ЛАБОРАТОРНА РОБОТА №6

УСТАНОВКА ДОМЕНУ НА БАЗІ ACTIVE DIRECTORY СІМЕЙСТВА СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ WINDOWS ТА ВИКОРИСТАННЯ СЛУЖБИ DHCP

Тема: Установка домену на базі ACTIVE DIRECTORY сімейства серверних операційних систем WINDOWS та використання служби DHCP.

Мета: Ознайомитися з сервісом DHCP, а також отримати навички в його налаштуванні

ЗАВДАННЯ

1. Встановити DHCP- сервер.
2. Створити область адрес в DHCP- сервері.
3. Виключити дві адреси з цього діапазону та налаштувати парметри для шлюзу, DNS, WINS серверів.
4. Авторизувати сервер DHCP в ACTIVE DIRECTORY та перезапустити служби DHCP.
5. В налашуваннях VMWARE відключити службу DHCP.
6. Налаштувати клієнта для отримання IP-адреси й інших необхідних параметрів стека TCP/IP.
7. Використовувати команди командного рядку для очищення та отримання IP-адреси й інших необхідних параметрів стека TCP/IP.
8. Зарезервувати по MAC-адресі клієнта необхідну IP-адресу з діапазону та перевірити можливість її отримання клієнтом.

ТЕОРЕТИЧНИЙ МАТЕРІАЛ

Частина 1
Мережні служби DHCP, WINS

Служба DHCP

Служба DHCP (Dynamic Host Configuration Protocol) - це одна із служб підтримки протоколу TCP/IP, розроблена для спрощення адміністрування IP-мережі за рахунок використання спеціально доданого сервера для централізованого управління IP-адресами і іншими параметрами протоколу TCP/IP, необхідними мережним вузлам. Сервер DHCP позбавляє мережного адміністратора від необхідності ручного виконання таких операцій, як:

- автоматичне призначення мережним вузлам IP-адрес і інших параметрів протоколу TCP/IP (наприклад, маска підмережі, адресу основного шлюзу підмережі, адреси серверів DNS і WINS);
- недопущення дублювання IP-адрес, що призначаються різним вузлам мережі; - звільнення IP-адрес вузлів, видалених з мережі;
- ведення централізованої БД виданих IP-адрес.

Особливості служби DHCP в системах сімейства Windows Server:
- Інтеграція з DNS - DHCP-сервери можуть здійснювати динамічну реєстрацію видаваних IP-адрес і FQDN-імен мережних вузлів у базі даних DNS-сервера (це особливо актуально для мережних клієнтів, які не підтримують динамічну реєстрацію на DNS-сервері, наприклад, Windows 95/98/NT4);
- Авторизація сервера DHCP в Active Directory - якщо мережний адміністратор встановить службу DHCP на сервері Windows 2000/2003, то DHCP-сервер не буде функціонувати, поки не буде авторизований в AD (це забезпечує захист від установки несанкціонованих DHCP-серверів);
- Резервне копіювання бази даних DHCP - Створена резервна копія може використовуватися згодом для відновлення працездатності DHCP-сервера.

Визначимо основні терміни, пов'язані з службою DHCP:
- Клієнт DHCP - мережний вузол з динамічною IP-адресою, отриманою від сервера DHCP; - Період оренди - термін, на який клієнту надається IP-адреса;
- Область - це повний послідовний діапазон допустимих IP-адрес в мережі (найчастіше області визначають окрему фізичну підмережу, для якої надаються послуги DHCP);
- Виключний діапазон - це обмежена послідовність IP-адрес в області, яка виключається з числа адрес, запропонованих службою DHCP (виключені діапазони гарантують, що сервер не запропонує жоден адрес з цих діапазонів DHCP-клієнтам в мережі);
- Доступний пул адрес в області - адреси, що залишилися після визначення області DHCP і виключних діапазонів (адреси з пулу можуть бути динамічно призначені сервером DHCP-клієнтам в мережі);
- Резервування - призначення DHCP-сервером певному мережевому вузлу постійної IPадреси (резервування гарантують, що вказаний мережевий вузол буде завжди використовувати один і той же IP-адрес).

Розглянемо технологію надання IP-адрес DHCP-сервером DHCP-клієнтам:

При завантаженні комп'ютера, налаштованого на автоматичне отримання IP-адреси, або при зміні статичного налаштування IP-конфігурації на динамічну, а також при оновленні IPконфігурації мережного вузла відбуваються наступні дії:

1. Комп’ютер посилає широкомовний запит на оренду IP-адреси (точніше, на виявлення доступного DHCP-сервера, DHCP Discover);

2. DHCP-сервери, що одержали цей запит, посилають даному мережному вузлу свої пропозиції IP-адреси (DHCP Offer);
3. Клієнт відповідає на пропозицію, яку отримав першою, відповідному серверу запитом на вибір орендованої IP-адреси (DHCP Request);
4. DHCP-сервер реєструє у своїй БД видану IP-конфігурацію (разом з іменем комп'ютера і фізичнию адресою його мережного адаптера) і посилає клієнту підтвердження на оренду IP-адреси (DHCP Acknowledgement).

Даний процес зображений на Рис.5.1

Рис.5.1

Планування серверів DHCP

При плануванні серверів DHCP необхідно враховувати в першу чергу вимоги продуктивності та відмовостійкості (доступності) даної служби. Тому основні рекомендації при розгортанні служби DHCP в корпоративній мережі будуть наступними:

- бажано в кожній IP-мережі встановити окремий DHCP-сервер;
- якщо немає можливості встановити свій сервер в кожній IP-мережі, необхідно на маршрутизаторах, що об'єднують IP-мережі, запустити і налаштувати агент ретрансляції DHCP-запитів (DHCP Relay Agent) таким чином, щоб він пересилав широкомовні запити DHCP з підмережі, в якій немає DHCP -сервера, на відповідний DHCP-сервер, а на самому DHCP-сервер створити області для всіх обслуговуваних IP-мереж;
- для підвищення відмовостійкості слід встановити кілька серверів DHCP, при цьому на кожному DHCP-сервер, крім областей для "своїх" IP-мереж, необхідно створити області для інших підмереж (при цьому діапазони IP-адрес в таких резервних областях не повинні перетинатися з основними областями , створеними на серверах DHCP у "своїх" підмережах);
- у великих IP-мережах DHCP-сервери повинні мати потужні процесори, досить великі обсяги оперативної пам'яті і швидкодіючі дискові підсистеми, тому що обслуговування великої кількості клієнтів потребує інтенсивної роботи з базою даних DHCP-сервера.

Запуск сервера Microsoft DHCP

Сервер Microsoft DHCP - це програма, яка використовується для управління, відстеження та призначення налаштувань конфігурації TCP/IP, а також протоколу для передачі цих налаштувань клієнтам DHCP. Сервер DHCP, який поставляється разом з Windows 2000 Server, запускається як служба після його установки зі сторінки Local Area Connections Properties (Властивості з’яднань

локальної мережі) або за допомогою аплету Add/Remove Programs (Установка й видалення програм) з панелі керування (Control Panel). Крім того, є оснастка DHCP, яка може використовуватися мережними адміністраторами для визначення настройок конфігурації, що надаються клієнтам DHCP.

Щоб встановити DHCP Server за допомогою майстра Manage Your Server Wizard, виконайте наступні кроки. (Рис. 5.2)

1. Відкрийте майстер Manage Your Server Wizard (який автоматично запускається при завантаженні) з меню Administrative Tools (Адміністрування).
2. Виберіть варіант Add or remove a role (Додавання або видалення ролі). Майстер перевірить, що ваше мережне з'єднання працює належним чином; клацніть на кнопку Next (Далі).
3. Виберіть сервер DHCP в меню ролей серверів (Server Role Menu).

Рис. 5.2

Після цього майстер запускає New Scope Wizard (Майстер нової області).

Для встановлення сервера DHCP з панелі управління виконайте наступні кроки.

- Двічі клацніть на аплет Add/Remove Programs в панелі керування (Control Panel). - Виберіть Add/Remove Windows Components у вікні Add/Remove Programs. (Рис. 5.3)

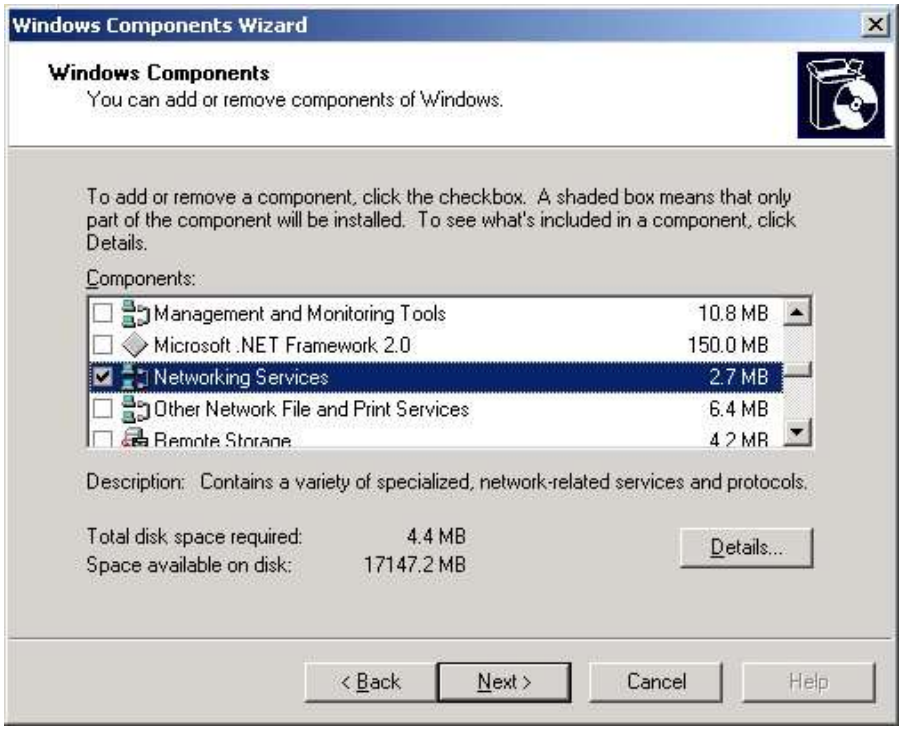


Рис. 5.3

- Виберіть Networking Services (Мережні служби) у вікні Windows Components Wizard (Майстер компонентів Windows) і клацніть на кнопці Details (Докладно).
- Встановіть прапорець поруч із Dynamic Host Configuration Protocol (DHCP), і клацніть на кнопці OK. (Рис. 5.4)

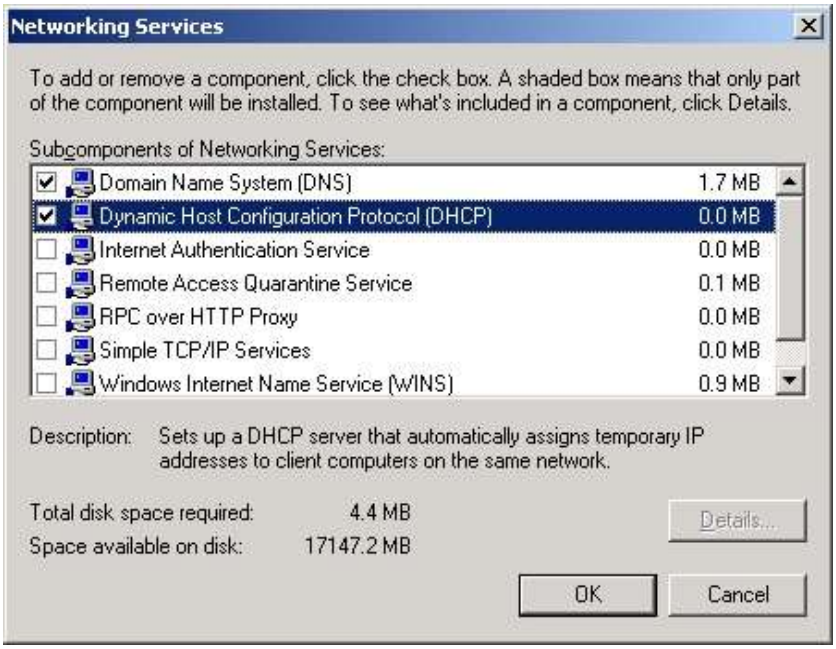


Рис. 5.4

- Клацніть на кнопку Next у вікні Windows Components Wizard, щоб встановити цю службу.
- Клацніть на кнопку Finish, щоб завершити встановлення. Тепер ви можете конфігурувати сервер DHCP.

Конфігурування клієнта для використання DHCP

Якщо ви вирішили зробити машину Windows XP/2000 клієнтом DHCP, то вам потрібно клацнути на кнопку вибору сторінки властивостей Internet Protocol (TCP/IP) (Рис. 5.5) Properties, щоб всі необхідні налаштування конфігурації TCP/IP були автоматично призначені для вашої машини. Крім того, всі ці налаштування зберігаються в одному централізованому місці - на сервері DHCP, - що рятує вас від необхідності ручного введення записів про призначення IPадрес.

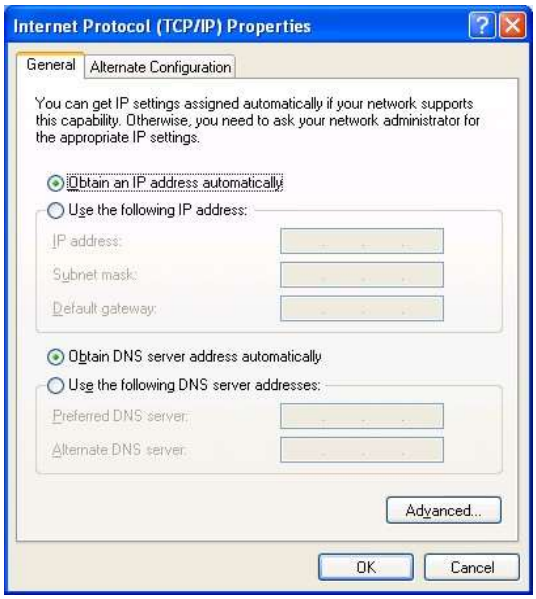


Рис. 5.5

Клієнтом DHCP може бути практично будь-який мережний пристрій, налаштований на автоматичне отримання IP-адреси. З операційних систем корпорації Microsoft клієнтом DHCP можуть бути всі системи, що мають стек TCP/IP (аж до системи MS-DOS).

Клієнти посилають запит на оренду IP-адреси під час свого першого завантаження, при зміні налаштування отримання IP-адреси із статичної на динамічну, а також за допомогою команд ipconfig /release (звільнення орендованого IP-адреси) і ipconfig /renew (запит на нову оренду) .

Сервер DHCP обов'язково повинен мати статичні IP-адреси на всіх встановлених у ньому мережних адаптерах.

На клієнтському комп'ютері можна також застосовувати задані клієнтом значення багатьох параметрів клієнта DHCP (за винятком IP-адреси і маски підмережі). Заданий клієнтом значення завжди заміняє значення, задане сервером DHCP. З цієї причини під час перетворення комп'ютерів з локальної конфігурації в DHCP не забувайте видаляти жорстко кодовані налаштування TCP / IP комп'ютера клієнта.

Примітка. За відсутності в мережі DHCP-сервера клієнти, налаштовані на автоматичне налаштування IP-адреси будуть самостійно призначати собі IP-адреси з підмережі класу B - 169.254.0.0/16. Дана технологія називається автоматичною IP-адресацією (APIPA, Automatic Private IP Addressing) і підтримується операційними системами Microsoft, починаючи з Windows 98.

Авторизація сервера DHCP

Для авторизації сервера DHCP в БД Active Directory необхідно запустити консоль управління службою DHCP, що з'явилася в розділі "Адміністрування"(Рис. 5.6).

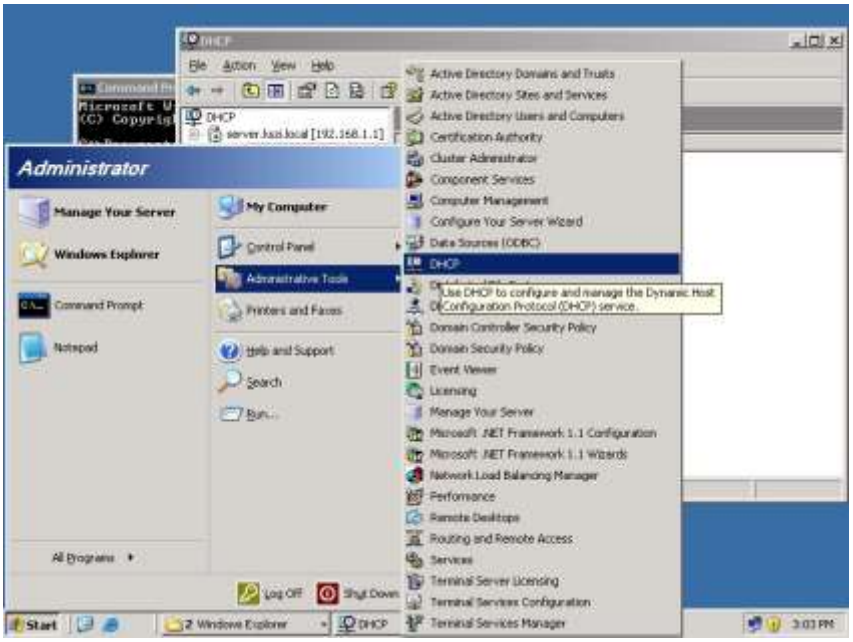


Рис. 5.6

Для авторизації сервера необхідно в консолі DHCP вибрати сервер, натиснути на ім’я сервера правою кнопкою миші і вибрати пункт меню "Авторизувати" (Рис. 5.7). Коли авторизація буде завершена, значок з ім'ям сервера зміниться - замість червоної стрілки, спрямованої вниз, з'явиться зелена стрілка, спрямована вгору.

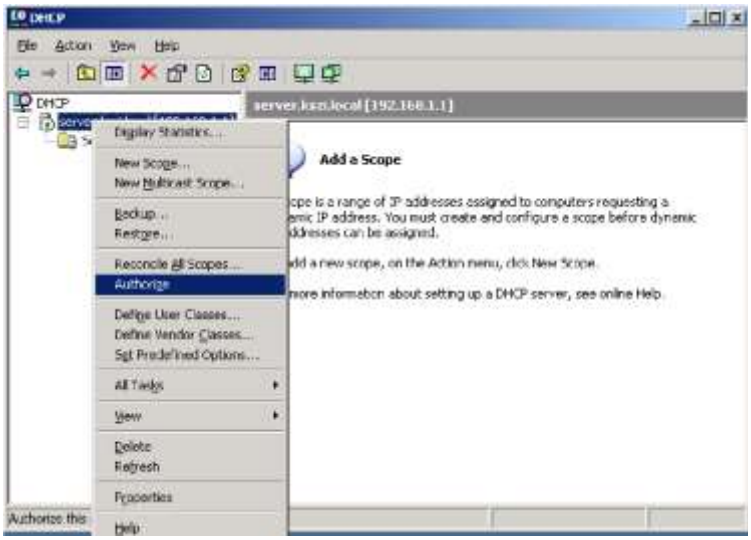


Рис. 5.7

Конфігурування сервера DHCP

Конфігурування налаштувань TCP/IP виконується в DHCP Manager і полягає в створенні областей та подальшому призначенні для них властивостей. Область - це набір IP-адрес, які можуть динамічно або автоматично виділятися клієнтам DHCP в міру необхідності.

Створення області та налаштування її параметрів

Створити область можна, клацнувши правою кнопкою миші на імені сервера і вибравши пункт меню "Створити область (New Scope)" (або вибравши аналогічний пункт в меню "Дія" консолі DHCP) (Рис. 5.8).

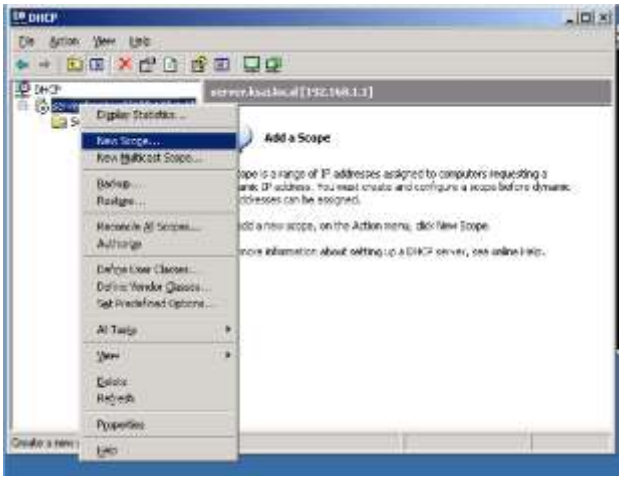


Рис. 5.8

Консоль запустить "Майстер створення області (New Scope Wizard)", який дозволяє по кроках визначити всі необхідні параметри:

1. І’мя і опис області. У великих мережах іменування областей і завдання їх короткого опису полегшує роботу адміністратора за рахунок більш наочного відображення в консолі всіх створених областей. (Рис. 5.9)

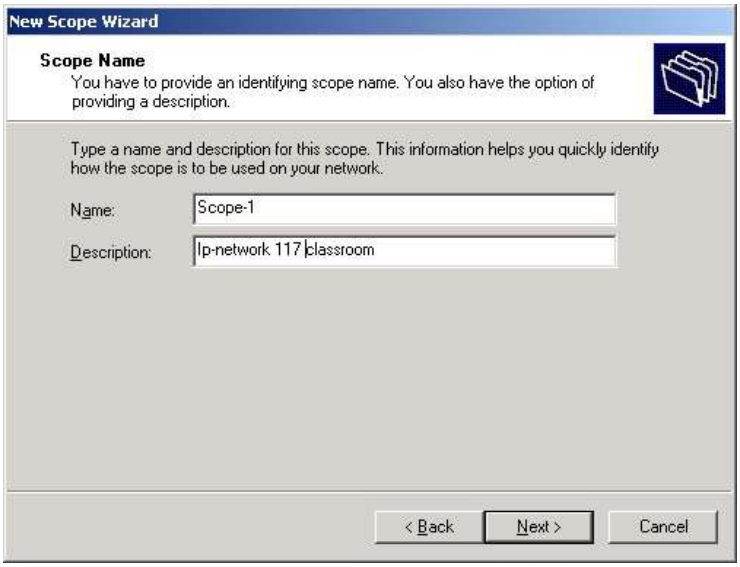


Рис. 5.9

2. Визначення діапазону IP-адрес і маски підмережі (Рис. 5.10)

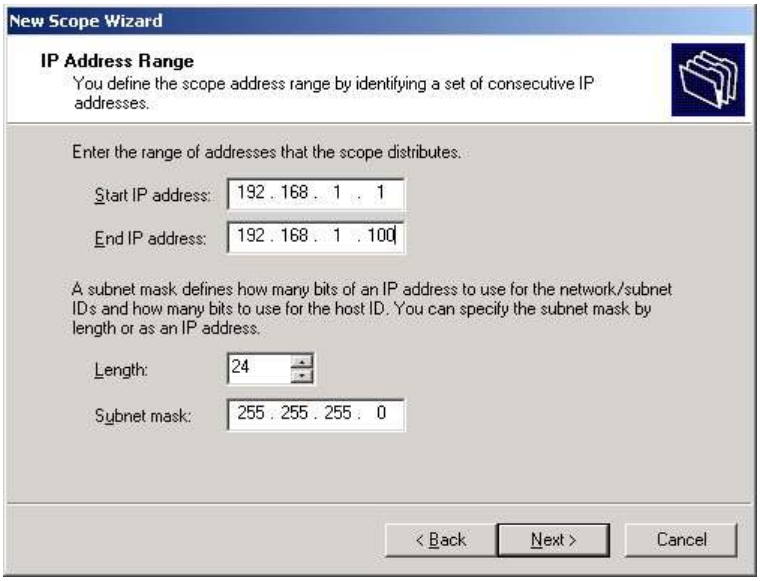


Рис. 5.10

3. Додавання винятків. На цьому кроці задаються діапазони IP-адрес, який будуть виключені з процесу видачі адресів клієнтам.
4. Срок дії оренди. Стандартний термін дії - 8 днів. Якщо у вашій мережі рідко відбуваються зміни (додавання або видалення мережних вузлів, переміщення мережних вузлів з однієї

підмережі в іншу), то термін дії можна збільшити, це скоротить кількість запитів на оновлення оренди. Якщо ж ваша мережа більш динамічна, то строк оренди можна скоротити, це дозволить швидше повертати в пул вільних ті IP-адреси, які належали комп'ютерам, вже видаленим з даної підмережі.

5. Далі майстер запропонує налаштувати параметри, специфічні для вузлів IP-мережі, що відносяться до даної області:

- маршрутизатор (основний шлюз) (Рис. 5.11);

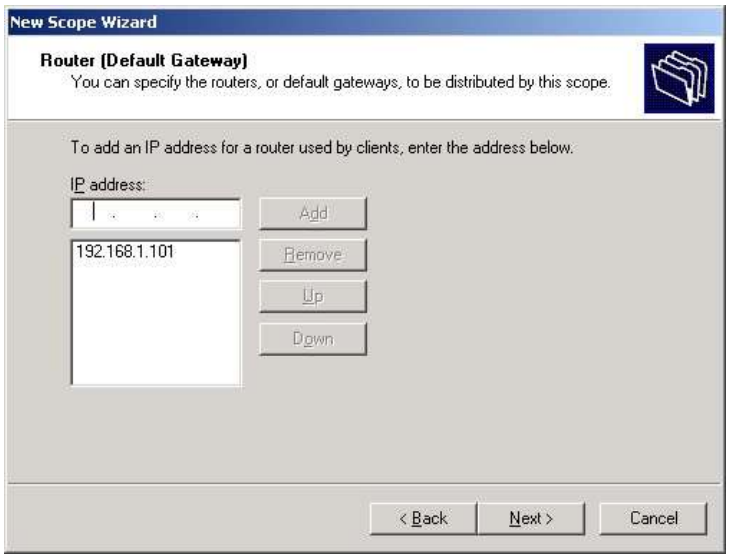


Рис. 5.11

- адреса DNS-сервера (можна призначити декілька адрес) (Рис. 5.12);

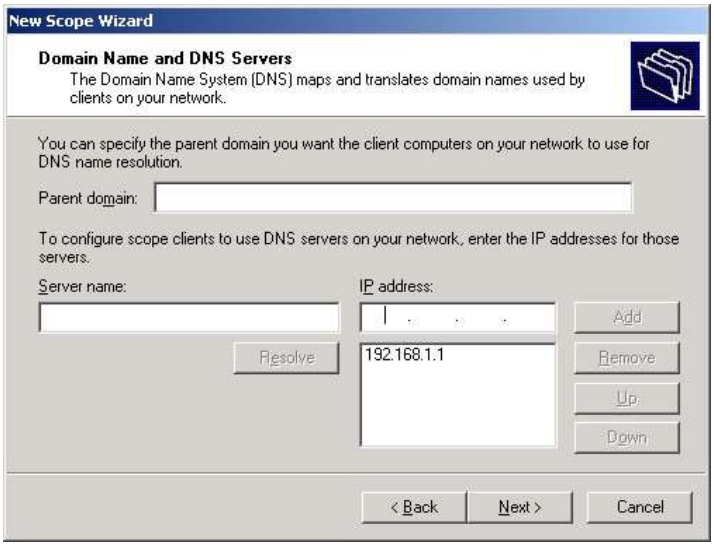


Рис. 5.12

- адреса WINS-сервера (аналогічно DNS-серверу; можна також призначити декілька адрес);

6. Запит на активацію області. IP-адреси, задані в створеній області, не будуть видаватися клієнтам, поки область не буде активована (Рис. 5.13):

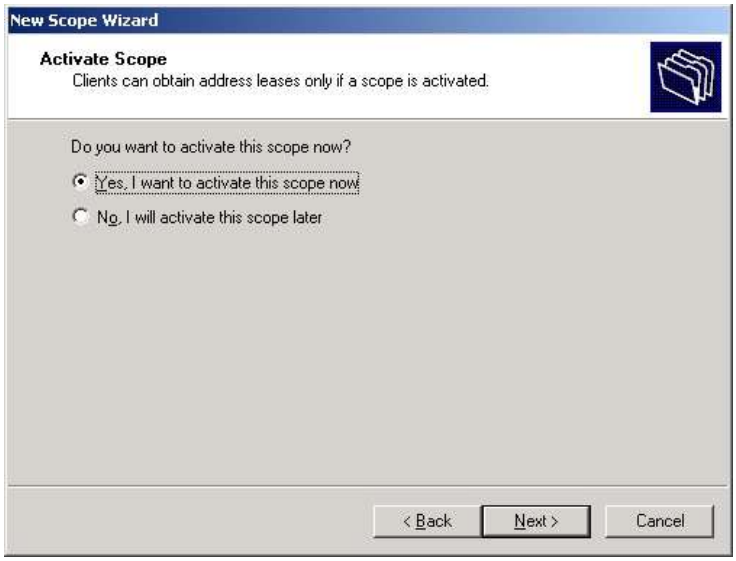


Рис. 5.13

Натискаємо кнопку "Готово" і завершуємо роботу майстра. Область готова до використання (Рис. 5.14).

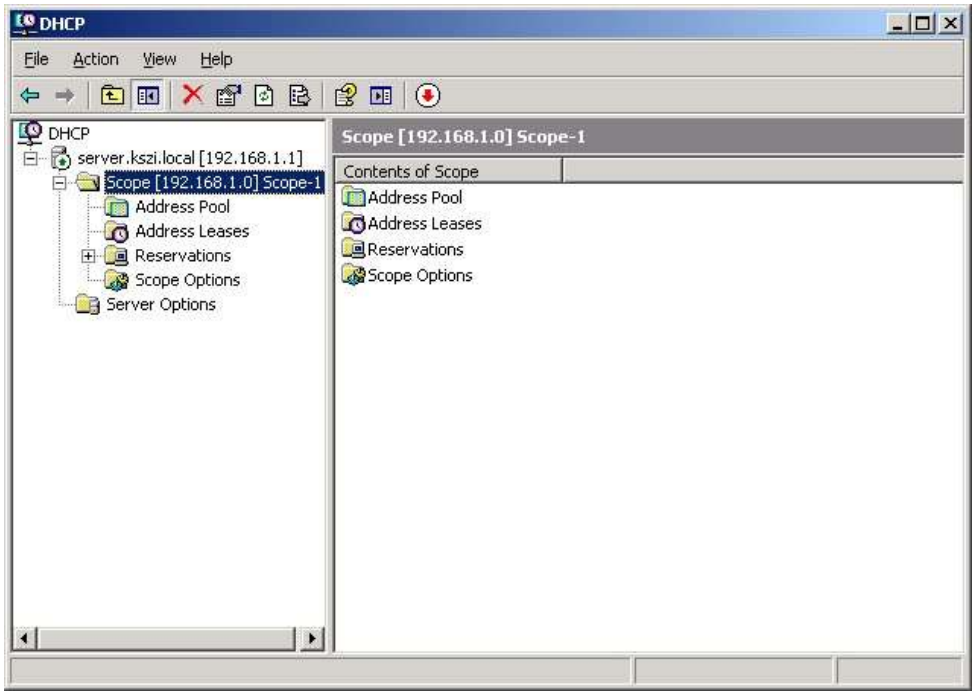


Рис. 5.14

Якщо які-небудь параметри (наприклад, адреси серверів DNS або WINS) є спільними для всіх областей, керованих даними DHCP-сервером, то такі параметри краще визначити не в розділі параметрів кожної області (Scope Options) (Рис. 5.15), а в розділі параметрів самого сервера (Server Options).

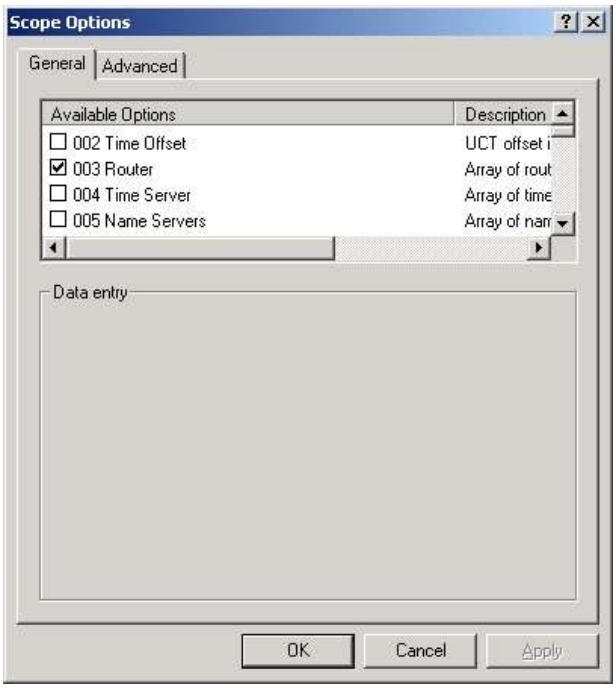


Рис. 5.15

Примітка. Ви можете конфігурувати сервер DHCP, але він не буде обслуговувати клієнтів, поки ви не авторизуєте його.

Сервер DHCP не може сам використовувати DHCP для отримання своєї власної конфігурації TCP/IP (навіть від іншого сервера DHCP). Його налаштування повинні бути сконфігуровані вручну в діалоговому вікні Internet Protocol (TCP/IP) Properties.

Агент ретрансляції DHCP-запитів

Як вже говорилося вище, один сервер DHCP може обслуговувати клієнтів, розташованих в різних IP-мережах. Щоб широкомовні запити на оренду IP-адреси досягали DHCP-сервер з будьякої підмережі, необхідно на маршрутизаторах, які об'єднують різні IP-мережі в єдину мережу, встановити та налаштувати агент ретрансляції DHCP (DHCP Relay Agent). Приклад такої конфігурації зображений на Рис. 5.16.

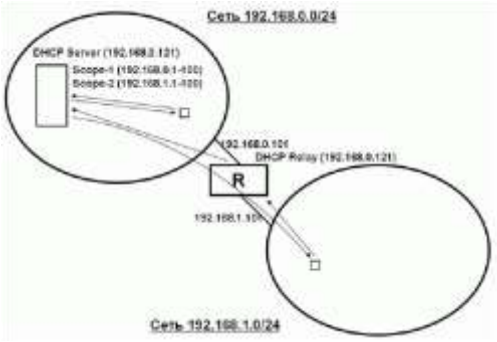


Рис. 5.16

У даному прикладі зображено дві IP-мережі класу C - 192.168.0.0/24 і 192.168.1.0/24. DHCPсервер (що має IP-адресу 192.168.0.121) встановлений в першій підмережі і містить 2 області - Scope-1 з діапазоном адрес 192.168.0.1-192.168.0.100 і Scope-2 з діапазоном адрес 192.168.1.1192.168.1.100. Між двома підмережами встановлено маршрутизатор R, який має в першій підмережі мережний інтерфейс з IP-адресою 192.168.0.101, а в другій підмережі мережний інтерфейс з IP-адресою 192.168.1.101. На маршрутизаторі запущено агент ретрансляції DHCPзапитів, налаштований на перенаправлення широкомовних DHCP-запитів на сервер з IP-адресою 192.168.0.121.

Клієнти DHCP, що знаходяться в першій підмережі, посилають широкомовні запити на оренду IP-адресів, які напряму потрапляють на DHCP-сервер.

Клієнти DHCP, що знаходяться в другій підмережі, також посилають широкомовні запити на оренду IP-адреси, які не можуть напряму потрапити на DHCP-сервер, тому що маршрутизатори не пропускають широкомовні пакети з однієї підмережі в іншу. Але якщо широкомовний пакет є запитом на оренду IP-адреси, то агент ретрансляції перехоплює цей пакет і пересилає його прямо на DHCP-сервер. DHCP-сервер, бачучи від агента ретрансляції, що запит прийшов з другої підмережі, видає клієнтові IP-адресу з пулу адрес, заданих в другій області.

Служба WINS

Служба WINS (Windows Internet Name Service) виконує завдання, аналогічні завданням служби DNS, - динамічна реєстрація імен комп'ютерів та інших мережних вузлів і їх IP-адрес в БД сервера WINS і дозвіл імен комп'ютерів в IP-адреси. Головна відмінність у тому, що WINS функціонує в зовсім іншому просторі імен, т.зв. просторі імен NetBIOS, яке ніяк не перетинається з простором FQDN-імен, в якому працює служба DNS. З цієї причини службу WINS ще інакше називають NetBIOS Name Service (NBNS).

До появи системи Windows 2000 мережний програмний інтерфейс NetBIOS був основним мережним інтерфейсом для обміну даними між комп'ютерами в мережах на базі технологій Microsoft (технологія SMB - надання спільного доступу до файлів і друку - працювала тільки за допомогою мережевого інтерфейсу NetBIOS), і тому служба WINS була основною службою дозволу імен комп'ютерів в IP-адреси. Після виходу Windows 2000 служба файлів і друку може

працювати без NetBIOS, і основною технологією розпізнавання імен в IP-адреси стала служба DNS. Якщо у вашій мережі немає операційних систем Windows 95/98/ME/NT, то вам служба WINS може взагалі не знадобитися.

Простір імен NetBIOS

Імена NetBIOS не утворюють жодної ієрархії в своєму просторі, це простий лінійний список імен комп'ютерів, точніше служб, що працюють на комп'ютері. Імена комп'ютерів складаються з 15 видимих символів плюс 16-й службовий символ. Якщо видимих символів менше 15, то символи, що залишилась заповнюються нулями (не символ нуля, а байт, що складається з двійкових нулів). 16-й символ відповідає службі, яка працює на комп'ютері з такою назвою.

Переглянути перелік імен простору NetBIOS, які є на даному комп'ютері, можна за допомогою команди "nbtstat -n".

Розглянемо приклад на (Рис. 5.17) На малюнку зображено вивід команди "nbtstat -n" на сервері server.kszi.local, що є списком NetBIOS-імен, згенерованих даними сервером.

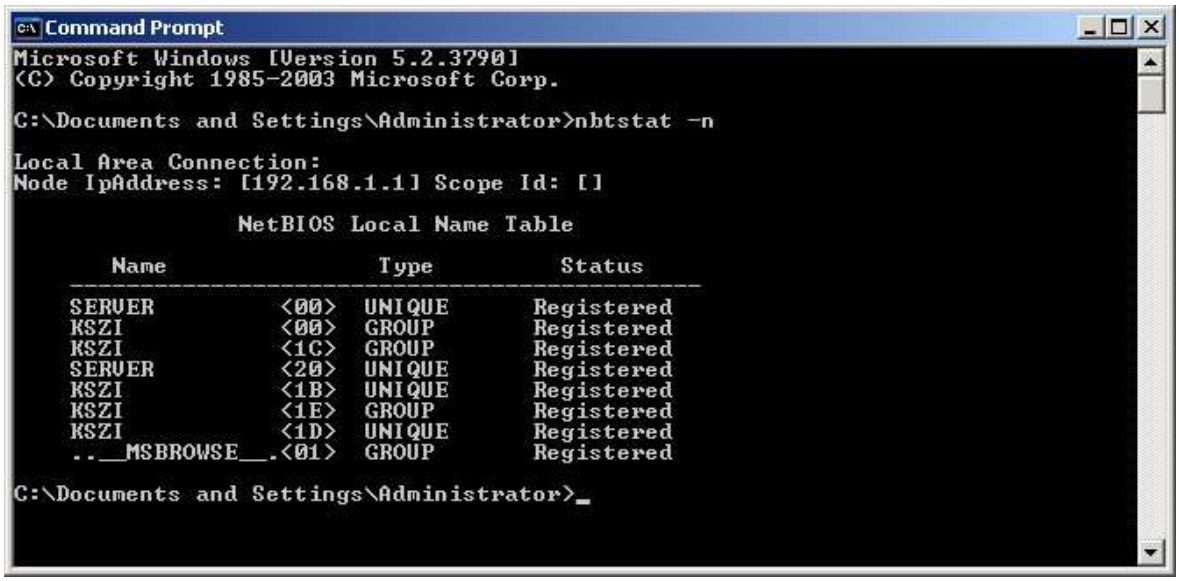


Рис. 5.17

У кутових дужках вказано шістнадцятирічний код 16-го службового символу будь-якого імені. Наприклад, ім'я SERVER і 16-й символ "00" відповідають службі "Робоча станція", яка виконує роль клієнта при підключенні до ресурсів файлів і друку, що надаються іншими комп'ютерами мережі. А те ж саме ім'я SERVER і символ з кодом "20" відповідають службі "Сервер", яка надає ресурси файлів і друку цього сервера для інших комп'ютерів мережі. Ім'я KSZI відповідає або Net-BIOS-імені домену kszi.local, або імені т.зв. мережної робочої групи, яка відображається в мережному оточенні будь-якого Windows-комп'ютера.

Ім'я "..__ MSBROWSE__. " говорить про те, що цей комп'ютер є Оглядачем мережного оточення по протоколу TCP/IP. Тобто якщо на будь-якому комп'ютері з системою Windows відкрити "Мережне оточення", то цей комп'ютер буде запитувати список комп'ютерів, згрупованих в мережній робочій групі KSZI, саме з сервера SERVER.

Всі ці імена, перелічені у цій таблиці, будуть автоматично реєструватися в базі даних сервера WINS після того, як цей сервер буде встановлений в мережі і даний комп'ютер стане клієнтом сервера WINS.

Установка служби WINS

Установка служби WINS виконується за тією ж схемою, що й установка служби DHCP: "Пуск" - "Панель керування" - "Установки і видалення програм" - "Установки компонентів Windows" - "Мережні служби" - кнопка "Склад" - вибрати пункт "WINS" - кнопки "ОК", "Далі" і "Готово" (якщо буде потрібно, то вказати шлях до дистрибутиву системи) (Рис. 5.18).

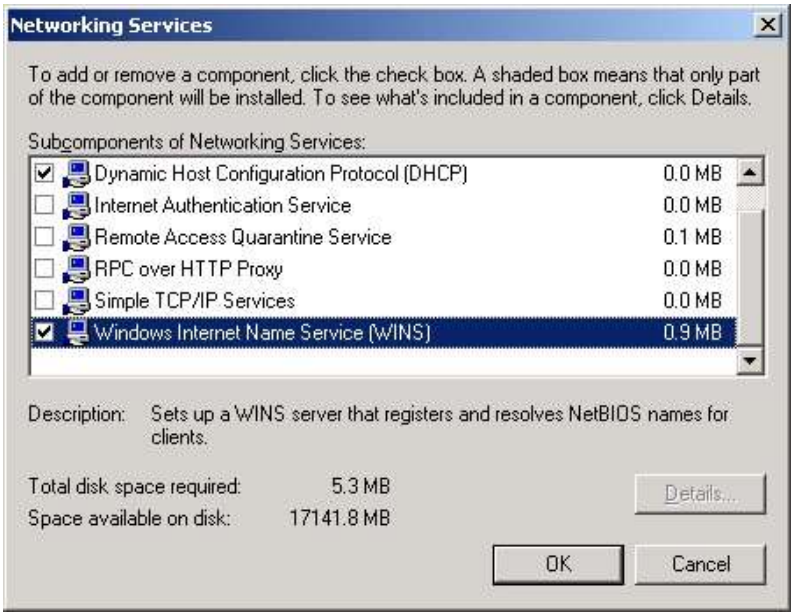


Рис. 5.18

Налаштування клієнта WINS

Для налаштування мережних комп'ютерів для використання ними сервера WINS необхідно в Властивостях протоколу TCP/IP на закладці "WINS" вказати IP-адреси що використовуються в мережі WINS-серверів (для вузлів зі статичними IP-адресами) або додати необхідні параметри у властивостях відповідної області сервера DHCP (для вузлів з динамічними IP-адресами) (Рис. 5.19; Рис. 5.20).

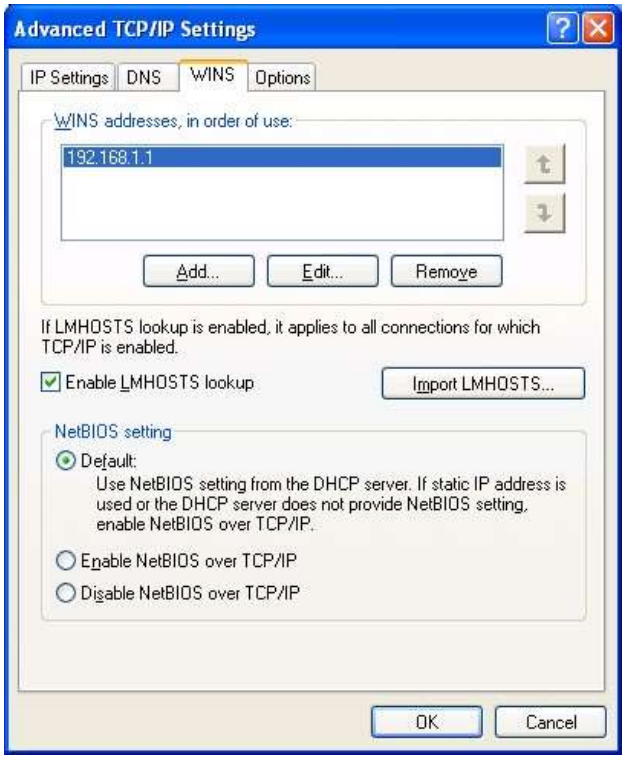


Рис. 5.19

Рис. 5.20

Клієнт після таких змін зробить спробу автоматичної реєстрації своїх даних на сервері WINS. Автоматична реєстрація клієнта на WINS-сервері здійснюється також у процесі завантаження системи на комп'ютері або командою "nbtstat -RR" (Рис. 5.21).

```
C:\Documents and Settings\Administrator>nbtstat -rr

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 4
    Resolved By Name Server   = 20

    Registered By Broadcast   = 18
    Registered By Name Server = 0

    NetBIOS Names Resolved By Broadcast
    -----------------------------------

            SERVER
            SERVER
            KSZI            <1B>
            SERVER
```

Рис. 5.21

Перегляд записів, зареєстрованих в БД сервера WINS

Для перегляду записів, що зберігаються в БД WINS-сервера, необхідно відкрити консоль управління WINS, розкрити в консолі вузол, що відноситься до цього сервера, клацнути правою кнопкою миші на розділі "Активні реєстрації" і вибрати "Показати записи" (Рис. 5.22)

Рис. 5.22

Потім натиснути кнопку «Знайти» (Рис. 5.23)

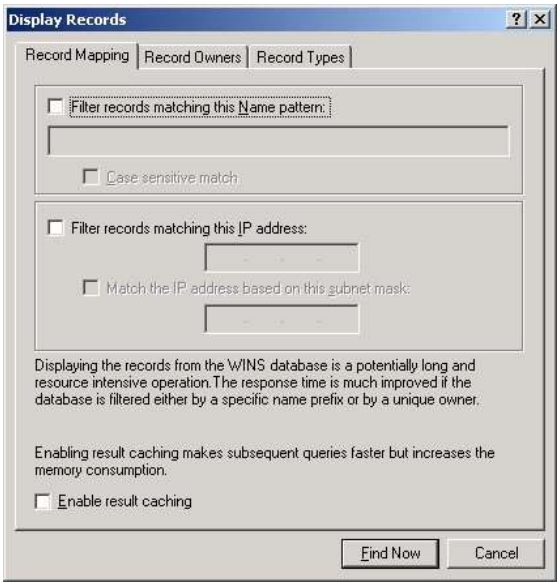


Рис. 5.23

На екрані консолі буде таблиця яка зображена на Рис. 5.24:

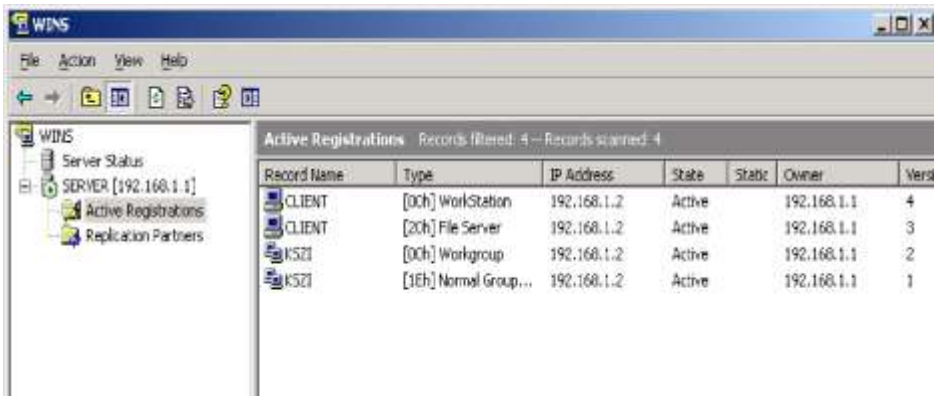


Рис. 5.24

Якщо система, що підтримує NetBIOS, при цьому не підтримує автоматичну реєстрацію в БД WINS-сервера, мережний адміністратор може занести в БД сервера WINS статичні записи для таких комп'ютерів.

Служба RRAS

Служба RRAS (Routing and Remote Access Service, Служба Маршрутизації і віддаленого доступу) - служба системи Windows Server, що дозволяє вирішувати наступні завдання:

- підключення мобільних (або домашніх) користувачів до корпоративної мережі через комутовані телефонні лінії та інші засоби комунікацій (наприклад, мережі Frame Relay, X.25);

- підключення до мережі головного офісу компанії віддалених офісів (через телефонні лінії та мережі Frame Relay, X.25);
- організація захищених з'єднань (віртуальні приватні мережі) між мобільними користувачами, підключеними до мереж загального користування (наприклад, Інтернет), і корпоративною мережею;
- організація захищених з'єднань між офісами компанії, підключеними до мереж загального користування;
- маршрутизація мережного трафіку між різними підмережами корпоративної мережі, з'єднаними як за допомогою технологій локальних мереж, так і за допомогою різних засобів віддалених комунікацій (наприклад, по комутованих телефонних лініях).

Служба RRAS має багатий набір функцій і можливостей.

Служби віддаленого доступу, реалізовані різними виробниками, використовують два основні комунікаційні протоколи, які утворюють рівень, який знаходиться між засобами комунікацій (комутовані телефонні лінії, Frame Relay, X.25) і мережними протоколами (TCP/IP, IPX/SPX): - протокол SLIP (Serial Line Interface Protocol) - досить старий протокол, реалізований переважно на серверах віддаленого доступу, що функціонують в системах сімейства UNIX (розроблений спеціально для підключення користувачів до мережі Інтернет); системи сімейства Windows підтримують даний протокол тільки на клієнтській частині (SLIP дозволяє працювати тільки з мережним стеком TCP/IP, вимагає написання спеціальних сценаріїв для підключення клієнта до сервера, не дозволяє створювати віртуальні приватні мережі);

- протокол PPP (Point-to-Point Protocol) - використовуваний повсюду комунікаційний протокол (точніше, сімейство протоколів), що дозволяє користувачам прозоро підключатися до сервера віддаленого доступу, використовувати різні мережні протоколи (TCP/IP, IPX/SPX, NetBEUI, AplleTalk), створювати віртуальні приватні мережі (служба віддаленого доступу серверів Windows використовує саме цей комунікаційний протокол).

Почнемо з прикладу, що показує процес встановлення початкового налаштування служби, і обговоримо термінологію, технології, а також всі необхідні нам параметри, функції і можливості даної служби.

Установка і початкова настройка служби RRAS

Службу RRAS не потрібно додавати через вікно додавання Компонент Windows. Ця служба встановлюється при установці системи, але за замовчуванням вона відключена. Її необхідно включити і налаштувати.

Натиснемо кнопку "Start", виберемо "All Programs" - "Administrative Tools" - "Routing and Remote Access". Відкриється консоль управління службою RRAS, виберемо у вікні консолі ім'я сервера, клацнемо правою кнопкою миші і виберемо пункт меню "Налаштувати і включити маршрутизацію та віддалений доступ" (Рис. 5.25).

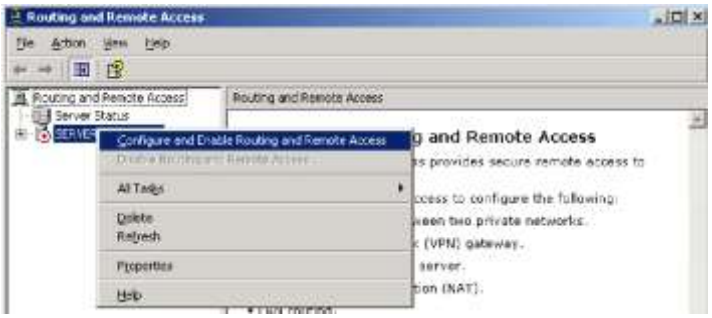


Рис. 5.25

Запуститься Майстер встановлення сервера маршрутизації та віддаленого доступу:

1. Спочатку майстер просить вибрати один з сценаріїв використання служби RRAS. Для нашого навчального прикладу виберемо варіант "Особлива конфігурація" (щоб побачити всі можливості служби) (Рис. 5.26).

Рис. 5.26

2. Далі для варіанту "Особлива конфігурація" треба вибрати потрібні нам функції служби (відзначимо всі варіанти) (Рис. 5.27).

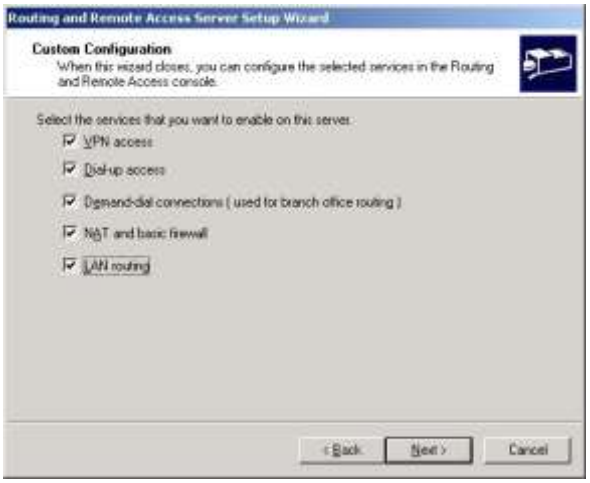


Рис. 5.27

3. Натиснемо кнопку "Finish". Майстер запитає, чи запустити службу відразу після налаштування, натиснемо кнопку "Yes". Вікно консолі управління службою набуде вигляду який зображений на Рис. 5.28

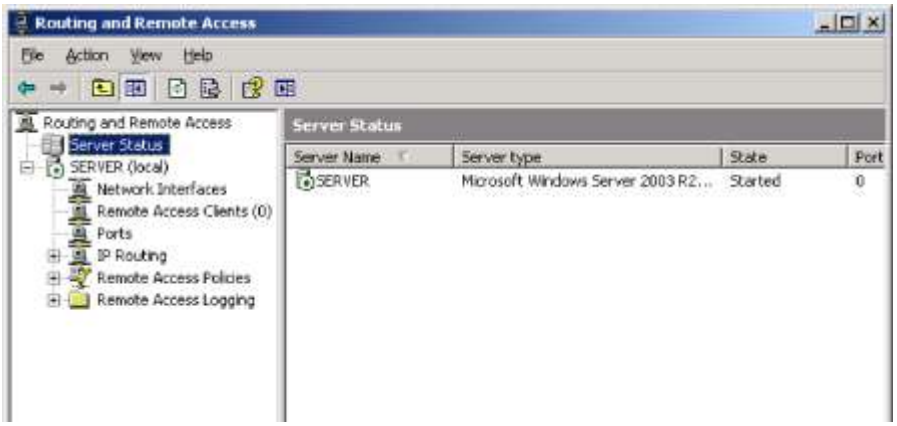


Рис. 5.28

Використання служби RADIUS

Служба RADIUS (Remote Authentication Dial-in User Service) є проміжною ланкою між сервером віддаленого доступу (який в даному випадку називають клієнтом RADIUS) і службою каталогів корпоративної мережі. Сервер RADIUS дозволяє вирішити два основні завдання:

- інтеграція в єдину систему серверів віддаленого доступу від різних виробників;
- централізоване управління доступом в корпоративну мережу (служба RRAS в системі Windows Server настроюється індивідуально для кожного сервера RRAS).

Служба RADIUS працює за наступною схемою:

- спочатку встановлюється телефонне (або інше) з'єднання між клієнтом і сервером віддаленого доступу;
- користувач пересилає серверу RAS запит на аутентифікацію (свої ім'я і пароль);
- сервер віддаленого доступу (що є клієнтом сервера RADIUS) пересилає даний запит серверу RADIUS;
- сервер RADIUS перевіряє запит на аутентифікацію в службі каталогів (наприклад, у службі Active Directory) і посилає у відповідь RAS-серверу дозвіл чи заборону даному користувачеві на підключення до сервера віддаленого доступу;
- сервер віддаленого доступу або підключає користувача до корпоративної мережі, або видає відмову у підключенні.

Реалізація служби RADIUS в системі Windows Server називається службою IAS (Internet Authentication Service).

Розділ "Network Interfaces" консолі "Routing and Remote Access"

У даному розділі консолі перераховуються всі мережні інтерфейси, встановлені на сервері (мережні адаптери, модеми). Нагадаємо, що інтерфейс "Внутрішній (Internal)" - це інтерфейс, до якого підключаються всі клієнти віддаленого доступу, незалежно від типу підключення (по комутованих телефонних лініях, через віртуальну приватну мережу і т.д.) (Рис. 5.29).

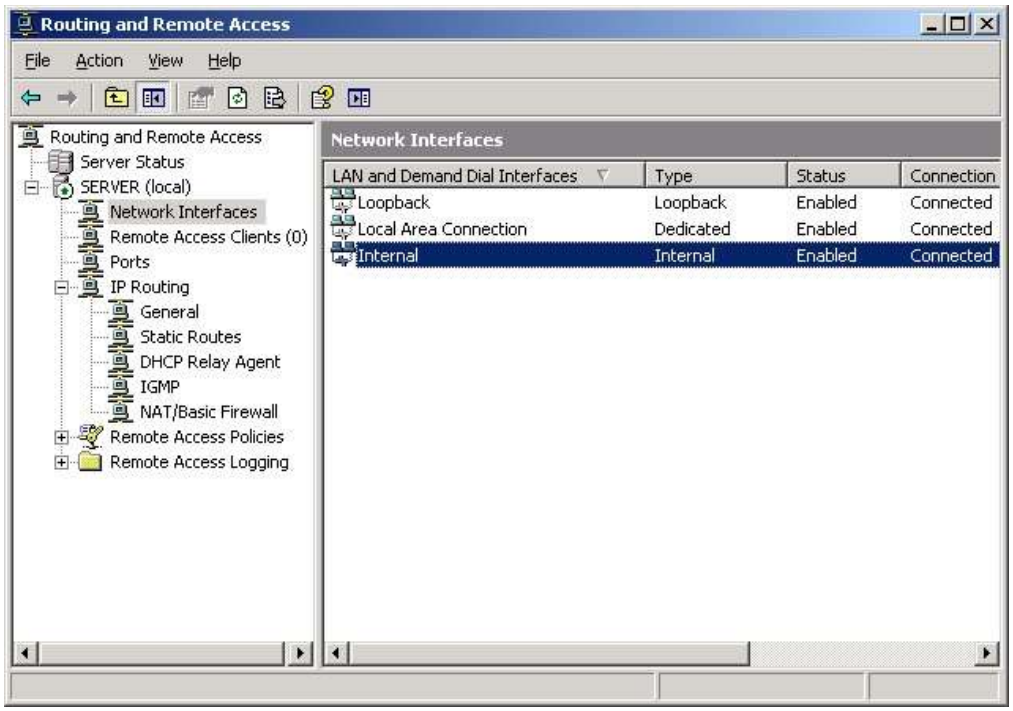


Рис. 5.29

Розділ "Remote Access Clients" консолі "Routing and Remote Access"

У даному розділі здійснюється моніторинг у реальному часі клієнтів, які підключилися до сервера віддаленого доступу.

Розділ "Ports" консолі "Routing and Remote Access"

У розділі "Ports" перераховуються всі доступні точки підключення до служби віддаленого доступу:

- паралельний порт (для прямого з'єднання двох комп'ютерів через порт LPT);
- модеми, доступні для служби віддаленого доступу;
- порти, доступні для підключень за допомогою віртуальних приватних мереж (якщо адміністратор під час налаштування сервера вказав, що будуть використовуватися віртуальні приватні мережі, то на сервер автоматично додаються по 128 портів для кожного з протоколів PPTP і L2TP, надалі адміністратор може змінити кількість портів, доступних для того чи іншого протоколу).

Розділ "IP-routing" консолі "Routing and Remote Access"

У цьому розділі додаються, видаляються і настроюються як статичні маршрути, так і необхідні динамічні протоколи маршрутизації (Рис. 5.30):

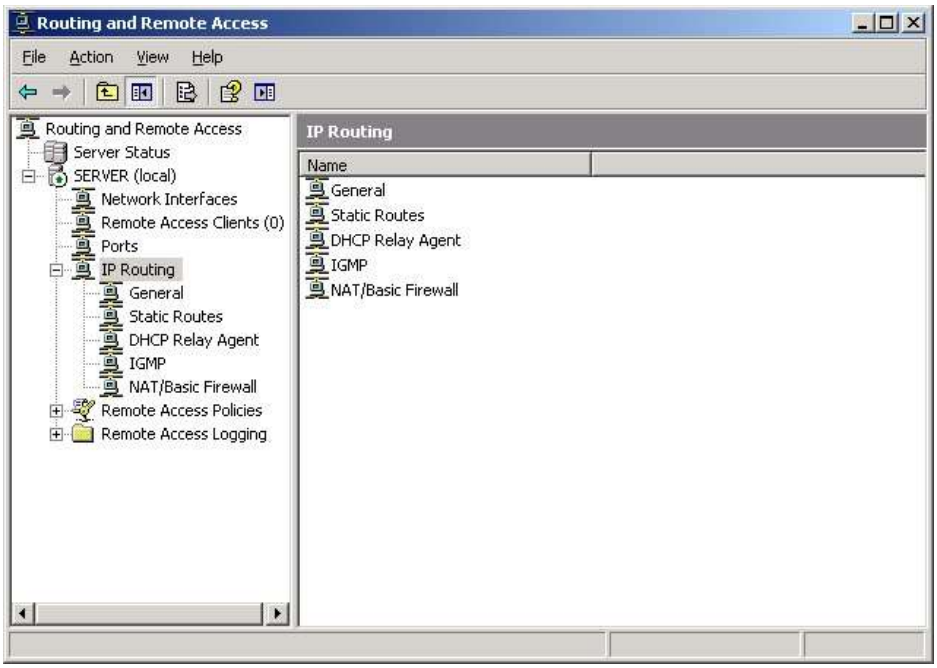


Рис. 5.30

- Агент ретрансляції DHCP-запитів (DHCP Relay Agent) - використання агента ретрансляції запитів DHCP докладно обговорювалося в пункті, присвяченому службі DHCP, налаштування даного агента приводиться саме в цьому розділі служби RRAS;

- Протокол IGMP - даний протокол призначений для маршрутизації multicast-пакетів протоколу TCP/IP (даний вид пакетів і адрес використовується в основному при передачі мультимедіа-інформації);
- Служба трансляції мережних адрес (NAT, Network Address Translation) - дана служба дозволяє обмінюватися інформацією між мережами з внутрішніми IP-адресами та мережами з адресами, зареєстрованими в мережі Інтернет (спрощений варіант проксісервера);

Налаштування прав користувачів для підключення до сервера віддаленого доступу

При відсутності сервера RADIUS, дозволи на підключення користувача до серверів віддаленого доступу визначаються комбінацією властивостей користувача і політик віддаленого доступу, що настроюються індивідуально для кожного сервера віддаленого доступу.

Якщо домен Active Directory працює в змішаному режимі, то дозволи на віддалений доступ визначаються тільки у Властивостях користувача на закладці "Вхідні дзвінки" (Dial-In). При цьому є тільки два варіанти - дозволити або заборонити (Рис. 5.31).

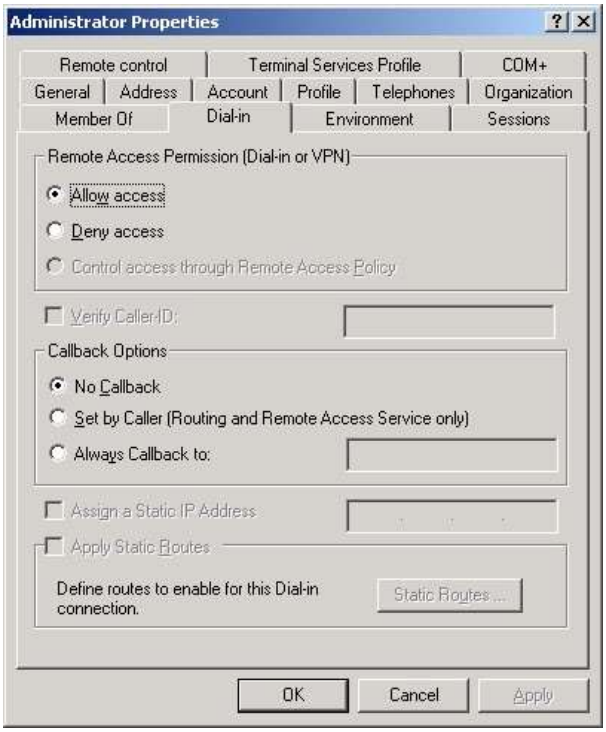


Рис. 5.31

За замовчуванням для кожного нового користувача задається забороняюче правило. Крім «дозволити/заборони» можна також налаштувати Зворотній виклик сервера (Call-back).

Тут є три варіанти:

- "У відповідь виклик не виконується" - при підключенні користувача до сервера віддаленого доступу спочатку встановлюється телефонне з'єднання між модемом користувача і модемом клієнта, якщо доступ дозволений, то встановлюється мережне з'єднання і користувач отримує можливість працювати в мережі;
- "Встановлюється викликаючим" - у цьому варіанті після встановлення телефонного з'єднання між модемами і перевірки прав доступу система запросить у клієнта ввести номер телефону, з якого підключається даний клієнт, після цього сервер розриває зв'язок і вже самостійно утворює з'єднання з клієнтом по тому номеру телефону, який повідомила ця особа (даний варіант зручний для мобільних користувачів - користувач економить на телефонному дзвінку і підвищується захищеність доступу, тому що в ідеалі ніхто, крім користувача, не повинен знати номер телефону, з якого користувач ініціював з'єднання);
- "Завжди за цим номером" (із зазначенням номера телефону) - даний варіант схожий на попередній, тільки номер телефону вже введений в параметри користувача і сервер буде передзвонювати саме на цей номер (цей варіант буде цікавий домашнім користувачам - тут теж користувач економить на телефонному дзвінку і, крім того, додатковий захист - зловмисникові важко буде підключитися до сервера, навіть якщо йому відомі ім'я і пароль користувача).

Якщо домен працює в основному режимі Windows 2000 або Windows 2003, то можна або в явному вигляді дозволяти або забороняти доступ до серверів віддаленого доступу, причому до всіх відразу, або налаштовувати дозвіл через Політики віддаленого доступу. Зауважимо, що явний дозвіл або явна заборона мають більш високий пріоритет, ніж політики віддаленого доступу.

В основному режимі у властивостях користувача стають доступні додаткові параметри:

- "Перевіряти код тих хто дзвонить" (Caller ID) - якщо оператор телефонного зв'язку передає модему номер телефону, з якого був зроблений дзвінок, то сервер буде дозволяти підключення тільки при виклику з даного номера (це ще один рівень захисту від зловмисників);
- "Статична IP-адреса користувача" - при встановленні з'єднання користувачеві призначається фіксована IP-адреса;
- "Використовувати статичну маршрутизацію" - при встановленні з'єднання користувачеві пересилається зазначений список маршрутизаторів.

Налаштування властивостей сервера

Знову виберемо у вікні консолі ім'я сервера, клацнемо правою кнопкою миші і виберемо пункт меню "Властивості" (Рис. 5.32).

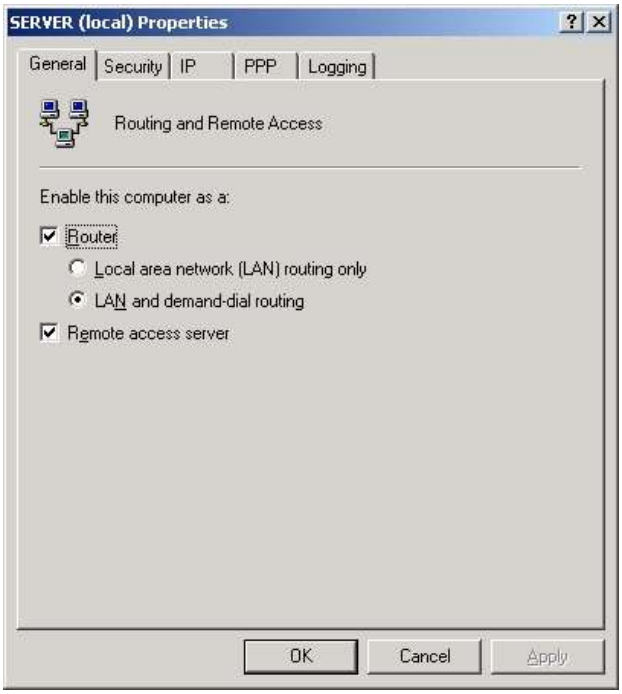


Рис. 5.32

1. На закладці "Загальні" можна змінити сценарії використання служби:
   - тільки як маршрутизатор (або тільки для локальної мережі, або для локальної мережі і віддалених мереж, підключений через засоби віддалених комунікацій);
   - тільки як сервер віддаленого доступу;

2. На закладці "Безпека" налаштовуються методи перевірки достовірності (аутентифікації) користувачів, що підключаються до служби віддаленого доступу (Рис. 5.33).

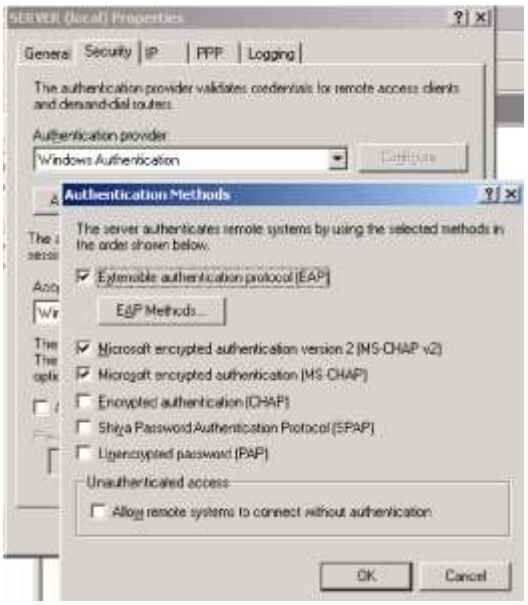


Рис. 5.33

Служба RRAS системи Windows Server підтримує наступні методи аутентифікації (за ступенем зростання захищеності даної процедури):

- протокол розширеної перевірки автентичності EAP (Extensible Authentication Protocol) - дозволяє використання смарт-карт при аутентифікації користувача (потрібні сертифікати як для сервера RRAS, так і для користувачів).
- протокол MS-CHAP версії 2 (Microsoft Challenge Handshake Authentication Protocol version 2) - посилена версія MS CHAP (більш довгий ключ шифрування при передачі пароля, обчислення нового ключа при кожному новому сеансі підключення, взаємна аутентифікація користувача й сервера віддаленого доступу);
- протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) - версія протоколу CHAP, реалізована корпорацією Microsoft з хеш-функцією MD-4;
- протокол CHAP (Challenge Handshake Authentication Protocol) - для шифрування пароля використовується метод хешування MD-5 (по мережі передається значення хеш-функції пароля), даний протокол є одним з галузевих стандартів і реалізований в багатьох системах віддаленого доступу, його рекомендується використовувати при підключенні клієнтів , що працюють не на платформі Windows, за замовчуванням також вимкнений;
- протокол SPAP (Shiva Password Authentication Protocol) - використовує протокол шифрування паролів, розроблений компанією Shiva (в минулому - один з розробників засобів віддаленого доступу), алгоритм шифрування паролів слабкіше, ніж в методах CHAP і MS CHAP, за замовчуванням цей метод також вимкнений;
- протокол PAP (Password Authentication Protocol) - найпростіший протокол, успадкований від старих версій служб віддаленого доступу (реалізовані не тільки в системі Windows), при цьому протоколі ім'я та пароль користувача передаються через засоби комунікацій відкритим текстом, за замовчуванням цей метод аутентифікації вимкнений;
- без перевірки справжності - при даному варіанті взагалі не перевіряються ім'я та пароль користувача, а також права доступу користувача до служби RRAS (ні в якому разі не рекомендуємо використовувати на практиці цей метод, тому що відкриває можливість підключення до корпоративної мережі будь-якого охочого, що має інформацію про точку підключення, наприклад, номери телефонів на модемному пулі);
- клієнти віддаленого доступу, наявні в системах Windows, при підключенні до сервера віддаленого доступу завжди починають використовувати самий захищений метод аутентифікації. Якщо на сервері не реалізований запитуваний протокол аутентифікації, клієнт пробує менш захищений протокол. І так до тих пір, поки не буде підібрано протокол, підтримуваний обома сторонами.

Крім зазначених протоколів можна здійснювати підключення до служби RRAS за допомогою служби RADIUS.

На цій же закладці налаштовується використання служби обліку сеансів користувачів (служба обліку Windows, служба обліку RADIUS, або відсутність служби обліку), за замовчуванням - служба обліку Windows.

І тут же задається загальний секрет при використанні протоколу L2TP для організації віртуальних приватних мереж (VPN). Можливість використання загального секрету для VPN на базі протоколу L2TP є тільки в Windows Server 2003, у версії Windows 2000 протокол L2TP можна було використовувати тільки при наявності сертифікатів для обох сторін приватної мережі.

3. На закладці "IP" налаштовується дозвіл маршрутизації IP-пакетів між комп'ютером клієнта і корпоративною мережею (за замовчуванням) і задається спосіб формування пулу IP-адрес, які видаються RRAS-сервером клієнтам, що підключаються до нього (Рис. 5.34).

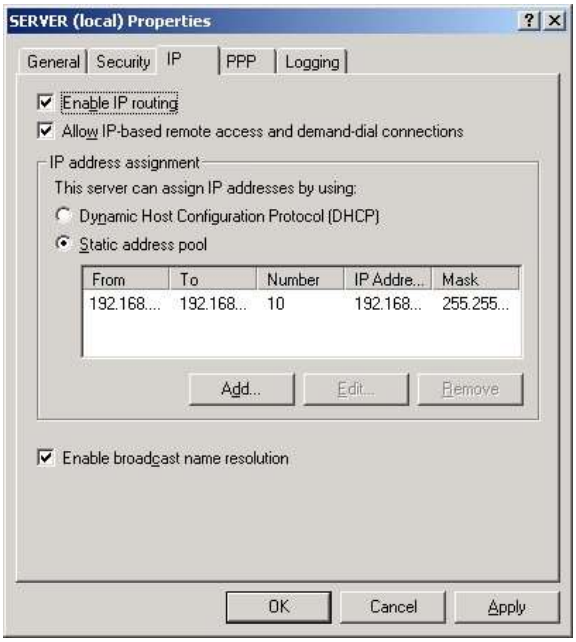


Рис. 5.34

Є два способи формування пулу - використання сервера DHCP, встановленого в корпоративній мережі, і задання пулу IP-адрес на самому сервері віддаленого доступу (при цьому способі 1-й IP-адрес з пулу буде призначений інтерфейсу "Внутрішній" на самому сервері RRAS, а інші в пулі адреси будуть призначатися RRAS-клієнтам)

4. Закладка "PPP" (Рис. 5.35).

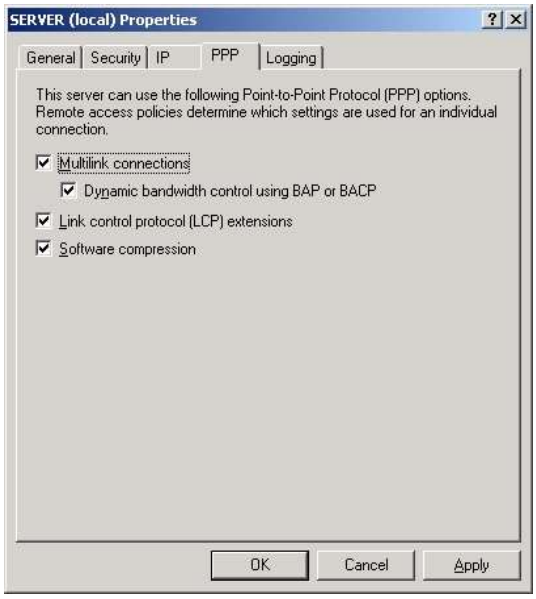


Рис. 5.35

Тут дозволяється або забороняється використання багатоканальних підключень протоколу PPP (multilink PPP). Протокол PPP дозволяє використовувати кілька комунікаційних каналів (наприклад, кілька комутованих телефонних ліній і, відповідно, одночасне використання декількох модемів на серверній і на клієнтській стороні) як одне підключення з відповідним збільшенням пропускної здатності і призначенням по одній IP-адресі на стороні клієнта і сервера. При цьому можливе використання динамічного керування пропускною спроможністю (за допомогою протоколів BAP/BACP, Bandwidth Allocation Protocol/Bandwidth Allocation Control Protocol), які дозволяють при зростанні трафіку активізувати додаткові телефонні лінії з наявного пулу телефонних ліній, а при зменшенні трафіку - відключати телефонні лінії.

5. Закладка "Ведення журналу" (Рис. 5.36). На цій закладці налаштовується рівень протоколювання подій, пов'язаних з сеансами роботи віддалених користувачів.

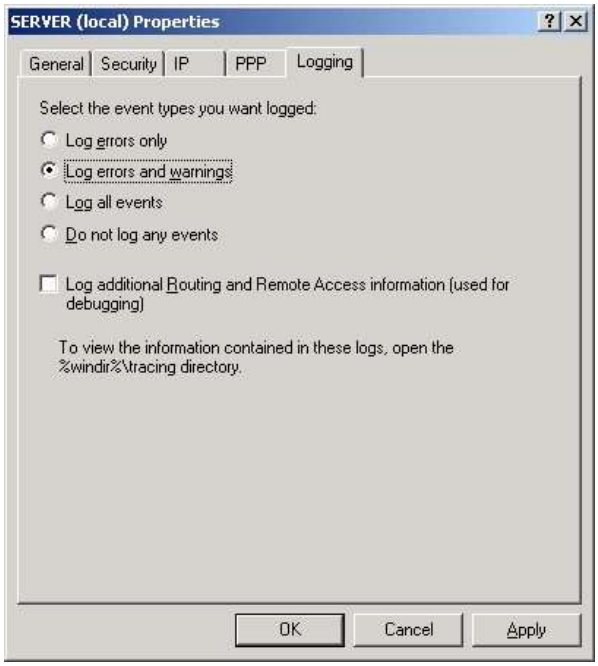


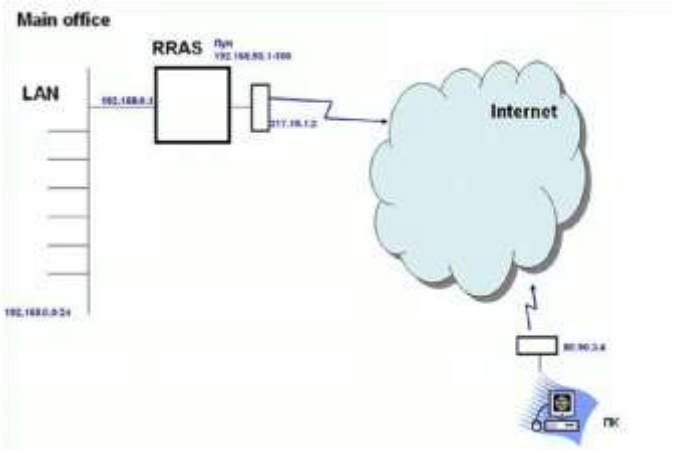
Рис. 5.36

Віртуальні приватні мережі

Віртуальні приватні мережі (Virtual Private Networks) - технологія створення захищених підключень між комп'ютерами, підключеними до публічних мереж (наприклад, до мережі Інтернет).

Розглянемо приклад на Рис. 5.37

.



(Рис. 5.37)

Припустімо, якийсь мобільний користувач бажає підключитися до корпоративної мережі. Він може це зробити, підключившись до корпоративного серверу віддаленого доступу по комутованій

телефонній лінії. Однак, якщо користувач знаходиться в іншому місті чи навіть іншій країні, такий дзвінок може обійтися дуже дорого. Може виявитися значно дешевше підключитися до мережі Інтернет через місцевого Інтернет-провайдера. Корпоративна мережа, в свою чергу, теж має своє підключення до Інтернет. У цьому випадку потрібно вирішити два завдання:

- як отримати доступ в корпоративну мережу (в даному прикладі IP-адреси корпоративної мережі належать до діапазону внутрішніх адрес і пакети від мобільного користувача не зможуть потрапити в цю мережу);
- як захистити дані, що передаються через Інтернет (усі мережні пакети, що передаються через Інтернет, містять інформацію у відкритому тексті, і грамотний зловмисник може перехопити пакети і витягти з них інформацію).

Обидва ці завдання вирішуються створенням VPN-підключень між віддаленим користувачем і сервером віддаленого доступу. У даному прикладі користувачеві необхідно створити ще одне підключення, але не через модем, а через "Підключення до віртуальної приватної мережі". При цьому в якості "номер телефону" виступить IP-адреса зовнішнього інтерфейсу сервера віддаленого доступу.

Процес створення підключення виглядає наступним чином:

1. Запускаем Майстер нових підключень (кнопка "Start" - "Control Panel" - "Network Connections" - "New Connections Wizard") (Рис. 5.38)
2. Обираємо тип мережного підключення - "Підключитися до мережі на робочому місці":

Рис. 5.38

3. Вибираемо спосіб мережного підключення - "Підключення до віртуальної приватної мережі" (Рис. 5.39):

Рис. 5.39

4. Задаємо ім'я підключення. 5. Вказуємо VPN-сервер (ім'я або IP-адресу; в даному прикладі - 217.15.1.2) (Рис. 5.40):

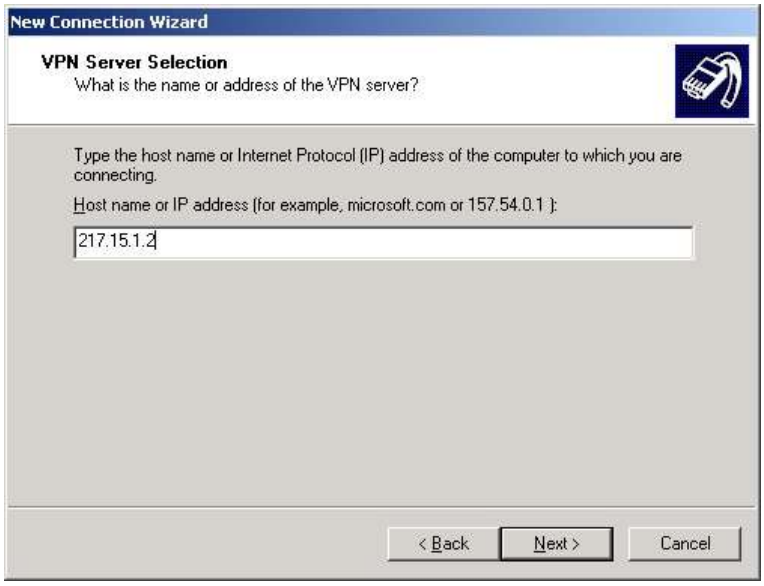


Рис. 5.40

6. Визначаємо доступність ярлика цього підключення (для даного користувача; для всіх користувачів).
7. Натискаємо кнопку "Finish".
8. Вводимо ім'я та пароль користувача, натискаємо кнопку "Підключення" (Рис. 5.41):

Рис. 5.41

Якщо всі налаштування зроблені правильно, то буде встановлено з'єднання з корпоративним сервером віддаленого доступу. Мережна конфігурація буде така, як зображено на Рис. 5.42:

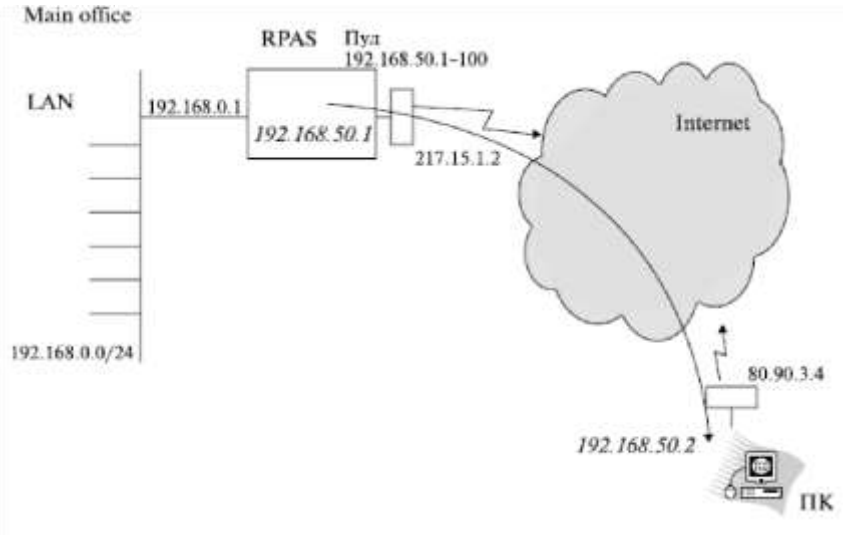


Рис. 5.42

Між ПК мобільного користувача і сервером віддаленого доступу буде встановлено захищений "віртуальний" канал, клієнтський ПК отримає IP-адресу з пулу адрес сервера RRAS (таким чином буде вирішена задача маршрутизації IP-пакетів між клієнтом і корпоративною мережею), всі пакети, що передаються між клієнтом і корпоративною мережею, будуть шифруватися.

Аналогічно можна створити захищене віртуальне з'єднання між двома офісами корпоративної мережі, підключеними до різних Інтернет-провайдерів (Рис. 5.43):

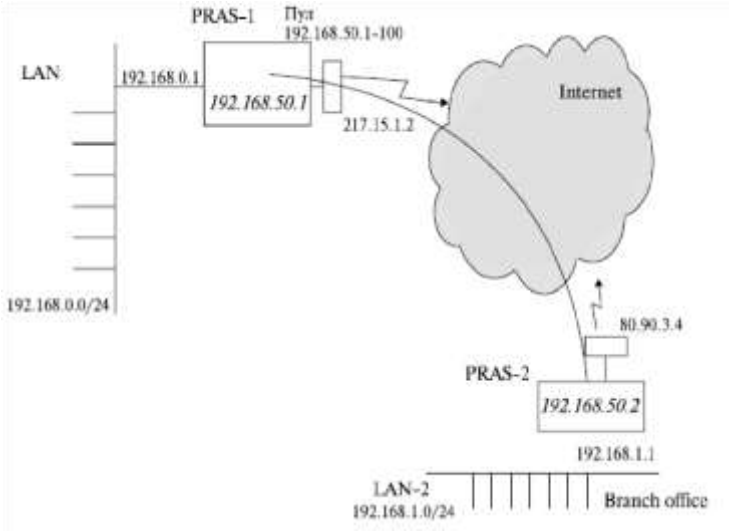


Рис. 5.43

Технології віртуальних приватних мереж

Для створення віртуальних приватних мереж у системах сімейства Windows використовуються два різних протоколи - PPTP розробки корпорації Microsoft (Point-to-Point Tunneling Protocol) і L2TP, що об'єднав найкращі риси протоколів PPTP і L2F компанії Cisco (Level 2 Tunneling Protocol). Основний принцип роботи обох протоколів полягає в тому, що вони створюють захищений "тунель" між користувачем і корпоративною мережею або між двома підмережами. Тунелювання полягає в тому, що пакети, що передаються в захищеній мережі, забезпечуються спеціальними заголовками (в обох протоколів свої заголовки), вміст даних в цих пакетах шифрується (у PPTP - алгоритмом MPPE компанії Microsoft, в L2TP - технологією IPSec), а потім пакет, призначений для захищеної корпоративної мережі і має заголовок з IPадресами внутрішньої корпоративної мережі, інкапсулюється в пакет, що передається по мережі Інтернет і має відповідний заголовок та IP-адреси відправника і одержувача.

Відмінності між двома протоколами наступні:

- алгоритми шифрування (MPPE для PPTP, IPSec для L2TP);
- транспортне середовище (PPTP працює тільки поверх протоколу TCP/IP, L2TP може працювати також поверх протоколів X.25, Frame Relay, ATM, хоча реалізація L2TP в системі Windows працює тільки поверх TCP/IP);
- L2TP здійснює взаємну аутентифікацію обох сторін, що беруть участь у створенні захищеної мережі, для цього використовуються сертифікати X.509 або загальний секрет (preshared key). Загальний секрет (попередній ключ) реалізований починаючи з версії Windows 2003, встановлюється у Властивостях служби RRAS на закладці "Безпека" (Рис. 5.44).

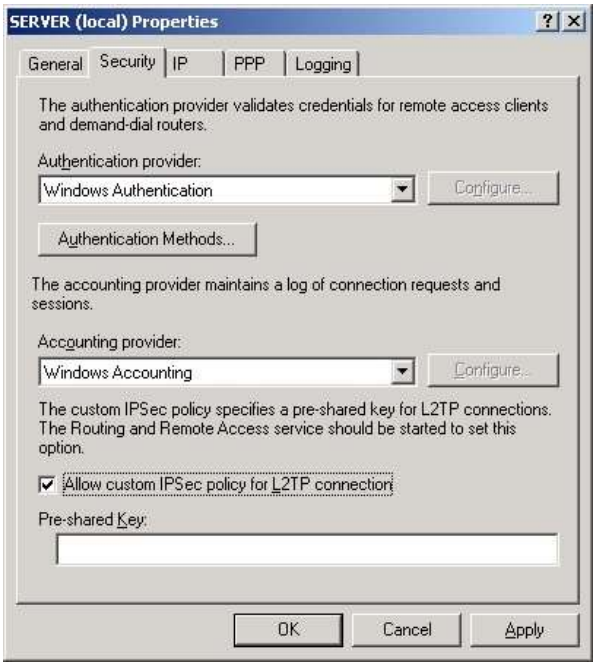


Рис. 5.44

Політики віддаленого доступу

Як вже говорилося вище, в основному режимі домену Windows 2000/2003 дозволами на підключення до служби віддаленого доступу можна керувати за допомогою політик віддаленого доступу. Нагадаємо, що політики віддаленого доступу застосовуються до облікового запису користувача при його спробі підключитися до служби віддаленого доступу тільки в тому випадку, якщо в Властивостях цього облікового запису вказано "Управління на основі політики віддаленого доступу". Якщо в явному вигляді зазначено дозвіл або заборону підключення, то політики не перевіряються.

Кожна політика складається з трьох компонентів:

- Умови (Conditions) - визначаються умови підключення користувача (у мережах на базі MS Windows Server найбільш цікаві умови - день тижня і час, а також членство у певній групі);
- Профіль (Profile) - визначаються якісь параметри підключення (наприклад, тип аутентифікації або вид комунікацій);
- Дозволи (Permissions) - дозволити або заборонити підключення.

На початку перевірки політики завжди перевіряються умови - якщо жодна з умов не збігається з параметрами облікового запису користувача, то відбувається перехід до наступної політики. Якщо умови збіглися, то перевіряються параметри профілю підключення, якщо параметри політики та користувача не збігаються, то також відбувається перехід до наступної політики. Якщо ж параметри профілю співпали і дана політика дозволяє підключення, то

користувачеві видається дозвіл на підключення до сервера віддаленого доступу. Якщо ж політика забороняє підключення, то користувачеві видається відмова на підключення до сервера.

Частина 2

Служба резервного копіювання

Архівація і відновлення файлових ресурсів

Системи сімейства Windows не містять компоненти резервного копіювання в сенсі системної служби (service). Всі операції по створенню резервних копій і відновлення даних здійснюються утилітою ntbackup. Цю утиліту можна запустити з Головного меню системи (кнопка "Пуск" - "Всі програми" - "Стандартні" - "Службові" - "Архівація даних"), а можна запустити більш швидко з командного рядка (кнопка "Пуск" - "Виконати" - "ntbackup" - кнопка "ОК")(Рис. 5.45). При першому запуску утиліти рекомендуємо забрати галочку біля поля "Завжди запускати в режимі майстра".

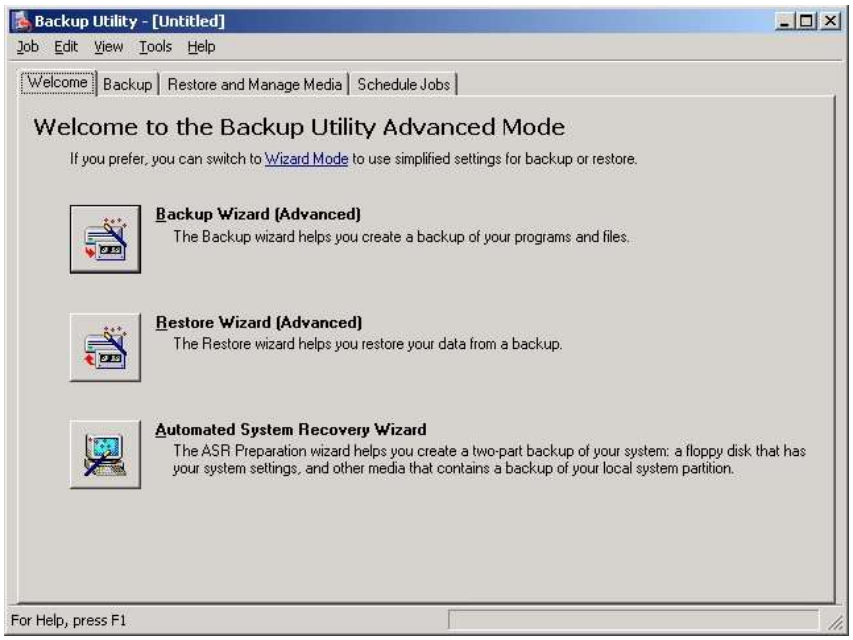


Рис. 5.45

Резервне копіювання файлових ресурсів

Кожен файл, що зберігається на диску комп'ютера, незалежно від типу файлової системи, має атрибут archive, який у Властивостях файлу відображається як "Файл готовий для архівування" (відкрийте Властивості файлу і натисніть кнопку "Інші"). Якщо у властивостях файлу вручну прибрати галочку у цього атрибуту, то при будь-якій зміні у файлі операційна система автоматично

знову встановить цей атрибут. На використанні змін даного атрибуту засновані всі використовувані в системі Windows методики резервного копіювання.

Типи резервного копіювання

Утилітою ntbackup можна створювати резервні копії різних типів. Розглянемо їх відмінні особливості і різні варіанти їх застосування.

Звичайний (Normal)

При виконанні даного типу архівування утиліта ntbackup архівує всі файли, відмічені для архівації, при цьому у всіх заархівованих файлів очищається атрибут "Файл готовий для архівування". Даний вид архівування необхідний для створення щотижневих повних резервних копій будь-яких великих файлових ресурсів. Якщо в компанії або організації є достатньо ресурсів, то можна щодня здійснювати повне архівування даних.

Різницевий (Differential)

При виконанні різницевого архівування утиліта ntbackup з файлів, позначених для архівування, архівує тільки ті, у яких встановлений атрибут "Файл готовий для архівування", при цьому цей атрибут не очищається. Використання звичайного та різницевого архівування дозволяє заощадити простір на носіях з резервними копіями та прискорити процес створення щоденних копій. Наприклад, якщо раз на тиждень (як правило, у вихідні дні) створювати звичайні копії, а протягом тижня щодня (як правило, в нічний час) - Різницеві, то виходить виграш в обсязі носіїв для резервного копіювання. При такій комбінації архівування "Звичайний + різницевий" процес відновлення даних у випадку втрати інформації вимагатиме виконання двох операцій відновлення - спочатку з останньої Повної копії, а потім з останньої різницевої резервної копії.

Додатковий (Incremental)

При виконання додаткової архівації утиліта ntbackup з файлів, позначених для архівування, архівує тільки ті, у яких встановлений атрибут "Файл готовий для архівування", при цьому цей атрибут очищається. Використання звичайного (раз на тиждень по вихідним) і додаткових (щодня в робочі дні) архівування також дозволяє заощадити простір на носіях з резервними копіями та прискорити процес створення щоденних копій. Але процес відновлення даних при використанні комбінації "Звичайний + Додатковий" вже буде виконуватися інакше: в разі втрати інформації для відновлення даних буде потрібно спочатку відновити дані з останньої повної копії, а потім послідовно з усіх доданих копій, створених після повної копії.

Скопійований (Copy)

При такому типі архівування утиліта ntbackup заархівує всі позначені файли, при цьому атрибут "Файл готовий для архівування" залишається без змін.

Щоденний (Daily)

Щоденний тип архівування створює резервні копії тільки тих файлів, які були модифіковані в день створення резервної копії.

Два останні типи не використовуються для створення регулярних резервних копій. Їх зручно застосовувати в тих випадках, коли з якої-небудь метою потрібно зробити копію файлових ресурсів, але при цьому не можна порушувати налаштовані регулярні процедури архівування.

Створення завдання на виконання архівації даних

Для створення архівів призначені "Майстер архівації" і закладка "Архівація". В обох випадках використовуються параметри за замовчуванням. Щоб переглянути або змінити ці параметри, виконайте наступні дії:

- клацніть посилання "Розширений режим (Advanced Mode)" в першому вікні "Майстра архівації або відновлення" (Рис. 5.46);
- виберіть у меню "Сервіс (Tools)" пункт "Параметри (Options)".

Вікно, що відкрилося містить п'ять закладок: "Загальні (General)", "Відновлення (Restore)", "Тип архіву (Backup Type)", "Журнал архівації (Backup Log)" і "Виключення файлів (Exclude Files)".

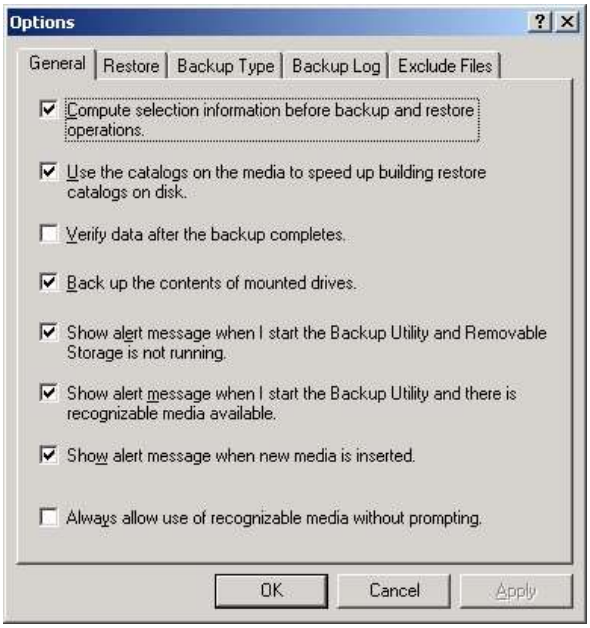


Рис. 5.46

Налаштування вкладки General

У вкладці General (Загальні) виберіть або вимкніть наступні можливості.

- Compute selection information before backup and restore operations (Розраховувати інформацію про вибір, перш ніж виконувати операції резервного копіювання і

відновлення). Система розрахує кількість папок і файлів у обраній вами множині резервного копіювання, а також простір на диску, який їм потрібен, перш ніж розпочати роботу. У разі резервного копіювання це необхідно тільки в тому випадку, якщо ємність диска або дисків, які ви копіюєте, набагато більше ємності ваших цільових носіїв і ви хочете знати, скільки стрічок або дисків вам буде потрібно. У разі відновлення це необхідно тільки в тому випадку, якщо відновлення виконується на диск, який вже містить дані.

- Use the catalogs on the media to speed up building restore catalogs on disk (Використовувати каталоги на носіях, щоб прискорити створення каталогів відновлення на диску). При відновленні з резервної копії система створює каталог на цільовому диску, перш ніж відновлювати файли з носія резервної копії. Якщо каталог носіїв пошкоджений або у вас резервна копія на кількох стрічках та відсутня стрічка, що містить каталог, то ви не зможете використовувати цю опцію. Замість цього програма буде сканувати ваші носії резервної копії, щоб створити каталог на диску з "нуля".
- Verify data after the backup completes (Перевіряти дані після завершення резервного копіювання). У разі вибору цієї опції після завершення резервного копіювання запускається процес верифікації між цільовими носіями і жорстким диском. Однак цей процес фактично полягає в перевірці того, що ПЗ резервного копіювання може читати файл на цільовому носії. Це істотно відрізняється від порівняння по файлах, при якому гарантується збіг скопійованого файлу із вихідним файлом. Правда, якщо ПЗ резервного копіювання не може прочитати файл, це часто є ознакою, що є проблема носія або навіть типу носія. Хоча це важлива перевірка, більш надійним тестом є створення невеликої резервної копії та відновлення з цієї копії, після чого потрібно перевірити, що всі файли на диску залишилися такими ж, як до відновлення.
- Back up the contents of mounted drives (Резервне копіювання змонтованих дисків). Якщо ви використовуєте монтовані диски, це гарантує, що буде виконано резервне копіювання даних змонтованого диска. Якщо відключити цю опцію, то в резервне копіювання буде включена тільки інформація про шлях до змонтованому диску.
- Show alert message when I start the Backup Utility and Removable Storage is not running (Виводити попередження, якщо я запускаю Backup Utility, а служба Removable Storage не працює). Виберіть цю опцію, щоб отримувати попередження, коли не запущена служба Removable Storage. Це необхідно тільки в тому випадку, якщо ваш цільовий носій управляється службою Removable Storage, тобто це стрічка або оптичний диск.
- Show alert message when I start the Backup Utility and there is recognizable media available (Виводити попередження, якщо я запускаю Backup Utility і є допустимий носій). Виберіть цю опцію, якщо ви використовуєте носій, який керується службою Removable Storage, і ви хочете знати, чи існує і коли буде доступний новий носій в пулі носіїв.
- Show alert message when new media is inserted (Виводити попередження, коли відбувається вставка нового носія). Виберіть цю опцію, якщо ви використовуєте носій, який керується службою Removable Storage, і хочете знати, що новий носій був встановлений в цільовий пристрій.

- Always allow use of recognizable media without prompting (Завжди дозволяти використання допустимого носія без запиту користувача). Виберіть цю опцію, якщо ви використовуєте носій, який керується службою Removable Storage, і хочете автоматично переміщати новий носій, який не виявлений цією службою, з доступного пулу носіїв в пул, який використовується програмою Backup.

Установки вкладки Restore

Параметри конфігурації вкладки Restore (Відновлення) застосовуються для випадків часткового відновлення, але не для повного відновлення після аварії диска, коли ви знову створюєте систему на новому диску. Виберіть поведінку за умовчанням для відновлення файлів, які вже є на диску, серед наступних варіантів (Рис. 5.47).

- Don't replace existing files (Не замінювати існуючі файли).
- Replace existing files when the files on the disk are older than the files on the restore media (Замінювати існуючі файли, якщо файли на диску змінювалися раніше, ніж файли на носії резервної копії).
- Always replace the file on my computer (Завжди замінювати файли на моєму комп'ютері).

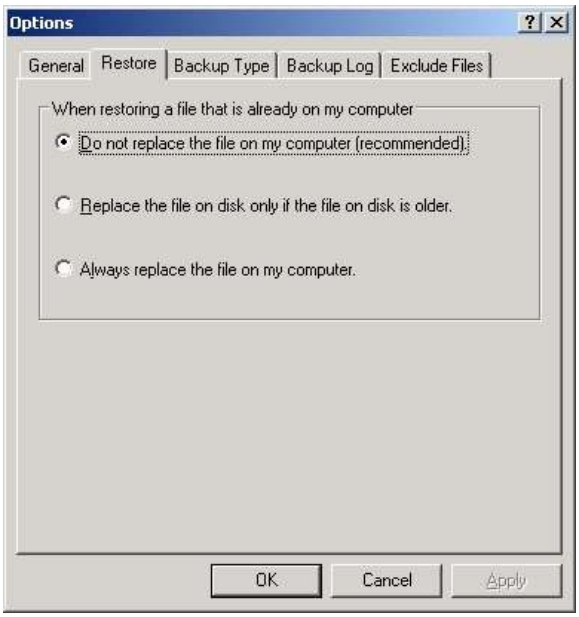


Рис. 5.47

Звичайно, безпечніше всього використовувати перший варіант. Однак нагадаємо, що ви задаєте тільки конфігурацію за замовчуванням, а при реальному відновленні ви маєте можливість змінити налаштуваня за замовчуванням.

Установки вкладки Backup Type (Тип резервного копіювання)

Використовуйте список, що розкривається в цій вкладці, щоб вибрати тип резервного копіювання за замовчуванням (всі п'ять типів описані вище у розділі "Типи резервного

копіювання"). Ця установка за замовчуванням для вашого сеансу резервного копіювання, і ви можете змінити тип, коли буде виконуватися резервне копіювання (Рис. 5.48).

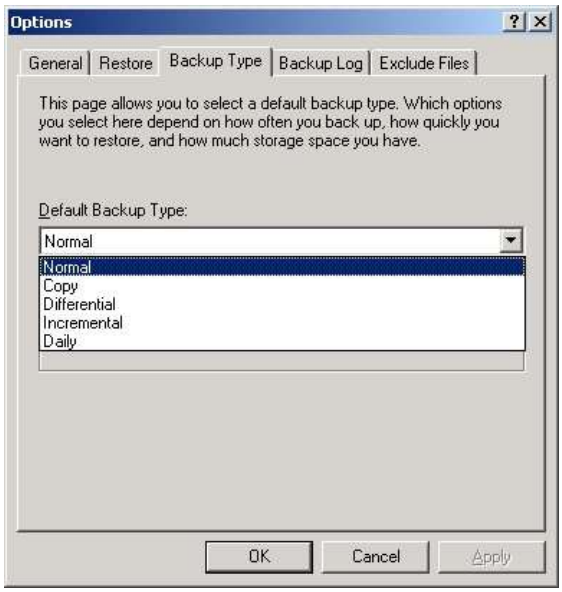


Рис. 5.48

Установки вкладки Backup Log (Журнал резервного копіювання)

Виберіть варіант журналу для операції резервного копіювання. У вас є наступні варіанти (Рис. 5.49).

- Detailed (Докладно). У журнал включаються імена всіх копійованих файлів і папок.
- Summary (Підсумок). У журнал записуються головні процеси, включаючи час початку резервного копіювання і список всіх файлів, які не вдається скопіювати.
- None (Немає). Означає, що не підтримується ніякий журнал.

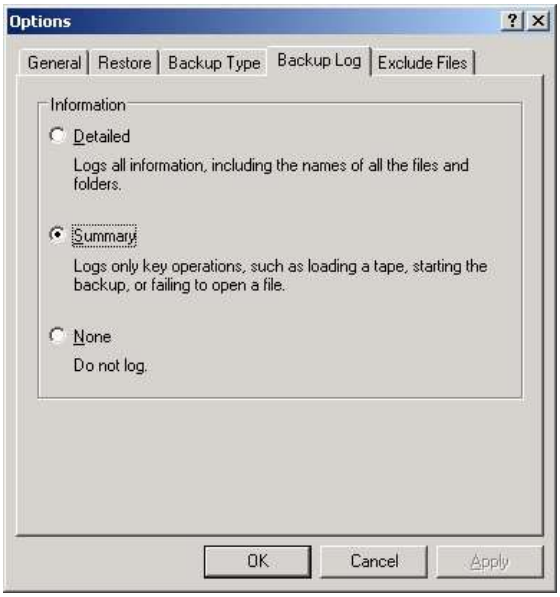


Рис. 5.49

Журнали резервного копіювання мають імена backupXX.log (де XX починається з 01) і містяться в папці \Documents and Settings\<Ім'я користувача, що виконав вхід>\Local Settings\Application Data\Microsoft\Windows NT\NTBackup\data. На відміну від Windows Backup в Windows NT ви не можете змінити це місцезнаходження.

Установки вкладки Exclude Files

У вкладці Exclude Files (файли, що виключаються) виводиться список файлів, які виключаються з резервного копіювання. Ви можете додавати файли до цього списку і застосовувати ці нові винятки до даного комп'ютера (незалежно від користувача, що виконав вхід) або до резервного копіювання, яке відбувається після того, як ви виконали ваш вхід (Рис. 5.50).

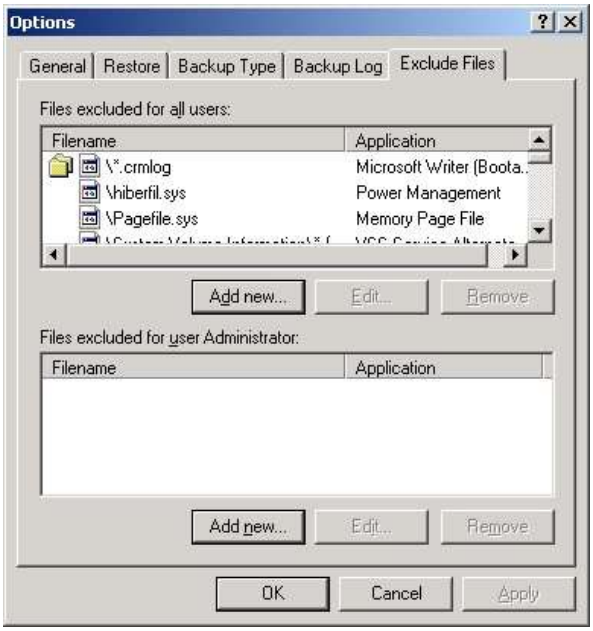


Рис. 5.50

Щоб виключити певні файли для всіх користувачів, клацніть на кнопку Add New (Додати нові файли) під секцією Files Excluded For All Users (Файли, виключені для всіх користувачів).

Щоб виключити файли в резервному копіюванні, яке виконується вами, клацніть на кнопку Add New під секцією Files Excluded for Ім'я користувача (Файли, виключені для Ім'я користувача).

Список виключених файлів записується в розділ реєстру HKEY LOCAL MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToBackup. Тому такі файли виключаються незалежно від програми резервного копіювання, яку ви використовуєте, - Windows Backup або програма від стороннього постачальника.

Приклад створення завдань на автоматичне виконання резервних копій

У даному прикладі на одному з дискових носіїв є папка з файлами Folder1, для якої буде створюватися резервна копія (Рис. 5.51).

1. Запустимо утиліту резервного копіювання ntbackup.
2. Запустимо "Майстер архівації (Backup Wizard)" (на сторінці "Ласкаво просимо (Welcome)" натиснути кнопку "Майстер архівації (Backup Wizard)"):

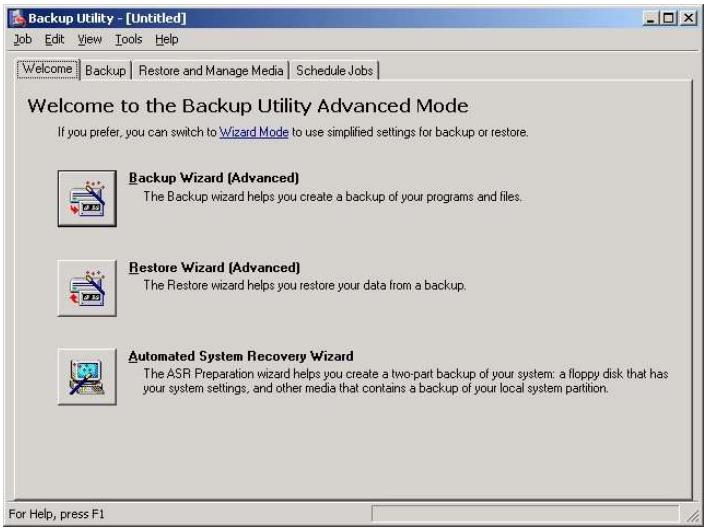


Рис. 5.51

3. Після запуску майстра натиснемо кнопку "Next" і виберемо, що нам потрібно архівувати, в даному прикладі - "Архівувати вибрані файли, диски або мережні дані" (Рис. 5.52):

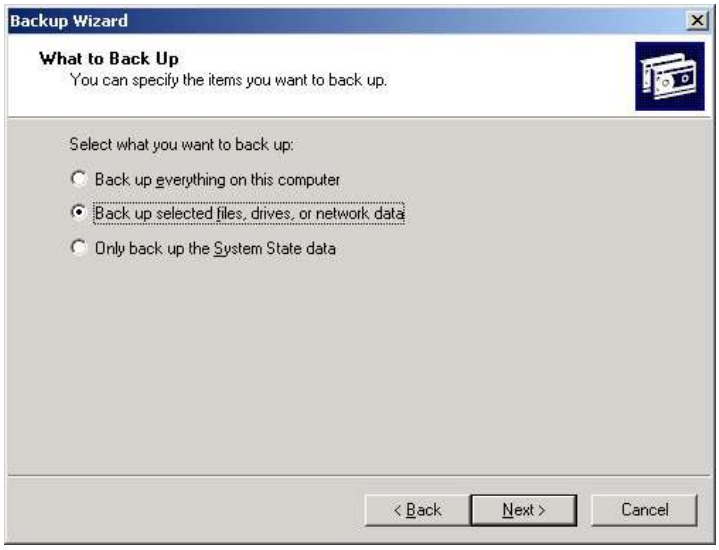


Рис. 5.52

4. Виберемо для архівування папку Folder1 (Рис. 5.53):

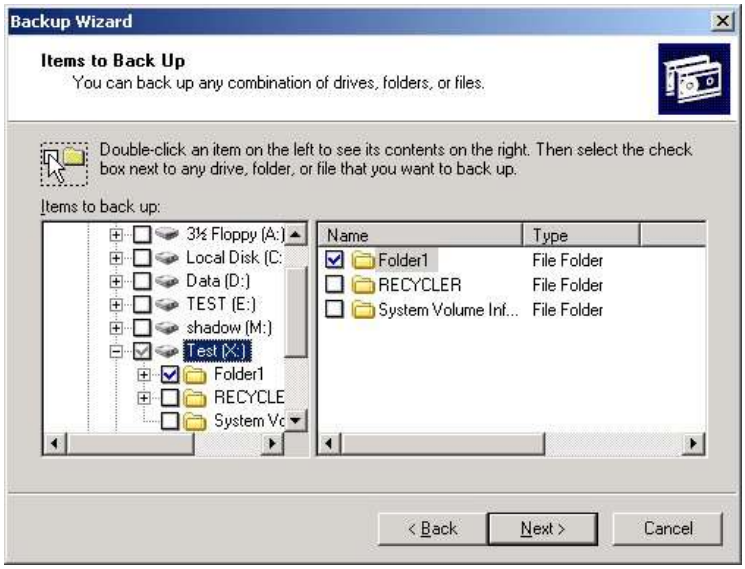


Рис. 5.53

5. Виберемо місце для створення резервної копії, створимо файл з ім'ям "Folder1-Backup", цьому файлу автоматично буде призначено розширення ". Bkf" (Рис. 5.54):

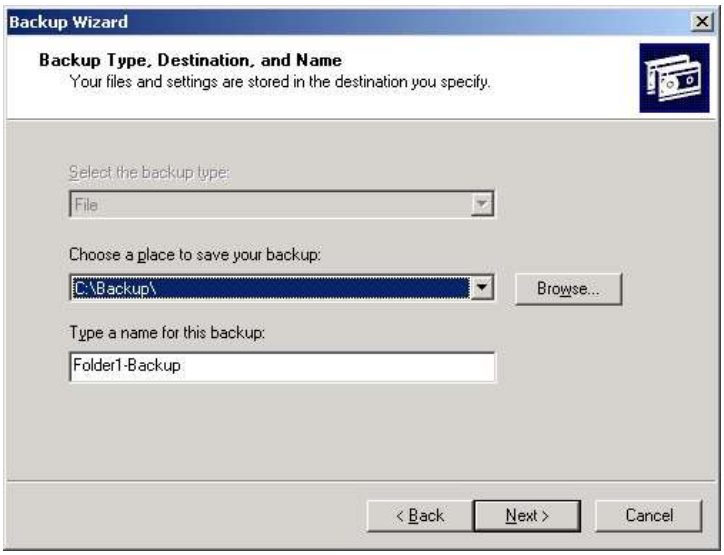


Рис. 5.54

6. Вибір додаткових можливостей. Якщо на наступному кроці натиснути кнопку "Finish", то утиліта резервного копіювання одноразово створить резервну копію папки Folder1. Натиснемо кнопку "Advanced", щоб задати додаткові параметри (Рис. 5.55):

Рис. 5.55

7. Вибираємо тип архівування (вибираємо «Звичайний») (Рис. 5.56).

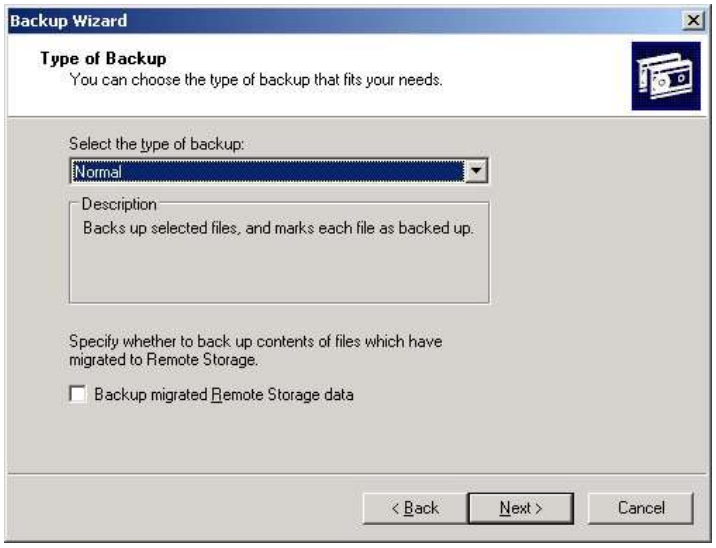


Рис. 5.56

8. Нічого не змінюємо на сторінці «Способи архівації» (Рис. 5.57)

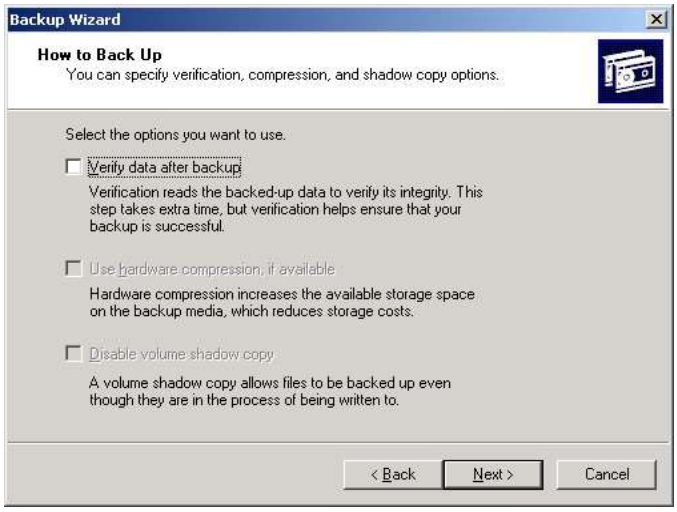


Рис. 5.57

9. На сторінці "Параметри архівації" можна вибрати заміну існуючих архівів або додавання архіву (якщо файл з архівною копією вже існує) (Рис. 5.58).

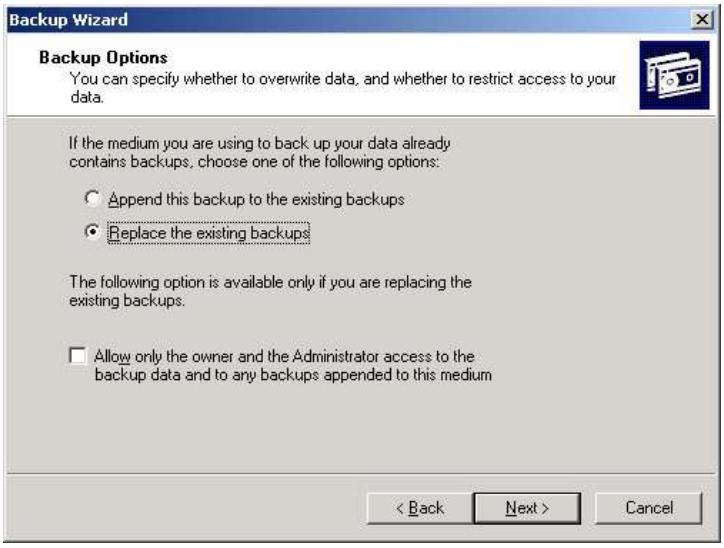


Рис. 5.58

10. На сторінці "Коли архівувати" задамо розклад для автоматичного створення резервної копії - виберемо варіант "Пізніше" і задамо розклад архівування (Рис. 5.59; Рис. 5.60).

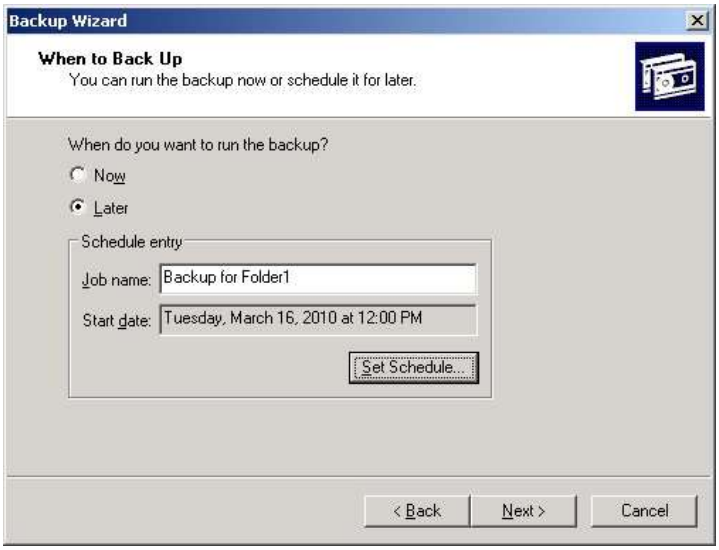


Рис. 5.59

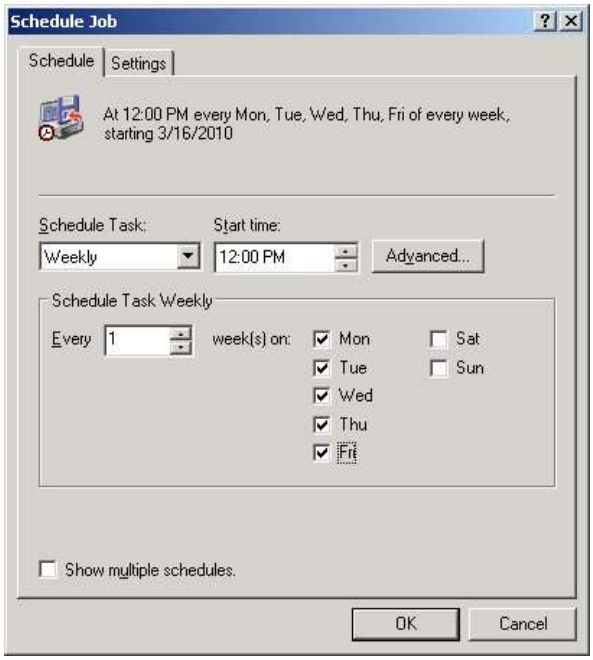


Рис. 5.60

11. Система запросить ім'я та пароль користувача, з чиїми повноваженнями буде виконуватися завдання архівації. Рекомендуємо для виконання завдань резервного копіювання створити спеціальні облікові записи, що володіють достатніми правами (як мінімум члени групи "Оператори архіву") (Рис. 5.61).

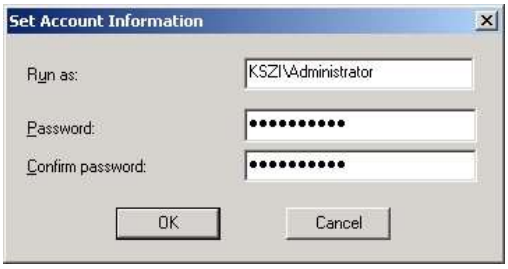


Рис. 5.61

12. Натиснемо кнопку "Finish", завдання буде створено, і воно з'явиться в списку "Призначених завдань". Тепер воно буде виконуватися регулярно відповідно до розкладу (Рис. 5.62; Рис. 5.63).

Рис. 5.62

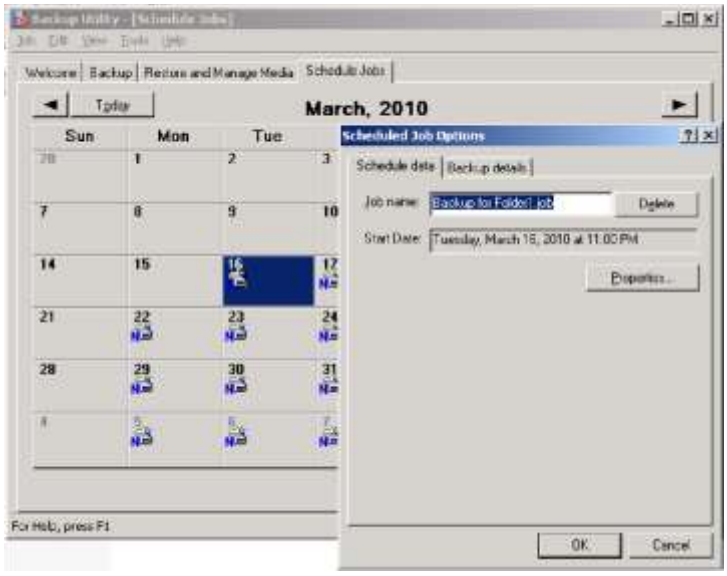


Рис. 5.63

Примітка. Дані прийоми архівування працюють тільки з файловими ресурсами. Для архівування інших видів ресурсів (наприклад, баз даних MS SQL Server) необхідно використовувати спеціалізовані механізми створення резервних копій.

Відновлення даних з резервної копії

Для відновлення даних у разі будь-якої аварії можна також створити завдання на автоматичне відновлення. Але зазвичай дані відновлюються вручну.

Розглянемо приклад відновлення кількох втрачених файлів з тієї ж папки Folder-1 (Рис. 5.64).

1. Запустимо утиліту резервного копіювання ntbackup. 2. Перейдемо на закладку "Відновлення і керування носієм".

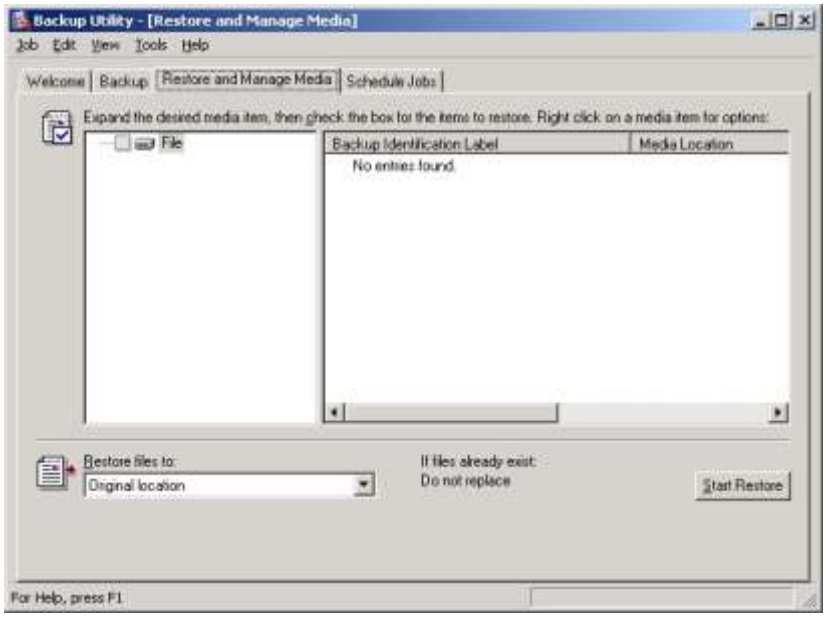


Рис. 5.64

3. Якщо в списку каталогізованих архівів немає потрібно архівного файлу, то його потрібно каталогізувати. Виберемо пункт меню "Tools" - "Catalog a backup file" і вкажемо шлях до архівного файлу (Рис. 5.65; Рис. 5.66).

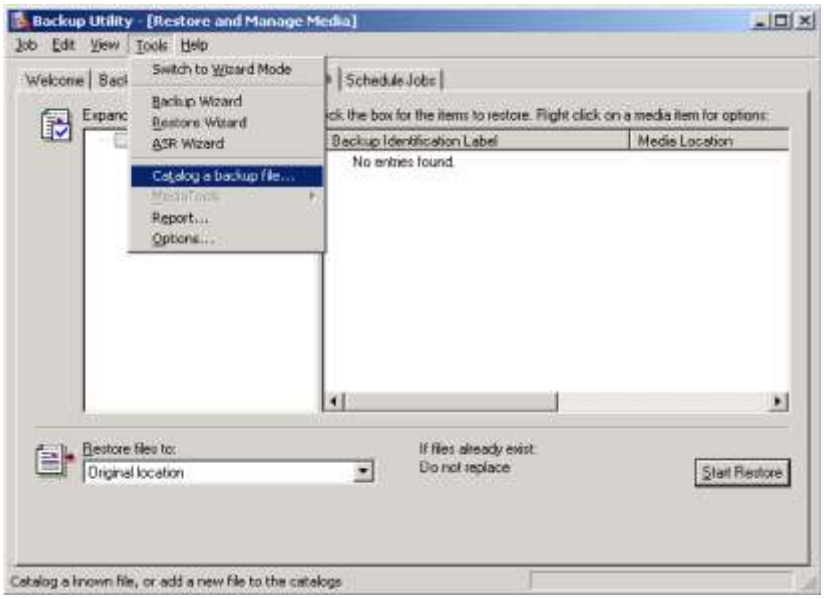


Рис. 5.65

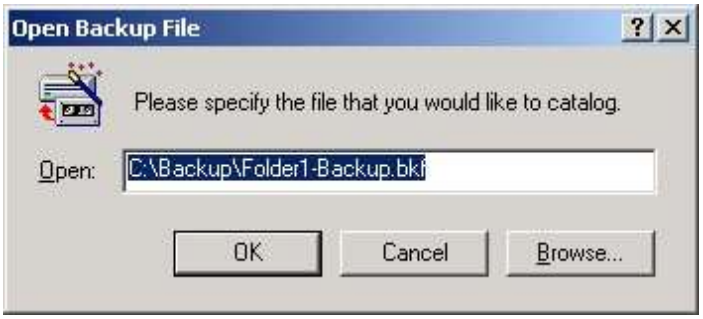


Рис. 5.66

4. Після появи в списку архівних файлів потрібного архіву розкриємо цей архів і виберемо файли для відновлення з резервної копії. При цьому ми можемо відновити файли в те місце, де вони були раніше ("Початкове розміщення") або вибрати інший шлях для їх збереження ("Альтернативне розміщення"). Після визначення всіх параметрів відновлення натиснемо кнопку "Відновити", загублені дані будуть відновлені (Рис. 5.67; Рис. 5.68):

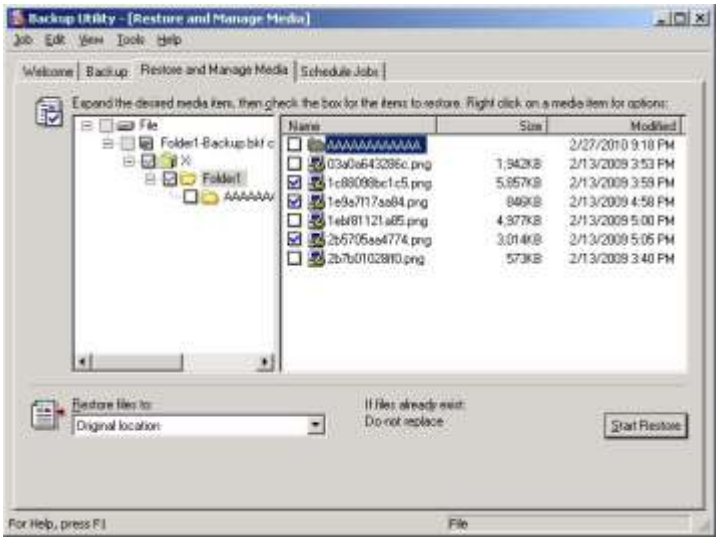


Рис. 5.67

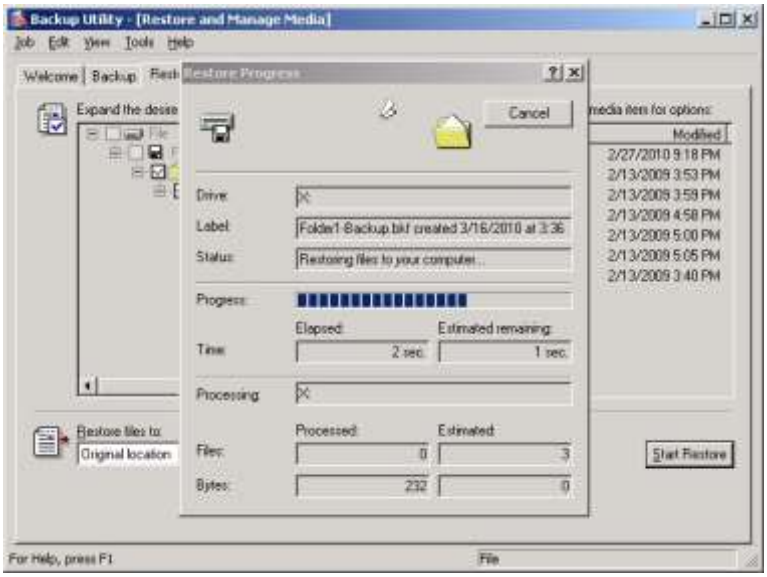


Рис. 5.68

5. Після відновлення можна вивчити звіт про виконання даної процедури (натиснути кнопку "Звіт") (Рис. 5.69):

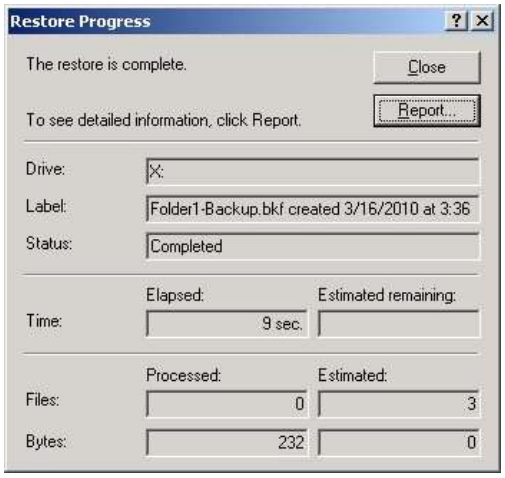


Рис. 5.69

Ступінь деталізації звіту можна налаштувати в меню "Сервіс" - "Параметри" - "Журнал архівації". При короткому зведенні в журналі реєструються тільки моменти початку і закінчення роботи утиліти ntbackup і кількість заархівованих або відновлених файлів, а також повідомлення про наявність помилок. При повному зведенні в журналі реєструється повний список всіх заархівованих або відновлених файлів. Журнали з реєстрацією останніх десяти процедур архівації/відновлення знаходяться в папці "% system drive%\Documents and Settings\Адміністратор\Local Settings\Application Data\Microsoft\Windows NT\NTBackup\data". Параметр "% system drive%" - це змінна оточення в системі Windows, значення якої - буква диска, на якому дана система встановлена. У даному прикладі вказаний обліковий запис "Адміністратор", насправді журнали будуть створюватися у профілях тих користувачів, від імені яких працювали завдання архівації / відновлення.

Архівація і відновлення стану системи

Більшу частину робіт з резервного копіювання складають завдання на копіювання бізнесінформації. Але є також можливість створення резервних копій для відновлення функціонування самої операційної системи. Є два варіанти архівування системних даних - архівування стану системи (System State) і створення набору для автоматичного відновлення системи після аварії (Automated System Recovery).

Для створення резервної копії стану системи необхідно в утиліті резервного копіювання ntbackup при створенні завдання на архівування відзначити галочкою пункт System State (Рис. 5.70):

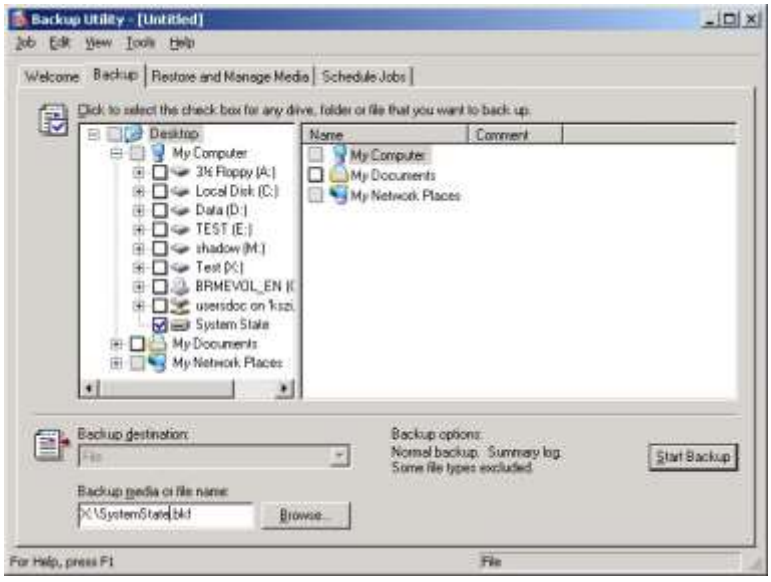


Рис. 5.70

При цьому будуть архівуватися наступні дані:

- системний реєстр;
- база даних зареєстрованих класів об'єктів (Class Registration);
- системні завантажувальні файли;
- база даних служб сертифікатів (тільки на серверах, на яких встановлена служба сертифікатів);
- база даних Active Directory і папка SYSVOL (на контролерах доменів).

Для архівування стану системи, а також для подальшого відновлення, обов'язково потрібні права адміністратора даного комп'ютера. Відновлення Active Directory необхідно виконувати тільки при завантаженні системи в режимі відновлення служб каталогів (запуск меню вибору режима завантаження операційної системи вибирається в початковий момент завантаження натисканням клавіші F8).

База даних Active Directory - це інформація, що відноситься до Каталогу, включаючи об'єкти і атрибути домену, схему, конфігурацію та інформацію Глобального Каталогу.

Базу даних Active Directory розглядають як транзакційну, що означає, що кожна зміна що в ній виконується, виконується як окрема транзакція (транзакція - неподільна операція, тобто поки обидві сторони, що беруть участь в транзакції, не завершать своєї частини її обробки, транзакція не вважається завершеною). Ця природа бази даних допомагає підтримувати її цілісність у разі збоїв. База даних Active Directory складається з декількох файлів:

- Ntds.dit - це файл бази даних, в якому зберігаються всі Об'єкти, за замовчуванням цей файл (та інші, вказані тут) розташований в папці "% systemroot% \ NTDS";
- Edb *. log - цей файл є журналом транзакцій; перш ніж будь-яка зміна буде записана в базу даних, інформація про неї спочатку заноситься в журнал транзакцій; кожен файл edb *. log

має розмір 10 МБ, за замовчуванням використовується "кругове" ведення журналу, тобто якщо журнал заповнений, то файл починає перезаписувати дані про самі старі зміни; якщо "кругове" ведення журналу відключено, то після заповнення файлу він перейменовується в файл edbxxxxx.log, з цифрами xxxxx, що представляють його порядковий номер, починаючи з 00001;

- Edb.chk - це файл контрольних точок, що використовуються AD для відстеження змін, які записуються в файл ntds.dit; він використовується для цілей відновлення (наприклад, якщо контролер домену пошкоджений і інформація про зміни не заноситься до бази даних, файл контрольних точок служить в якості маркера, який відзначає, які з записів у журналі повинні бути записані в базу даних у подальшому);
- Res1.log і Res2.log - є резервними файлами журналів, по 10 МБ кожен. Їх призначення - дозволити Active Directory продовжувати ведення журналу змін у разі, якщо на жорсткому диску не залишається вільного місця, тому в резерві завжди залишається 20 МБ вільного дискового простору, який використовується тільки у разі необхідності;

Автоматичне аварійне відновлення системи

На відміну від резервного копіювання стану системи, при якому зберігається лише частина файлів операційної системи, резервне копіювання для автоматичного аварійного відновлення системи (ASR, Automated System Recover) архівує більший обсяг інформації - практично весь той, на якому встановлена операційна система. І процедура відновлення системи стає більш складною.

Розглянемо спочатку процес створення резервної ASR-копії, а потім процес відновлення системи з цієї резервної копії.

Створення ASR-копії

На даному етапі буде потрібний носій для створення резервної копії системного тому (порядка декількох гігабайт), причому у випадку відновлення системи цей носій має бути доступний майстру установки операційної системи (тобто це або стрічковий накопичувач з драйверами для контролера і накопичувача, або дисковий накопичувач з відповідними драйверами), а також чиста відформатована дискета для збереження інформації про конфігурацію резервної копії. 1. Запустимо утиліту резервного копіювання ntbackup.

2. Запустимо "Automated System Recovery Wizard - Майстер аварійного відновлення системи" (кнопка з відповідною назвою на сторінці "Welcom") (Рис. 5.71).

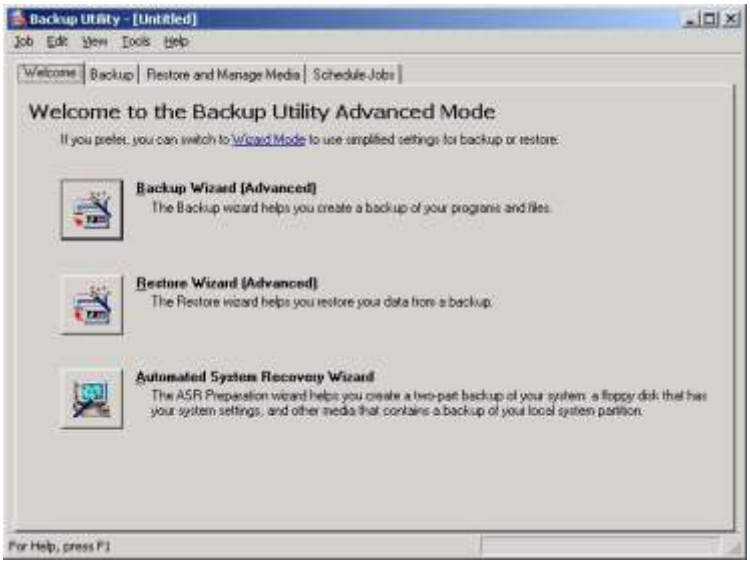


Рис. 5.71

2. Вкажемо шлях для збереження архіву (Рис. 5.72)

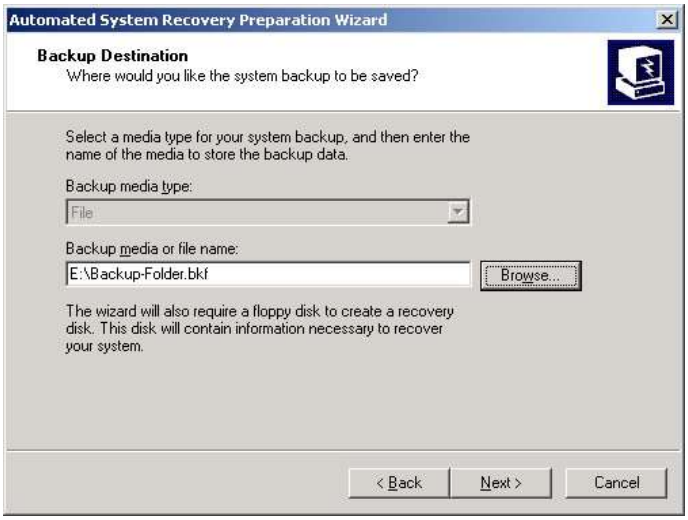


Рис. 5.72

Натиснути кнопку "Finish". Утиліта резервного копіювання почне створення резервної ASR-копії, в потрібний момент буде зроблено запит вставити чисту дискету. Після запису конфігурації резервної копії утиліта попросить помітити дискету з відповідною інформацією (назва резервної копії та дата створення).

Відновлення системи за допомогою ASR-копії

1. Підготовте все необхідне для аварійного відновлення системи: інсталяційний CD з дистрибутивом операційної системи, носій з резервною копією, дискету з конфігурацією ASR-копії.

2. Запустіть процес установки операційної системи з завантажувального компакт-диска.
3. На першій сторінці майстра установки системи натиснути клавішу F2 для запуску процесу аварійного відновлення.

Далі майстер установки системи виконає нову установку системи з форматуванням системного тома.

4. Після виконання установки операційної системи автоматично запуститься утиліта резервного копіювання, і система попросить вас вказати шлях до резервної копії для аварійного відновлення і вставити дискету з конфігурацією ASR-копії. Буде виконано відновлення системи з аварійної резервної копії.

Після завершення процесу відновлення буде відтворений працездатний сервер в тій конфігурації, яка була до аварії (за умови, звичайно, що, крім самої системи, будуть також відновлені, і дані, необхідні для роботи сервера).

Корпорація Microsoft рекомендує використовувати даний метод відновлення для серверів, що виконують особливі функції, які важко відновити простим встановленням заново і відновленням даних, наприклад, контролер домену, який є господарем операцій (Господар схеми, Господар іменування доменів та ін.) Якщо сервер не виконує будь-які особливі ролі, то Microsoft рекомендує на таких серверах архівувати лише дані, а в разі аварії заново перевстановити сервер, знову включити його в домен і відновити дані з резервних копій.

ПРАКТИЧНЕ ЗАВДАННЯ

1. Встановлення служби DHCP

- Перевірте чи встановлена служба DHCP на сервері, якщо немає встановіть її.

2. Авторизація сервера DHCP в Active Directory

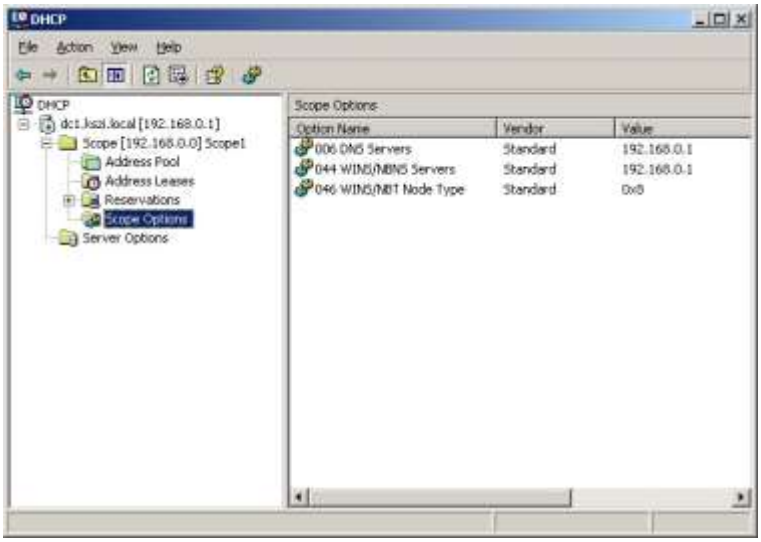
- Відкрийте консоль управління службою DHCP
- Клацніть правою кнопкою миші на імені вашого сервера - Виберіть "Авторизувати"
- Зачекайте, поки не закінчиться процес авторизації (на значку сервера колір індикатора повинен змінитися з червоного на зелений)

3. Створення області та налаштування параметрів сервера DHCP

- Створіть область на сервері DHCP з наступними параметрами: ○ ім'я області - Scope-1

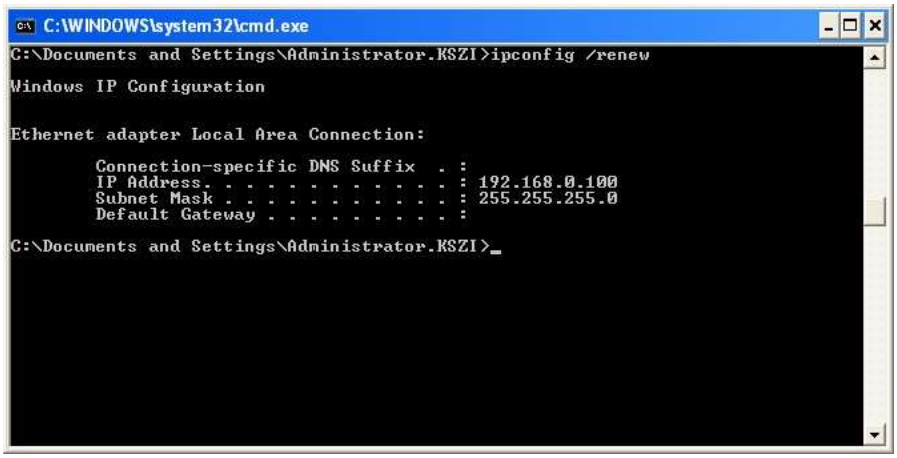
  ○ початковий і кінцевий IP-адреси вашого діапазону і маска підмережі - 192.168.0.1-192.168.0.100, маска підмережі - 24 біта ○ IP-адреса DNS-сервера - 192.168.0.1

- Вивчіть в консолі DHCP параметри створеної вами області
- Змініть параметри створеної вами області
- Додайте IP-адресу WINS-сервера - 192.168.0.1



4. Конфігурування клієнта для використання DHCP

- Для клієнта домену встановіть опцію "Автоматичне отримання IP-адреси" і "Автоматичне отримання адреси DNS-сервера" у властивостях TCP/IP протоколу
- У командному рядку виконайте команду ipconfig /renew (запит на нову оренду) щоб оновити адресу, що виділена для клієнта DHCP-сервером



- Перевірте працездатність мережі через Мережне оточення і утиліту ping командного рядка

5. Встановлення служби WINS

- Встановіть на сервері службу WINS

6. Налаштування клієнтської частини протоколу TCP/IP на використання служби WINS

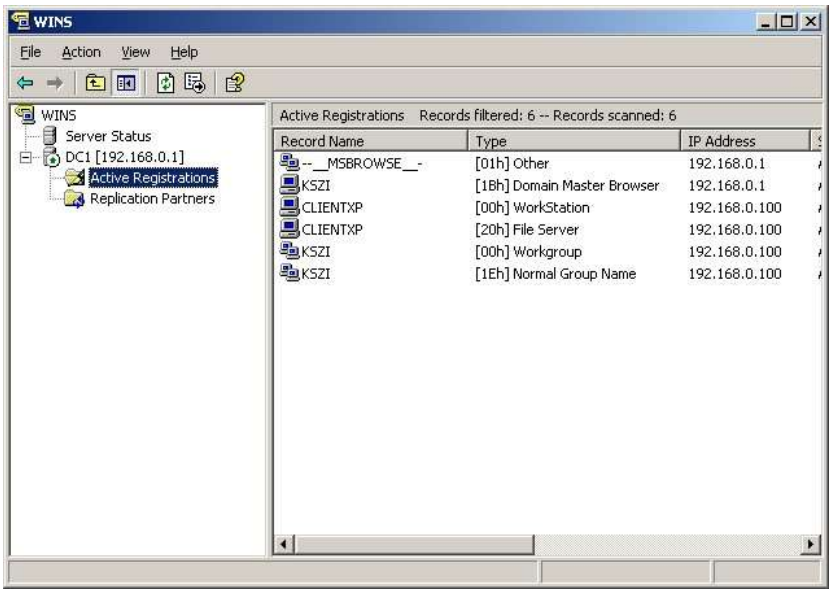
- для вузлів зі статичними IP-адресами: у властивостях протоколу TCP/IP на закладці "WINS" вкажіть IP-адресу WINSсервера 192.168.0.1
- для вузлів з динамічними IP-адресами:

додайте IP-адресу WINS-сервера - 192.168.0.1 у властивостях відповідної області сервера DHCP

7. Аналіз записів служби WINS

- Відкрийте консоль управління службою WINS
- Розкрийте інформацію про ваш сервер
- Клацніть правою кнопкою миші на "Активні реєстрації" - "Показати записи" - Кнопка "Знайти" - Виберіть мишею "Активні реєстрації"

- Вивчіть записи сервера WINS

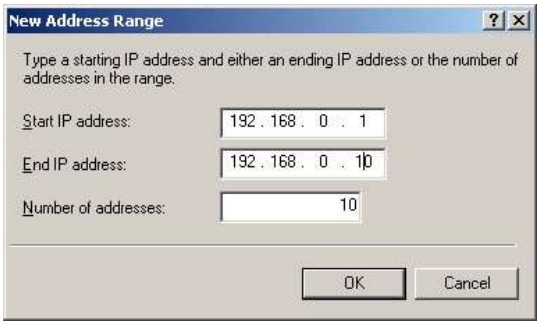


8. Увімкнення та настроювання служби маршрутизації та віддаленого доступу

- Відкрийте консоль "Routing and Remote Access":
  Кнопка "Start" - "All programs" - "Administrative Tools" - "Routing and Remote Access"
- Запустіть майстер настроювання служби:
  Клацнути правою кнопкою миші на імені сервера - Вибрати "Configure and Enable Routing and Remote Access" - Вибрати "Custom configuration" - Вибрати всі служби

9. Налаштування параметрів сервера і дозволів на підключення до сервера через Active Directory

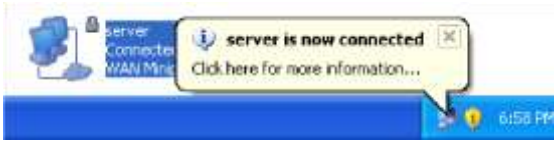
- Налаштуйте параметри сервера:
  Клацнути правою кнопкою миші на імені сервера - "Properties" - Закладка "IP" - Вибрати "Static address pool" - Кнопка "Add" - "Start IP" - ввести 192.168.0.1 - "End IP" - ввести 192.168.0.10



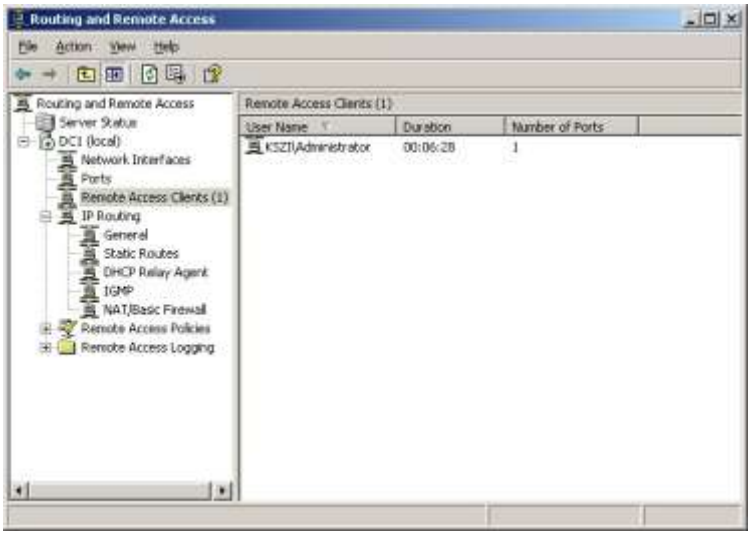
- Дозвольте користувачеві "Адміністратор" підключення до служби віддаленого доступу:
  Консоль "Active Directory Users and Computers" - Властивості користувача "Адміністратор" - Закладка "Dial-in" - Вибрати "Allow Access"

10. Налаштування та підключення клієнта віртуальної приватної мережі (VPN-клієнта)

- У цьому завданні наш сервер в домені буде виконувати роль сервера віддаленого доступу, клієнт буде VPN-клієнтом.
- Запустіть майстер налаштування клієнтських підключень у клієнта:
  Кнопка "Start" - "Control Panel" - "Network Connections" - "New connections Wizard"
- Налаштування клієнтського підключення:
  - Вибрати "Connect to the network at my workplase" ○ Вибрати "Virtual private network connection" ○ Ім'я підключення (введіть ім'я вашого сервера) ○ Вибір VPN-сервера (введіть IP-адресу сервера 192.168.0.1)
- Підключіться до сервера віддаленого доступу:
  У панелі підключення Введіть ім'я користувача і пароль - Кнопка "Connect" (система зробить підключення до сервера)



- Перевірте налаштування мережних інтерфейсів вашого комп'ютера: На обох серверах і клієнтах домену введіть у командному рядку команду
  ipconfig /all
  Вивчіть налаштування мережних інтерфейсів сервера
  На сервері, що виконує роль сервера віддаленого доступу, в консолі "Routing and Remote Access", в розділі "Remote Access Clients" вивчіть стан підключеного до вашого сервера комп'ютера

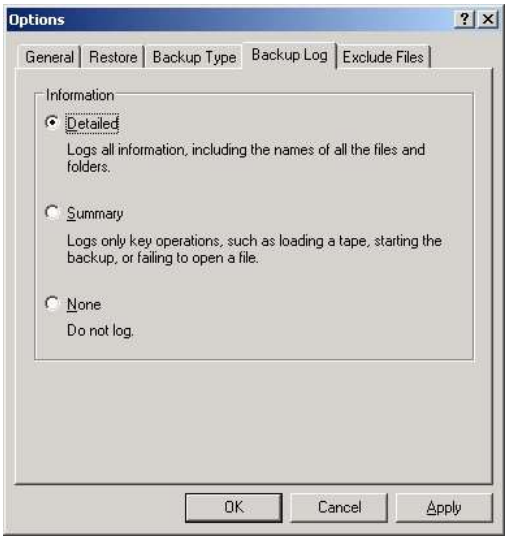


11. Запуск програми резервного копіювання і відновлення даних

- Запустіть програму резервного копіювання і відновлення даних: Кнопка "Start" - "Run" - "ntbackup"-Кнопка "ОК"
- На панелі, що відкрилась, прибрати галочку біля поля "Always start in wizard mode - Завжди запускати в режимі майстра" (якщо така сторінка з'явилася при запуску програми) - Кнопка "Cencel"

12. Налаштування параметрів програми резервного копіювання і відновлення даних

- Запустіть програму резервного копіювання і відновлення даних: Кнопка "Start" - "Run" - "ntbackup"-Кнопка "ОК"
- Налаштуйте параметри журналу архівації:
  Відкрийте меню "Tools" - "Options" - На закладці "Backup Log" - Встановіть тип інформації - "Detailed"



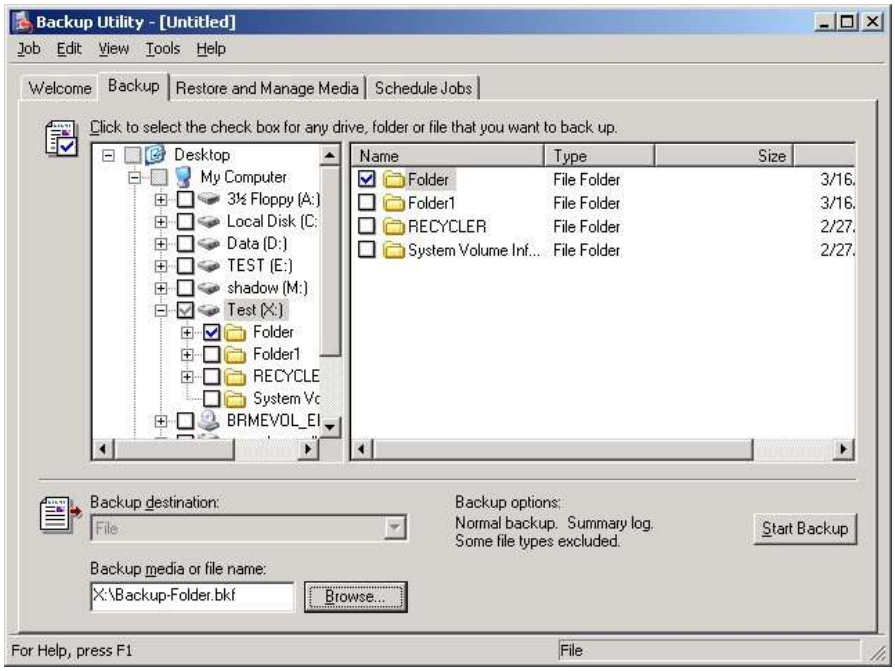
- Закрийте програму

13. Створення резервної копії папки з документами

- Запустіть програму резервного копіювання і відновлення даних - Вибрати дані для архівування:

  Закладка "Backup" - У лівій частині вікна виберіть папку для архівації (наприклад, папка X:\Folder)
- Виберіть місце для створення архіву:

  У полі "Backup Madia or file name - Носій архіву або ім'я файлу" вкажіть шлях та ім'я файлу архіву (наприклад, X:\Backup-Folder.bkf)
- Створіть резервну копію (Кнопка "Start backup")



- По закінченні процесу архівування вивчіть звіт про створення резервної копії: Кнопка "Звіт"
- Закрийте програму

14. Видалення документа з папки

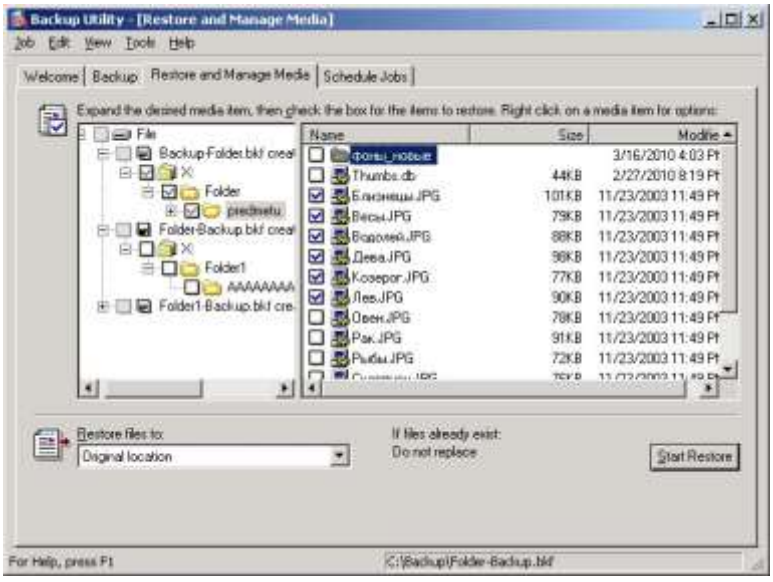
- Видаліть один з документів у тій папці, для якої була створена резервна копія (будь-який документ у папці X:\Folder)

15. Відновлення документа з резервної копії

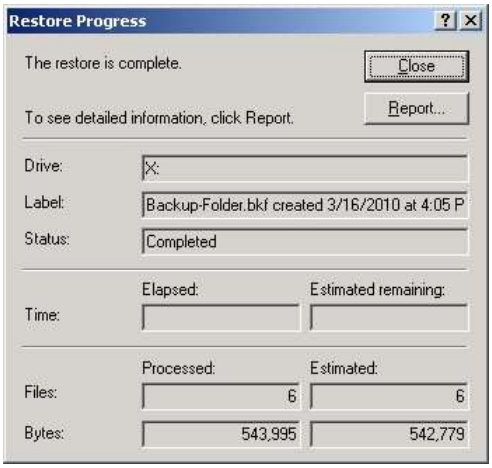
- Запустіть програму резервного копіювання і відновлення даних
- Відкрийте каталог резервної копії (Закладка "Відновлення і керування носієм")
  Якщо в правій частині вікна немає каталогу створеного архіву, то каталогізуйте створений вами архів
- Виберіть файл для відновлення:

У відкритому каталозі розкрийте папки до потрібного рівня, знайдіть і виберіть файл, який потрібно відновити (відновіть раніше видалений файл) - Виберіть місце для відновлення:

- У полі "Відновити файли в" виберіть "Початкове розміщення"
- Здійсніть відновлення



- Після закінчення процесу відновлення вивчіть звіт про архівування



- Закрийте програму
- Перевірте правильність відновлення файлу

16. Створення резервної копії стану системи

- Запустіть програму резервного копіювання і відновлення даних - Вибрати дані для архівування:

Закладка "Backup" - У лівій частині вікна виберіть System State -

Виберіть місце для створення архіву:

У полі "Носій архіву або ім'я файлу" вкажіть шлях та ім'я файлу архіву (наприклад, X:\System.bkf)

- Створіть резервну копію (Кнопка "Start Backup")

- По закінченні процесу архівування вивчіть звіт про створення резервної копії

- Закрийте програму