	2,4 — 2,5 або 5,0 ГГц
WiMax	802.16d	WMAN	до 75 Мбіт/с	6–10 км	1,5–11 ГГц
WiMax	802.16e	Mobile WMAN	до 30 Мбіт/с	1–5 км	2–6 ГГц

Безпека

Стандарт 802.11b забезпечує контроль доступу на MAC рівні (другий рівень у моделі OSI) і механізми шифрування, відомі як Wired Equivalent Privacy (WEP), метою яких є забезпечення бездротової мережі засобами, еквівалентними засобам безпеки кабельних мереж. Коли включений WEP, він захищає тільки пакет даних, але не захищає заголовки фізичного рівня, так що інші станції в мережі можуть переглядати дані, необхідні для керування мережею. Для контролю доступу кожна крапку доступу містить так званий ESSID (або WLAN Service Area ID), без знання якого мобільна станція не зможе підключитися до крапки доступу. Додатково крапка доступу може зберігати список дозволених MAC адрес, який називається списком контролю доступу (Access Control List, ACL), дозволяючи доступ тільки тим клієнтам, чиї MAC адреси перебувають у списку.

Протокол WEP є свого роду аналогом кабельної безпеки (в усякому разі, розшифровується він саме так), проте реально ніякого еквівалентного кабельним мережам рівня безпеки він, звичайно ж, не надає.

Протокол WEP дозволяє шифрувати потік даних на основі алгоритму RC 4 з ключем розміром 64 або 128 бітів. Дані ключі мають так звану статичну складову завдовжки від 40 до 104 бітів, додаткову динамічну складову розміром 24 біта, звану вектором ініціалізації (Initialization Vector, IV).

На простому рівні процедура WEP-шифрування виглядає таким чином: спочатку передавані в пакеті дані перевіряються на цілісність (алгоритм CRC-32), після чого контрольна сума

(integrity check value, ICV) додається в службове поле заголовка пакету. Далі генерується 24-бітовий вектор ініціалізації і до нього додається статичний (40-або 104-бітовий) секретний ключ. Отриманий таким чином 64-або 128-бітовий ключ і є початковим ключем для генерації псевдовипадкового числа, що використовується для шифрування даних. Далі дані змішуються (шифруються) за допомогою логічної операції XOR із псевдовипадковою ключовою послідовністю, а вектор ініціалізації додається в службове поле кадру. Протокол безпеки WEP передбачає два способи аутентифікації користувачів: Open System (відкритий) і Shared Key (загальний). При використанні відкритої аутентифікації ніякої аутентифікації, власне, і не існує, тобто будь-який користувач може дістати доступ в безпровідну мережу. Проте навіть при використанні відкритої системи допускається використання WEP-шифрування даних.

Технологія WPA складається з наступних основних компонентів:

- протокол 802.1x - універсальний протокол для аутентифікації, авторизації і обліку (AAA);
- протокол EAP (Extensible Authentication Protocol) - розширений протокол аутентифікації;
- протокол TKIP (Temporal Key Integrity Protocol) - протокол тимчасової цілісності ключів, інший варіант перекладу - протокол цілісності ключів в часі;
- MIC (Message Integrity Code) - криптографічна перевірка цілісності пакетів;
- протокол RADIUS.

Функції аутентифікації покладаються на протокол EAP, який сам по собі є лише каркасом для методів аутентифікації. Протокол дуже просто реалізувати на аутентифікаторі (крапці доступу), оскільки йому не потрібно знати ніяких специфічних особливостей різних методів аутентифікації. Аутентіфікатор служить лише передавальною ланкою між клієнтом і сервером аутентифікації. Методів же аутентифікації існує досить багато:

- EAP-SIM, EAP-AKA - використовуються в мережах GSM мобільного зв'язку;
- LEAP - метод від Cisco;
- EAP-MD5 - простий метод, аналогічний CHAP;
- EAP-MSCHAP V2 - метод аутентифікації на основі логіна/пароля користувача в MS-мережах;
- EAP-TLS - аутентифікація на основі цифрових сертифікатів;
- EAP-SecureID - метод на основі одноразових паролів.

Окрім вище перелічених, слід зазначити наступні два методи: EAP-TTLS і EAP-PEAP. На відміну від попередніх, ці два методи перед безпосередньою аутентифікацією користувача спочатку утворюють TLS-тунель між клієнтом і сервером аутентифікації. А вже усередині цього тунелю здійснюється сама аутентифікація з використанням як стандартного EAP (MD5, TLS), так і старих не-EAP методів (PAP, CHAP, MS-CHAP, MS-CHAP v2), останні працюють тільки з EAP-TTLS (PEAP використовується тільки спільно із EAP методами). Попереднє тунелювання підвищує безпеку аутентифікації, захищаючи від атак типу «man-in-middle», «Session hihacking» або атаки за словником.

Клієнти, наприклад, Windows XP SP3 можуть використовувати MD5-Challenge, PEAP (Protected EAP - дозволяє проводити аутентифікацію на основі сертифікатів або логіна/пароля). Якщо використовувати сертифікати, необхідно буде створити інфраструктуру відкритих ключів (PKI). Без неї ж досить підключити RADIUS-сервер до якої-небудь бази з користувачами і проводити аутентифікацію користувачів за нею. Також є варіант Smart Card or Other Certificate - звичайний EAP-TLS. Він являється єдиним способом отримати працюючий зв'язок безпровідних користувачів в Windows-домені.

Протокол WEP має ряд серйозних недоліків і не є для хакерів важкою перешкодою. Тому в 2003 році був представлений наступний стандарт безпеки — WPA (Wi-Fi Protected Access). Головною особливістю цього стандарту є технологія динамічної генерації ключів шифрування даних, побудована на базі протоколу TKIP (Temporal Key Integrity Protocol), що є подальшим розвитком алгоритму шифрування RC 4. По протоколу TKIP мережеві пристрої працюють з 48-бітовим вектором ініціалізації (на відміну від 24-бітового вектора WEP) і реалізують правила зміни послідовності його бітів, що виключає повторне використання ключів. У протоколі TKIP передбачена генерація нового 128-бітового ключа для кожного пакету, який передається. Крім того, контрольні криптографічні суми в WPA розраховуються за новим методом під назвою MIC (Message Integrity Code). У кожен кадр тут поміщається спеціальний восьмибайтний код цілісності повідомлення, перевірка якого дозволяє відображати атаки із застосуванням підроб-

лених пакетів. У результаті виходить, що кожен пакет даних має власний унікальний ключ, а кожен пристрій безпровідної мережі наділяється динамічно змінним ключем.

Крім того, протокол WPA підтримує шифрування за стандартом AES (Advanced Encryption Standard), тобто за вдосконаленим стандартом шифрування, який відрізняється стійкішим криптоалгоритмом, ніж в протоколах WEP і TKIP.

Фільтрація MAC-адрес, яка підтримується всіма сучасними крапками доступу і безпровідними маршрутизаторами, хоча і не є складовою частиною стандарту 802.11, тим не менш, як вважається, дозволяє підвищити рівень безпеки безпровідної мережі. Для реалізації даної функції в налагодженнях крапки доступу створюється таблиця MAC-адрес безпровідних адаптерів клієнтів, авторизованих для роботи в даній мережі.

Ще один запобіжний засіб, який часто використовують в безпровідних мережах, – це режим прихованого ідентифікатора мережі. Кожній безпровідній мережі призначається свій унікальний ідентифікатор (SSID), який є назвою мережі. Коли користувач намагається увійти до мережі, то драйвер безпровідного адаптера перш за все сканує ефір на наявність в ній безпровідних мереж. При використанні режиму прихованого ідентифікатора (як правило, цей режим називається Hide SSID) мережа не відображається в списку доступних, і підключитися до неї можна тільки в тому випадку, якщо, по-перше, точно відомий її SSID, і, по-друге, заздалегідь створений профіль підключення до цієї мережі.

В домашніх умовах або невеликих офісах зазвичай використовується варіант протоколу безпеки WPA на основі загальних ключів – WPA-PSK (Pre Shared Key).

Після того, як станція підключається до крапки доступу, всі передані дані можуть бути зашифровані з використанням цього ключа. Коли використовується шифрування, крапка доступу буде посилати зашифрований пакет будь-якої станції, що намагається підключитися до неї. Клієнт повинен використовувати свій ключ для шифрування коректної відповіді для того, щоб аутентифікувати себе й одержати доступ до мережі. Вище другого рівня мережі стандарту 802.11b підтримують ті ж стандарти для контролю доступу й шифрування (наприклад, IPSec), що й мережі стандарту 802.

Недостатня безпека бездротових мереж стала сьогодні основною перешкодою до їхнього використання, особливо в корпоративному середовищі. Коли говорять про безпеку WLAN, звичайно розглядають три різних компоненти: аутентифікацію користувача, конфіденційність даних і їхню цілісність. WLAN-індустрія поступово рухається до моделі безпеки, що базується на технології Wi-Fi Protected Access (WPA). Відповідно до специфікації WPA, аутентифікація виконується з використанням протоколу 802.1x, конфіденційність даних – за допомогою шифрування трафіка TKIP, а цілісність інформації забезпечується контрольною сумою MIC (Message Integrity Check).

Розподілена архітектура не залишає вибору для локалізації цих функцій: всі вони повинні бути реалізовані на межі мережі в крапках доступу. Інакшою є справа у випадку централізованої архітектури. Тут виробники можуть вирішувати самі, де розташувати функції безпеки. Деякі залишають їх у крапках доступу, інші — в бездротових комутаторах, треті — розподіляють між цими двома пристроями. Наприклад, на комутатори покладається аутентифікація користувачів, а шифруванням і цілісністю даних займаються крапки доступу. Але все-таки вірніше, коли аутентифікація виконується на межі мережі. Якщо зловмисник намагається одержати доступ до мережі, то краще перехопити його якомога раніше.

У розподіленій архітектурі DOS-атака здійснюється тільки на одну крапку доступу (КД). Оскільки остання блокує весь неавторизований трафік, то інші компоненти мережі будуть ізольовані від атаки. У мережі із централізованою архітектурою, де функції аутентифікації виконує комутатор, КД не може заблокувати неавторизований трафік. Він направляється до бездротового комутатора, що не пропускає його в корпоративну мережу. Однак цей трафік буде передаватися через всі пристрої, що перебувають на шляху від атакованої крапки доступу до комутатора.

При розподіленій архітектурі всі функції безпеки зосереджені в КД, проте одним із аргументів проти такої архітектури є її фізична уразливість. Іншими словами, крапку доступу досить легко украсти. А оскільки в ній зберігаються ключі шифрування й інші установки із забезпечення безпеки, то це створює досить серйозні проблеми. Зловмисник, що викрав крапку доступу, може потім у лабораторії отримати з неї досить важливу інформацію, включаючи MAC-адреси інших мережевих пристроїв. Більше того, установивши украдену КД у своїй мережі, він

може "захопити" повноправного клієнта останньої й розкрити реєстраційну інформацію. Правда, подібний сценарій не настільки небезпечний у випадку індустріальних реалізацій розподіленої архітектури, де крапки доступу можуть розташовуватися на висоті декількох десятків метрів.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте безпровідні мережі.
2. Які Ви знаєте типи безпровідних мереж?
3. Що Ви розумієте під терміном крапка доступу?
4. Охарактеризуйте стандарти безпровідних мереж.
5. Якому діапазону повинні належати IP-адреси комп'ютерів, що входять в ICS-мережу?
6. Яка різниця між мобільними та локальними мережами?
7. Охарактеризуйте основні види топології безпровідних мереж.
8. Охарактеризуйте безпровідні ЛОМ із радіопередачею даних.
9. Охарактеризуйте складові безпровідних мереж.
10. Охарактеризуйте принцип дії мережі прямої видимості.
11. Охарактеризуйте принцип дії мережі на розсіяному випромінюванні.
12. Як здійснюється підключення до безпровідної мережі?
13. Як здійснюється налагодження Wi-Fi-мережі на ПК і ноутбуках?
14. Опишіть налагодження роутера.
15. Охарактеризуйте режими роботи роутера.
16. Які стандарти в області безпровідних мереж Ви знаєте?
17. Охарактеризуйте архітектуру мережі " Ad-hoc".
18. Охарактеризуйте режими роботи безпровідної мережі.
19. Яка послідовність надання доступу до файлу або каталогу в мережі?
20. Яка послідовність заборони доступу до файлу або каталогу в мережі?
21. Яка послідовність надання доступу до принтера в мережі?
22. Яка послідовність заборони доступу до принтера в мережі?
23. Яка послідовність зміни мереженого паролю?
24. Охарактеризуйте процес підключення до безпровідної мережі.
25. Охарактеризуйте налагодження Wi-Fi-мережі.
26. Охарактеризуйте налагодження Ad-Hoc-мережі.
27. Охарактеризуйте безпеку безпровідних мереж.

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

ОСНОВНА ЛІТЕРАТУРА

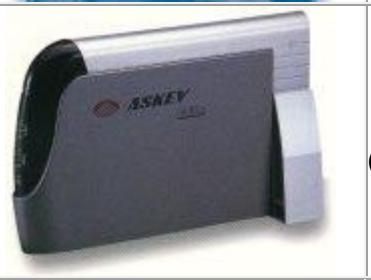
1. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. – Львів: БаК, 2003. – 584 с.
2. Дуглас К. Компьютерные сети и Internet. -Диалектика, 2002. – 640 с.
3. Закер К. Компьютерные сети. – BHV-СПб, 2001. – 1008 с.
4. Одом У. Компьютерные сети: Первый шаг./ пер. с анг. – М.: Издательский дом «Вильямс» , 2006. – 432с.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. – СПб: ПИТЕР, 2003. – 864 с.

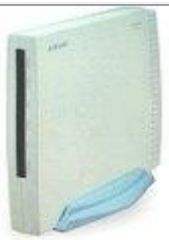
ДОДАТКОВА ЛІТЕРАТУРА

6. Alexander Zamyatin. Передача данных по оптоволоконным линиям. http://www.ccc.ru/magazine/depot/98_12/read.html.
7. Eugene Shakhtarin. Операционная система Linux Copyleft 1995, 1996 <http://eugene.mplik.ru/> <eugene@mplik.ru> .
8. Netware Версия 3.12. Концепции.-Novell Inc./Пер. с англ. – НПО Информатика. г.Иваново. – Novell Inc.,1994 .
9. TCP/IP. Для професионалов. 3-е изд. /Т. Паркер, К. Сиян. – СПб.: Питер, 2004. – 959с.
10. Александров Е.Л. Интернет – легко и просто. Популярный самоучитель. – СПб.: БХВ-Петербург, 2005. – 208 с.
11. Бегелоу С. Сети: поиск неисправностей, поддержка и востановление: пер. с анг. – СПб.: БХВ-Петербург, 2005. – 1200 с.
12. Бертескас Д., Галлагер Р. Сети передач данных. / Пер. с анг.под ред. Цыбакова Б.З. – М.: Мир, 1989.
13. Бертескас Д., Галлагер Р. Сети передачи данных. /Пер. с анг.под ред. Цыбакова Б.З. –М.: Мир, 1989.
14. Богуславский Л.Б., Дрожжинов В.И. Основы построения вычислительных сетей для автоматизированых систем. – М.: Энергоатомиздат, 1990.
15. Борисов М. Новые стандарты высокоскоростных сетей. // Открытые системы, 1994, вып. 3 – с. 20-31.
16. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. – СПб.: Питер, 2006. – 703 с.
17. Буравчик Дж. Локальная сеть без проблем:учебное пособие – М.: Лучшие книги, 2005. – 224 с.
18. Ватаманюк А.И. Беспроводная сеть своими руками. – СПб.: Петербург, 2006. – 192 с.
19. Весли П. М. Корпоративные информационные архитектуры: и все-таки они меняются Gartner Group, 56 Top Gallant Road, Stamford, Connecticut 06904, 203-975-6533 .
20. Веттинг Д. Novell Netware /Пер. с нем. – К.: Торгово-издательское бюро, 1993.
21. Вычислительные машины, системи и сети /Под ред. Пятибратова А.П. – М.: Финансы и статистика, 1991.
22. Галіцин В. К., Левченко Ф. А. Багатокористувацькі системи та мережі: Посібник. – 1998 р. – 360с.
23. Гальперович Д.Я. Тенденции развития проводки для ЛВС. // Сети. – 1994, N5 – с. 44-51.
24. Гилберт Хелд. Воплощение в реальность // Сети. – М.:Открытые Системы. – №6, 1998.
25. Горностаев Ю.М., Соколов В.В., Невдяев Л.М. Перспективные спутниковые системы связи. – М.: Горячая линия Телеком, МЦНТИ, 2000. – 132 с.
26. Дженнингс Ф. Практическая передача данных: Модемы, сети и протоколы / Пер. с англ. – М.: Мир, 1989.
27. Като М. и др. Построение сетей ЭВМ. – М.:Мир,1988.
28. Компьютерные сети: 4-е изд. /Э. Таненбаум. – СПб.: Питер, 2003. – 992 с.
29. Кулаков Ю.А., Луцкий Г.М. Компьютерные сети : Учебное пособие, К.: Юниор, 1998. – 350 с.
30. Куроуз Дж., Росс К. Компьютерные сети – СПб.: Питер, 2004. – 765 с.
31. Леонтьев В. Мобильный Интернет – М.: ОЛМА Медиа Групп, 2008.

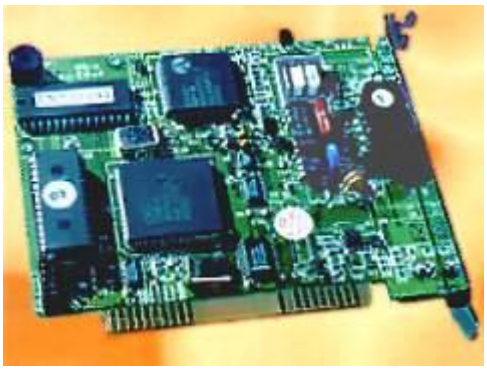
32. Максимов Н.В., Попов И.И. Компьютерные сети: учебное пособие для студентов среднего профессионального образования. – 3 изд. – М.: ФОРУМ, 2008. – 448 с.
33. Новиков Ю.В., Кондратенко С.В. М.Основы локальных сетей: учебное пособие. Интернет-университет информационных технологий , 2005. – 360 с.
34. Овчинников В.В., Рыбин И.М. Техническая база интерфейсов локальных вычислительных сетей. – М.: Радио и связь, 1988.
35. Оглтри Т. Практическое применение межсетевых экранов. / Пер. с анг. – М.:ДМК Пресс, 2001. – 400 с.
36. Олаф Кирч. Руководство администратора сети в ОС Linux. 1992-1994. http:// ttc.ryazan.ru/archive/nag.htm.
37. Поляк-Брагинский А.В. Администратирование сети на примерах. – СПб.: БХВ-Петербург, 2005. – 320 с.
38. Семенов А.Б., Стрижаков С.К.,Сунчелей И.Р. Структурированные кабельные системы: 4-е изд., перераб. и доп. – М.: ДМК Пресс, 2002. – 640 с.
39. Стандарты по локальным вычислительным сетям: Справочник. / Под ред. З.Н. Самойленко. – М.: Радио и связь, 1990.
40. Уолл Д. и др. Использование World Wide Web. 2-е издание / Пер. с англ. – К.: Диалектика, 1997. – 432 с.
41. Учебное пособие. Введение в сети/ Составитель: Д.К.Морозов. – г.Ярославль, 1995.
42. Флинт Л. Локальные сети ЭВМ. Архитектура, принцип построения, реализация.– М.: Финансы и статистика.

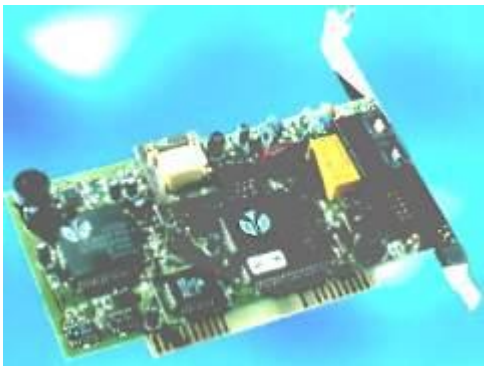
Додаток 1
Кабельні модеми

	**PCX 1000** від **Toshiba** Цей модем перший із двох, що одержали DOCSIS сертифікат. Він побудований на Libit (тепер Texas Instruments) чипі, який об'єднує в собі модулятор-демодулятор і MAC чип від TurboNet Communications.
	**DCM105** від **Thomson Consumer Electronics** Це другий із перших двох модемів, що одержали DOCSIS сертифікат. Він базується на наборі мікросхем Broadcom.
	**U.S. Robotics Cable Modem CMI і CMX** від **3Com Corporation** CMI – це внутрішній модем для ISA шини. CMX – зовнішній кабельний модем, сертифікований на DOCSIS.
	**SB2100** від **General Instrument**
	**CM-100** від **Arris Interactive** (колишня Nortel Networks)
	**CM010** від **Askey Computer Corp. in Taiwan** (використаний референсний дизайн від Cisco)
	**UBR904** і **UBR924** від **Cisco**. Ці модеми більше орієнтовані на SOHO ринок. Вони об'єднують в собі кабельний модем, маршрутизатор (router) і невеликий концентратор (hub).
	**PD10d** від **Philips Electronics** (використаний референсний дизайн від Cisco).

	**Inforanger** від **Samsung Information Systems America** (використаний референсний дизайн від Cisco).
	**Sony Corp** (використаний референсний дизайн від Cisco).
	**Terayon** мав кабельний модем сертифікований на DOCSIS 1.0 на початку вересня 1999 р. Виходячи із пресс-реліза, він називається TeraJetTM.
	**DoxPort 101** – це low-end модель. DoxPort 1010 – це high-end модель, яка була серед чотирьох сертифікованих в той час модемів.
	**Best Data** має **Smart One DOCSIS 1.0** кабельний модем, сертифікований у грудні 1999 р. Best Data створила модем спільно з TurboNet Communications, і продукт використовує TurboNet's MAC і PHY чип від Texas Instruments.

Внутрішні модеми





ДОДАТОК 2
Глосарій із мережевих технологій
Цифрові терміни

10 Mbps – 10 Мегабіт у секунду – швидкість передавання в мережі Ethernet.

100 Mbps – 100 Мегабіт у секунду – швидкість передавання в мережі Fast Ethernet і FDDI.

10Base-2 – реалізація стандарту IEEE 802.3 Ethernet з використанням тонкого коаксіального кабелю. Називається також Thinnet.

10Base-5 – реалізація стандарту IEEE 802.3 Ethernet з використанням товстого коаксіального кабелю. Називається також Thicknet.

10BASE-F – реалізація стандарту IEEE 802.3 Ethernet з використанням оптичного кабелю.

10BASE-T – специфікація IEEE 802.3i для мереж Ethernet з використанням неекранованого кабелю типу «скручена пара».

100BASE-T – специфікація IEEE 802.3us для мереж Ethernet із швидкістю передавання 100 Мбіт/с на основі неекранованого кабелю типу «скручена пара».

100BASE-FX – специфікація IEEE 802.3us для мереж Ethernet із швидкістю передавання 100 Мбіт/с на основі оптичного кабелю.

A

AAL (ATM Adaptation Level) – правила, що визначають спосіб підготовки інформації для передавання мережею ATM.

Abstract syntax (абстрактний синтаксис) – опис структури даних, незалежний від апаратної реалізації й способу кодування.

AES-CCMP – розширений стандарт шифрування (Advanced Encryption Standard) – використовується для шифрування аутентифікаційної інформації так, щоб не було можливості отримати її шляхом прослуховування ефіру. CCMP – один з двох методів, які можуть бути використані в стандарті 802.11i; поєднує в собі дві технології: counter mode і CBC-MAC, подробиці про яких цікаві лише фахівцям, і досить утруднює зламування. AES-CCMP вимагає використання спеціалізованого чіпа в маршрутизаторі або безпровідному пристрої, тому використовується для організації надійного шифрованого каналу з вищим рівнем безпеки в порівнянні з широко поширеним шифруванням TKIP.

Access method (метод доступу) – набір правил, що забезпечують арбітраж доступу до середовища передавання. Прикладами методів доступу є CSMA/CD (Ethernet) і передавання маркера (Token Ring).

ACSE: Association Control Service Element – метод, що використовуэться в OSI для організації зв'язку між двома застосуваннями. Перевіряє ідентичність і контекст додатків, і може виконувати перевірку автентичності.

Address (адреса) – унікальний ідентифікатор, що привласнюється мережі або мережевому пристрою для того, щоб інші мережі й пристрої могли розпізнати його при обміні інформацією.

Address mask (адресна маска) – бітова маска, що використовуться для вибору бітів з адреси Internet для адресації підмережі. Маска має розмір 32 біта й виділяє мережеву частину адреси Inetrnet і один або декілька бітів локальної частини адреси. Іноді називається маскою підмережі.

Address resolution (дозвіл адреси) – використовується для перетворення адрес мережевого рівня (Network Layer) в обумовлені середовищем (media-specific) адреси.

ADMD: Administration Management Domain – Домен адміністративного управління, адміністративний домен. Приклади: MCImail і ATTmail в США, British Telecom Gold400mail у Великобританії. ADMD всіх країн спільно утворюють магістраль X.400 (backbone).

Adjacency (суміжність) – співвідношення, що встановлюється між сусідніми маршрутизаторами для обміну інформацією про маршрутизацію. Суміжними є не всі пари сусідніх маршрутизаторів.

ADPCM (Adaptive Differential Pulse Code Modulation - адаптивна диференціальна імпульсно-кодова модуляція) – стандартизована ITU методика кодування аналогового сигналу (мова) в цифрову форму із смугою 32 Кбіт/с (половина стандартної смуги PCM).

agent (агент) – стосовно SNMP термін агент означає систему, що управляє. У моделі клієнт-сервер – частина системи, що виконує підготовку інформації й обмін нею між клієнтською й серверною частиною.

Algorithm (алгоритм) – набір упорядкованих кроків для вирішення завдання, такий як математична формула або інструкція в програмі. У контексті кодування мови алгоритмами називають математичні методи, використовувані для компресії мови. Унікальні алгоритми кодування мови патентуються. Конкретні реалізації алгоритмів у комп'ютерних програмах також є суб'єктом авторського права.

American National Standards Institute (Американський інститут стандартів) – організація, відповідальна в США за розроблювання й публікацію стандартів, пов'язаних із кодуванням, передаванням сигналів і тому подібне. ANSI є членом Міжнародного комітету зі стандартизації (ISO).

Analog (аналоговий) – сигнал, представлений безперервною (на відміну від дискретного цифрового) зміною тієї або іншої фізичної величини (наприклад, людська мова).

AOWAPI (Application Program Interface – Інтерфейс прикладного програмування) – набір угод, що визначають правила викликання функцій і передавання параметрів із прикладних програм.

API: Application Program Interface (Інтерфейс прикладних програм) – набір угод, що визначають правила викликання функцій і передавання параметрів із прикладних програм.

Application Layer (Рівень додатків) – верхній рівень моделі OSI, що забезпечує такі комунікаційні послуги, як електронна пошта й перенесення файлів.

ARP: Address Resolution Protocol (Протокол дозволу адрес) – протокол Internet, що використовується для динамічного перетворення адрес Internet у фізичні (апаратні) адреси пристроїв локальної мережі. У загальному випадку ARP вимагає передавання широкомовних повідомлень усіх вузлів, на яке відповідає вузол із відповідною запиту IP-адресою.

ARPA: Advanced Research Projects Agency – зараз називається DARPA – державне агентство США, яке організувало мережу ARPANET.

ARPANET – мережа з комутацією пакетів, організована на початку 70-х років. Ця мережа була прообразом сьогоднішньої мережі Internet. ARPANET розформована в червні 1990.

ARQ (Automatic Request for Repeat or Retransmission – автоматичний запит повторного передавання) – режим зв'язку, при якому одержувач запитує у відправника повторення блока даних або кадру при виявленні помилок.

ASCII (American Standard Code for Information Interchange – американський стандартний код для обміну інформацією) – набір символів.

Asynchronous Transmission (асинхронне передавання) – метод передавання, що використовується для пересилання даних по одному символу, при цьому проміжки між передаванням символів можуть бути нерівними. Кожному символу передують стартові біти, а закінчення передавання символу позначається стоп-бітами. Іноді цей метод передавання називають старт-стоповим (start-stop transmission).

ATM (Asynchronous Transfer Mode – асинхронний режим передавання) – стандартизована ITU технологія комутації пакетів фіксованої довжини – осередків (cell). Режим ATM є асинхронним у тому сенсі, що осередки від окремих користувачів передаються аперіодично. Ця технологія призначена для передавання даних зі швидкістю від 1.5 Мбіт/с до 2 Гбіт/с і забезпечує ефективне передавання різних типів даних (голос, відео, мультимедіа, трафік ЛОМ) на значні відстані. Специфікації ATM розробляються Форумом ATM (ATM Forum) – незалежною асоціацією виробників і користувачів.

B

Baseband modem – модем для прямого (немодульованого) передавання даних.

Baud (бод) – одиниця швидкості передавання сигналу, яка вимірюється числом дискретних переходів або подій у секунду. Якщо кожною подією є один біт, бод еквівалентний біт/с (у реальних комунікаціях це часто не виконується).

BIND (Berkeley Internet Name Domain) – програма для підтримки сервера імен доменів, спочатку написана для UNIX 4.3BSD. У даний час є найпопулярнішою реалізацією DNS і

перенесена практично на всі платформи. BIND задає структуру баз даних, функції DNS і конфігураційні файли, потрібні для установлення й функціонування сервера імен.

BISDN (Broadband Integrated Services Digital Network – широкосмугова цифрова мережа з інтеграцією послуг) – наступне покоління мереж ISDN, що дозволяють передавати цифрові дані, голос і динамічні зображення (відео). ATM забезпечує комутацію, а SONET або SDH фізичний транспорт.

Bps (Bits Per Second – біт/с) – одиниця вимірювання швидкості при послідовному передавання даних.

bridge (міст) – пристрій, що сполучає дві або декілька фізичних мереж і передає пакети з однієї мережі в іншу. Мости можуть фільтрувати пакети, тобто передавати в інші сегменти мережі тільки частину трафіку, на основі інформації канального рівня (MAC-адрес).

broadband (широкосмугова мережа) – широкосмугова технологія, здатна забезпечити одночасне передавання голосу, даних, відео. Зазвичай це здійснюється шляхом мультиплексування з розділенням частот. Широкосмугова технологія дозволяє декільком мережам використовувати один загальний кабель – трафік однієї мережі не впливає на передавання сигналів іншої мережі, оскільки «розмова» відбувається на різних частотах.

broadcast (широкомовлення) – система доставки пакетів, при якій копія кожного пакету передається всім хостам, підключеним до мережі. Прикладом широкомовної мережі є Ethernet.

BSD (Berkeley Software Distribution) – термін, що використовується для опису різних версій операційної системи Berkeley UNIX (наприклад, 4.3BSD UNIX).

Buffer (буфер) – пристрій [тимчасового] зберігання, що у загальному випадку використовується для компенсації різниці швидкостей при обміні даними між пристроями. Буферизація також використовується для зменшення тремтіння (jitter).

Bus (шина) – шлях (канал) передавання даних. Зазвичай, це шина реалізована у вигляді електричного з'єднання з одним або декількома провідниками й усі підключені до шини пристрої отримують сигнал одночасно.

Bus topology (шинна топологія) – топологія мережі, при якій в якості середовища передавання використовується єдиний кабель (він може складатися з послідовно сполучених відрізків), до якого підключаються всі мережеві пристрої. Така топологія широко застосовувалася спочатку в мережах Ethernet, але зараз вона використовується достатньо рідко через властиві їй обмеження й у зв'язку зі значними складнощами при розширенні мережі або перенесенні комп'ютерів. Крім того, при пошкодженні кабелю весь сегмент перестає працювати, а локалізація пошкоджень є складним завданням.

C

Channel (канал) – шлях передавання сигналів між двома або декількома крапками. Використовуються також терміни: link, line, circuit і facility.

Channel Bank – устаткування, що підключає численні голосові канали до високошвидкісного каналу за рахунок перетворення голосу в цифрову форму й мультиплексування з розділенням часу (Time Division Multiplexing).

CLNP (Connectionless Network Protocol) – протокол OSI для забезпечення OSI Connectionless Network Service (datagram service). CLNP представляє в OSI еквівалент протоколу IP в Internet, його іноді називають ISO IP.

Clock (годинник, тактовий генератор) – пристрій, що генерує періодичні сигнали, які використовуються для синхронізації інших пристроїв або передавання даних.

CLTP (Connectionless Transport Protocol) – забезпечує наскрізну (end-to-end) адресацію передавання даних (за допомогою Transport selector) і контроль помилок (за допомогою контрольної суми), але не може гарантувати доставку або забезпечувати управління потоком. У OSI є еквівалентом UDP.

CMIP (Common Management Information Protocol – протокол загальної інформації, що управляє) – стандартний протокол мережевого управління для мереж OSI. Цей протокол визначає ряд функцій, відсутніх в SNMP і SNMP-2. Складність протоколу CMIP зумовила його малу поширеність, проте, у деяких випадках обійтися без нього не вдається.

Collision (конфлікт, колізія) – спроба двох (або більше) станцій одночасно почати передавання пакету в мережі CSMA/CD. При виявленні конфлікту обидві станції припиняють передавання і намагаються відновити його після закінчення певного інтервалу часу, що визнача-

ється випадковим чином. Використання випадкової затримки дозволяє вирішити проблему виникнення повторного конфлікту.

Collision domain (область колізій, колізійний домен) – частина мережі (сегмент), у якому станції використовують загальне середовище передавання. При спробі одночасного передавання даних двома або більше станціями виникає конфлікт (колізія). Для вирішення конфліктів використовується протокол CSMA/CD.

Contention (з'єднання) – стан, що виникає при обміні даними між двома або декількома станціями за однією лінією або каналом.

Control Characters (управляючі символи) – у комунікаціях це будь-які додаткові символи, що використовуються для управління передаванням або його полегшення (наприклад, символи, пов'язані з опитом, кадруванням, синхронізацією, контролем помилок і тому подібне).

Core gateway (внутрішній шлюз) – історично один із набору шлюзів (маршрутизаторів), що працюють в Internet Network Operations Center. Система внутрішніх шлюзів формує центральну частину системи маршрутизації Internet, у якій усі групи повинні пропонувати шляхи у свої мережі із внутрішнього шлюзу з використанням протоколу Exterior Gateway Protocol (EGP).

CRC (Cyclic Redundancy Check – циклічна перевірка парності з надмірністю) – схема визначення помилок при передаванні даних. На основі поліноміального алгоритму обчислюється контрольна сума передаваного модуля даних і передається разом із даними. Пристрій, що отримав пакет, наново обчислює контрольну суму за тим же алгоритмом й порівнює її з набутим значенням. Відсутність розбіжностей говорить про високу вірогідність безпомилкового передавання.

CSMA/CD (Carrier sense multiple access/collision detection – множинний доступ до середовища з виявленням конфліктів і детектуванням) – метод доступу до середовища передавання (кабелю), визначений у специфікації IEEE 802.3 для локальних мереж Ethernet. CSMA/CD вимагає, щоб кожен вузол, розпочавши передавання, продовжував "прослуховувати" мережу на предмет виявлення спроби одночасного передавання іншим пристроєм – колізії. При виникненні конфлікту передавання повинно бути негайно перервано, і може бути відновлено після закінчення випадкового проміжку часу. У мережі Ethernet із завантаженням 35-40% колізії виникають достатньо часто й можуть істотно вповільнити роботу. При невеликій кількості станцій вірогідність колізій істотно знижується.

Current Loop (струмова петля) – метод передавання даних. Одиниці в цьому випадку представляються імпульсом струму в петлі, нулі – відсутністю струму.

D

Data (дані) – представлена в цифровій формі інформація, що включає мову, текст, факсимільні повідомлення, динамічні зображення (відео) і тому подібне.

Data Link Layer – рівень 2 в моделі OSI. Цей рівень забезпечує організацію, підтримку й розрив зв'язку на рівні передавання даних між елементами мережі. Основною функцією рівня 2 є передавання модулів інформації або кадрів і пов'язаний із цим контроль помилок.

Data Rate, Data Signaling Rate – показник швидкості передавання даних, що вимірюється в біт/с (bps).

DCE (Data Communications Equipment – устаткування для передавання даних) – пристрої, що забезпечують організацію й розрив з'єднань, а також управління ними для передавання даних. Прикладом такого пристрою є модем.

DCE (Distributed Computing Environment) – архітектура стандартних інтерфейсів програмування, угод і функцій серверів (наприклад, іменування, розподілена файлова система, віддалений виклик процедур) для розподілених застосувань, що працюють у гетерогенних мережах. Розробляється й управляється Фондом відкритих програм (Open Software Foundation – OSF), консорціумом HP, DEC і IBM.

DDNS (Dynamic Domain Name System) – динамічна система імен доменів, визначена в IBM OS/2 Warp server для динамічного виділення імен хостам на підставі їх IP-адрес.

Designated Router (відмічений маршрутизатор) – у кожній мережі, що має принаймні 2 маршрутизатори, є відмічений маршрутизатор. Доповнений протоколом вітання (Hello Protocol), цей маршрутизатор генерує інформацію про стан каналу для мережі з множинним доступом і виконує ряд інших дій.

Diagnostics (діагностика) – процедури й системи, що детектують й ізолюють помилки й некоректно працюючі пристрої, мережі і системи.

Digital (цифровий) – двійкова інформація, що виводиться з комп'ютера або терміналу. У комунікаційній сфері дискретне (імпульсне) передавання інформації (на відміну від безперервного аналогового).

Domain (домен) – у мережі Internet – частина ієрархії імен. Синтаксично доменне ім'я Internet містить послідовність імен, розділених крапками, наприклад, tundra.mpk.ca.us. У OSI термін «домен» використовується як адміністративне ділення складних розподілених систем, як в MHS Private Management Domain (PRMD) і Directory Management Domain (DMD).

DNS (Domain Name System – система імен доменів) – розподілений механізм імен/адрес, використовуваних у мережі Internet. Використовується для дозволу логічних імен в IP-адресах. DNS використовується в мережі Internet, забезпечуючи можливість роботи зі зрозумілими іменами, що легко запам'ятовуються, замість чисел IP-адрес.

DXI (Data Exchange Interface – інтерфейс обміну даними) – протокол, використовуваний між маршрутизатором і DSU для SMDS і ATM.

E

E1 – використовувана в Європі цифрова мережа передавання даних зі смугою 2.048 Мбод.

E3 – європейський стандарт для високошвидкісного (34 Мбод) передавання цифрових даних.

EARN (European Academic Research Network – Європейська академічна дослідницька мережа) – мережа, що використовує технологію BITNET для об'єднання університетів і дослідницьких центрів у Європі.

EAP, LEAP і PEAP. Різні виробники безпровідного устаткування реалізовували несумісні технології авторизації, що робило несумісними різні пристрої. Розширюваний протокол аутентифікації (EAP) був створений для узгодження різних технологій, щоб пристрої різних виробників могли погоджувати між собою протоколи перевірки аутентифікаційних даних. Light EAP (LEAP) був прийнятий компанією Cisco і став стандартом де-факто. Protected EAP (PEAP) є новою версією цієї технології, вона стійкіша до зламування, але не сумісна з більшістю устаткування і програмним забезпеченням, випущеними до 2002 року.

EGP (Exterior Gateway Protocol) – протокол маршрутизації, використовуваний шлюзами дворівневої мережі. EGP використовується в ядрі Internet.

End system (кінцева система) – система OSI, що містить процеси, здатні забезпечити передавання через усі сім рівнів протоколів OSI. Еквівалент хоста в Internet.

Ethernet – стандарт організації локальних мереж (ЛОМ), описаний у специфікаціях IEEE і інших організацій. IEEE 802.3. Ethernet використовує смугу 10 Мбіт/с і метод доступу до середовища CSMA/CD. Найпопулярнішою реалізацією Ethernet є 10Base-T. Розвитком технології Ethernet є Fast Ethernet (100 Мбіт/с).

Ethernet LAN – стандарт де-факто, запропонований компанією Xerox і розширений спільно Xerox, Intel і DEC. Локальні мережі Ethernet (LAN або ЛОМ) спочатку використовували коаксіальний кабель RG-11 (зараз використовується в основному кабель типу «скручена пара» категорії 3 або 5 і в деяких випадках коаксіальний кабель RG-58) і метод множинного доступу з виявленням конфліктів (CSMA/CD). Мережа Ethernet може мати шинну або зіркову топологію.

F

FARNET (Federation of American Research NETworks) – федеральні американські дослідницькі мережі.

FDDI (Fiber Distributed Data Interface) – високошвидкісний мережевий стандарт. Середовищем передавання даних є оптичне волокно, а топологія – Token Ring із подвійним підключенням.

Four-Wire Circuit (чотирипровідний пристрій/канал) – комунікаційний канал, що складається із двох пар провідників, одна з яких використовується для приймання, а друга – для передавання.

FPS (Fast Packet Switching) – швидка комутація пакетів.

FRAD (Frame Relay Access Device) – маршрутизатор, мультиплексор або інший пристрій у мережі Frame Relay.

Fragmentation (фрагментація) – процес розділення дейтаграми IP на декілька дрібних частин для виконання вимог даної фізичної мережі. Зворотний процес називають дефрагментацією (reassembly).

Frame Relay – високошвидкісна технологія, заснована на комутації пакетів, для передавання даних між інтелектуальними крайовими пристроями типу маршрутизаторів або FRAD, що працюють зі швидкістю від 56 Кбіт/с до 1.544 Мбіт/с. Дані діляться на кадри змінної довжини передавальним пристроєм, а кожен кадр містить заголовок з адресою одержувача. Кадри передаються цифровим пристроєм і збираються на приймальному кінці.

FTP (File Transfer Protocol) – використовуваний в Internet протокол (і програма) передавання файлів між хост-компьютерами.

Full Duplex (повнодуплексний) – канал або пристрій, що виконує одночасно приймання і передавання даних.

G

Gateway (шлюз) – оригінальний термін Internet, для позначення таких пристроїв використовується термін маршрутизатор (router) або точніше маршрутизатор IP. У сучасному варіанті терміни «gateway» і «Application gateway» використовуються для позначення систем, що виконують перетворення з одного природного формату в інший. Прикладом шлюзу може служити перетворювач X.400 - RFC 822 electronic mail.

GOSIP (Government OSI Profile) – підтримувані державою специфікації для протоколів OSI в США.

H

Half Duplex (напівдуплексний) – пристрій або канал, здатний у кожен момент тільки передавати або приймати інформацію. Приймання і передавання, таким чином, повинні виконуватися за чергою.

HDLC (High-level Data Link Control) – високорівневий протокол управління каналом) – міжнародний комунікаційний протокол, розроблений ISO.

Hello Protocol (протокол вітання) – частина протоколу OSPF, що використовується для організації і підтримки зв'язків між сусідніми пристроями. У мережах із множинним доступом (multiaccess) Hello Protocol може також динамічно виявляти сусідні маршрутизатори.

I

IAB (Internet Activities Board) – технічна група, що відповідає за розвиток набору протоколів Internet (у загальному випадку званого TCP/IP). Група ділиться на дві частини - IRTF і IETF, кожна з яких займається вирішенням своїх завдань.

ICMP (Internet Control Message Protocol) – протокол, який використовується для контролю за помилками й повідомленнями на рівні IP. Насправді ICMP є частиною протоколу IP.

IEEE (Institute of Electrical and Electronic Engineers – інститут інженерів за електротехнікою й радіоелектронікою) – професійне об'єднання, що випускає свої власні стандарти. Членами IEEE є ANSI і ISO.

IEEE 802.3 – специфікація IEEE для локальних мереж CSMA/CD.

IEEE 802.5 – специфікація IEEE для локальних мереж Token Ring.

IESG (Internet Engineering Steering Group) – виконавський комітет IETF.

IETF (Internet Engineering Task Force) – одна із груп IAB ради з архітектури Internet. IETF відповідає за вирішення інженерних завдань Internet. Включає понад 40 робочих груп. IETF випускає більшість RFC, використовуваних виробниками для впровадження стандартів в архітектуру TCP/IP.

IGP (Interior Gateway Protocol) – протокол, який використовується для обміну інформацією про маршрутизацію між спільно працюючими маршрутизаторами в мережі Internet. Прикладами IGP є RIP і OSPF.

Interior Gateway Protocol – протокол, який використовується для обміну інформацією про маршрутизацію між спільно працюючими маршрутизаторами в мережі Internet. Прикладами IGP є RIP і OSPF. Кожна автономна система має 1 IGP, роздільні автономні системи можуть використовувати різні IGP.

internet – група зв'язаних маршрутизаторами мереж, здатна функціонувати як одна велика віртуальна мережа.

Internet (із заголовної букви) – найбільша у світі мережа internet, що містить великі національні магістральні (backbone) мережі (такі, як MILNET, NSFNET, CREN) і величезну

кількість регіональних, і локальних мереж у всьому світі. Мережа Internet використовує набір протоколів IP. Для підключення до Internet потрібно мати IP-з'єднання, тобто можливість працювати з іншими системами, або використовувати ping. Мережі лише з поштовим підключенням насправді не є частиною Internet.

Internet address – 32-бітова адреса, пов'язана з хостом, який використовує TCP/IP.

IONL (Internal Organization of the Network Layer) – стандарт OSI для детальної архітектури мережевого рівня. У загальному випадку це частина мережевого рівня підмереж, сполучених за допомогою протоколів конвергенції (convergence protocols), еквівалентна міжмережевим протоколам, що створюються в тих випадках, коли Internet викликає catenet або internet.

IP (Internet Protocol) – протокол мережевого рівня з набору протоколів Internet.

IP datagram – фундаментальна одиниця інформації, яка передається через Internet. Містить адреси джерела й одержувача разом із даними й поля, що визначають довжину дейтаграми, контрольну суму заголовка й прапори, що говорять про фрагментацію дейтаграми.

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

IRTF (Internet Research Task Force) – один із підрозділів IAB, що відповідає за дослідження й розробку набору протоколів Internet.

ISDN (Integrated Services Digital Network – цифрова мережа з інтеграцією послуг) – технологія, запропонована спочатку для міжнародного телефонного зв'язку. ISDN об'єднує голосові й цифрові мережі в єдиному середовищі, даючи користувачеві можливість передавання мережею голосу й даних. Керівні стандарти ISDN створюються CCITT.

IS-IS (Intermediate system to Intermediate system protocol) – протокол OSI, за допомогою якого проміжні системи (intermediate systems) обмінюються інформацією про маршрутизацію.

ISO (International Organization for Standardization – міжнародна організація зі стандартизації) – асоціація національних організацій зі стандартизації, що забезпечує розробку й підтримку глобальних стандартів у сфері комунікацій і обміну інформацією. Добре відома семирівнева модель OSI/ISO, що визначає стандарти взаємодії комп'ютерів у мережах.

L

LAN (Local Area Network – локальна мережа, ЛОМ) – сполучені разом швидкісним каналом комп'ютери й інші пристрої, розташовані на незначному віддаленні один від одного (кімната, будівля, підприємство).

Leased Line (орендована лінія) – лінія, зарезервована для виняткового використання замовником без комутації (постійне з'єднання). Частіше використовується термін «виділена лінія».

Line Driver (драйвер лінії) – перетворювач сигналу, що забезпечує посилення для передавання на значні відстані.

Link State Advertisement – описує локальний стан маршрутизатора або мережі, включаючи стан інтерфейсів, і суміжні маршрутизатори. Інформація LSA передається через весь домен. На основі цієї інформації маршрутизатори формують базу даних про протоколи й топологію мережі.

M

MAC (Media Access Control – управління доступом до середовища) – протокол, використовуваний для визначення способу отримання доступу робочих станцій до середовища передавання, найчастіше використовуваний у локальних мережах. Для ЛОМ, відповідних стандартам IEEE, MAC-рівень є нижнім підрівнем каналу передавання даних (data link layer).

Mail exploder – частина системи доставки електронної пошти, яка забезпечує доставку повідомлень групам адресатів. Такі програми використовуються для реалізації списків розсилання (mailing list). Користувач посилає повідомлення за єдиною адресою (наприклад, hacks@somehost.edu) і програма забезпечує їх доставку за кожною з включених в список адрес.

mail gateway (поштовий шлюз) – комп'ютер, що сполучає дві або більше систем електронної пошти (поштові системи двох різних мереж, що істотно відрізняються) і передає повідомлення між ними. Іноді перетворення адрес і трансляція можуть бути достатньо складні й у

загальному випадку потрібні використання схеми «зберегти й переслати», коли повідомлення приходить з однієї системи, воно спочатку записується, а потім транслюється й передається в іншу систему.

Master Clock (основний годинник, тактовий генератор) – джерело тактових сигналів (або сам сигнал), за яким здійснюється синхронізація годинника всієї мережі.

Mesh Network – мережа передавання даних, що забезпечує можливість передавання інформації між двома крапками за різними шляхами. При організації таких мереж дуже важливу роль грає вибір пристроїв, що сполучають локальні мережі (маршрутизаторів).

MHS (Message Handling System – система управління повідомленнями) – система повідомлень, призначених для користувача агентів, агентів передавання повідомлень, зберігання повідомлень і модулів доступу, що спільно забезпечують функціонування електронної пошти OSI. MHS підтримується серією рекомендацій X.400 CCITT.

Modem (Modulator-Demodulator – модулятор-демодулятор) – пристрій, що використовується для перетворення послідовності цифрових даних із передавального DTE у сигнал, відповідний для передавання на значну відстань. У разі приймання виконується зворотне перетворення й дані сприймаються приймальним DTE.

Modem Eliminator (замінник модему) – пристрій, що використовується для з'єднання локального терміналу з портом комп'ютера. Даний пристрій замінює собою пару модемів, потрібних при звичайному підключенні.

Modulation (модуляція) – зміна параметрів відповідно до передаваного сигналу. Для модуляції зазвичай використовується амплітуда, фаза або частота сигналу.

MTA (Message Transfer Agent – агент передавання повідомлень) – прикладний процес OSI, використовуваний для збереження й пересилання повідомлень в X.400 Message Handling System. Еквівалент поштового агента Internet.

MTU (Maximum Transmission Unit) – максимально можливий модуль даних, який можна передати через дане фізичне середовище. Приклад: MTU для Ethernet складає 1500 байт.

Multicast – спеціальна форма широкомовлення, при якій копії пакетів доставляються тільки підмножині всіх можливих адресатів.

Multicasting – доставка пакетів від одного відправника до декількох одержувачів із реплікацією пакетів тільки при необхідності.

Multiplexer (мультиплексор) – пристрій, що дозволяє передавати однією лінією декілька сигналів одночасно.

N

Name resolution (дозвіл імен) – процес перетворення імені у відповідну адресу.

NDIS – специфікація стандартного інтерфейсу мережевих адаптерів, розроблена компанією Microsoft для того, щоб зробити комунікаційні протоколи незалежними від мережевого встаткування ПК. Драйвер може працювати одночасно з декількома стеками протоколів.

Neighboring Routers (сусідні маршрутизатори) – два маршрутизатори, підключені до однієї мережі. У мережах із множинним доступом сусіди визначаються динамічно за допомогою протоколу OSPF Hello.

NETBEUI (NETBIOS Extended User Interface) – транспортний протокол, використовуваний Microsoft LAN Manager, Windows for Workgroups, Windows NT і інших мережевих ОС.

NETBIOS (Network Basic Input Output System – мережева базова система введення-виводу) – стандартний мережевий інтерфейс, запропонований для IBM PC і сумісних систем.

Network (мережа) –

1.З'єднання групи вузлів (комп'ютерів або інших пристроїв).

2.Група вузлів або станцій, сполучених комунікаційними каналами, й набір устаткування, що забезпечує з'єднання станцій і передавання між ними інформації.

Network Layer – мережевий рівень – рівень моделі OSI, що відповідає за маршрутизацію, перемикання й доступ до підмереж через усе середовище OSI.

Network Management System – система управління мережею – система встаткування й програм, використовувана для моніторингу, управління й адміністрування в мережі передавання даних.

Network Mask – 32-бітове число, що показує діапазон IP-адрес, що знаходяться в одній IP-мережі/підмережі.

NFS(R) (Network File System – мережева файлова система) – розподілена файлова система, розроблена компанією Sun Microsystems, яка дозволяє групі комп'ютерів прозорий сумісний доступ до файлів один одного.

NNI (Network to Network Interfage) – інтерфейс, що визначає взаємодію комутаторів ATM.

O

Object (об'єкт) – об'єкт, у контексті управління мережею – числове значення, що характеризує той або інший параметр керованого пристрою. Послідовність чисел, розділених крапкою, що визначає об'єкт усередині MIB, називається ідентифікатором об'єкту.

ODI (Open Data Link Interface) – розроблена компанією Novell специфікація стандартного інтерфейсу, що дозволяє використовувати декілька протоколів з одним мережевим адаптером.

OSI (Open Systems Interconnection) – міжнародна програма стандартизації обміну даними між комп'ютерними системами різних виробників.

OSI model (Open Systems Interconnection model) – семирівнева ієрархічна модель, розроблена Міжнародним комітетом зі стандартизації (ISO) для визначення, специфікації й зв'язку мережевих протоколів.

OSPF (Open Shortest Path First) – ієрархічний алгоритм маршрутизації, при якому шлях вибирається на підставі інформації про стан каналу (Link state). Розроблений на основі протоколу RIP.

P

Packet (пакет) – впорядкована сукупність даних і інформації, яка передається через мережу як частина повідомлення.

Packet Switching (комутація пакетів) – метод передавання даних, при якому інформація ділиться на дискретні фрагменти, звані пакетами. Пакети передаються послідовно – один за іншим.

Parity Bit (біт парності) – додатковий біт, що додається в групу для того, щоб загальне число одиниць у групі було парним або непарним (залежно від протоколу).

Physical Layer (Фізичний рівень) – рівень моделі OSI, що забезпечує спосіб активізації й фізичного з'єднання для передавання бітів даних. Простіше кажучи, фізичний рівень забезпечує процедури перенесення одного біта через фізичне середовище.

Ping (Packet internet groper) – програма, використовувана для перевірки доступності адресата шляхом передавання йому спеціального сигналу (ICMP echo request – запит відгуку ICMP) і очікування відповіді. Термін використовується як дієслово: "Ping host X to see if it is up!"

Polling – механізм опиту, що забезпечує унікальну адресацію кожного пристрою.

Port (порт) – абстракція, яка використовується транспортними протоколами Internet для позначення численних одночасних з'єднань з єдиним хостом-адресатом. Фізичний інтерфейс комп'ютера, мультиплексора й тому подібне для підключення терміналу або модему.

PPP (Point-to-Point Protocol) – будучи спадкоємцем SLIPPPP забезпечує з'єднання маршрутизатор-маршрутизатор і хост-мережа як для синхронних, так і для асинхронних пристроїв.

Presentation Layer (Рівень уявлення) – рівень моделі OSI, що визначає спосіб представлення інформації прикладними програмами (кодування) для передавання її між двома кінцями системи.

PRMD (Private Management Domain) – система управління повідомленнями X.400 Message Handling System для поштового сервісу організації. Прикладом такої системи є NASA-mail.

Protocol (протокол) – формат опису передаваних повідомлень і правила, за якими відбувається обмін інформацією між двома або декількома системами.

Proxy – механізм, за допомогою якого одна система представляє іншу у відповідь на запити протоколу. Proxy-системи використовуються в мережевому управлінні, щоб позбавитися від необхідності реалізації повного стека протоколів для таких простих пристроїв, як модеми.

PSTN (Public Switched Telephone Network – комутована телефонна мережа загального користування) – комунікаційна мережа, для доступу до якої використовуються звичайні телефонні апарати, МІНІ-АТС і устаткування передавання даних.

PVC (Permanent Virtual Circuit – постійний віртуальний канал) – постійно існуюче з'єднання між двома кінцевими крапками мережі.

R

RADIUS (The Remote Authentication Dial-In User Service – сервіс віддаленої аутентифікації користувачів при комутованому підключенні) – програмне забезпечення, що дозволяє мережі або Інтернет-провайдеру перевірити вашу аутентифікаційну інформацію при здійсненні входу в мережу. RADIUS використовує протокол 802.1x, і якщо ваші мережеві пристрої налаштовані на аутентифікацію з використанням RADIUS-сервера, то ці пристрої можуть підключатися тільки до мереж, в яких є RADIUS-сервер.

Repeater (повторювач) – пристрій, який передає електричні сигнали з одного кабелю в інший без маршрутизації або фільтрації пакетів. У термінах OSI репітером є проміжний пристрій фізичного рівня.

RFS (Remote File System) – розподілена файлова система, подібна NFS, розроблена компанією AT&T і поширювана нею зі своєю операційною системою UNIX System V.

RIP (Routing Information Protocol) – протокол Interior Gateway Protocol (IGP), що поставляється з Berkeley UNIX. У мережах IP протокол RIP є внутрішнім протоколом маршрутизації, що використовується для обміну інформацією між мережами. У мережах IPX RIP є динамічним протоколом, що використовується для збору інформації про мережу й управління нею.

Round-trip collision delay – затримка детектування конфлікту при доступі до середовища.

Router (маршрутизатор) – система, що відповідає за ухвалення рішень про виборі одного з декількох шляхів передавання мережевого трафіку. Для виконання цього завдання використовуються протоколи, що маршрутизуються, містять інформацію про мережі й алгоритми вибору якнайкращого шляху на основі декількох критеріїв, званих метрикою маршрутизації (routing metrics). У термінах OSI маршрутизатор є проміжною системою мережевого рівня.

Router ID (ідентифікатор маршрутизатора) – 32-розрядний номер, що привласнюється кожному маршрутизатору, який використовує протокол OSPF. Ідентифікатор маршрутизатора є унікальним у масштабі автономної системи (AS).

Routing (маршрутизація) – процес вибору оптимального шляху для передавання повідомлення.

RS-232C – стандартний інтерфейс послідовного передавання даних.

S

SAP (Service Access Point) – крапка, у якій послуга якого-небудь рівня OSI стає доступною найближчому розміщеному вище рівню. SAP іменуються відповідно до рівнів, що забезпечують сервіс: наприклад, транспортні послуги забезпечуються за допомогою Transport SAP (TSAP) на верхній частині транспортного рівня.

SAP (Service Advertising Protocol) – у мережах IPX цей протокол використовується файловими серверами для передавання інформації про свою доступність і ім'я клієнтам.

SDH (Synchronous Data Hierarchy) – європейський стандарт на використання оптичних кабелів в якості фізичного середовища передавання даних для швидкісних мереж передавання на значні відстані.

Serial Transmission (послідовне передавання) – метод передавання інформації, при якому біти передаються послідовно, замість одночасного (паралельного) передавання за декількома лініями.

Session Layer (сеансовий рівень) – рівень моделі OSI, що забезпечує способи ведення управляючого діалогу між системами.

SGMP (Simple Gateway Management Protocol) – попередник SNMP.

Sharing Device (загальний пристрій) – пристрій, що допускає можливість його сумісного використання декількома іншими пристроями. Прикладами таких пристроїв можуть служити модеми, мультиплексори, порти комп'ютерів і тому подібне.

Short Haul Modem (модем для ближнього зв'язку) – модем, призначений для передавання на порівняно невеликі відстані за фізичними лініями. Для позначення таких модемів використовують також терміни limited distance modem (LDM) і short range modem (SRM).

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

SMDS (Switched Multimegabit Data Service) – високошвидкісна мережева технологія, запропонована телефонними компаніями США.

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

SNMP (Simple Network Management Protocol – простий протокол мережевого управління) – протокол мережевого адміністрування SNMP, дуже широко використовується в даний час. Управління мережею входить у стек протоколів TCP/IP.

SONET (Synchronous Optical NETwork – синхронна оптична мережа) – стандарт на використання оптичних кабелів як фізичного середовища передавання даних для швидкісних мереж передавання на значні відстані. Базова швидкість SONET складає 51.84 Мбіт/с і може бути збільшена до 2.5 Гбіт/с.

SQL (Structured Query Language) – міжнародна стандартна мова для визначення й доступу до реляційних баз даних.

Statistical Multiplexer (STM або STDM, статистичний мультиплексор) – пристрій, який об'єднує безліч каналів в один за рахунок динамічного виділення проміжків часу (timeslot) для передавання даних кожному каналу на основі його активності.

STP (Shielded Twisted Pairs – екрановані скручені пари) – термін, використовуваний для кабельних систем на основі екранованих скручених пар мідних провідників.

Subnetwork (підмережа) – набір кінцевих і проміжних систем OSI, керованих одним адміністративним доменом, і які використовують єдиний протокол доступу до мережі. Прикладами можуть служити приватні мережі X.25, ЛОМ із мостами.

SVC (Switched virtual circuit – комутований віртуальний зв'язок) – тимчасово існуюче віртуальне з'єднання між двома користувачами.

Switched 56 – система передавання даних, що забезпечує повнодуплексний цифровий синхронний обмін даними зі швидкістю 56 Кбіт/с.

Synchronous Transmission (синхронне передавання) – режим передавання, при якому біти даних пересилаються з фіксованою швидкістю, а приймач і передавач синхронізовані.

T

T3 – стандарт для високошвидкісного передавання цифрових даних.

TCP (Transmission Control Protocol) – основний транспортний протокол у наборі протоколів Internet, що забезпечує надійні, орієнтовані на з'єднання, повнодуплексні потоки.

TCP/IP (Transmission Control Protocol/Internet Protocol – протокол управління передаванням/протокол Internet) – відомий також як стек протоколів Internet (Internet Protocol Suite). Даний стек протоколів використовується в сімействі мереж Internet і для об'єднання гетерогенних мереж.

TDM (Time Division Multiplexer – мультиплексор із розділенням часу) – пристрій, що розділяє час доступу до швидкісного каналу між підключеними до мультиплексора низькошвидкісними лініями для передавання бітів, що чергуються (Bit TDM) або символів (Character TDM) даних від кожного терміналу.

Telnet – протокол віртуального терміналу в наборі протоколів Internet. Дозволяє користувачам одного хоста підключатися до іншого видаленого хосту й працювати з ним як через звичайний термінал.

Terminal adapter – устаткування, що використовується для з'єднання устаткування ISDN з іншими пристроями.

TFTP (Trivial File Transfer Protocol) – простий протокол передавання даних, що є значно спрощеним варіантом протоколу FTP. TFTP підтримує просте передавання даних між двома системами без аутентифікації. На відміну від протоколу FTP для використання TFTP потрібний протокол USD.

Token Ring – специфікація локальної мережі, стандартизована в IEEE 802.5. Кадр управління (supervisory frame), званий також маркером (token), послідовно передається від станції до сусідньої. Станція, яка хоче дістати доступ до середовища передавання, повинна чекати отримання кадру й лише після цього може почати передавання даних.

TKIP (The Temporal Key Integrity Protocol – протокол тимчасової цілісності ключів) являється одним з двох методів шифрування, використовуваних в стандарті 802.11i. TKIP – це той метод шифрування, який можна використовувати для забезпечення надійного шифрування реєстраційної інформації. При використанні TKIP періодично міняється ключ шифрування і тим самим ускладнюється можливість підбору.

Transceiver (трансивер) – приймач-передавач. Фізичний пристрій, який сполучає інтерфейс хоста з локальною мережею, такою як Ethernet.

Transport Layer (транспортний рівень) – рівень моделі OSI, що відповідає за надійне передавання даних між кінцевими системами.

U

UA (User Agent) – прикладний процес OSI, що представляє користувача або організацію в X.400 Message Handling System. Створює, передає й забезпечує доставку повідомлень для користувача.

UDP (User Datagram Protocol) – прозорий протокол у групі протоколів Internet. UDP, подібно TCP, використовує IP для доставки; проте, на відміну від TCP, UDP забезпечує обмін дейтаграмами без підтвердження гарантій доставки.

UTP (Unshielded Twisted Pair – неекрановані скручені пари) – загальний термін, використовуваний для позначення кабельних систем на основі неекранованих скручених попарно мідних провідників, використовується також термін «скручена пара».

UUCP (UNIX to UNIX Copy Program) – протокол, що використовується для обміну між узгодженими UNIX-системами.

V

VCI (Virtual Channel Identifier) – ідентифікатор віртуального каналу.

VPI (Virtual Path Identifier) – ідентифікатор віртуального шляху.

VPN – віртуальна приватна мережа, є закритим каналом передавання даних, який як транспорт використовує кабельну або безпровідну мережі, і призначений для захисту з'єднання користувача з сервером. VPN вимагає застосування відповідного програмного забезпечення на обох сторонах, яке здійснить шифрування даних і створить «туннель», або віртуальний канал між користувачем і сервером. Шляхом розділення кожного з'єднання в захищений канал, використання VPN знижує шанси на те, що хтось може блокувати підключення і отримувати конфіденційну інформацію або упроваджувати віруси або інші шкідливі програми в трафік.

W

WAN (Wide-Area Network – глобальна мережа) – мережа, що забезпечує передавання інформації на значні відстані з використанням комутованих і виділених ліній або спеціальних каналів зв'язку.

WINS (Windows Internet Naming Service) – служба імен Internet для Windows, запропонована Microsoft. WINS є базою даних імен комп'ютерів і пов'язаних з ними IP-адрес у середовищі TCP/IP. База даних автоматично оновлюється WINS-клієнтами при призначенні адрес серверами DHCP.

WEP (Wired Equivalency Protocol) – був стандартним способом захисту інформації, яка передається за безпровідною мережею до тих пір, поки не був прийнятий стандарт 802.11i. WEP легко піддавався зламуванню. Сьогодні WEP може використовуватися тільки на тому устаткуванні, яке не може використовувати 802.11i/WPA технології.

WPA (Wi-Fi Protected Alliance) – протокол аутентифікації пристроїв, що працюють за протоколом 802.11i. Протокол WPA кращий, ніж WEP за рахунок використання протоколу TKIP і надійного механізму аутентифікації на основі протоколів 802.1x і EAP (Extensible Authentication Protocol). Існує розширення стандарту 802.11i, яке називається WPA2.

WPA-PSK – полегшена версія WPA, що використовує заздалегідь відомий ключ (Pre-Shared Key). Застосовується переважно в невеликих мережах. Цей метод хоч і використовує заздалегідь визначений ключ на початковій стадії роботи мережі, але алгоритм TKIP періодично змінює його з часом.

WPA-Enterprise – також використовує метод TKIP, проте разом з ним використовується сервер аутентифікації (наприклад, Radius), які разом працюють за протоколом Extensible Authentication Protocol.

X

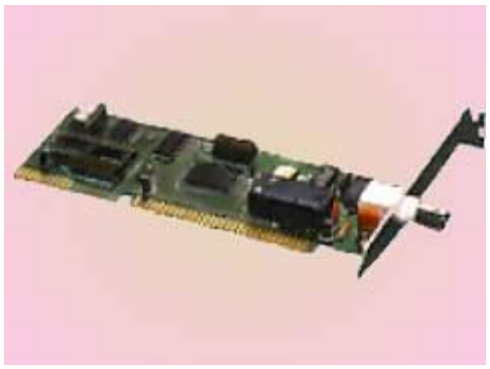
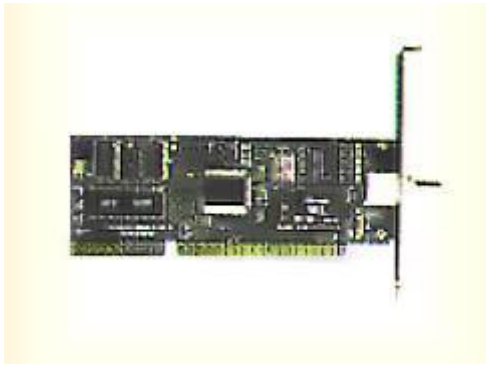
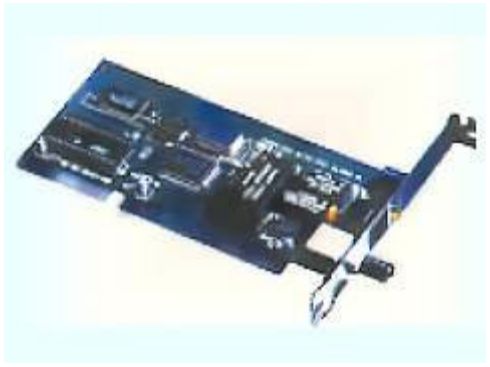
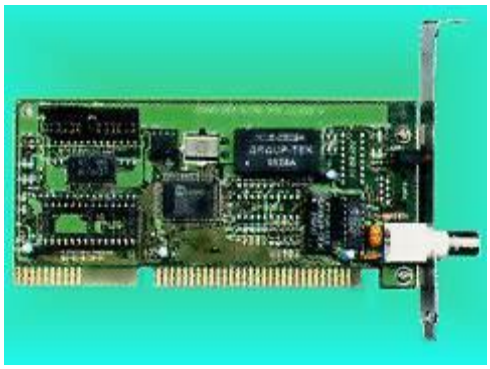
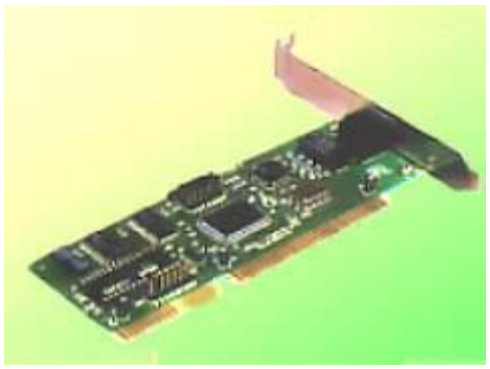
X.25 – рекомендації ITU - TSS (раніше CCITT МККТТ), що визначають стандарти для комунікаційних протоколів доступу до мереж з комутацією пакетів (packet data networks – PDN).

XNS/ITP (Xerox Network Systems' Internet Transport Protocol) – спеціальний комунікаційний протокол використовуваний у мережах. Функції XNS/ITP розташовані на рівнях 3 і 4 моделі OSI. Даний протокол подібний з TCP/IP.

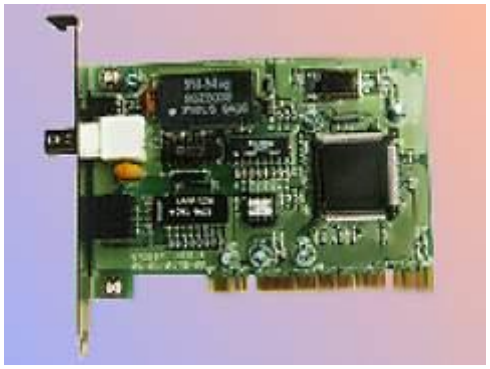
Додаток 3

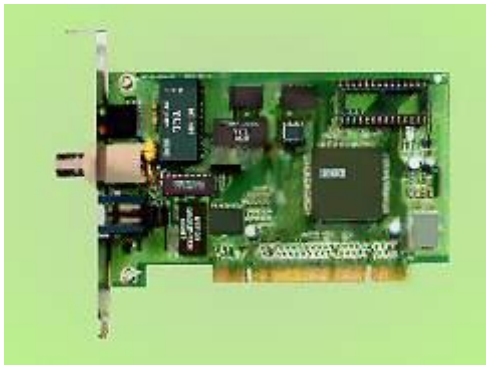
Мережеві карти

Мережеві карти ISA

Мережеві карти PCI

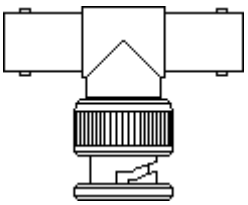





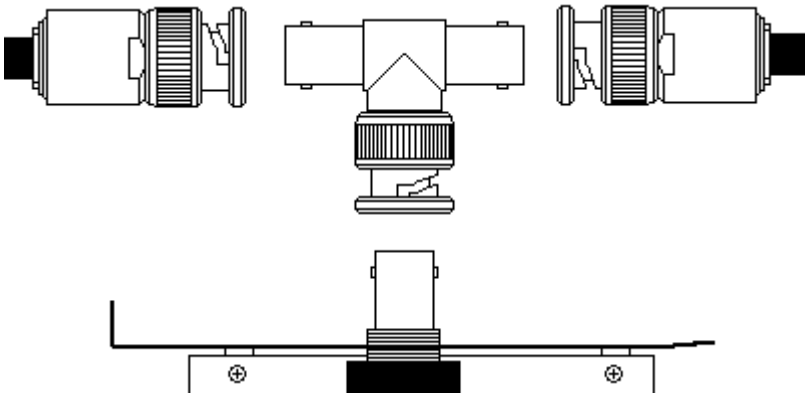
Додаток 4

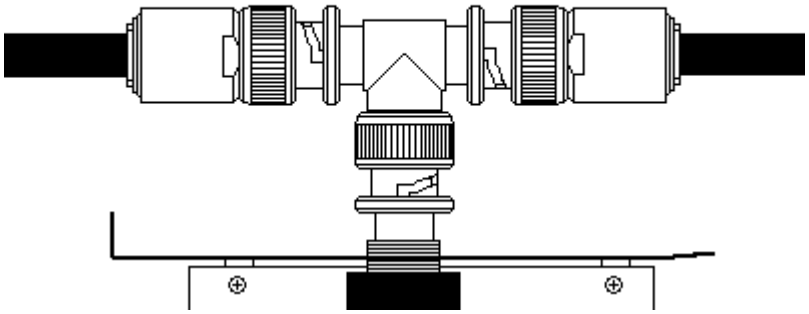
Роз’єми для монтування мережі на коаксиальному кабелі

T-Connector

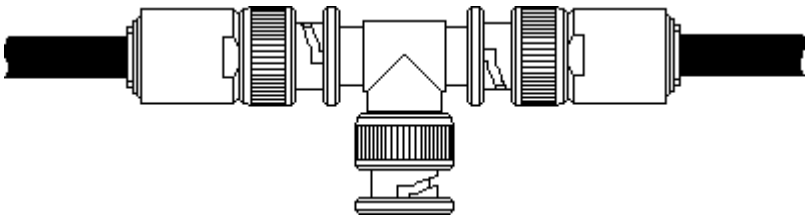


Призначений для підключення пристроїв до сегменту мережі на основі 10 Base-2 (тонкий Ethernet).

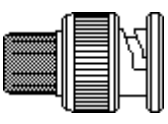




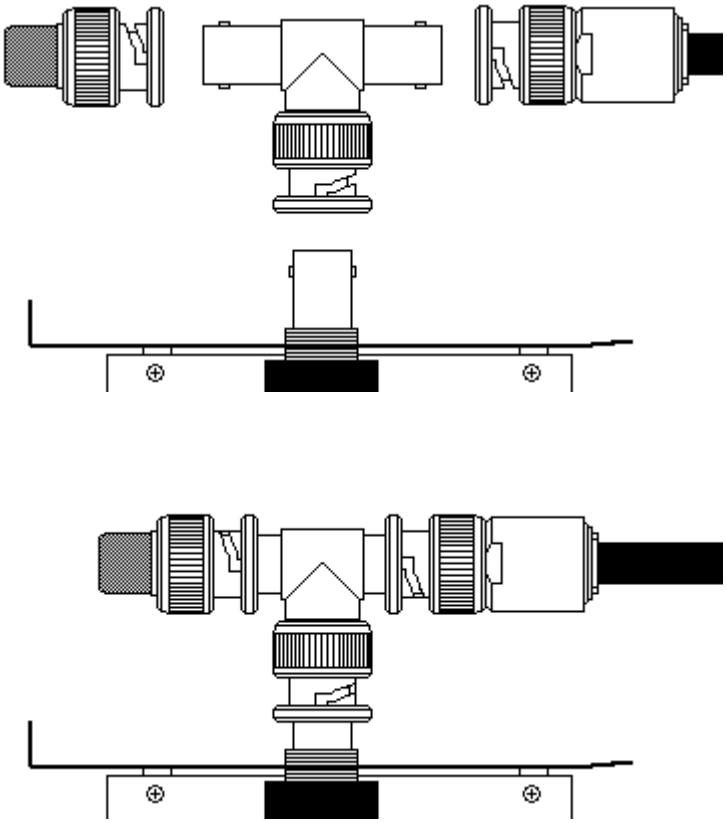
При відключенні пристрою, Т-конектор необхідно залишати в мережі, щоб не порушувати її працездатність, або замінювати Т-конектор на прямий з’єднувач (I-connector).



Термінатор



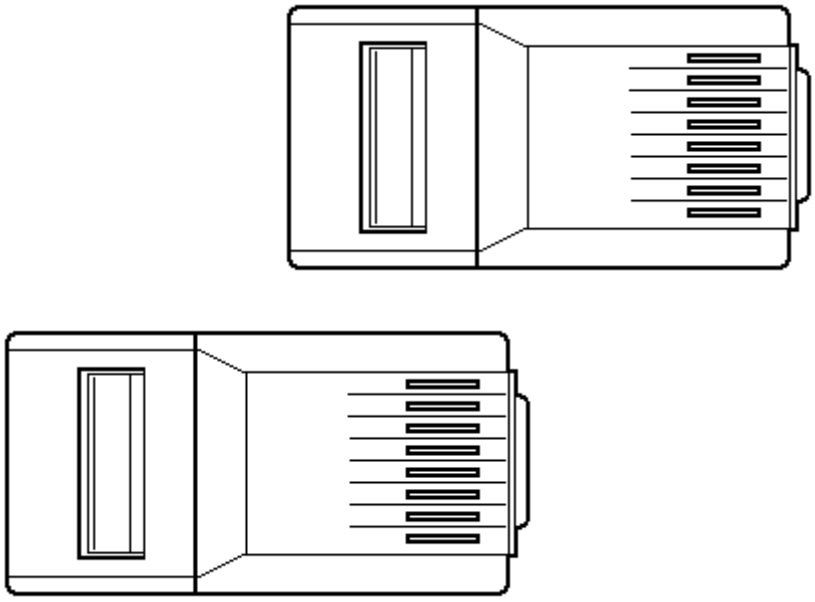
Це роз’єм із запаяним у нім, між центральним і зовнішнім контактами, резистором. Опір резистора повинен дорівнювати хвильовому опору кабелю. Для мереж типу 10Base-2, або тонкий Ethernet, ця величина складає 50 Ом. Тільки один термінатор у сегменті 10Base2 може бути заземлений (а може й взагалі не заземлятися). Для заземлення використовується термінатор із ланцюжком і контактом на його кінці.



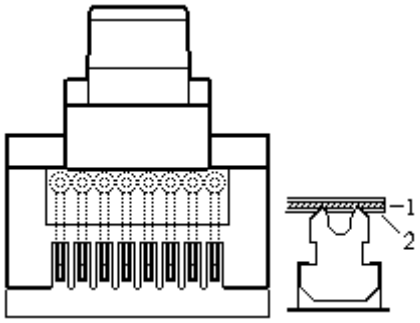
Роз’єми для монтування мережі на скрученій парі

Восьмиконтактний модульний з’єднувач (Вилка, Plug) "rJ-45"

Вилка «rJ-45» схожа на вилку від імпортних телефонів, тільки трохи більшого розміру й має вісім контактів. Вигляд із боку контактів

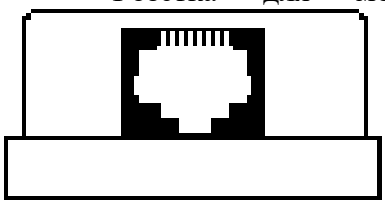


На новій, невикористаній вилці, контакти виходять за межі корпусу.



У процесі обтиску, вони будуть втоплені всередину корпусу, прорізатимуть ізоляцію (2) дроту і встромлятися в жилу (1).

Розетка для монтажу на стіну зовнішня, вигляд із боку роз’єму.



Додаток 5

Обладнання безпровідних мереж

Безпровідний високошвідкісний USB 2.0 адаптер N стандарту
usb адаптер WLn-301

Високопотужний 200 мВт (23 dbm),108 Мбіт/с, безпровідний USB 2.0 адаптер стандартів A.B.G (2,4 і 5 ГГц), з можливістю підключення зовнішньої антени. Дальність із застосуванням зовнішньої направленої антени може досягати 10 км.
usb адаптер EUB-862 EXT -200мВт стандарти A, B,g

Високопотужний (23 dbm) 108 Мбіт/с безпровідний USB 2.0 адаптер NUB 362. З направленою антеною дальність до 10 км.
usb адаптер EUB-362(EXT) 200мВт

Клієнтський (18 dbm) 54 Мбіт/с безпровідний USB 2.0 адаптер з круговою 5 дБ антеною і можливістю підключення зовнішньої антени, роз'єм R-SMA
usb адаптер WLU-803G

Eub 362 PLUS безпровідний, USB 2.0 адаптер підвищеної потужності з інтегрованою 15 Дб панельною антеною, що працює в діапазоні 802.11b/g (2.4GHz), забезпечує високошвидкісне безпровідне з'єднання із швидкістю передавання до 108 Мбіт/с.

usb адаптер EUB-362 PLUS

PCI Adapter стандартів 802.11b/g, до 108 Мбіт/с, 100мВт. Дальність зв'язку в закритому просторі 200 м, на відкритій місцевості з направленою антеною до 10 км.

wifi адаптер EPI-3601 (100 мВт)

Високопотужна (23dbm) комп'ютерна карта Conexant/Intersil. 200мВт. З можливістю підключення зовнішньої антени, роз'єм MMCX. Дальність зв'язку в закритому просторі 300 м, на відкритій місцевості від 1200 м і до 15 км. із застосуванням зовнішньої направленої антени.

EL-2511CD PLUS EXT2 200мВт + підключення антени

Високопотужна (20dbm) комп'ютерна карта Conexant/Intersil. 100мВт. Дальність зв'язку в закритому просторі 300 м, на відкритій місцевості 1200 м

NL-2511CD PLUS 2 MERCURY

2.4 ГГц кругова антена для безпровідної мережі (Wireless LAN). Коефіцієнт підсилення 8 Дб

wifi антена SAG-2408

2.4 ГГц кругова антена для безпровідної мережі (Wireless LAN). Коефіцієнт підсилення 12 Дб.

wifi антена ANT-012ON

Направлена панельна антена 2.4 ГГц для безпровідного пристрою.
Коефіцієнт підсилення 12 Дб

wifi антена SAP-2412

Wi-Fi-антена

ANT-115PN, безпровідна панельна направлена антена 2400 ~ 2483.5 МГц, 15 дБ з N-type коннектором і DC Ground грозозахистом, розроблена для зовнішнього застосування в мережах WLAN. Застосовується для забезпечення зв'язку між двома крапками доступу, наприклад для зв'язування мереж двох окремих будівель або більше.
wifi антена ANT-115PN

Високошвидкісний WI-FI роутер N стандарту від компанії PHEENET, до 300 Мбіт/с, гігабітний світч на 4 виходи.
роутер wifi WLn-401

Високошвидкісний wifi роутер N стандарту, до 300 Мбіт/с. Має три з'ємні антени, вбудований повно-дуплексний 10/100/1000 гігабітний світч з 4 портами, для підключення 4-х пристроїв Ethernet. EnGenius ESR-9710 підтримує стандарт 2.0 802.11n, який дозволяє передавання даних на швидкості в 6 разів більшій, ніж дозволяє стандарт 802.11g, при цьому залишаючись сумісним з пристроями стандарту 802.11g і 802.11b.

Антенний розгалуджувач на 4 антени WSS-204
SENAO

Senao NCB-3220 / ECB-3220/SCB-3220 802.11 b/g 400 мВт WDC – wireless distribution system – має можливість вибудовувати в ланцюжок декілька репітерів, чим збільшує зону покриття. Чіпсет – Atheros 6 покоління, підтримує всі сучасні стандарти. Дальність зв'язку складає 300 м в закритому просторі і до 20 км на відкритій місцевості із зовнішніми антенами.

wifi крапка доступу ECB-3220 400 мВт

EAP-3660 – крапка доступу/універсальний ретранслятор, який працює на 2.4 ГГц, підтримує 802.11b (2.4 ГГц, 11 Мбіт/с) стандарт і SUPERG до 108 Мбіт/с. Це найкраща внутрішня крапка доступу для внутрішньоофісного використання. Висока вихідна потужність 600 мВт.

wifi крапка доступу EAP-3660 600 мВт

WAP-654GP 200мВт крапка доступу, бридж, репітер підвищеного радіусу стандартів 802.11b/g, підтримка Radius client, WDS, зовнішній роз'єм SMA. Дальність зв'язку 300 м в закритому просторі і до 20 км на відкритій місцевості із зовнішніми антенами

wifi крапка доступу WAP-654GP 200 мВт

Інтернет-центр для підключення за виділеною лінією Ethernet з крапкою доступу Wi-Fi 802.11g, сервером додатків, DECT-станцією і адаптером IP-телефонії (2 FXS, 1 FXO).

інтернет центр P-2302HWUD EE

Безпровідний гігабітний маршрутизатор N стандарту, швидкість до 300 Мбіт/с, технологія QOS для кращої якості інтернет-телефонії і он-лайн ігор, 4 порти 10/100/1000 гігабітний комутатор ESR-9710

Wi-Fi-модуль

PCMCIA-адаптер безпровідних мереж для ноутбука

Wimax –Інтернет центр Max 206M2

Samsung Mondi – Інтернет-планшет для мереж WiMax

Роутер D-Link DIR 320 + WiMAX модем Samsung SWC-U200

Mobile WiMAX/Wi-Fi Center
Mobile WiMAX Wi Fi Center—устрій для организації колективного доступу в Інтернет

Роутер D-Link DIR-320 для підключення до мережі Yota WiMAX

Система берпровідного широкополосного доступу WiMIC-6000 основана на рекомендації IEEE 802.16-2004 WirelessMAN (WiMAX)

Зовнішня крапка доступу *DreamWiFi Bullet для WiMAX

Антена *Bester WiMax-27* Nfemale

Покажчики