МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

КОМП’ЮТЕРНІ МЕРЕЖІ

Лабораторний практикум

для студентів спеціальності 122 "Комп’ютерні науки"
освітньої програми "Комп’ютерні науки"
першого (бакалаврського) рівня

Харків
ХНЕУ ім. С. Кузнеця
2023

УДК 004.7(07.034)
К63

Укладачі: С. В. Мінухін
В. П. Коцюба
Ю. В. Савін

Затверджено на засіданні кафедри інформаційних систем.
Протокол № 8 від 21.11.2022 р.

Самостійне електронне текстове мережеве видання

Комп'ютерні мережі [Електронний ресурс] : лабораторний
К63 практикум для студентів спеціальності 122 "Комп'ютерні науки" освітньої програми "Комп'ютерні науки" першого (бакалаврського) рівня / уклад. С. В. Мінухін, В. П. Коцюба, Ю. В. Савін. – Харків : ХНЕУ ім. С. Кузнеця, 2023. – 122 с.

Подано методичні рекомендації до виконання лабораторних робіт, метою яких є здобуття знань і набуття навичок щодо організації роботи комп'ютерної мережі засобами операційних систем, вивчення та налаштування служб для управління роботою мережі, організації поштового сервісу з використанням поштової клієнтської програми, організації служб для передавання та публікації файлів і документів. Розглянуто навчальний матеріал із проєктування та моделювання складної мережі засобами мережевого симулятора. Для кожної лабораторної роботи визначено мету, завдання, засоби та порядок виконання, зміст звіту й контрольні запитання.

Рекомендовано для студентів спеціальності 122 "Комп'ютерні науки" першого (бакалаврського) рівня.

УДК 004.7(07.034)

Вступ

Розвиток та сучасні тенденції сучасних інформаційних технологій супроводжуються збільшенням ролі інформаційно-комунікаційних систем різного призначення, що функціонують на підґрунті технологій комп'ютерних мереж. Це зумовлено потребою більш швидкого передавання інформації, у тому числі й управлінської, для якої важливе значення мають час та оперативність її доставки до користувачів. Вагомішим стає використання засобів і технологій, пов'язаних із застосуванням програмного забезпечення розподілених інформаційних систем (систем GRID), у яких велике місце займають комунікаційні технології та протоколи передавання даних, а також технології управління глобальними, корпоративними та локальними комп'ютерними мережами. Це пояснюється необхідністю використання інформації, яка міститься в базах даних, що можуть розташовуватися як в окремих підрозділах підприємств та установ, так і за їхніми межами.

Для підвищення ефективності функціонування комп'ютерних мереж потрібно створювати програмні засоби їх масштабування під час збільшення кількості робочих станцій та користувачів, а також транзакційного навантаження на серверні пристрої. Це приводить до необхідності більш детального вивчення та використання роботи пристроїв і відповідних стандартів для застосування технологій об'єднання окремих локальних мереж у складену. Вибір певного стеку протоколів мережі передбачає налаштування її роботи згідно з вибраними стандартами та протоколами: вибір і обґрунтування системного програмного мережного забезпечення під час застосування клієнт-серверної технології доступу та оброблення запитів між вузлами мережі; налаштування різних сервісів, що забезпечують роботу мережі; перевірку роботи мережі за допомогою діагностичних команд тощо.

З метою виконання цих завдань, отримання знань і набуття навичок у предметній області комп'ютерних мереж у лабораторному практикумі наведено лабораторні роботи, присвячені вивченню питань з підключення до локальної мережі; налаштування сервісів для управління роботою комп'ютерної мережі; налаштування поштового сервісу, зокрема поштового сервера та поштової клієнтської програми; проєктування та моделювання роботи складених комп'ютерних мереж за допомогою мережевого симулятора.

Лабораторна робота 1
Створення й діагностика роботи комп'ютерної мережі засобами ОС Windows. Організація віддаленого доступу

Мета лабораторної роботи: ознайомлення з принципами роботи локальної комп'ютерної мережі (КМ), створеної на основі операційних систем сімейства *Microsoft Windows* з використанням віртуальних машин (ВМ).

Порядок виконання роботи

Запустити гіпервізор *VMware Workstation Player*. Створити в ньому дві ВМ з *Windows XP Professional* та *Windows Server 2003 Enterprise Edition* (рис. 1). Образи для встановлення ВМ отримати у викладача.

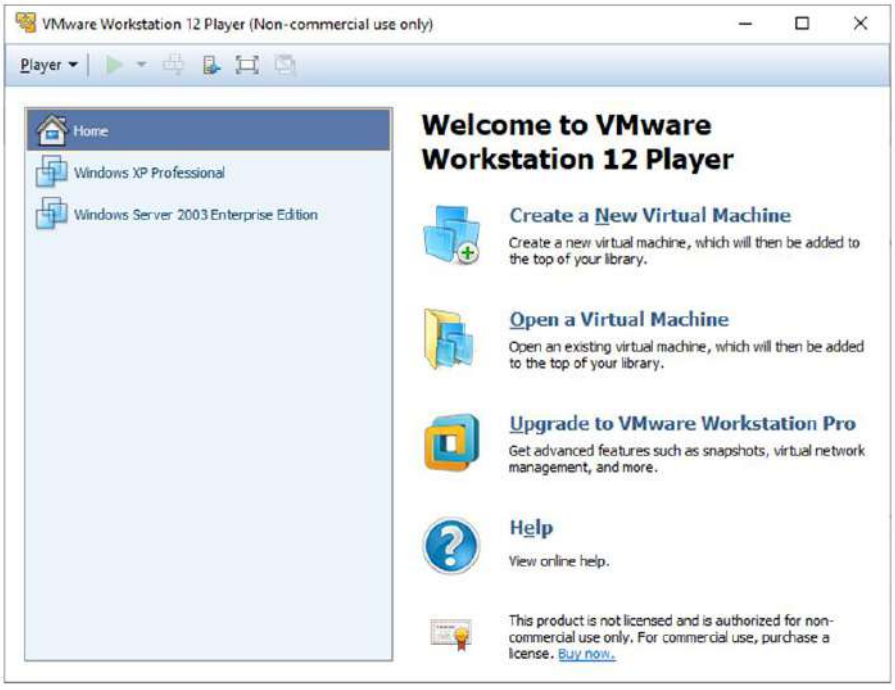

Рис. 1. **Основний екран VMware Workstation Player**

Установити для створених ВМ такі параметри (рис. 2 і 3):

- для параметра *Network adapter* значення *Host-only;*
- для параметра *Memory* значення 512 MB;
- для параметра *Hard Disk (IDE)* значення 15 GB.

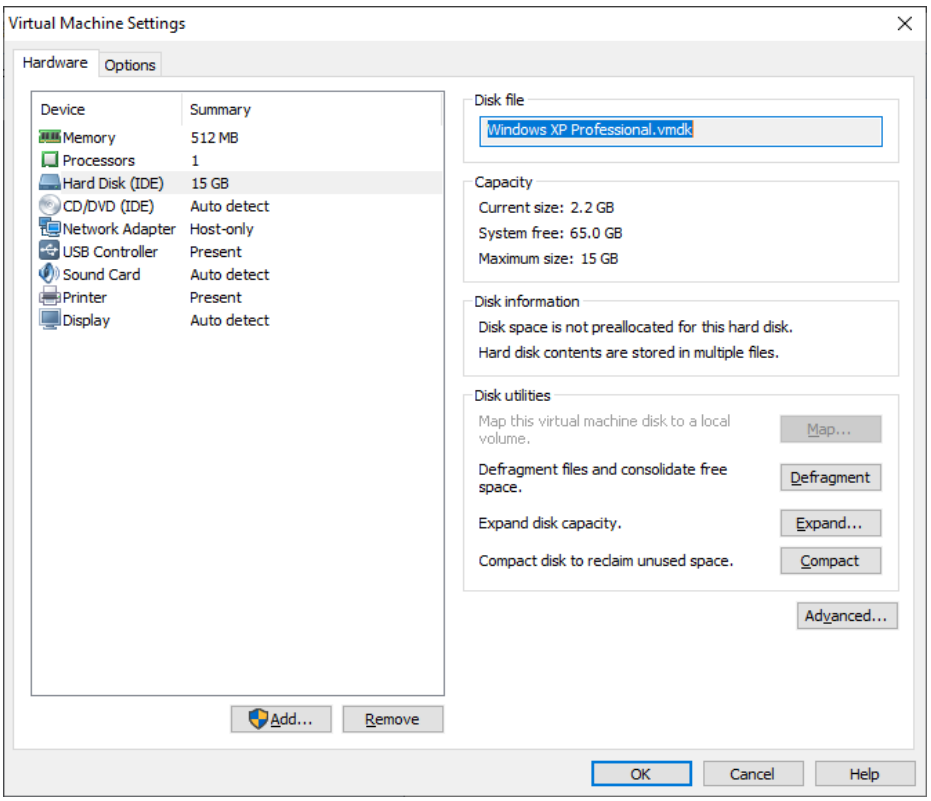

Рис. 2. **Налаштування ВМ з Windows XP Professional**

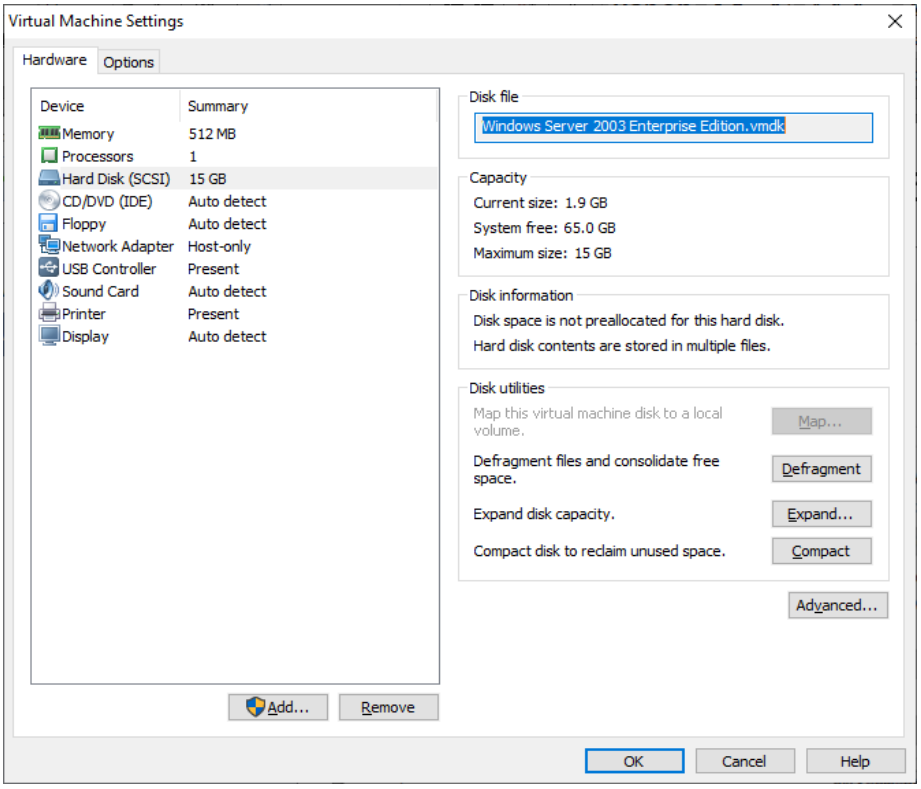

Рис. 3. **Налаштування ВМ з Windows Server 2003 Enterprise Edition**

Запускаємо ВМ з *Windows Server 2003 Enterprise Edition* кнопкою *Play virtual machine* (рис. 4).

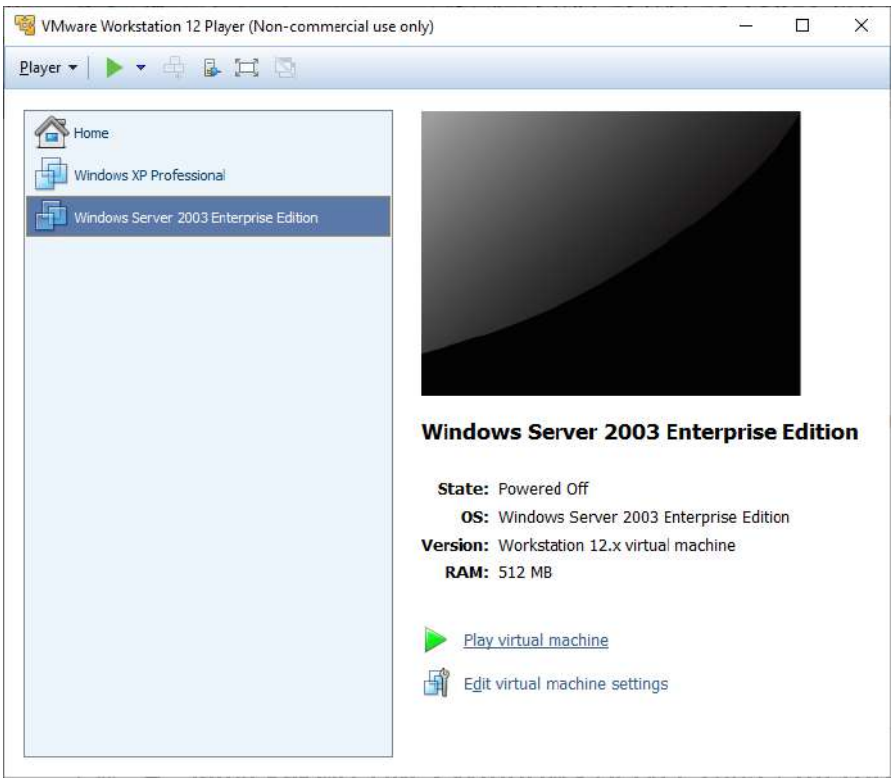

Рис. 4. **Запускаємо ВМ з Windows Server 2003 Enterprise Edition**

Заходимо в систему під обліковим записом *Administrator* та вводимо пароль, якщо його було створено (рис. 5).

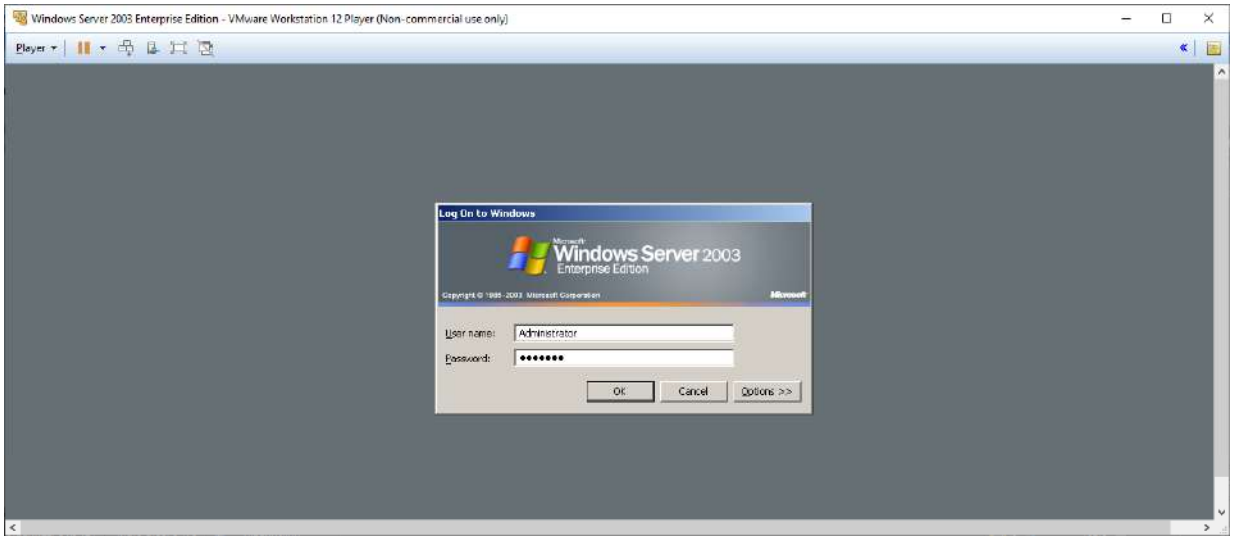

Рис. 5. **Вхід у систему**

Налаштування мережі у ВМ з Windows Server 2003 Enterprise Edition

Для цього переходимо в меню **Start -> Control Panel -> Network Connections -> Local Area Connection** (рис. 6).

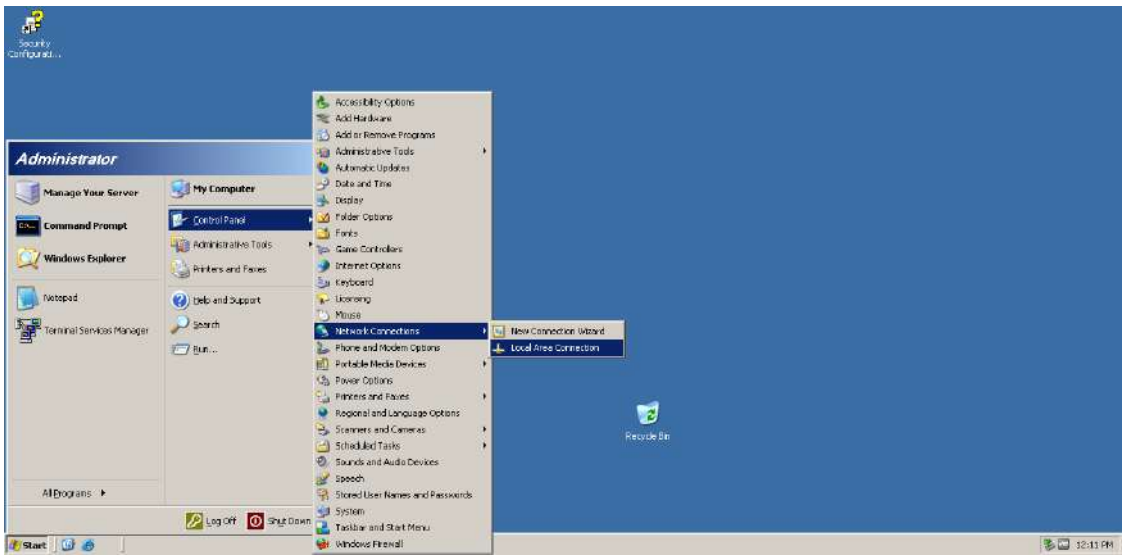

Рис. 6. **Налаштування мережевого адаптера на ВМ з Windows Server 2003 Enterprise Edition**

Переходимо кнопками меню **Properties -> Internet Protocol (TCP/IP) -> Properties**. У відчиненому вікні задаємо IP-адресу: **192.168.1.1** та маску підмережі: **255.255.255.0** (рис. 7). Маска підмережі відповідає мережі класу С.

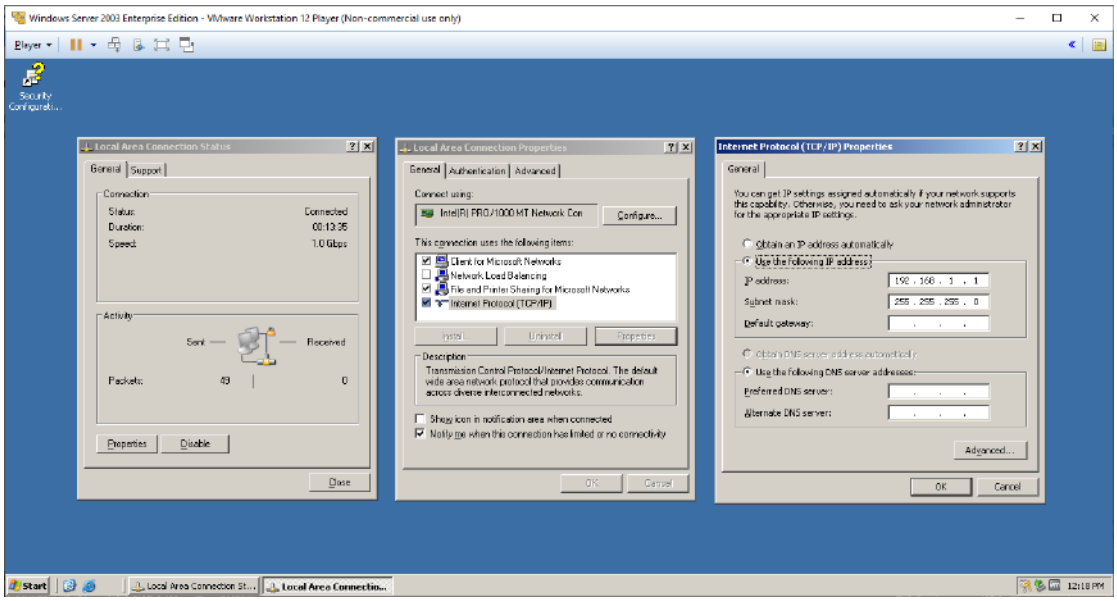

Рис. 7. **Налаштування IP-адреси та маски підмережі на ВМ з Windows Server 2003 Enterprise Edition**

Приймаємо зроблені зміни, натискаючи кнопку **ОК**. Повертаємося до вікна **Local Area Connection Properties**. Вибираємо вкладку **Advanced** та заходимо в налаштування **Windows Firewall**, натискаючи кнопку **Settings**. Умикаємо **Windows Firewall**, вибираючи пункт **On** (рис. 8).

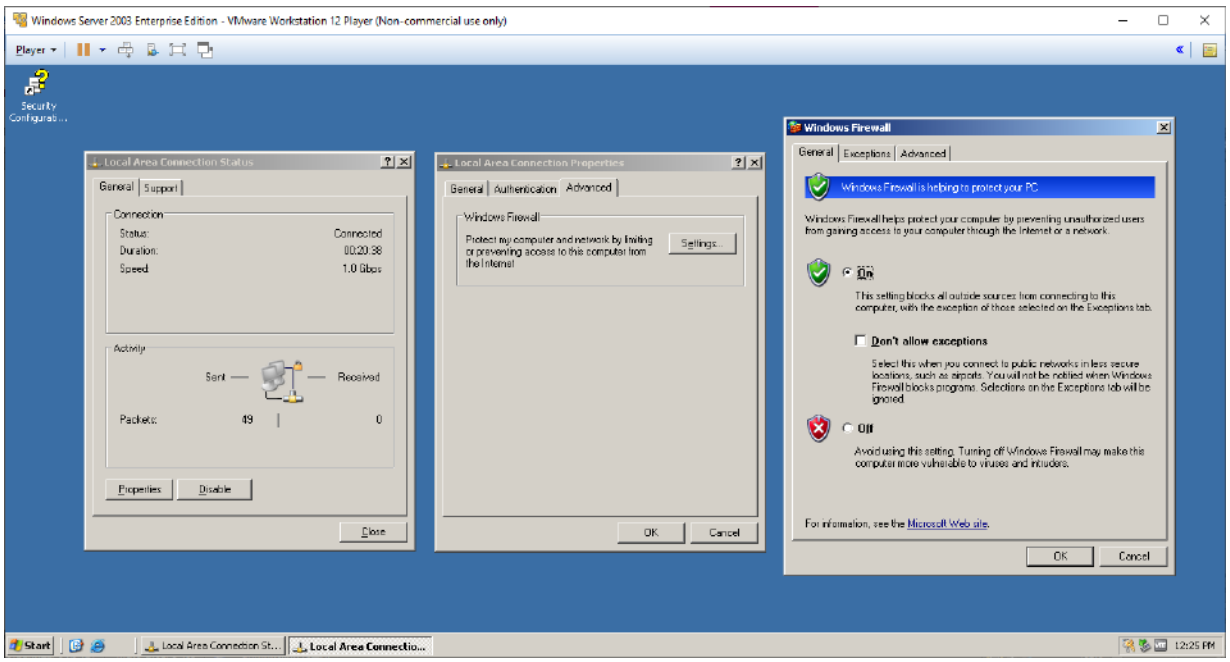

Рис. 8. **Увімкнення Windows Firewall**

Переходимо до вкладки **Exceptions**. У розділі **Program and Services** вибираємо пункти **File and Printer Sharing** та **Remote Desktop** (рис. 9).

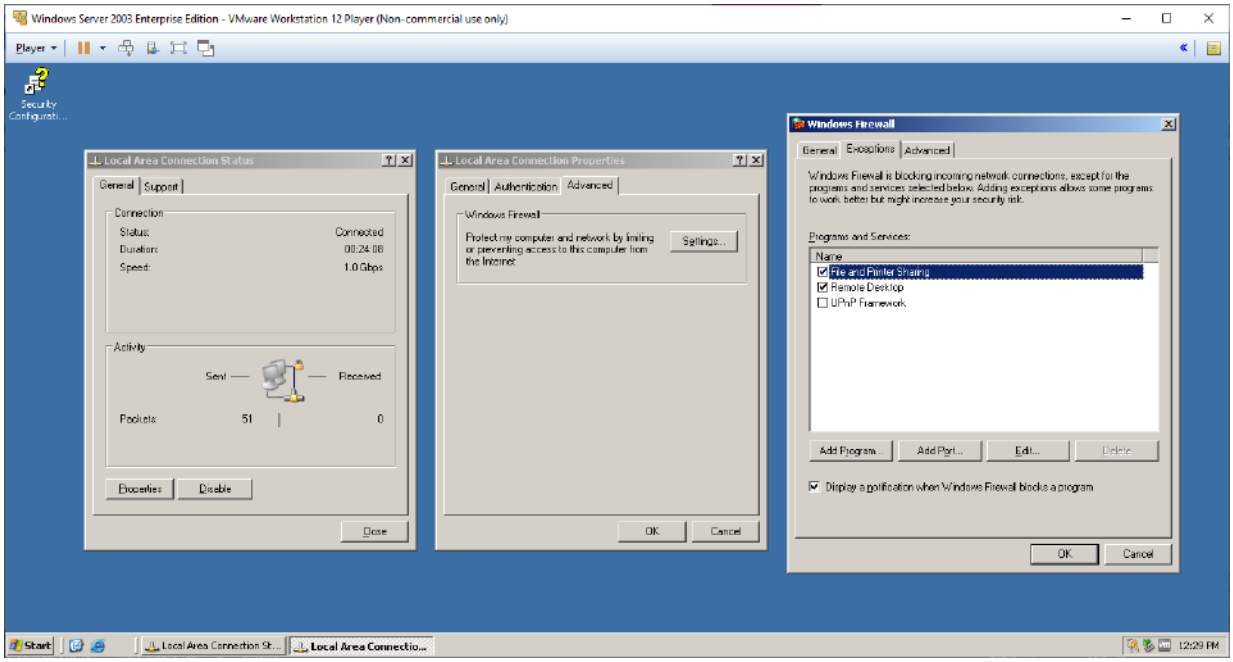

Рис. 9. **Налаштування дозволу на роботу із загальними ресурсами та віддаленим доступом**

У вкладці **Advanced** цього вікна вибираємо пункт **ICMP**, натискаючи кнопку **Settings**. Дозволяємо роботу з вхідними *echo*-запитами (рис. 10).

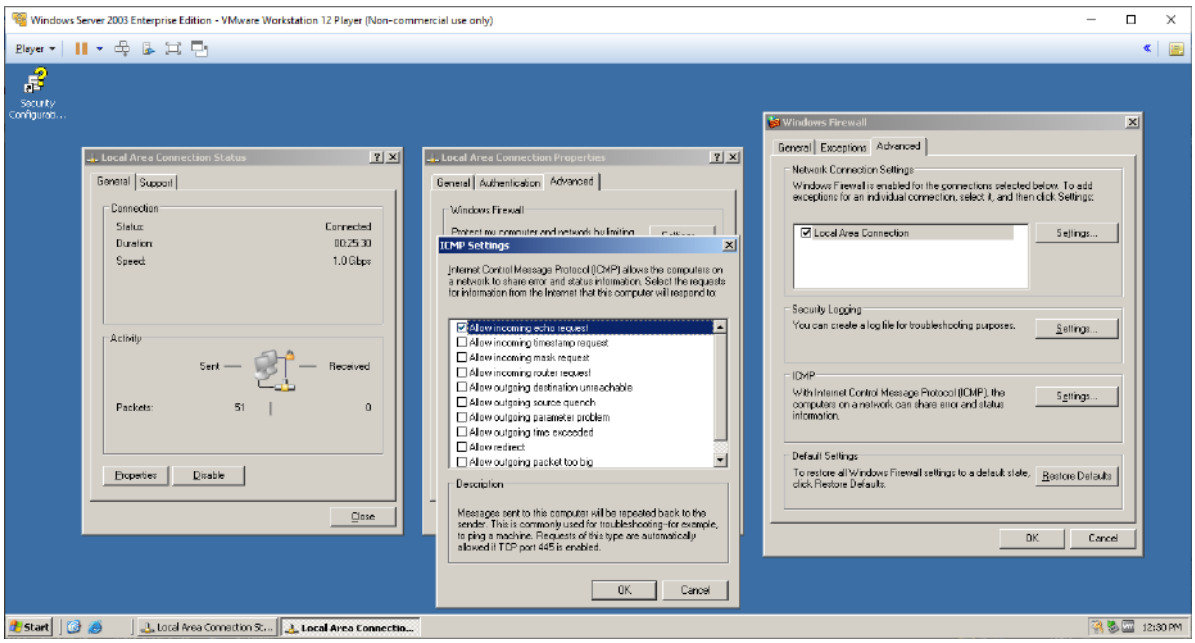

Рис. 10. **Налаштування дозволу на роботу з вхідними echo-запитами**

Приймаємо виконані зміни, натискаючи на кнопки **OK** та **Close**.

Переходимо до налаштувань імені та опису робочої станції (PC), а також перевірки імені робочої групи. Для цього заходимо в меню **Start** і натискаємо праву кнопку мишки на пункті **My Computer**. У меню, що відкриється, вибираємо пункт **Properties** (рис. 11).

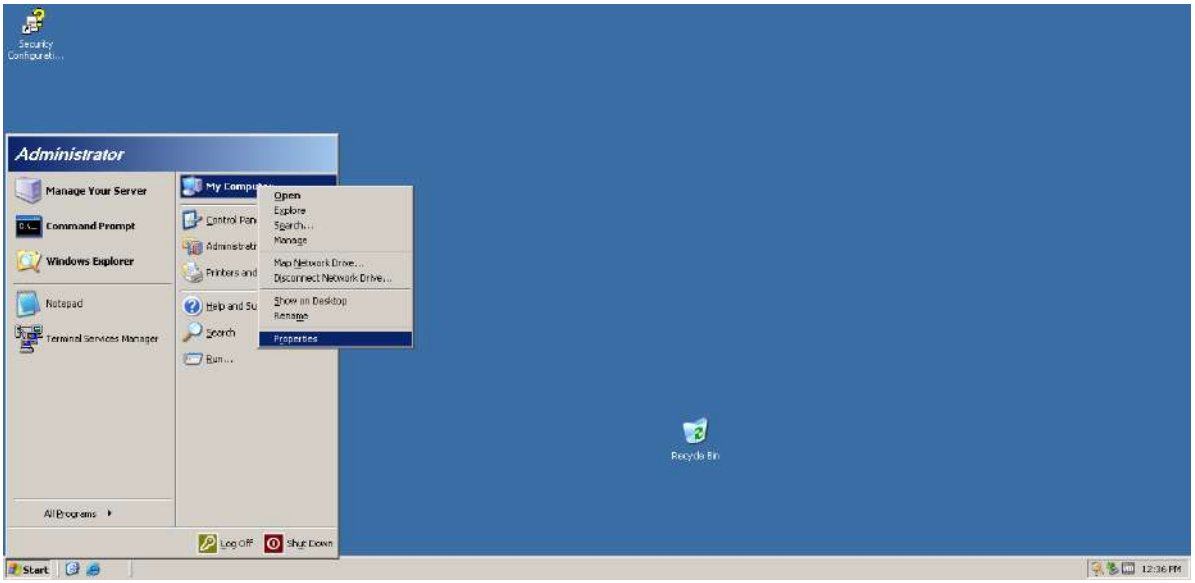

Рис. 11. **Вхід до вікна властивостей системи**

У вікні, що відкриється, вибираємо пункт **Computer Name**. У рядок **Computer description** вписуємо: **Server 2003**. Переходимо далі, натискаючи кнопку **Change**, де задаємо **Computer name**: **Server** та перевіряємо встановлену робочу групу: **WORKGROUP** (рис. 12).

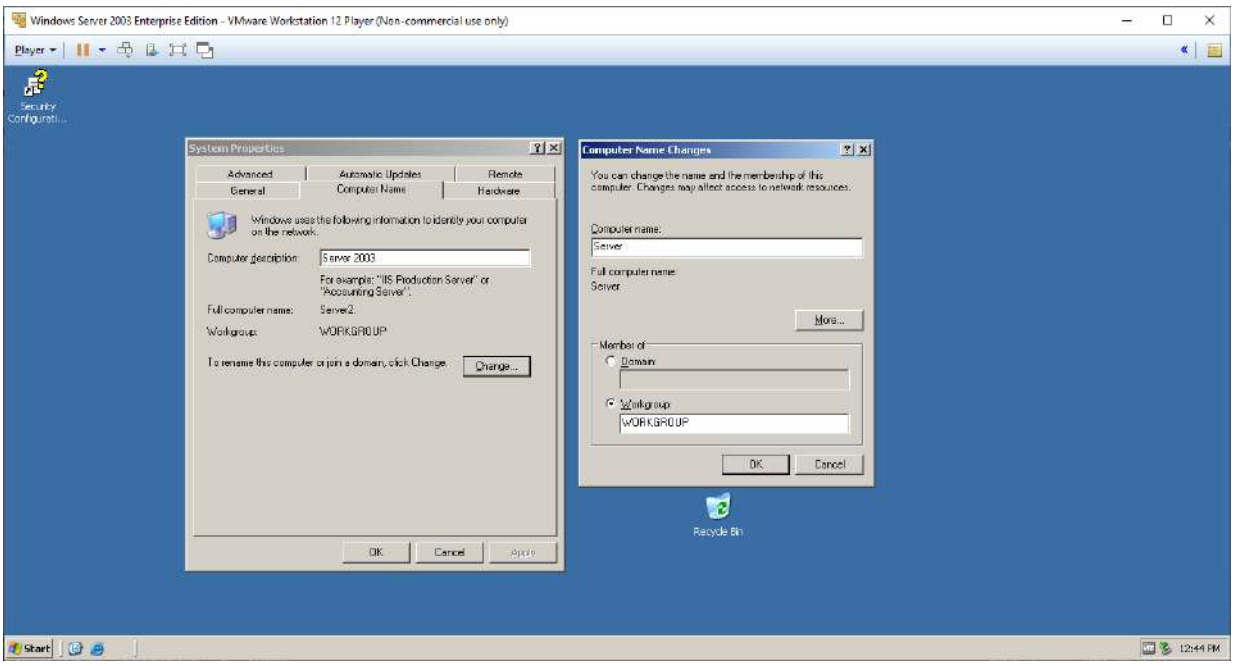

Рис. 12. **Налаштування опису, імені комп’ютера та робочої групи**

Перевіряємо введені значення та зберігаємо їх, натискаючи кнопку **ОК**. З’явиться попередження, що після перезавантаження РС зміни буде прийнято. Погоджуємося, натискаючи кнопку **ОК** (рис. 13).

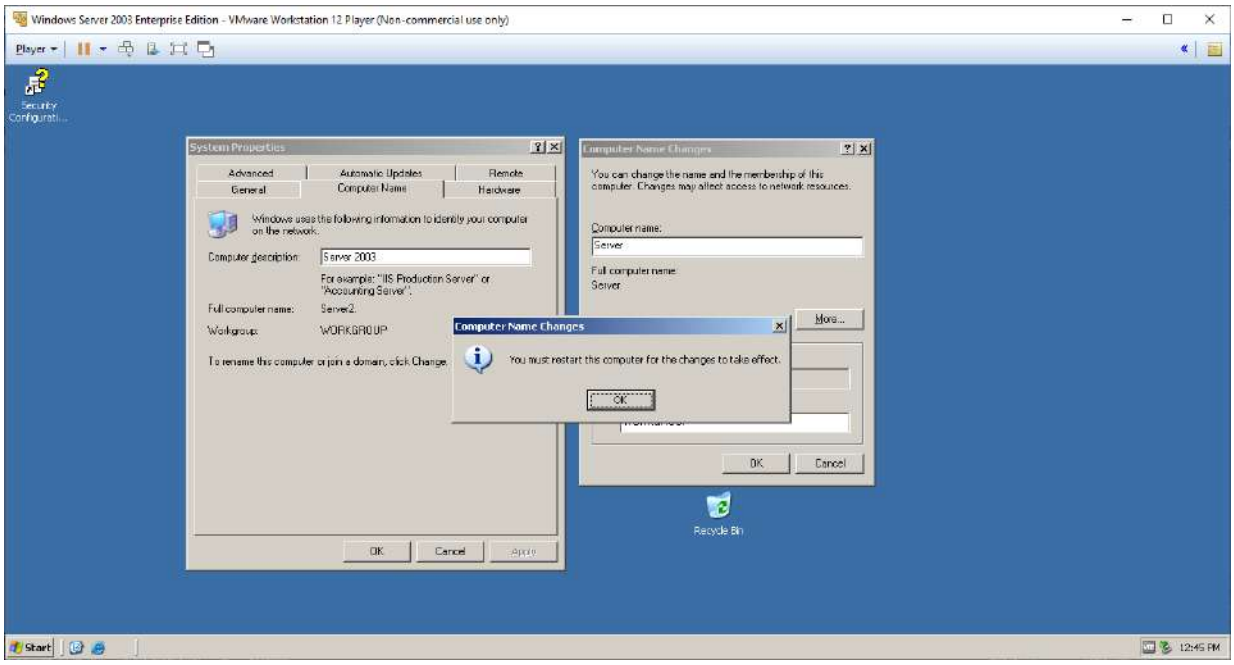

Рис. 13. **Попередження та погодження про прийняття змін**

У вікні **System Properties** застосовуємо зроблені зміни, натискаючи кнопку **Apply**. Виходимо з вікна **System Properties**, натискаючи кнопку **ОК** (рис. 14).

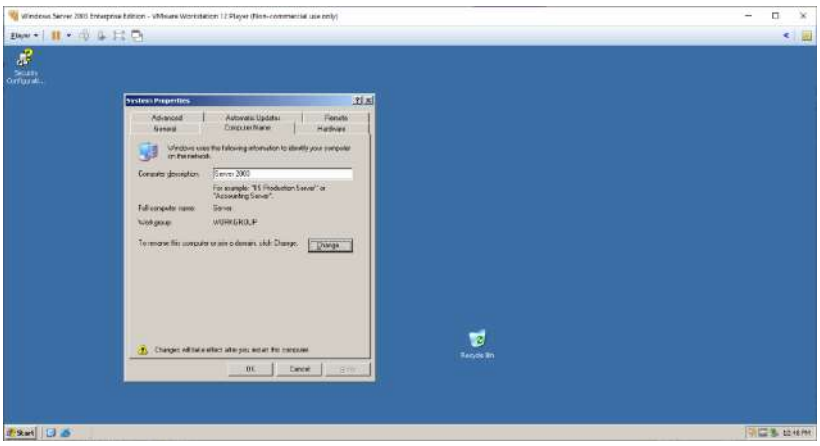

Рис. 14. **Вікно властивостей системи**

Далі треба перезавантажити РС для застосування виконаних змін (рис. 15).

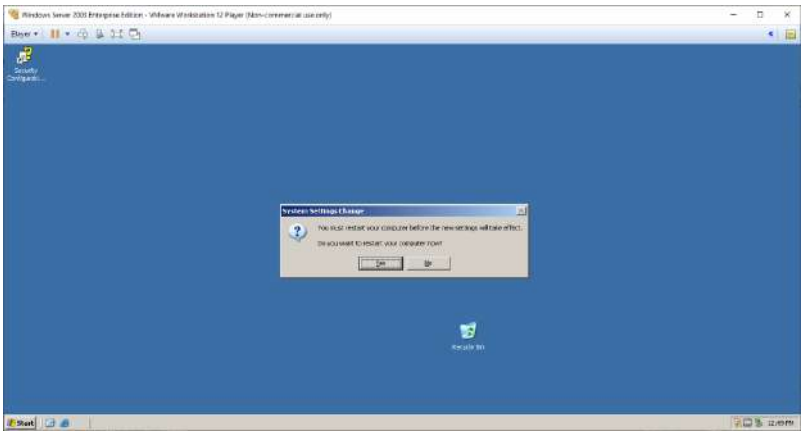

Рис. 15. **Перезавантаження РС для застосування змін**

На цьому налаштування мережі у ВМ з *Windows Server 2003 Enterprise Edition* можна вважати закінченим.

Налаштування мережі у ВМ з Windows XP Professional

Запускаємо ВМ з *Windows XP Professional* кнопкою **Play virtual machine** (рис. 16). Переходимо до налаштувань мережевого адаптера на *Windows XP Professional*. Для цього переходимо в меню **Start -> Connect to -> Show All Connections** (рис. 17). У вікні, що відкриється, треба навести покажчик мишки на пункт **Local Area Connection** та натиснути на праву кнопку. У меню, що відкриється, вибираємо пункт **Properties** (рис. 18). У вікні, що відкриється, вибираємо **Internet Protocol (TCP/IP)** та натискаємо кнопку **Properties**. У відчиненому вікні задаємо IP-адресу: **192.168.1.XX**, де **XX** – число, що дорівнює сумі числа 10 та числа, яке відповідає номеру студента в журналі групи.

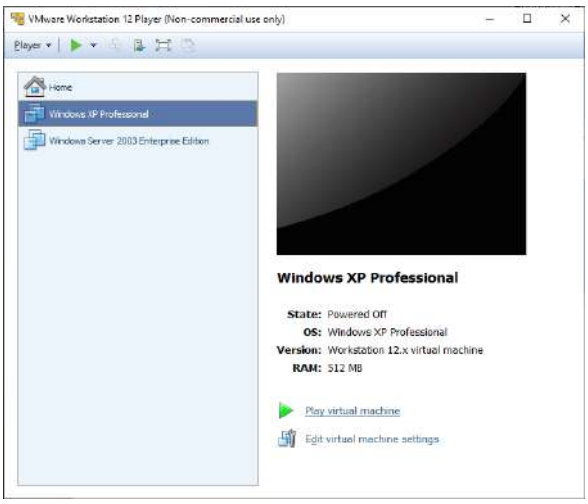

Рис. 16. **Запуск ВМ з Windows XP Professional**

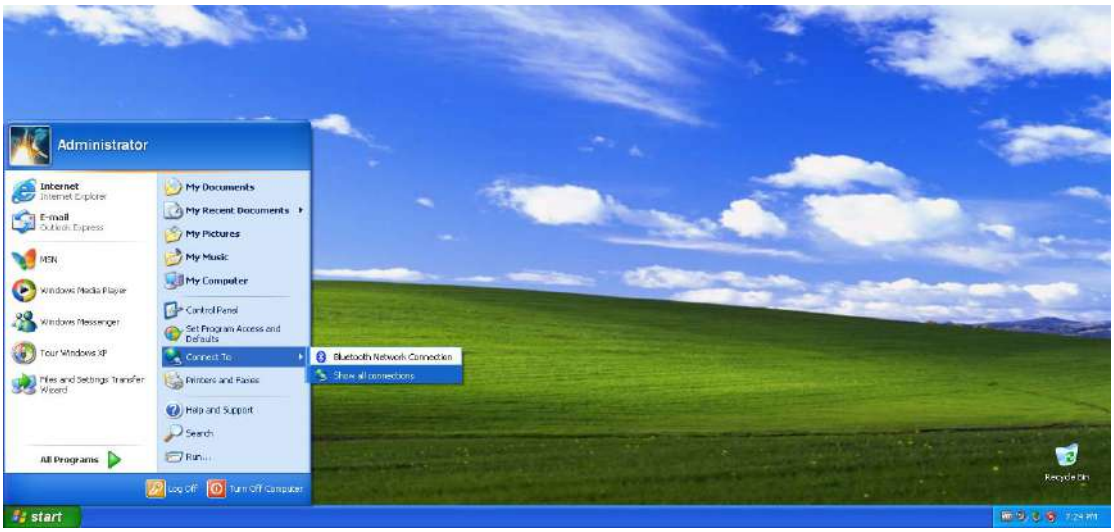

Рис. 17. **Налаштування мережевого адаптера на ВМ з Windows XP Professional**

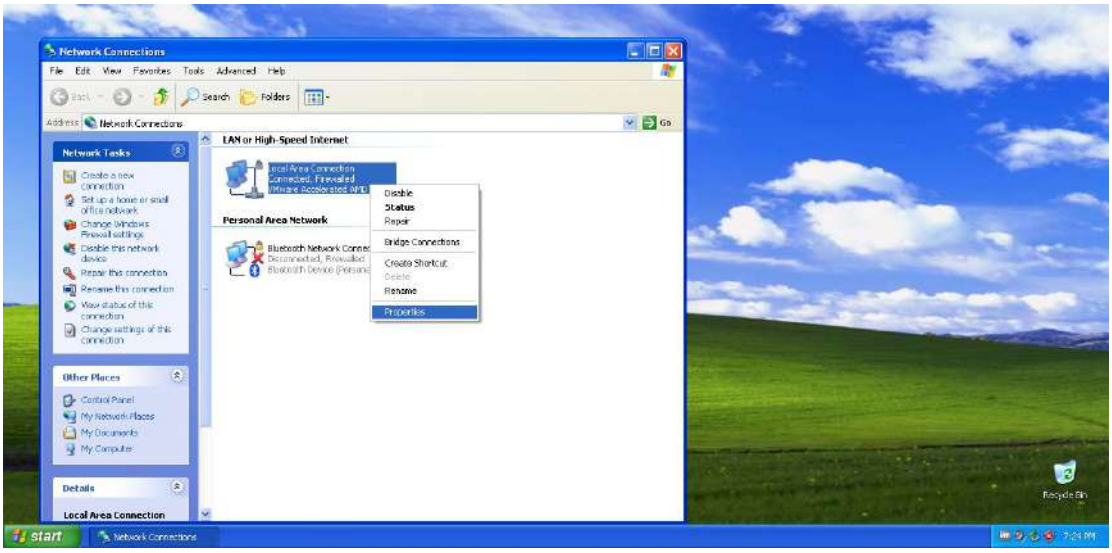

Рис. 18. **Відкриття вікна властивостей мережевого адаптера**

Установлюємо маску підмережі – **255.255.255.0**, яка відповідає мережі класу С. Установлюємо шлюз за замовчуванням. У створеній мережі шлюзом є вузол *Windows Server 2003 Enterprise Edition*. Тому в цей розділ треба вписати його IP-адресу – **192.168.1.1** (рис. 19).

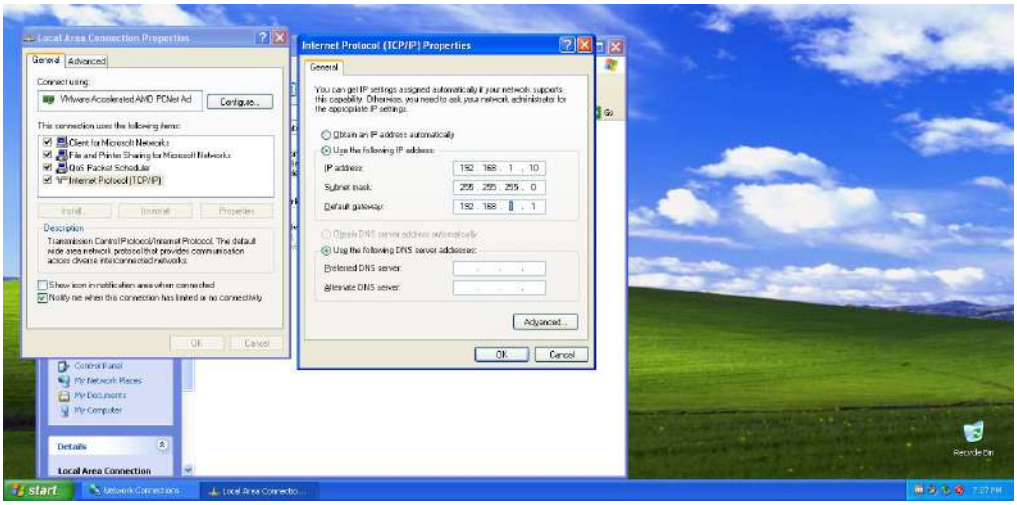

Рис. 19. **Налаштування IP-адреси, маски підмережі та шлюзу за замовчуванням**

Зберігаємо налаштування, натискаючи кнопку **ОК**. Переходимо до налаштування *Windows Firewall*. Відкриваємо вкладку **Advanced** і натискаємо кнопку **Settings** (рис. 20). У вікні, що відкриється, умикаємо *Windows Firewall*, вибираючи пункт **On**.

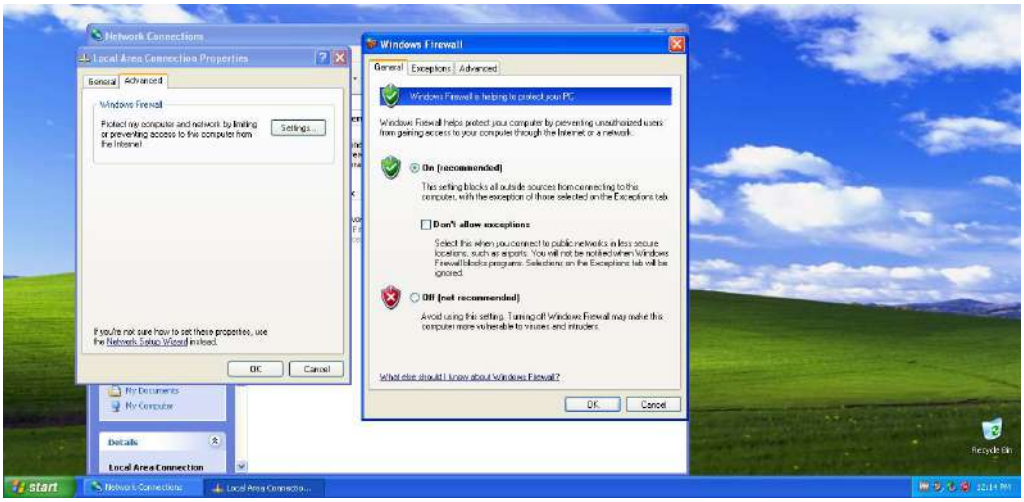

Рис. 20. **Ввімкнення Windows Firewall**

Переходимо до вкладки **Exceptions**. У розділі **Program and Services** вибираємо пункти **File and Printer Sharing** та **Remote Desktop** (рис. 21).

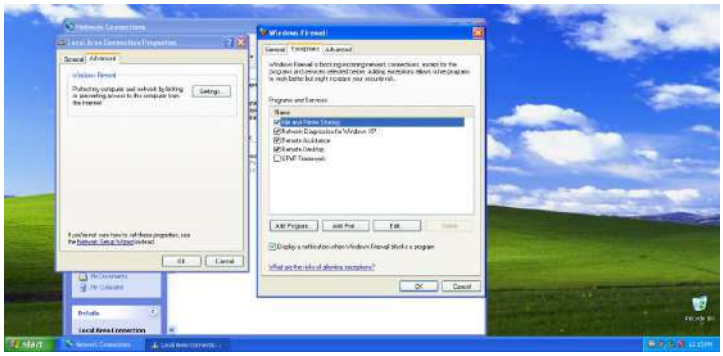

Рис. 21. **Налаштування дозволу на роботу із загальними ресурсами та віддаленим доступом**

У вкладці **Advanced** цього вікна вибираємо розділ ICMP, натискаючи кнопку **Settings** і дозволяємо роботу з вхідними echo-запитами, вибираючи пункт **Allow incoming echo request** (рис. 22). Приймаємо виконані зміни, натискаючи на кнопки **OK** та **Close**.

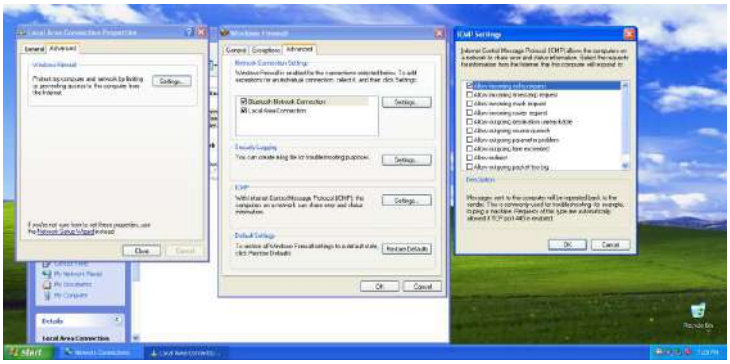

Рис. 22. **Налаштування дозволу на роботу з вхідними echo-запитами**

Переходимо до налаштувань імені та опису PC, а також перевірки імені робочої групи. Для цього заходимо в меню **Start** і натискаємо праву кнопку мишки на пункті **My Computer**. У меню, що відкриється, вибираємо пункт **Properties** (рис. 23).

Рис. 23. **Вхід до вікна властивостей системи**

У вікні, що відкриється, вибираємо пункт **Computer Name** (рис. 24).

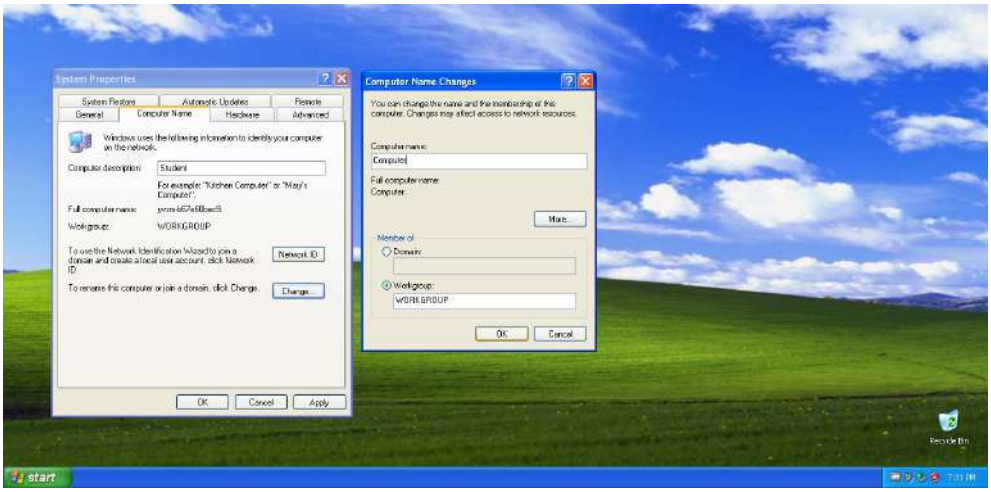

Рис. 24. **Налаштування опису, імені та робочої групи**

У рядок **Computer description** вписуєте: **ваше прізвище (латиницею)**. Переходимо у вікно **Computer Name Change**, натискаючи кнопку **Change**. У рядок **Computer name** вписуємо: **ComputerXX**, де **XX** – відповідає номеру студента в журналі групи. Вибираємо пункт **Workgroup** та вписуємо в рядок робочу групу: **Workgroup**. Перевіряємо введені значення та зберігаємо їх, натискаючи кнопку **ОК**. З'явиться попередження про перезавантаження РС для застосування введених змін. Погоджуємося, натискаючи кнопку **ОК** (рис. 25).

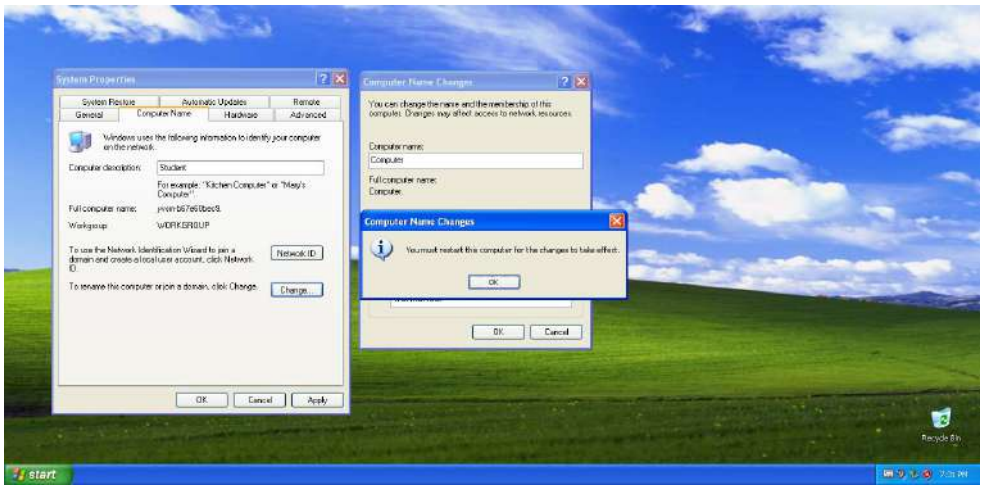

Рис. 25. **Попередження про прийняття та застосування змін**

У вікні **System Properties** застосовуємо зроблені зміни, натискаючи кнопку **Apply**. Закриваємо вікно **System Properties**, натискаючи кнопку **ОК**. Перезавантажуємо РС для прийняття зроблених змін (рис. 26). На цьому налаштування мережі у ВМ з *Windows XP Professional* закінчено.

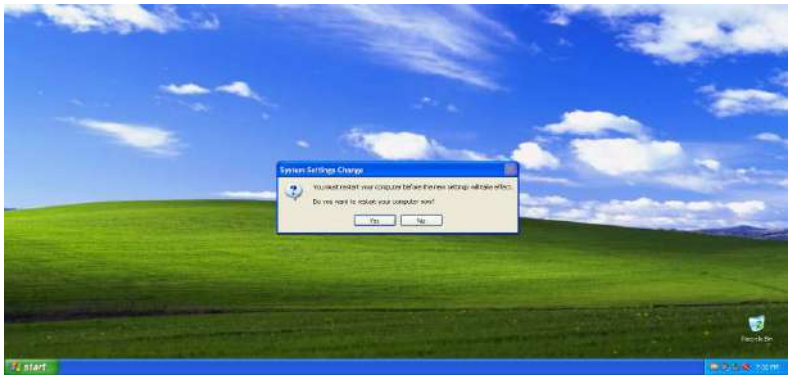

Рис. 26. **Перезавантаження РС для застосування змін**

Діагностика роботи налаштованих РС Windows XP Professional та Windows Server 2003 Enterprise Edition у локальній КМ

Команди, які використовують для діагностики роботи локальної КМ, слід виконувати у вікні командного рядка. Для виклику цього вікна потрібно вибрати: меню **Start -> Command Prompt**. На обох РС це вікно буде викликатись однаково (рис. 27 і 28).

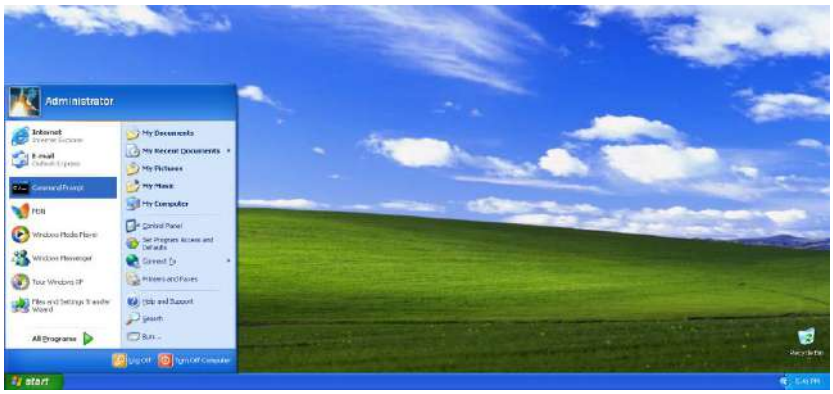

Рис. 27. **Виклик вікна Command Prompt на РС з Windows XP Professional**

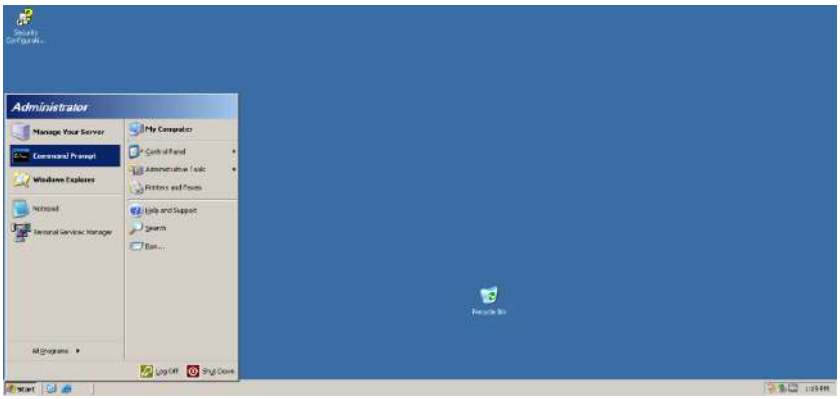

Рис. 28. **Виклик вікна Command Prompt на РС з Windows Server 2003 Enterprise Edition**

Перелік команд, що використовують для діагностики роботи РС у локальній КМ, наведено в табл. 1.

Таблиця 1

Команди діагностики для перевірки роботи мережі

Команда	Призначення
ping	Перевірка фізичного зв'язку з іншими РС мережі та працездатності мережевого адаптера
ipconfig	Отримання інформації про параметри мережевих налаштувань ОС
ipconfig /all	Отримання всіх параметрів мережевих налаштувань ОС
route PRINT	Отримання інформації про налаштування маршрутизації ОС
net view	Отримання інформації про всі РС робочої групи, до якої належить РС
net name	Отримання імені РС, на яке можливо відправити повідомлення в мережі
net send	Відправлення однобічних повідомлень на інші РС у мережі

Перевіряємо мережевий зв'язок між обома налаштованими РС командою **ping** (рис. 29 і 30).

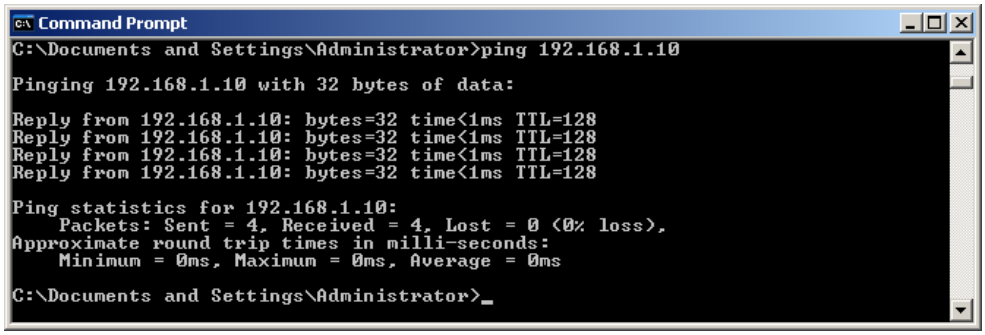

Рис. 29. **Результат виконання команди ping на ВМ з Windows Server 2003 Enterprise Edition**

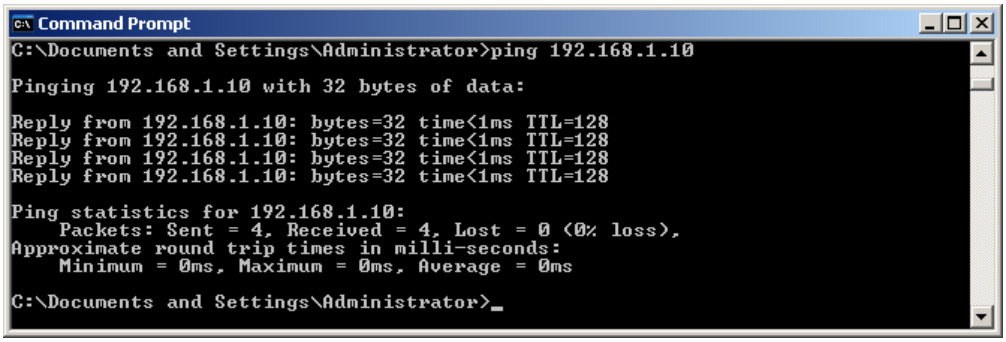

Рис. 30. **Результат виконання команди ping на ВМ Windows XP Professional**

Як видно з рис. 29 і 30, на чотири відправлених пакети було отримано чотири відповіді, утрачено нуль пакетів. Максимальний час пересилання становить 1 мс. Отже, перевірку наявності фізичного зв'язку між вузлами мережі та працездатності мережевого адаптера виконано.

Отримаємо інформацію щодо налаштування мережевих адаптерів, які фізично встановлено в РС командою **ipconfig** (рис. 31 і 32).

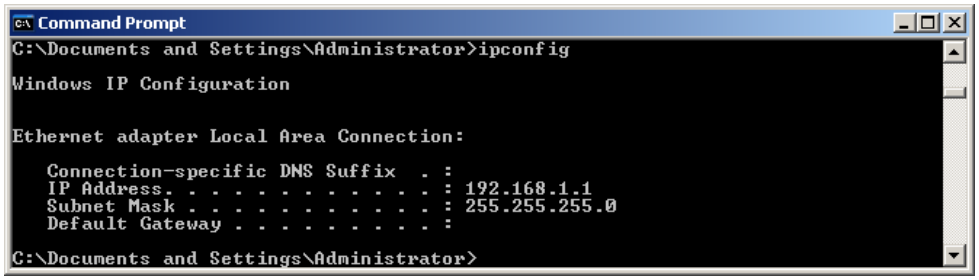

Рис. 31. **Результат виконання команди ipconfig на ВМ з Windows Server 2003 Enterprise Edition**

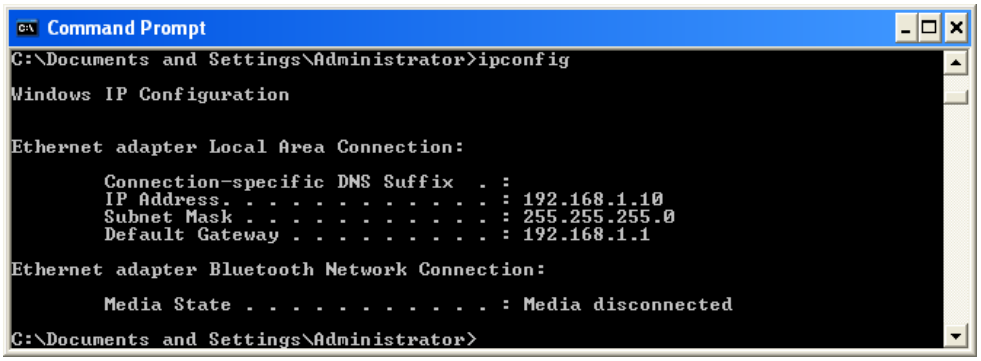

Рис. 32. **Результат виконання команди ipconfig на ВМ з Windows XP Professional**

Для отримання більш розгорнутої інформації треба виконати команду **ipconfig** з ключем **/all** (рис. 33 і 34).

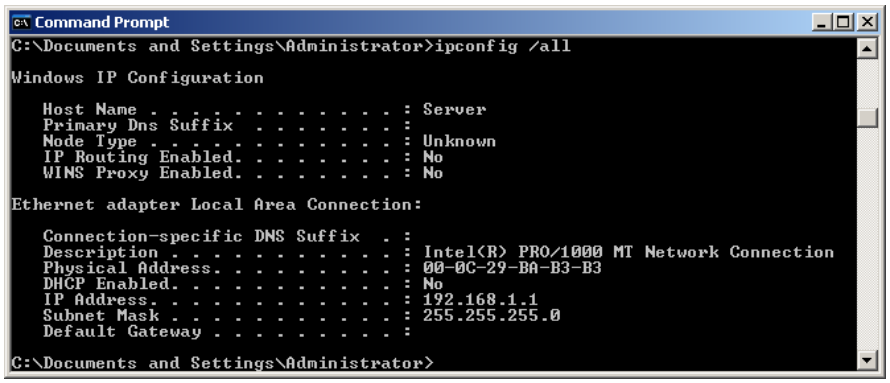

Рис. 33. **Результат виконання команди ipconfig з ключем all на ВМ з Windows Server 2003 Enterprise Edition**

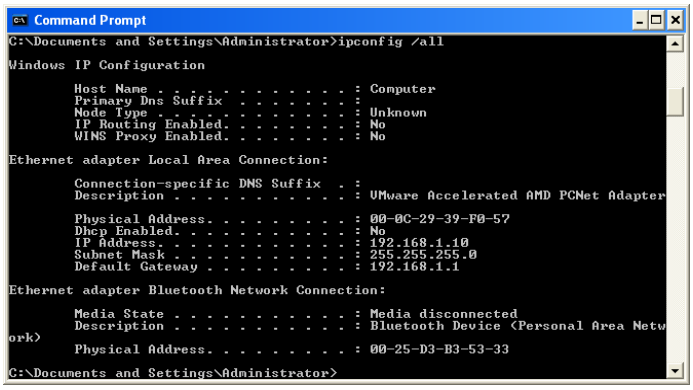

Рис. 34. **Результат виконання команди ipconfig з ключем all на ВМ з Windows XP Professional**

Як видно з рис. 33 і 34, у цьому режимі додається інформація з пункту **Windows IP Configuration** і більш розгорнута інформація в інших пунктах.

Отримаємо інформацію про налаштування маршрутизації на обох РС командою **route PRINT** (рис. 35 і 36).

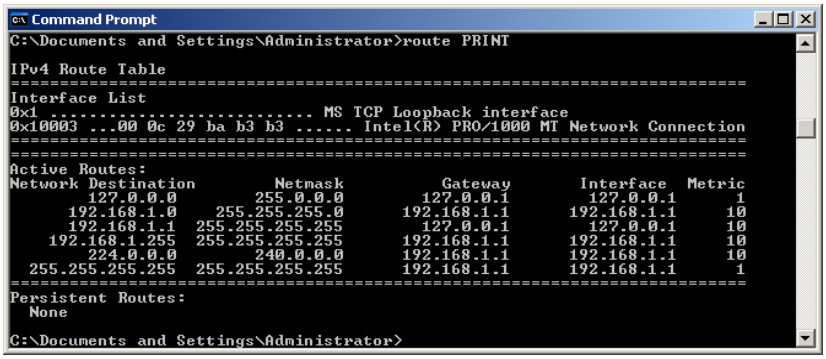

Рис. 35. **Результат виконання команди route з ключем PRINT на ВМ з Windows Server 2003 Enterprise Edition**

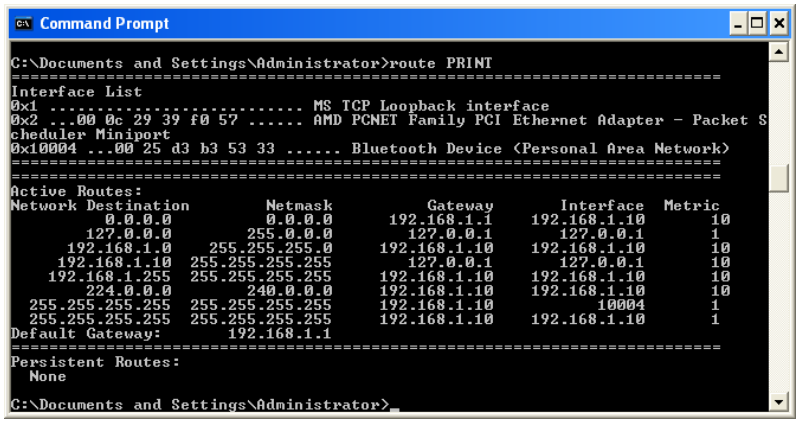

Рис. 36. **Результат виконання команди route з ключем PRINT на ВМ з Windows XP Professional**

Ця команда дозволяє перевірити всі можливі підмережі, налаштовані в РС, шлюзи за замовчуванням та інтерфейси, до яких вони належать.

Отримуємо інформацію про всі РС створеної робочої групи командою **net view** (рис. 37 і 38).

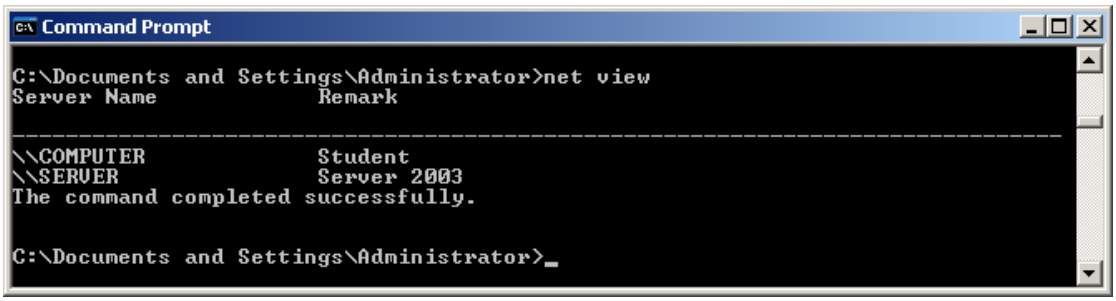

Рис. 37. **Результат виконання команди net з ключем view на ВМ з Windows Server 2003 Enterprise Edition**

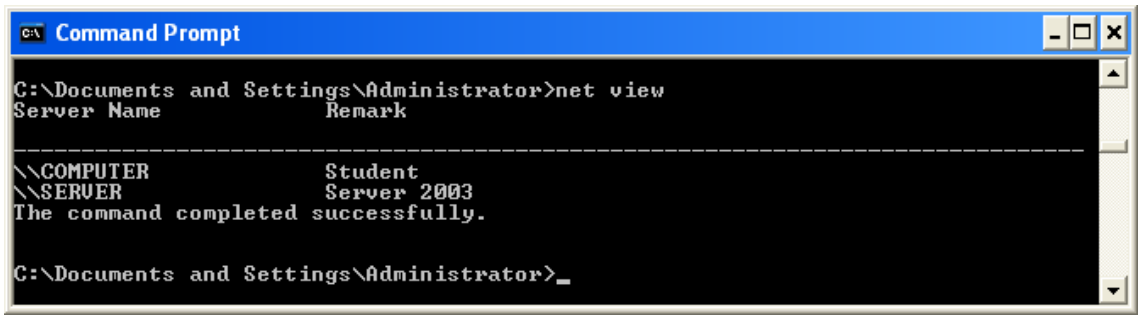

Рис. 38. **Результат виконання команди net з ключем view на ВМ з Windows XP Professional**

Отримаємо імена РС, на які відправимо повідомлення в мережі (рис. 39 і 40).

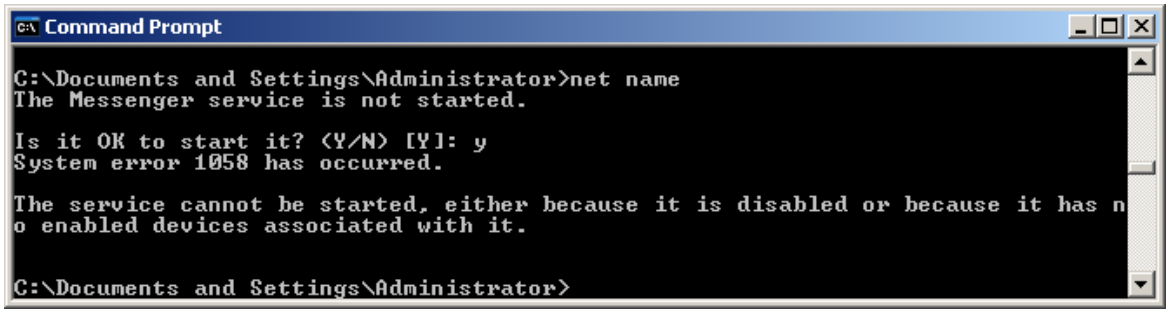

Рис. 39. **Помилка виконання команди net з ключем name на ВМ з Windows Server 2003 Enterprise Edition**

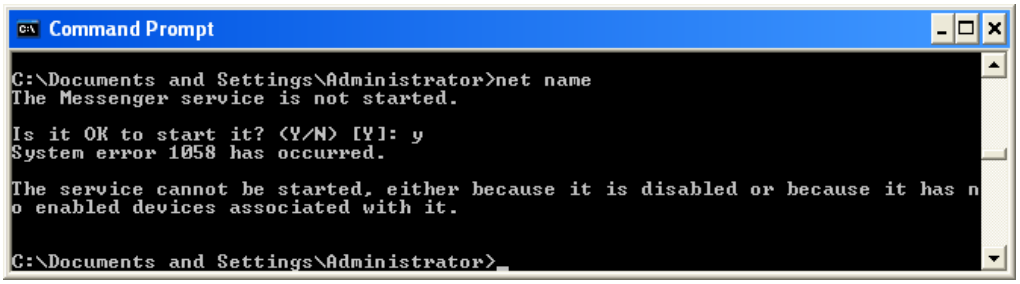

Рис. 40. **Помилка виконання команди net з ключем name у ВМ з Windows XP Professional**

Як видно з рис. 39 і 40, на обох РС виникає однакова помилка. Вона пов'язана зі службою **Messenger**, запуск якої за замовчуванням заборонено. Увімкнемо цю службу на обох РС. Для цього у ВМ з ОС *Windows Server 2003 Enterprise Edition* треба ввійти в меню **Start -> Administrative Tools -> Services** (рис. 41).

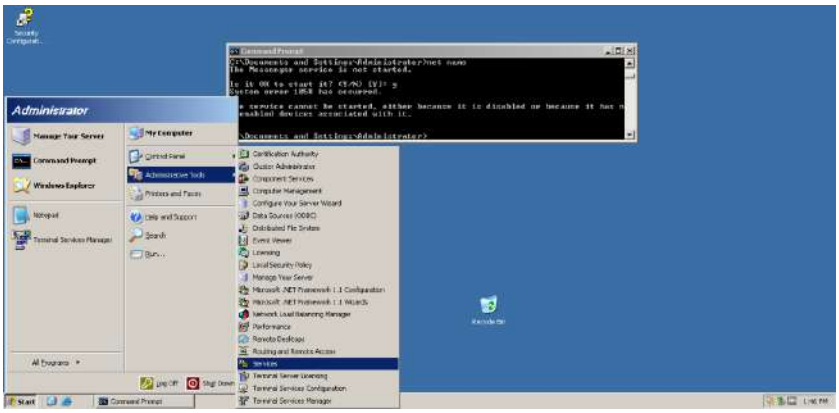

Рис. 41. **Відкриття вікна Services на ВМ з Windows Server 2003 Enterprise Edition**

У вікні **Services** знаходимо службу **Messenger**. Натискаємо її правою кнопкою мишки, і в меню, що відкриється, вибираємо розділ **Properties** (рис. 42 і 43).

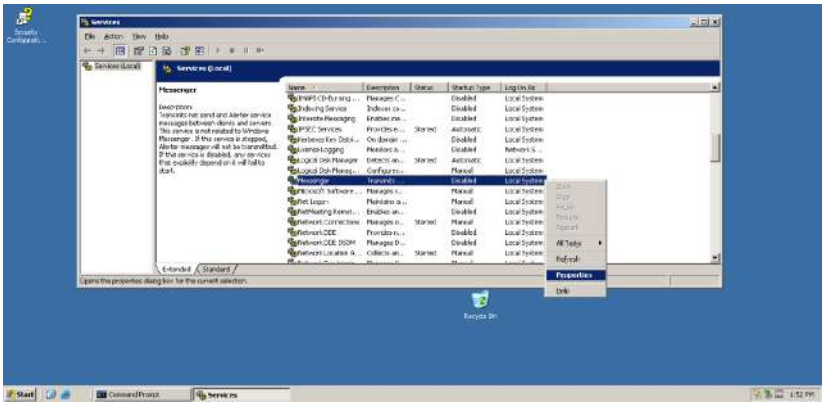

Рис. 42. **Вибір налаштувань служби Messenger**

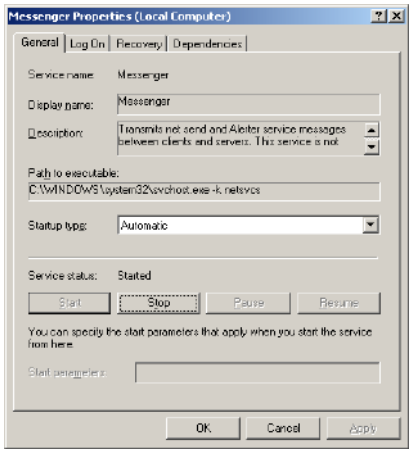

Рис. 43. **Налаштування служби Messenger**

У вікні, що відкриється, у пункті **Startup type** змінюємо значення **Disabled** на **Automatic** та натискаємо кнопку **Apply** для прийняття змін. Натискаємо кнопку **Start**, що стане доступною після прийняття змін, для завантаження служби в систему (див. рис. 43). Після цього повторюємо виконання команди **net name** (рис. 44).

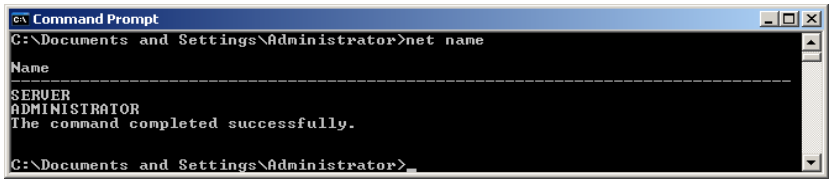

Рис. 44. **Виконання команди net з ключем name на ВМ з Windows Server 2003 Enterprise Edition**

Тепер команда працює. З отриманого результату роботи команди видно, що відправляти повідомлення можливо на імена **Server** і **Administrator**.

У ВМ з *Windows XP Professional* для переходу у вікно **Service** треба вибрати: у меню **Start -> Control Panel** (рис. 45).

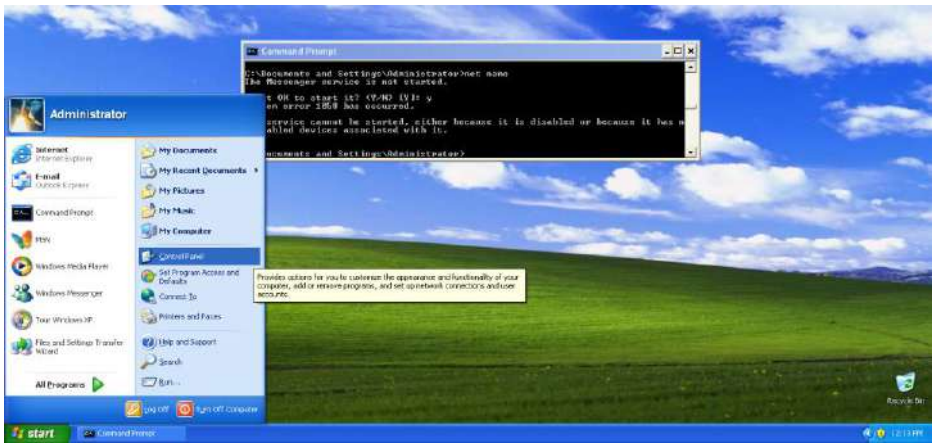

Рис. 45. **Виклик вікна Control Panel**

У вікні, що відкриється, вибрати пункт *Performance and Maintenance* (рис. 46).

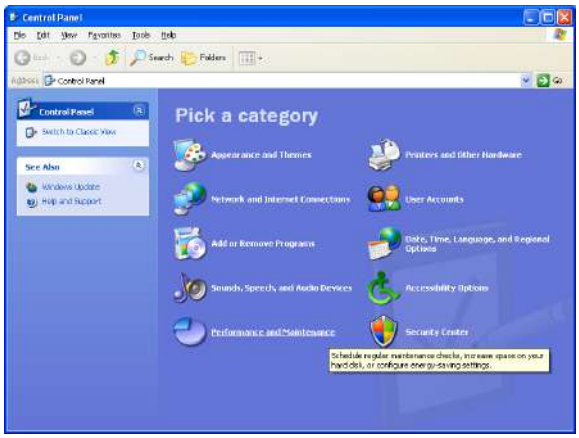

Рис. 46. **Вікно Control Panel**

У вікні, що відкриється, вибрати пункт **Administrative Tools** (рис. 47).

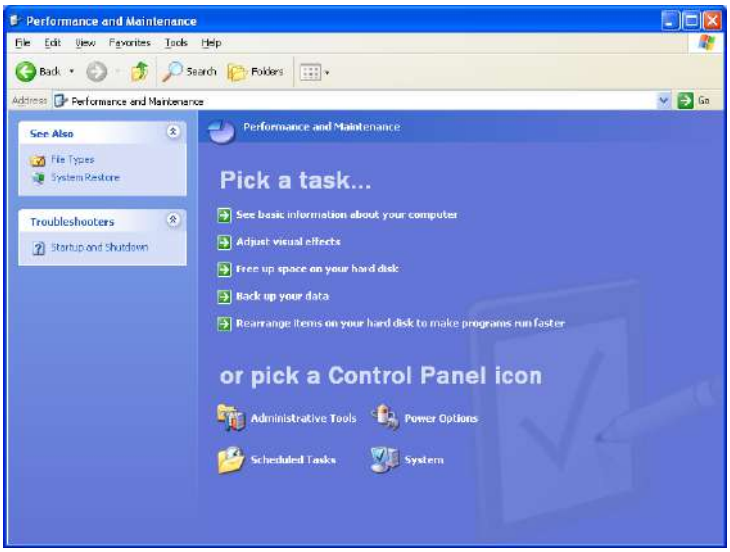

Рис. 47. **Вікно панелі Performance and Maintenance**

У наступному вікні вибрати пункт **Services** (рис. 48).

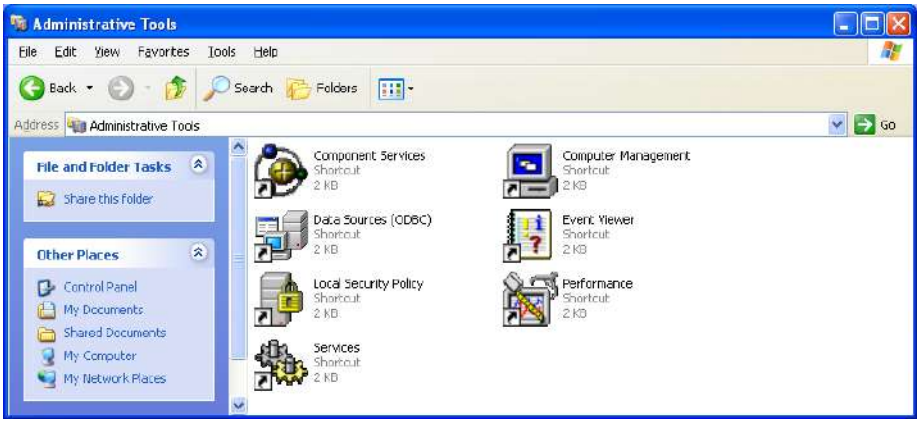

Рис. 48. **Вікно панелі Administrative Tools**

Далі повторюємо ті самі дії для завантаження служби **Messenger**, що й на попередній ВМ (див. рис. 42 і 43). Повторюємо виконання команди **net name** (рис. 49).

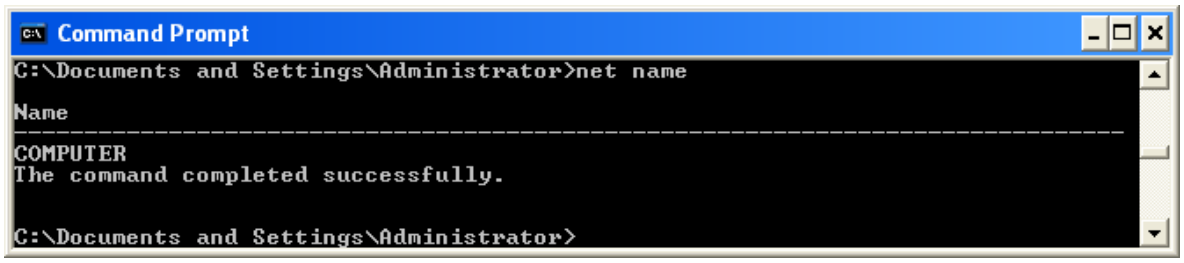

Рис. 49. **Виконання команди net з ключем name на ВМ з Windows XP Professional**

Тепер команда також працює. З отриманого результату роботи команди видно, що відправляти повідомлення можна на ім'я **Computer**.

Відправимо однобічне повідомлення з РС з вузла з *Windows Server 2003 Enterprise Edition* на вузол з *Windows XP Professional* та перевіримо отримання повідомлення (рис. 50 і 51).

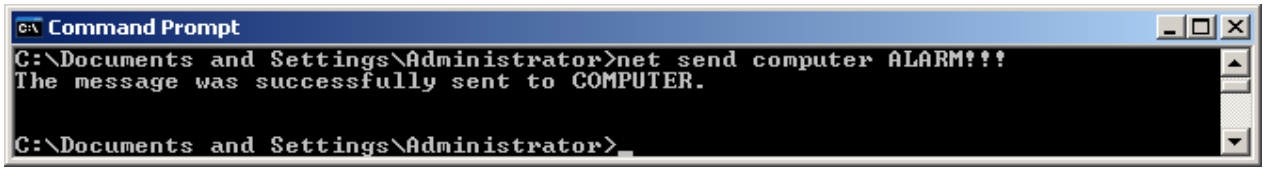

Рис. 50. **Відправлення однобічного повідомлення з РС з ім'ям Server на РС з ім'ям Computer**

Рис. 51. **Отримання однобічного повідомлення РС з ім'ям Computer від РС з ім'ям Server**

Відправимо однобічне повідомлення з РС (ВМ) з *Windows XP Professional* на РС (ВМ) з *Windows Server 2003 Enterprise Edition* та перевіримо отримання повідомлення на обидва імені (рис. 52 – 55).

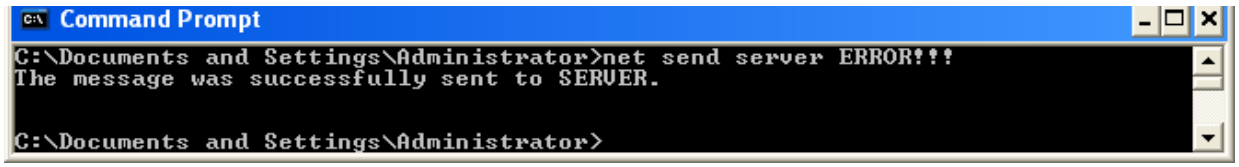

Рис. 52. **Відправлення однобічного повідомлення з PC з ім'ям Computer на PC з ім'ям Server**

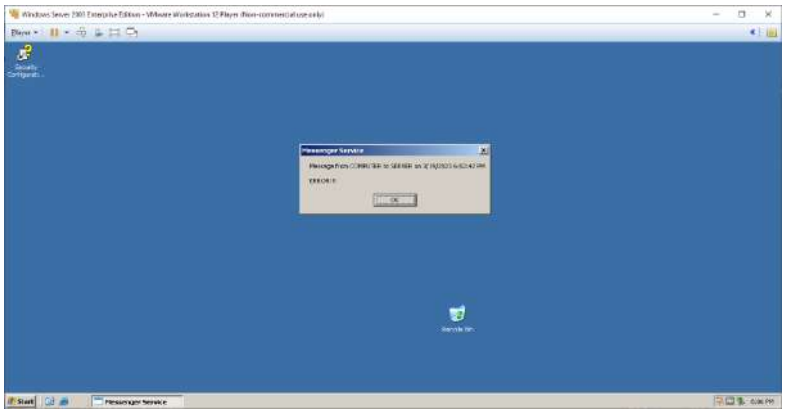

Рис. 53. **Отримання однобічного повідомлення PC з ім'ям Server від PC з ім'ям Computer**

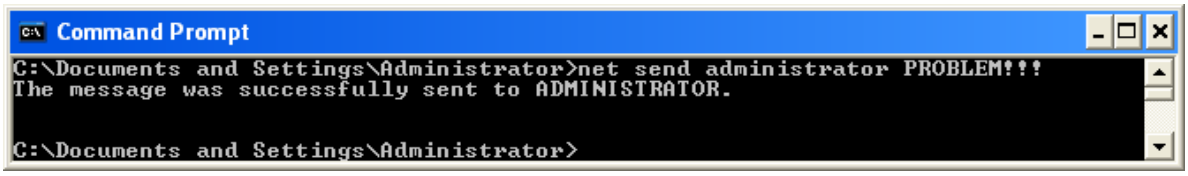

Рис. 54. **Відправлення однобічного повідомлення з PC з ім'ям Computer на PC з ім'ям Administrator**

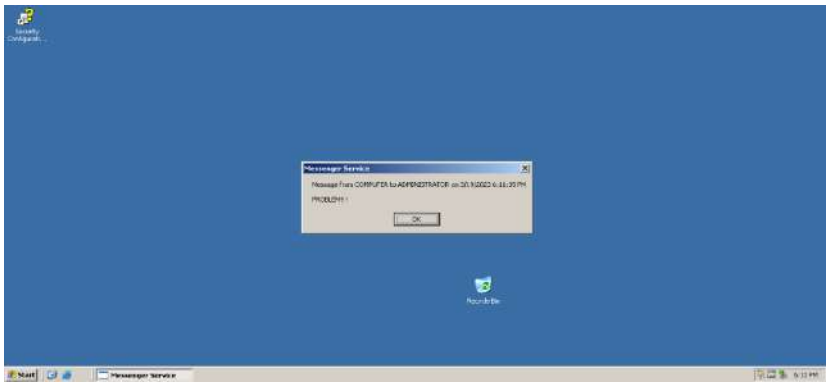

Рис. 55. **Отримання однобічного повідомлення PC з ім'ям Administrator від PC з ім'ям Computer**

Засобами ОС *Windows XP Professional* та ОС *WS 2003 Enterprise Editio*n можна переглянути мережеве оточення створеної робочої групи. Для цього треба ввійти в провідник та вибрати відповідний пункт меню (рис. 56 і 57).

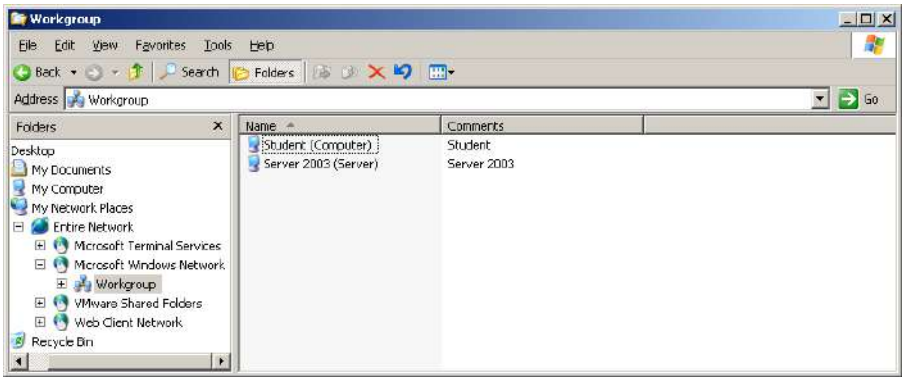

Рис. 56. **Вікно відображення мережевого оточення створеної робочої групи у ВМ з Windows Server 2003 Enterprise Edition**

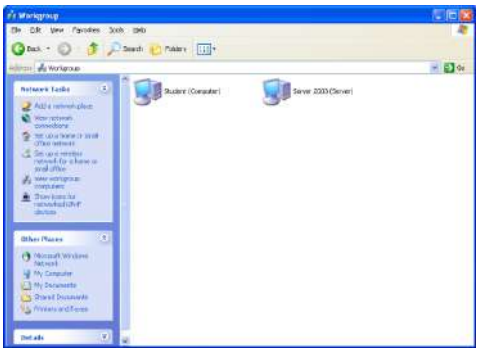

Рис. 57. **Вікно відображення мережевого оточення робочої групи у ВМ з Windows XP Professional**

Налаштування віддаленого доступу з ВМ з Windows Server 2003 Enterprise Edition до ВМ з Windows XP Professional

Є два інструменти для віддаленого доступу та технічної підтримки. *Remote Assistance*, який дозволяє віддалено надавати допомогу, використовують у разі виникнення проблем з роботою РС або встановлених на неї програм. *Remote Desktop,* який дозволяє віддалено керувати РС за допомогою мережевого або *dial-up* з'єднання, використовують, наприклад, під час віддаленої роботи, коли потрібно зайти на РС, що знаходиться в офісі, з будь-якого місця за межами офісу й отримати доступ до всіх необхідних ресурсів (робочих документів, баз даних, програм тощо) через робочий стіл.

Роботу *Remote Desktop* основано на технології *Terminal Services* (служби терміналів). Для з'єднання інструмент *Remote Desktop* застосовує локальну КМ (*LAN*) або віртуальну приватну мережу (*VPN*). З'єднання складається з двох компонентів: сервера, з яким установлюють з'єднання, і клієнта, з якого встановлюють з'єднання із сервером.

Для дозволу на віддалену допомогу РС слід увімкнути опцію **Allow Remote Assistance invitations to be sent from this computer**, а для дозволу на віддалене підключення до РС – опцію **Allow users to connect remotely to this computer**, які знаходяться на вкладці **Remote** вікна **System Properties** (рис. 58).

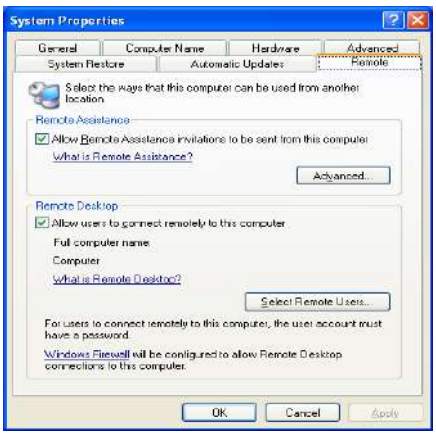

Рис. 58. **Вкладка Remote вікна System Properties**

У пункті **Select Remote Users** потрібно додати всі облікові записи користувачів, яким дозволено віддалений доступ до PC. Обліковий запис **Administrator** додається за замовчуванням та окремого додавання не потребує. Для віддаленого доступу до PC необхідно, щоб обліковий запис, під яким буде виконано з'єднання, мав пароль. Якщо пароля немає, то система видає повідомлення про помилку (рис. 59).

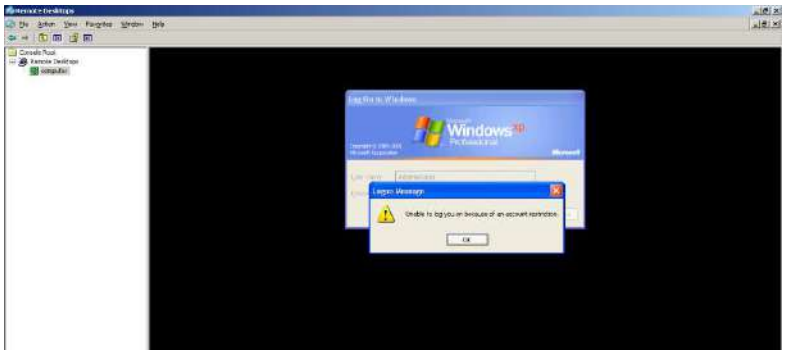

Рис. 59. **Повідомлення про помилку під час підключення до віддаленого PC у разі відсутності пароля облікового запису**

Для перевірки роботи *Remote Desktop* будемо використовувати вбудований обліковий запис **Administrator**. Створюємо для нього пароль на PC, до якої бажаємо підключитися (рис. 60 – 64).

Рис. 60. **Вхід до Control Panel**

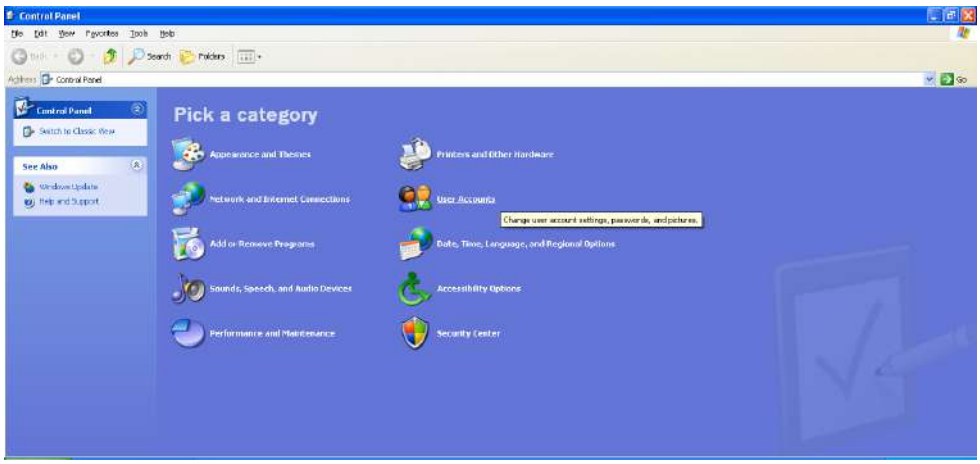

Рис. 61. **Вхід до панелі User Accounts**

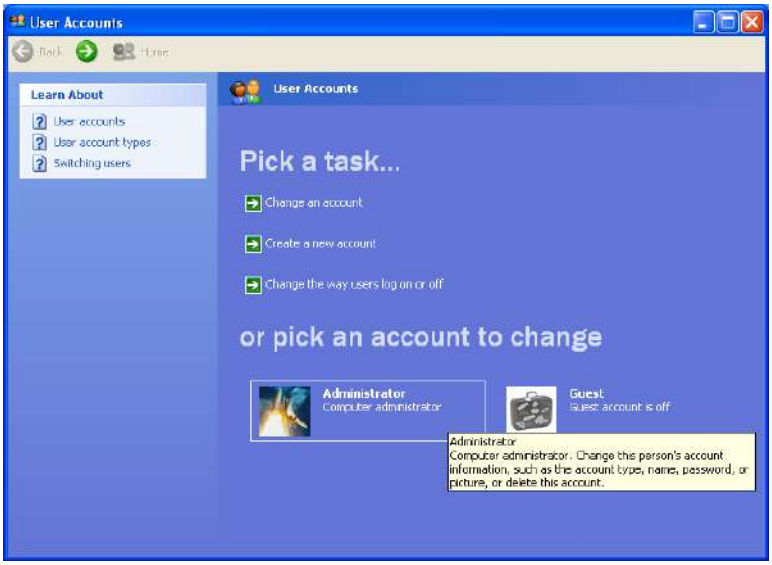

Рис. 62. **Вхід до облікового запису Administrator**

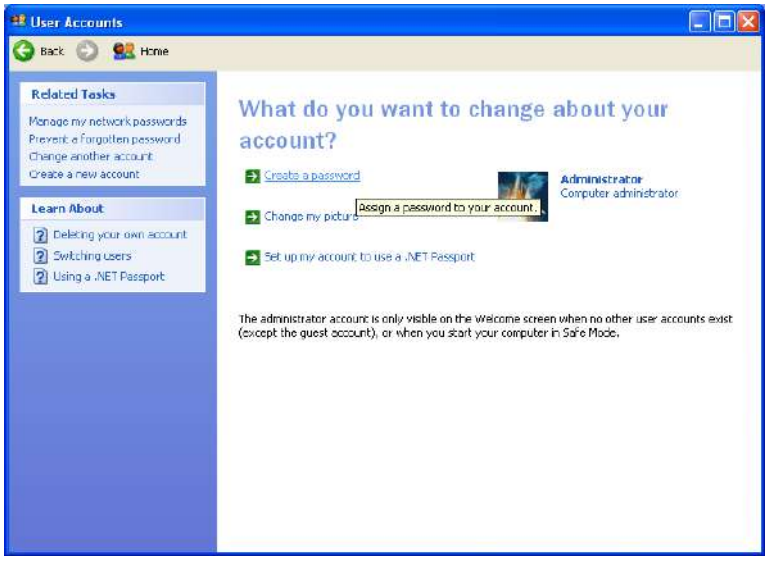

Рис. 63. **Вхід до вікна створення пароля для облікового запису Administrator**

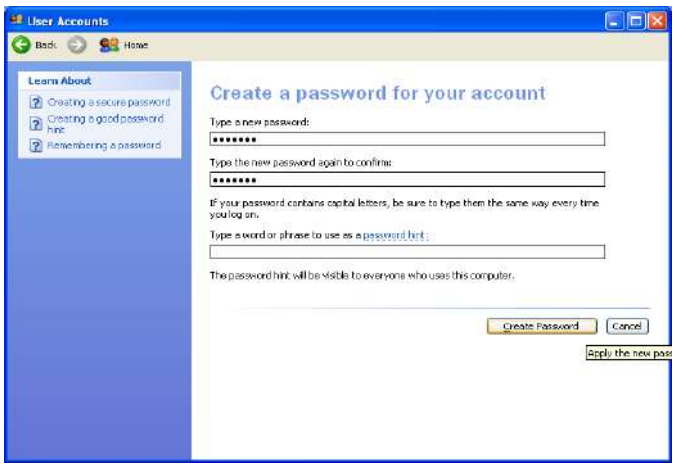

Рис. 64. **Створення пароля для облікового запису Administrator**

Після створення пароля, повертаємося до РС (ВМ) з ОС *Windows Server 2003 Enterprise Edition* та вибираємо в ній: меню **Start -> Administrative Tools -> Remote Desktop** (рис. 65).

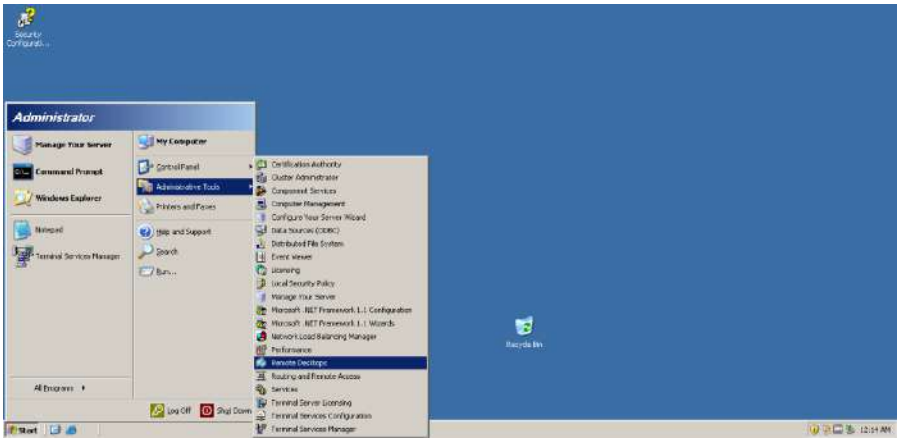

Рис. 65. **Виклик програми Remote Desktop**

У вікні, що відкриється, натискаємо праву кнопку мишки на пункті **Remote Desktop** та вибираємо в меню, що відкриється, пункт **Add new connection** (рис. 66).

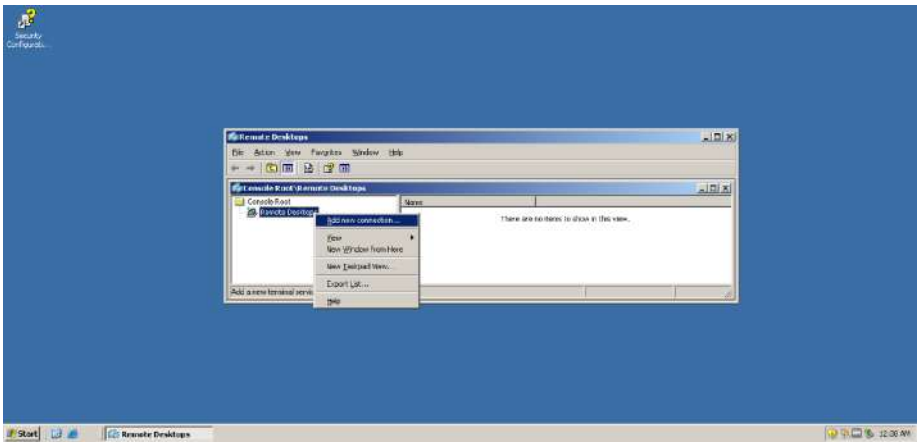

Рис. 66. **Додавання нового з’єднання**

Налаштовуємо віддалене з'єднання з PC **Computer** з використанням вбудованого облікового запису **Administrator** та вказуємо створений раніше для нього пароль (рис. 67). Після налаштування з'явиться пункт з іменем PC, з яким потрібно встановити з'єднання (рис. 68).

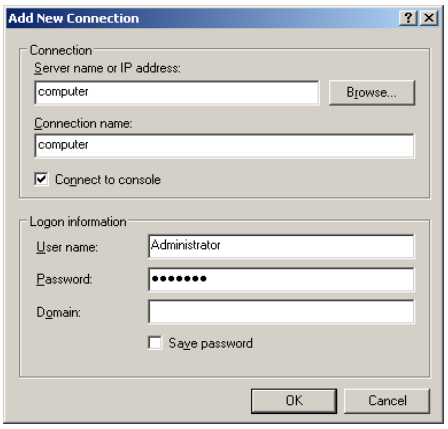

Рис. 67. **Налаштування віддаленого з'єднання**

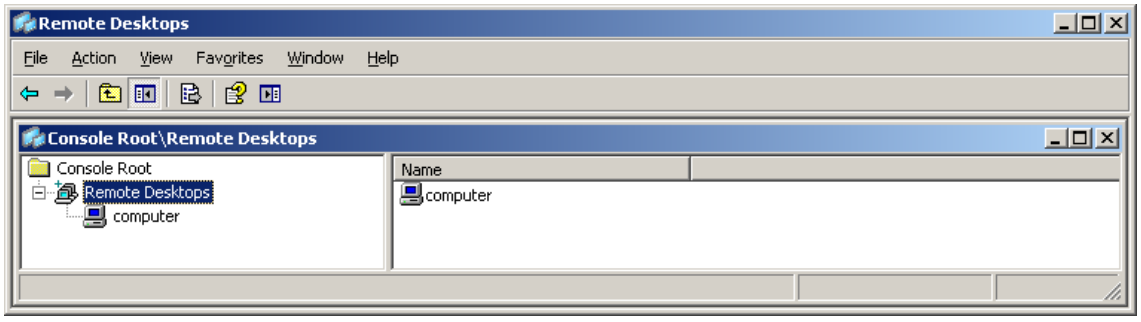

Рис. 68. **Створення пункту з ім'ям PC для віддаленого доступу**

Натискаємо ліву кнопку мишки на створеному пункті та отримуємо доступ до робочого столу віддаленої PC (ВМ) з *Windows XP Professional* (рис. 69).

Рис. 69. **Підключення до віддаленої PC**

Тепер є можливість працювати з віддаленою PC як із локальною. Для відключення від віддаленої PC натискаємо праву кнопку мишки на пункті **Computer** і в меню, що з'явиться, вибираємо пункт **Disconnect** (рис. 70).

Рис. 70. **Відключення від віддаленої PC**

На цьому сеанс зв'язку з робочим столом віддаленої PC закінчено.

Налаштування віддаленого доступу з PC (ВМ) з Windows XP Professional до PC (ВМ) з Windows Server 2003 Enterprise Edition.

На PC з *Windows Server 2003 Enterprise Edition* задаємо пароль для вбудованого облікового запису **Administrator**. Відкриваємо вікно **Computer Management**. Вибираємо меню **Start -> Administrative Tools -> Computer Management** (рис. 71).

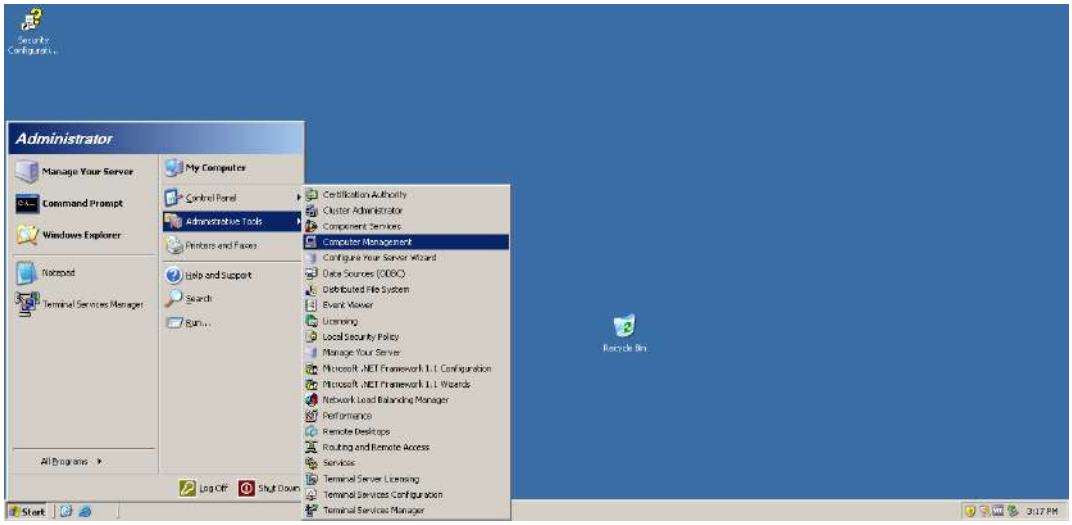

Рис. 71. **Відкриття вікна Computer Management**

У вікні, що відкриється, вибираємо пункти **Local Users and Groups -> Users**. Натискаємо лівою кнопкою мишки на вбудованому обліковому записі **Administrator** і вибираємо пункт **Set Password** (рис. 72).

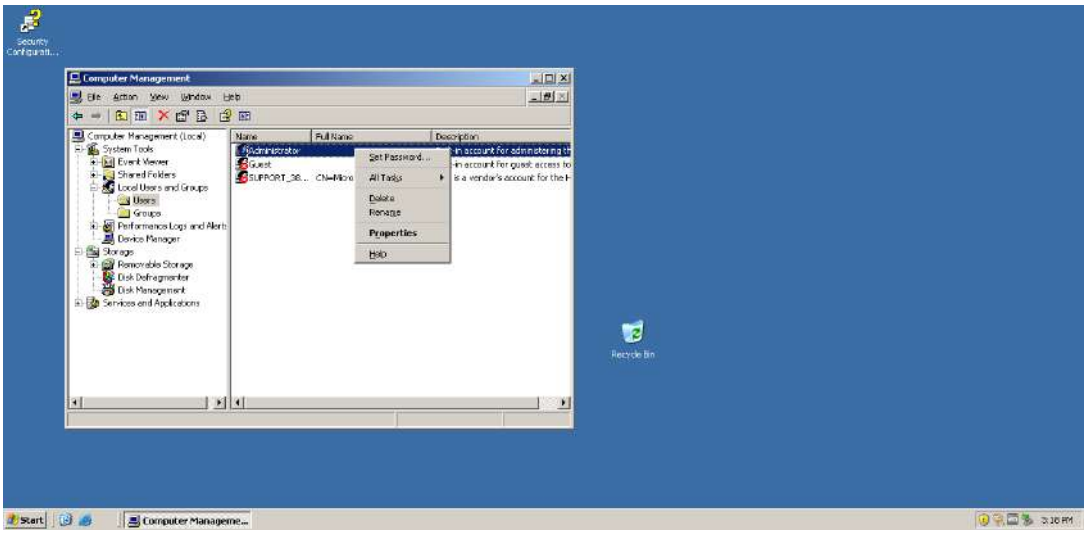

Рис. 72. **Установлення пароля для вбудованого облікового запису Administrator**

Перед уведенням пароля буде виведено попередження (рис. 73).

Рис. 73. **Вікно попередження перед уведенням пароля**

Задаємо пароль для вбудованого облікового запису **Administrator** (рис. 74).

Рис. 74. **Пароль вбудованого облікового запису Administrator**

З’явиться повідомлення про успішну зміну пароля (рис. 75).

Рис. 75. **Пароль було встановлено**

Для дозволу на віддалене підключення до PC потрібно вибрати опцію **Enable Remote Desktop on this computer**, яка знаходиться на вкладці **Remote** вікна **System Properties**, та погодитися з вікном попередження, натиснувши на кнопку **OK** (рис. 76 і 77).

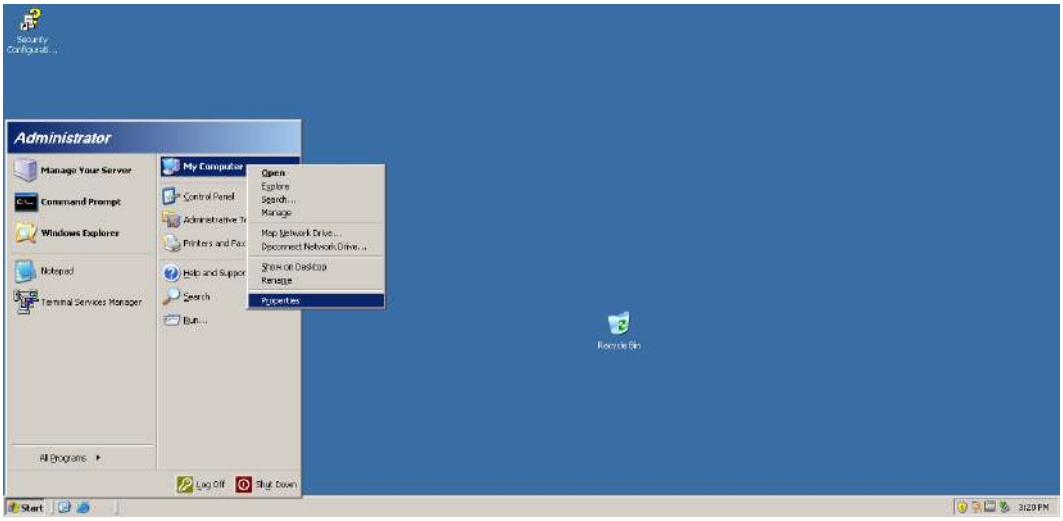

Рис. 76. **Виклик вікна System Properties**

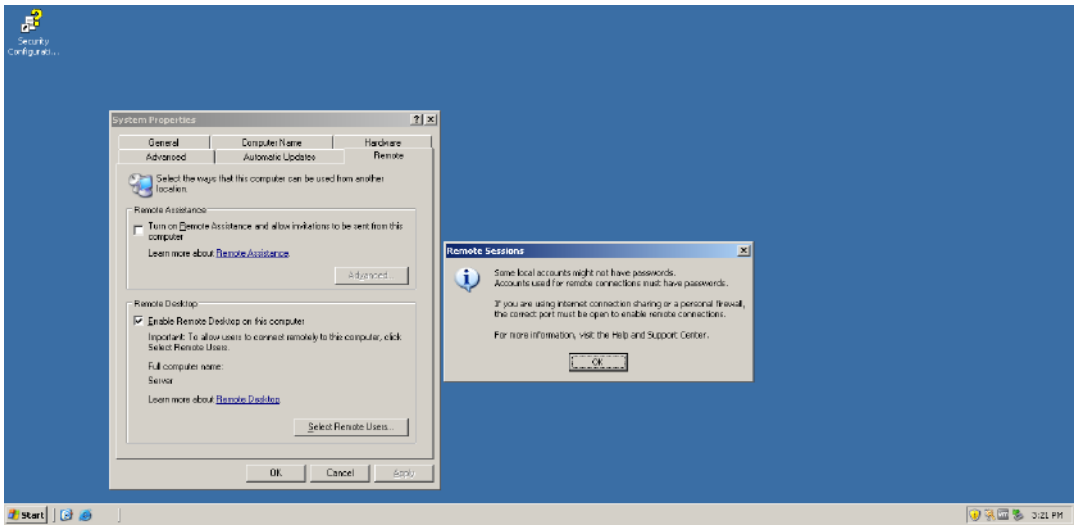

Рис. 77. **Дозвіл на віддалене підключення до PC**

Після виконання всіх попередніх налаштувань, переходимо до PC на *Windows XP Professional*. Викликаємо програму віддаленого доступу *Remote Desktop Connection*: вибираємо меню **Start -> All Programs -> Accessories -> Remote Desktop Connection** (рис. 78). У рядку **Computer:** уводимо ім'я PC, до якої бажаємо отримати віддалений доступ (рис. 79).

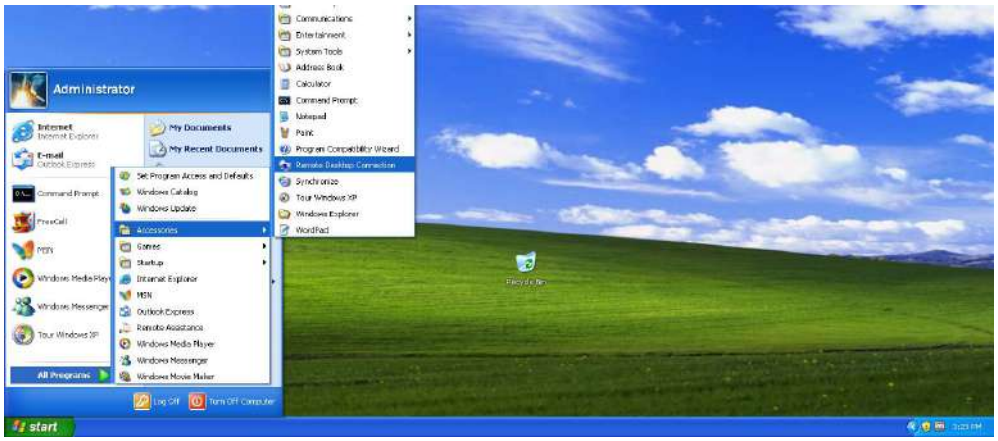

Рис. 78. **Виклик програми Remote Desktop Connection**

Рис. 79. **Вікно Remote Desktop Connection**

Для перевірки налаштувань треба вибрати кнопку **Options>>**, після чого з'явиться вкладка **General** вікна налаштувань (рис. 80).

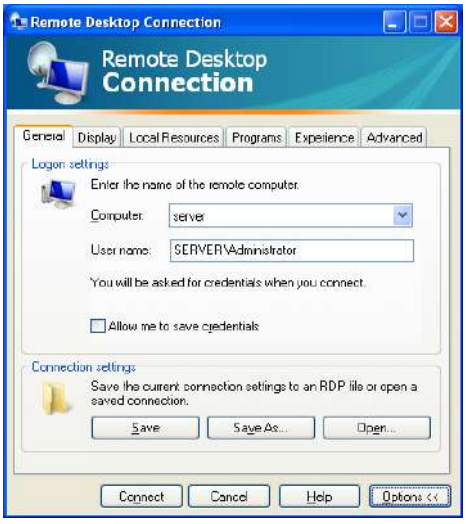

Рис. 80. **Вкладка General вікна налаштувань Remote Desktop Connection**

На цій вкладці є можливість:

- увести ім’я або задати IP-адресу PC, до якої слід отримати віддалений доступ, або вибрати значення зі списку, якщо його вже вводили раніше;
- увести ім’я облікового запису, під яким входимо на віддаленій PC. Також можна зберегти поточні параметри налаштування на встановлену віддалену сесію або завантажити раніше збережену.

На вкладці **Display** установлюємо розмір та кольорову палітру робочого столу віддаленої PC (рис. 81).

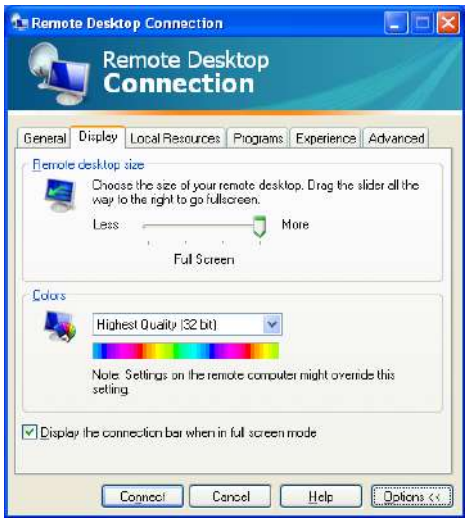

Рис. 81. **Вкладка Display вікна налаштувань Remote Desktop Connection**

Для вибору та встановлення складу ресурсів віддаленої PC треба вибрати вкладку **Local Resources**, де є можливість налаштувати параметри звуку, клавіатури та локальних пристроїв (рис. 82).

Рис. 82. **Вкладка Local Resources вікна налаштувань Remote Desktop Connection**

Для запуску потрібного додатка під час підключення до віддаленої PC на вкладці **Programs** потрібно вибрати (рис. 83):

- шлях до виконуваної програми та ім'я файлу запуску цієї програми;
- робочу папку, у якій опинимося після підключення.

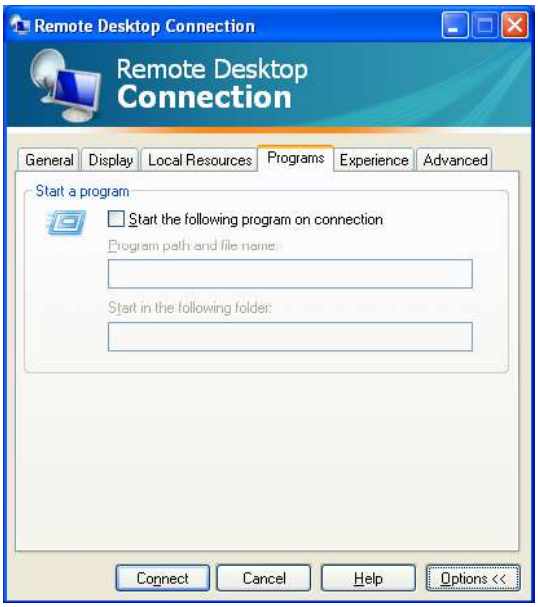

Рис. 83. **Вкладка Programs вікна налаштувань Remote Desktop Connection**

На вкладці **Experience** можна вибрати значення швидкості підключення, а також різні можливості щодо підвищення продуктивності роботи з віддаленою PC (рис. 84).

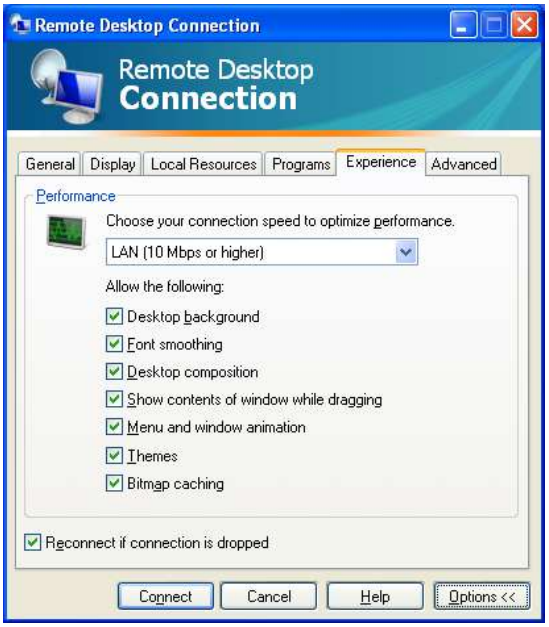

Рис. 84. **Вкладка Experience вікна налаштувань Remote Desktop Connection**

На вкладці **Advanced** можна вибрати спосіб автентифікації підключення з віддаленою PC (рис. 85).

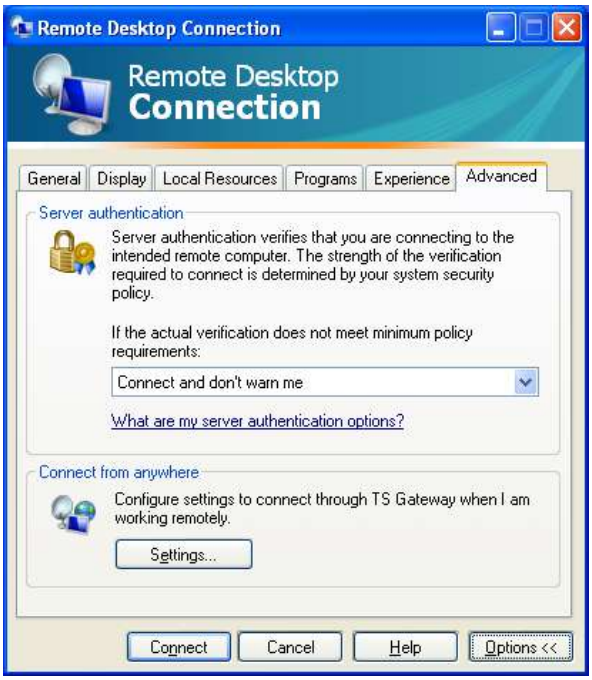

Рис. 85. **Вкладка Advanced вікна налаштувань Remote Desktop Connection**

Після перевірки налаштувань з'єднання натискаємо кнопку **Connect**. Відкриється вікно віддаленого доступу із запрошенням на вхід у систему (рис. 86).

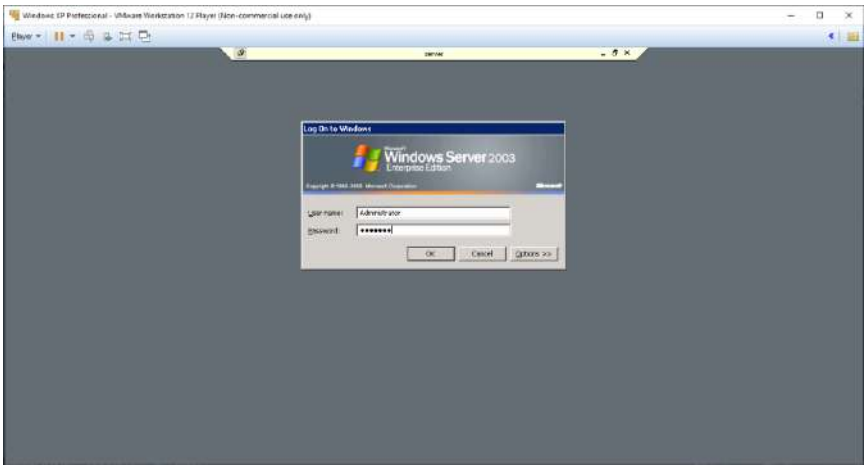

Рис. 86. **Вікно входу до віддаленої PC**

У рядку *User name* уводимо ім’я вбудованого облікового запису *Administrator*, а в рядку *Password* уводимо раніше створений для нього пароль.

Після цього відкриється вікно з робочим столом віддаленої PC (рис. 87). Тепер є можливість працювати з віддаленою PC як із локальною.

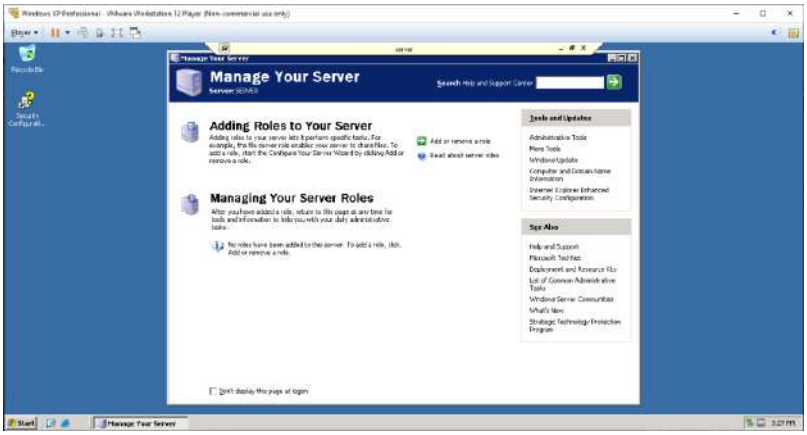

Рис. 87. **Робочий стіл віддаленої PC**

Для припинення сеансу з’єднання треба натиснути на кнопку **X** у меню, яке розташовано у верхній частині вікна посередині екрана. Буде виведено попередження про припинення сеансу (рис. 88). Натискаємо на кнопку **ОК**.

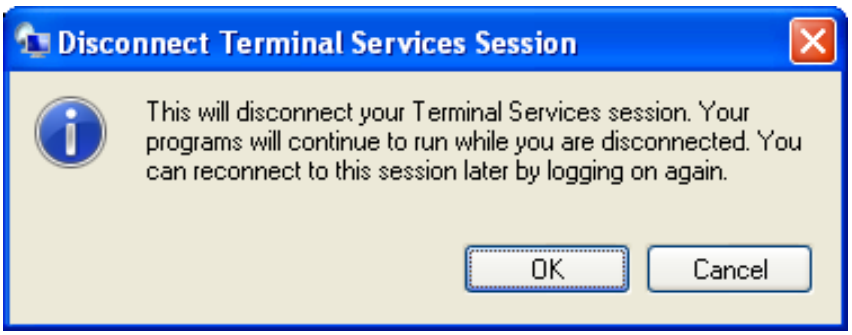

Рис. 88. **Попередження про припинення сеансу з’єднання з віддаленою PC**

На цьому сеанс зв’язку з робочим столом віддаленої PC закінчено.

Зміст звіту

1. Назва лабораторної роботи (ЛР), тема, мета й зміст завдань ЛР.

2. Вхідні дані до лабораторної роботи.

3. Навести скриншоти результатів виконання всіх етапів завдань лабораторної роботи.

4. Висновки за результатами виконання ЛР.

Контрольні запитання

1. Дайте визначення локальної КМ.

2. Визначте мету використання ресурсів КМ.

3. Дайте визначення робочої групи в КМ.

4. Наведіть основні способи підключення РС у робочу групу в комп'ютерній мережі.

5. Назвіть засоби ОС *Windows* для створення КМ і підключення РС до існуючої мережі.

6. Укажіть послідовність ідентифікації РС та робочої групи під час підключення РС до мережі.

7. Наведіть можливі випадки перезавантаження ОС після установки параметрів РС і робочої групи.

8. Наведіть команди діагностики КМ і вкажіть їхнє призначення. Наведіть параметри команд *ipconfig, net* і їхнє призначення.

9. Для чого в цій роботі використовують протокол TCP/IP?

10. Які основні функції віддаленого доступу та інструменти, за допомогою яких вони реалізуються?

11. Які складові реалізують віддалений доступ?

12. Яким чином вибирають користувачів, які мають доступ до віддаленої РС?

13. Які параметри підключення РС налаштовують під час віддаленого доступу?

Лабораторна робота 2
Конфігурування DHCP-сервера засобами Windows Server

Метою лабораторної роботи є конфігурування DHCP-сервера для автоматичного призначення IP-адрес робочих станцій (PC) комп'ютерної мережі в заданих діапазонах.

Порядок виконання роботи

Дослідження роботи DHCP-сервера здійснюють на віртуальній машині (ВМ) з установленим *Windows Server 2003 Enterprise Edition* (образ ОС отримати у викладача).

На початку роботи необхідно провести налаштування гіпервізора *VMware Workstation Player*. Для ВМ з *Windows 2003 Enterprise Edition* потрібно перевірити підключення до віртуального CD/DVD привода образу диска *en_win_srv_2003_r2_standard_with_sp2_X13-04790.iso*.

У вікні завантаженого гіпервізора вибираємо ВМ *Windows Server 2003 Enterprise Edition*. Натискаємо пункт меню **Edit virtual machine settings** (рис. 89).

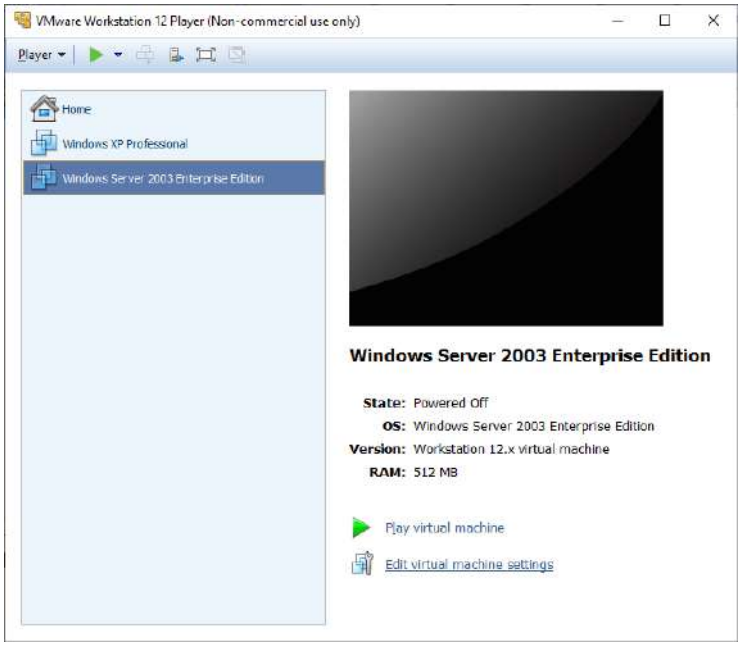

Рис. 89. **Запуск VMware Workstation Player**

У вікні, що відкрилося, перевіряємо налаштування віртуального CD/DVD привода (рис. 90).

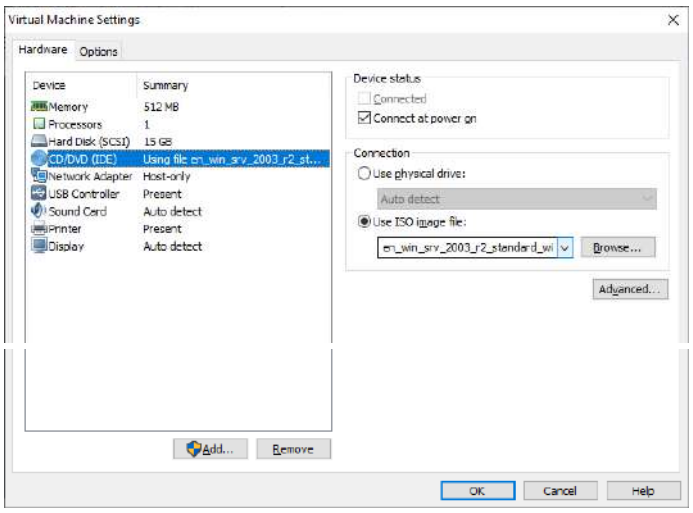

Рис. 90. **Перевірка налаштувань CD/DVD привода**

Для конфігурування DHCP-сервера необхідно налаштувати IP-адресу *Windows Server 2003 Enterprise Edition*. Вона буде мати вигляд 192.168.**XXX**.1, де **XXX** – визначається сумою числа 100 та номера студента в журналі групи. Маска підмережі **255.255.255.0**, що відповідає мережі класу С.

Для виконання цих налаштувань потрібно перейти в меню **Start -> Control Panel -> Network Connections -> Local Area Connection** (рис. 91).

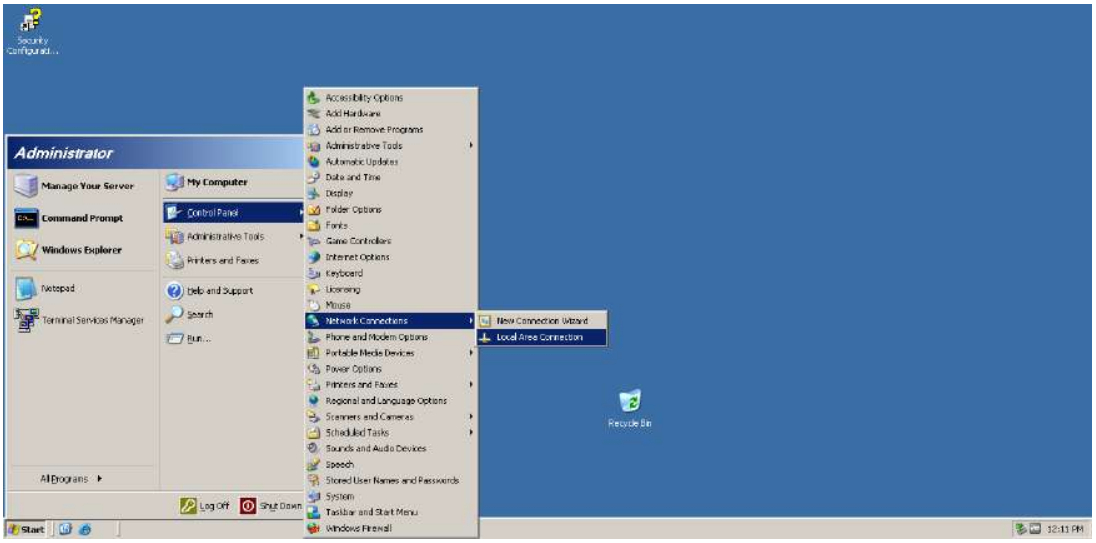

Рис. 91. **Вхід у вікно налаштувань мережевого адаптера на ВМ з Windows Server 2003 Enterprise Edition**

У вікні, що відкриється, слід перейти в меню **Properties -> Internet Protocol (TCP/IP) -> Properties,** внести потрібні зміни (рис. 92) та прийняти виконані зміни, натискаючи кнопки **ОК** і **Close**.

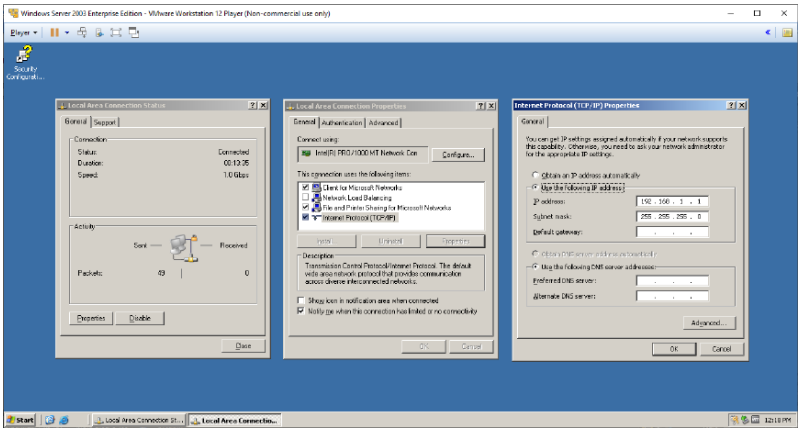

Рис. 92. **Налаштування IP-адреси та маски підмережі на ВМ з Windows Server 2003 Enterprise Edition**

Перевіряємо мережеві налаштування командою **ipconfig /all** (рис. 93).

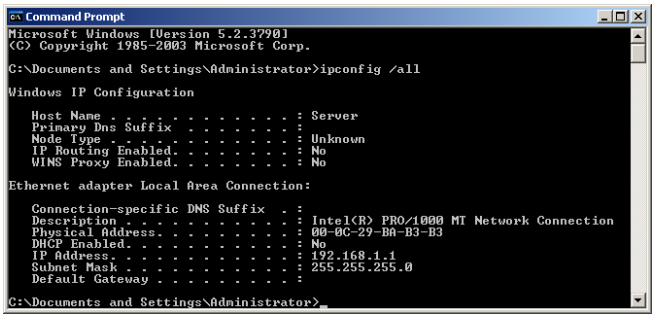

Рис. 93. **Перевірка мережевих налаштувань командою ipconfig /all**

Для подальших налаштувань DHCP-сервера необхідно на хостовій головній РС (РС, де встановлено гіпервізор з ВМ) відключити службу *VMware DHCP Service*. Для цього потрібно: увійти у вікно *Services*, знайти службу *VMware DHCP Service* та натиснути на ній правою кнопкою мишки. У меню, що з'явиться, виберіть пункт **Stop** (рис. 94).

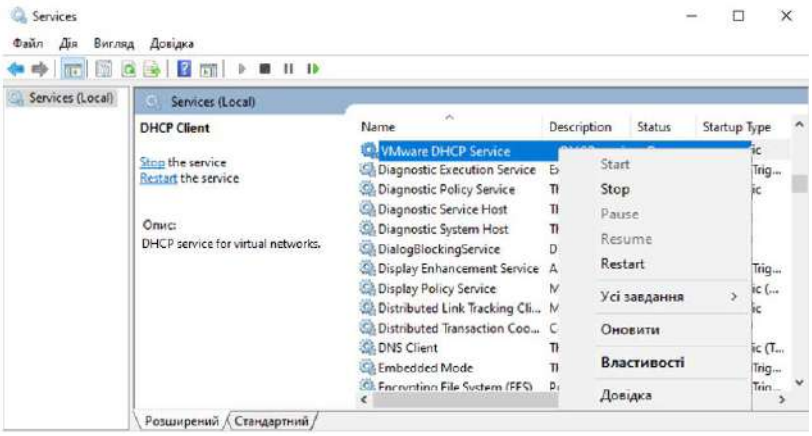

Рис. 94. **Відключення служби VMware DHCP Service у хостовій ОС**

Повертаємося до ВМ з *Windows Server 2003 Enterprise Edition*. Вибираємо меню **Start -> Administrative Tool -> Configure Your Server Wizard** (рис. 95).

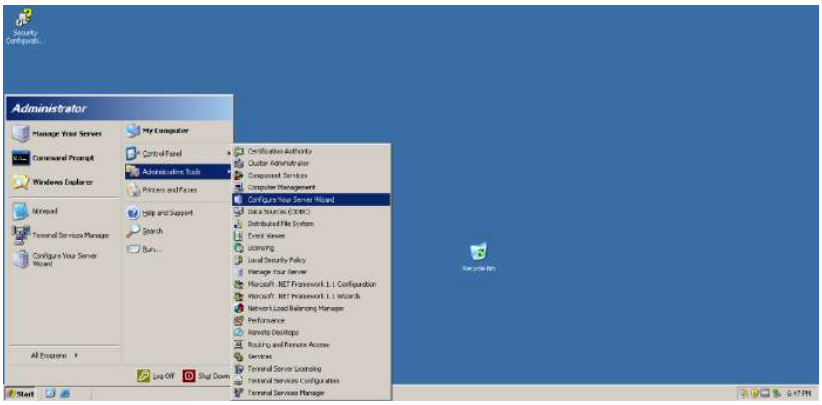

Рис. 95. **Запуск майстра налаштувань Windows Server 2003 Enterprise Edition**

У вікні, що відкриється, вибираємо кнопку **Next** для початку роботи майстра налаштувань (рис. 96). У наступному вікні вибираємо кнопку **Next** для визначення параметрів мережевих налаштувань (рис. 97).

Рис. 96. **Вікно початку роботи майстра налаштувань сервера**

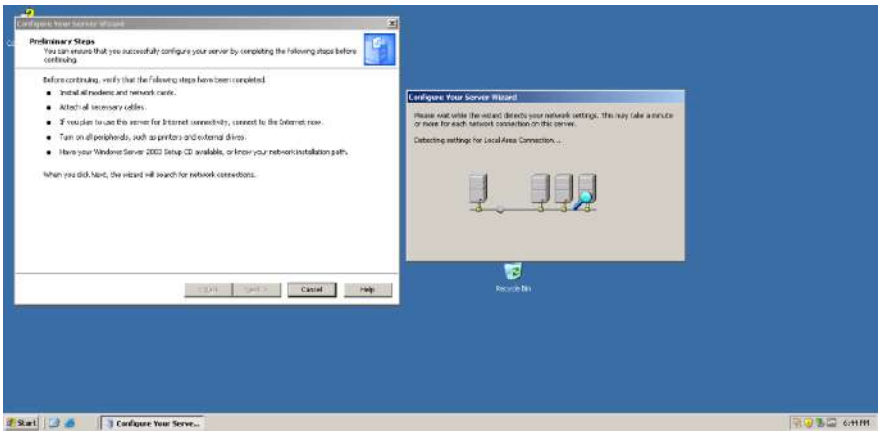

Рис. 97. **Визначення параметрів мережевих налаштувань**

Дозволяємо розблокування програми *Configure Your Server Wizard* у *Windows Firewall* кнопкою **Unblock** (рис. 98).

Рис. 98. **Розблокування Configure Your Server Wizard у Windows Firewall**

У вікні *Configuration Options* треба вибрати режим **Custom configuration** і натиснути кнопку **Next** (рис. 99).

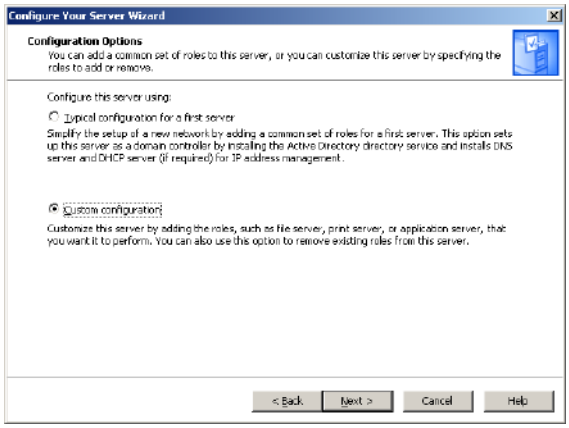

Рис. 99. **Вибір режиму налаштування сервера**

Для налаштування DHCP сервера вибираємо пункт **DHCP server** і натискаємо кнопку **Next** (рис. 100).

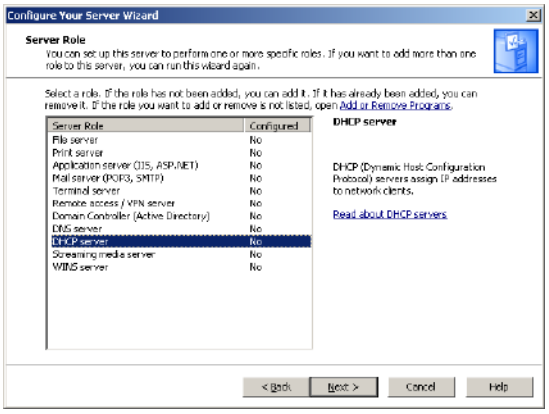

Рис. 100. **Вибір пункту налаштування DHCP сервера**

Починається встановлення DHCP-сервера (рис. 101). Воно буде складатися з двох етапів:

- установлення програми DHCP-сервера (рис. 102);
- запуску майстра створення зони видаваних IP-адрес (рис. 103).

Переходимо далі, натискаючи кнопки **Next** у кожному з перерахованих вікон.

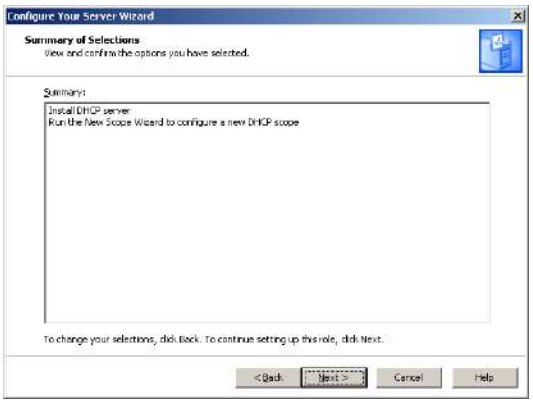

Рис. 101. **Вікно початку встановлення DHCP-сервера**

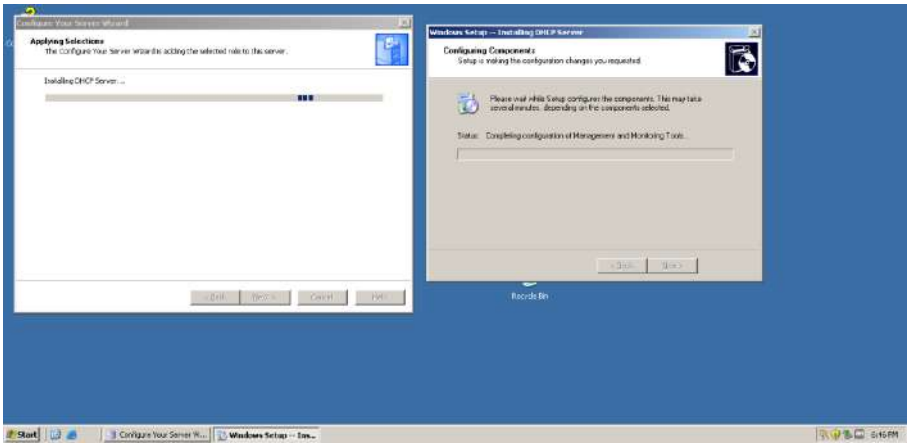

Рис. 102. **Установлення програми DHCP-сервера**

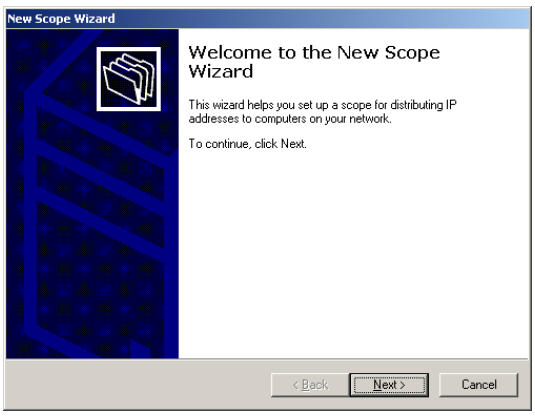

Рис. 103. **Запуск майстра створення зони IP-адрес**

Задаємо ім'я зони. У ньому слід використовувати **прізвище студента (латиницею)** (рис. 104).

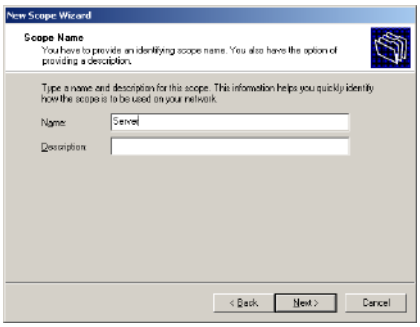

Рис. 104. **Задання імені області**

IP-адреса сервера та діапазон IP-адрес зони, що виділяються, повинні бути в одній підмережі. Вибирати діапазон адреси зони потрібно згідно з налаштуваннями IP-адреси та підмережі, які вже використовує DHCP-сервер (рис. 105).

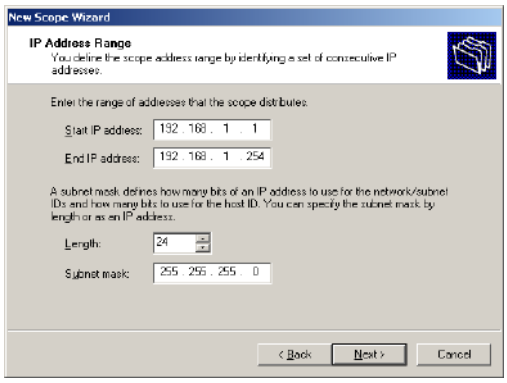

Рис. 105. **Задавання діапазону IP-адрес зони та підмережі**

Указуємо IP-адресу або діапазон IP-адрес зони, які виключені з розподілу DHCP-сервером (рис. 106). Вибираємо одну IP-адресу, прописану в налаштуваннях інтерфейсу DHCP-сервера.

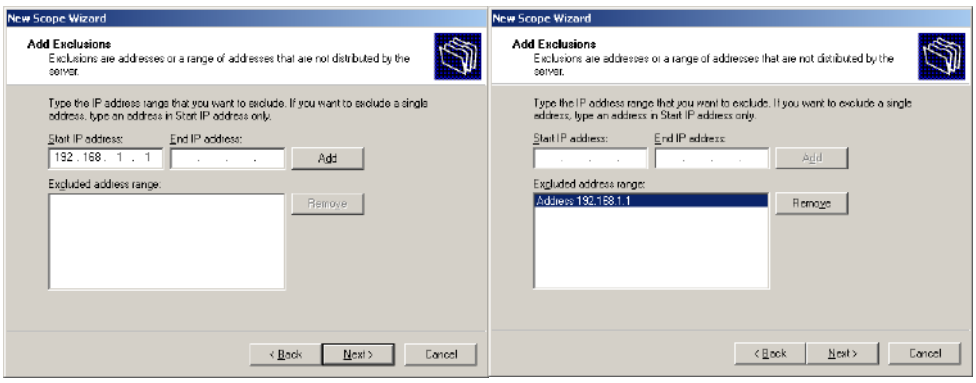

Рис. 106. **IP-адреси, виключені з розподілу DHCP-сервером**

Указуємо термін оренди IP-адреси PC (рис. 107).

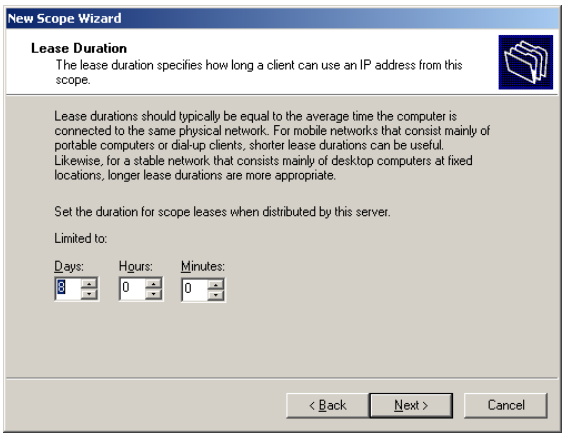

Рис. 107. **Визначення терміну оренди IP-адрес**

Завершуємо налаштування DHCP-сервера (рис. 108).

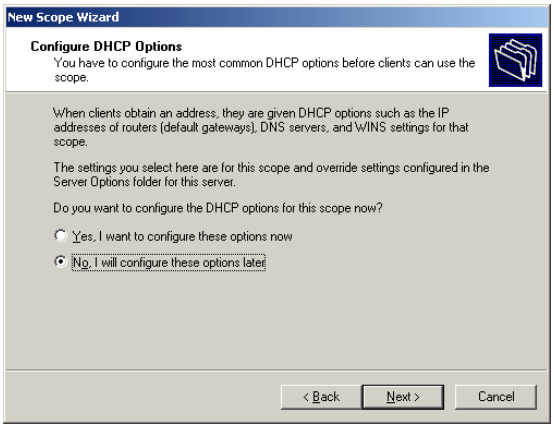

Рис. 108. **Завершення налаштування DHCP-сервера**

Погоджуємося з попередженнями та виходимо з майстра налаштувань сервера, натискаючи кнопки **Finish** (рис. 109).

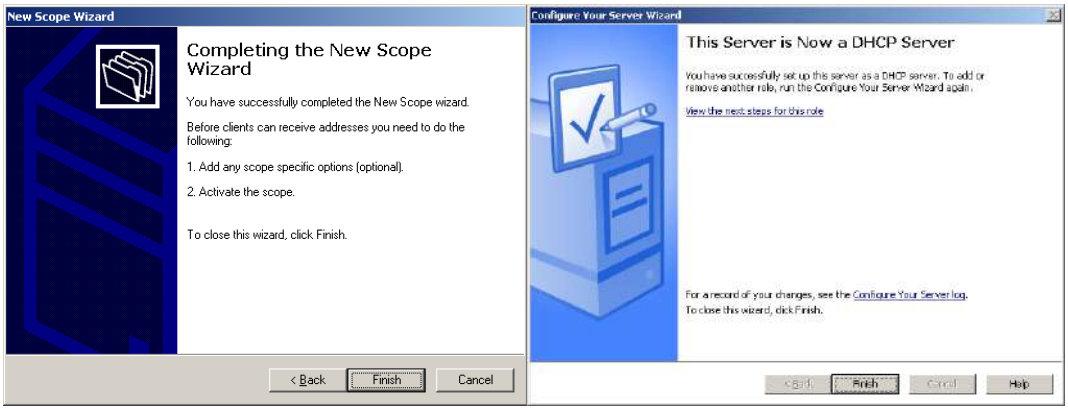

Рис. 109. **Вихід з майстра налаштувань сервера**

Викликаємо програму *Manage Your Server*: Вибираємо: меню **Start -> Manage Your Server** (рис. 110).

Рис. 110. **Виклик програми Manage Your Server**

У вікні, що відкриється, вибираємо пункт **Scope [192.168.1.0] Server**, натискаючи праву кнопку мишки. У меню, що відкриється, вибираємо пункт **Activate** (рис. 111).

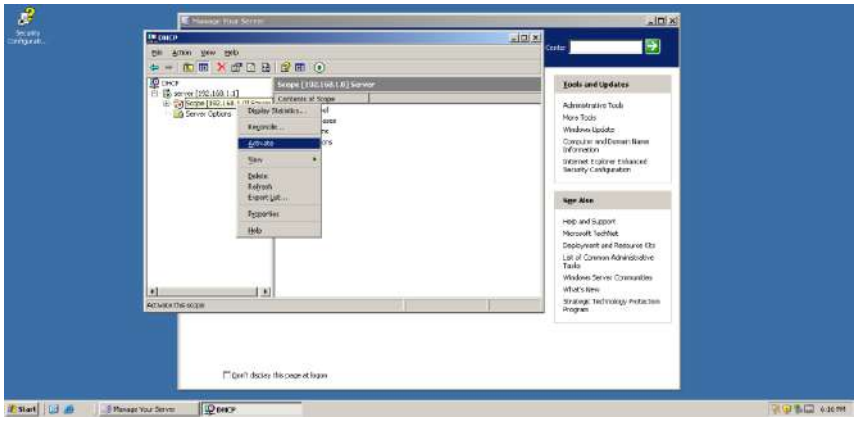

Рис. 111. **Активація діапазону IP-адрес зони**

Викликаємо програму *Windows Firewall*. Вибираємо меню **Start -> Control Panel -> Windows Firewall** (рис. 112).

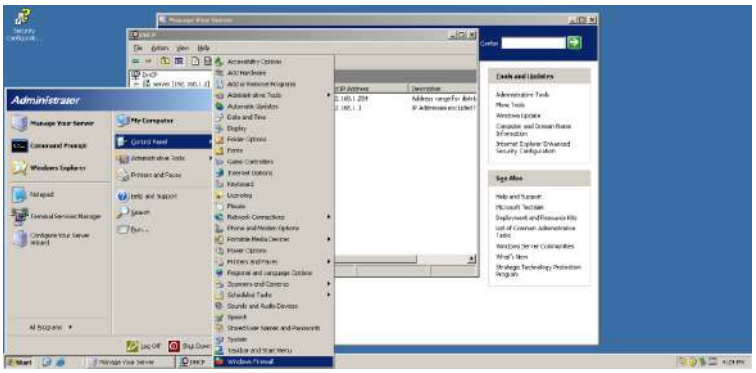

Рис. 112. **Виклик програми Windows Firewall**

Відкриваємо дозвіл на роботу з DHCP-сервером (рис. 113). Для цього у вкладці **Exceptions** вибираємо кнопку **Add Port**. Уводимо назву сервісу, до якого належить порт: **DHCP**. Номер порту: **67**. Вибираємо тип протоколу: **UDP**. Перевіряємо, для яких PC відкрито дозвіл, натискаючи кнопку **Change scope**.

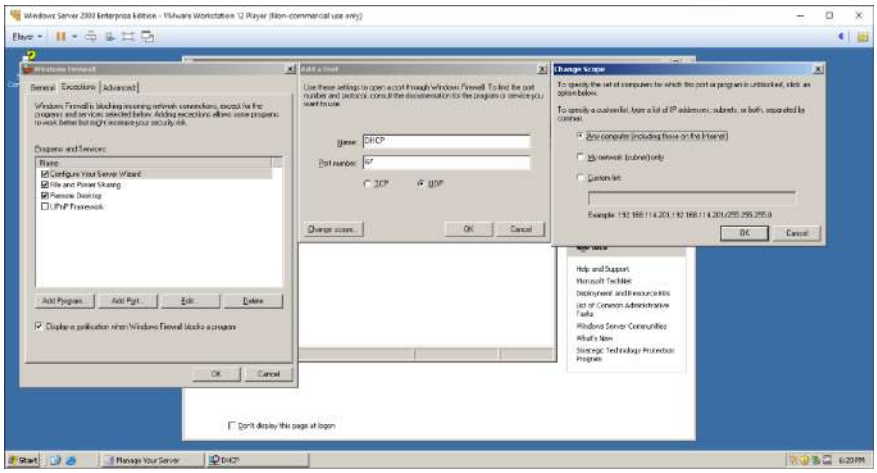

Рис. 113. **Відкриття дозволу на роботу DHCP-сервера в програмі Windows Firewall**

Після виконання відповідних налаштувань у розділі *Program and Services* з'явиться пункт DHCP, дозволяючи доступ до відповідної служби сервера (рис. 114). Закриваємо вікно *Windows Firewall*, натискаючи кнопку **ОК**.

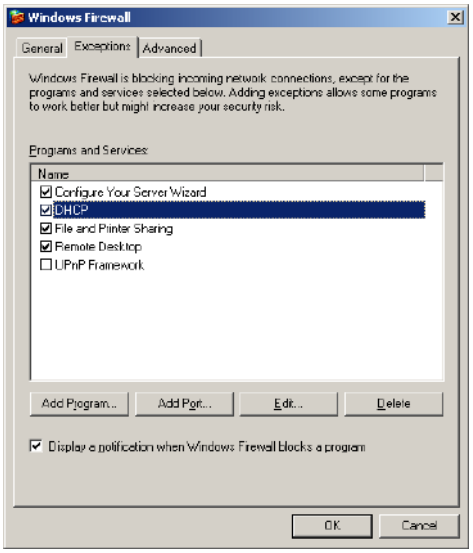

Рис. 114. **Дозвіл на роботу зі службою DHCP**

Завантажуємо ВМ з *Windows XP Professional*, вибираючи у відкритому вікні гіпервізора пункт **Play virtual machine** (рис. 115).

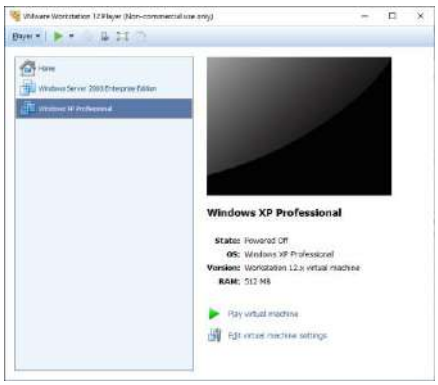

Рис. 115. **Завантаження ВМ з Windows XP Professional**

Налаштовуємо автоматичне отримання IP-адреси на ВМ з ОС *Windows XP Professional*. Відкриваємо вікно *Network Connections*, вибираючи: меню **Start -> Connect to -> Show all connections** (рис. 116).

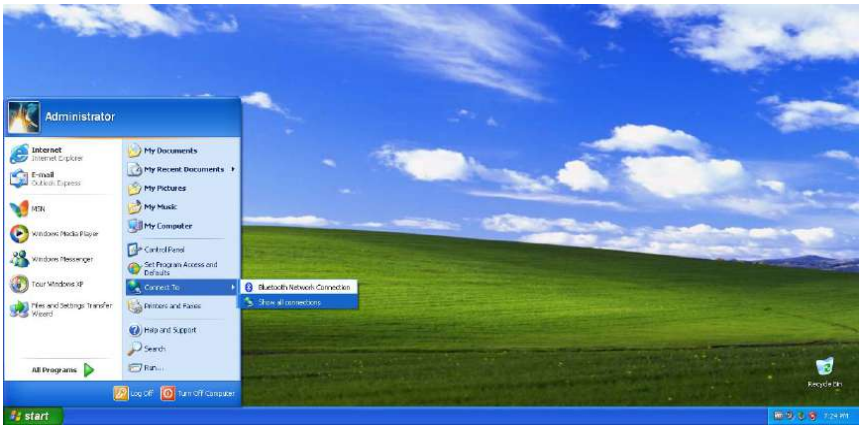

Рис. 116. **Відкриття вікна Network Connections на ВМ з ОС Windows XP Professional**

Натискаємо праву кнопку мишки на пункті **Local Area Connection**. У меню, що відкриється, вибираємо пункт **Properties** (рис. 117).

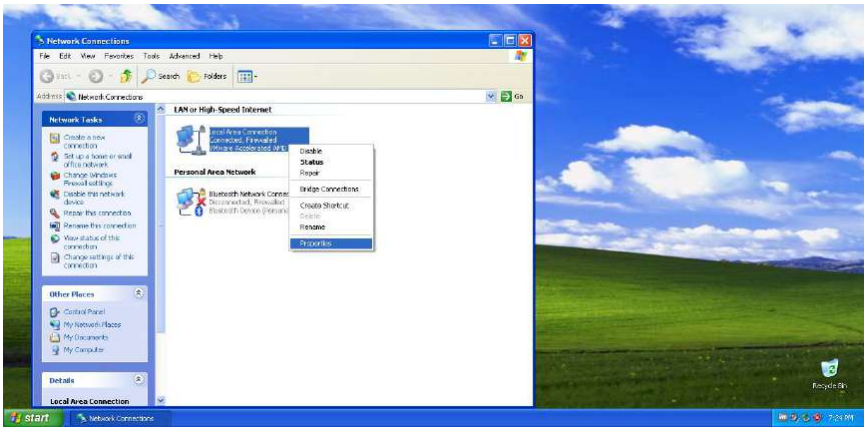

Рис. 117. **Відкриття вікна Local Area Connection Properties**

У вікні *Local Area Connection Properties* на вкладці *General* вибираємо пункт **Internet Protocol (TCP/IP) -> Properties.** У вікні *Internet Protocol (TCP/IP) Properties* на вкладці *General* вибираємо пункти **Obtain an IP address automatically** та **Obtain DNS server address automatically** (рис. 118).

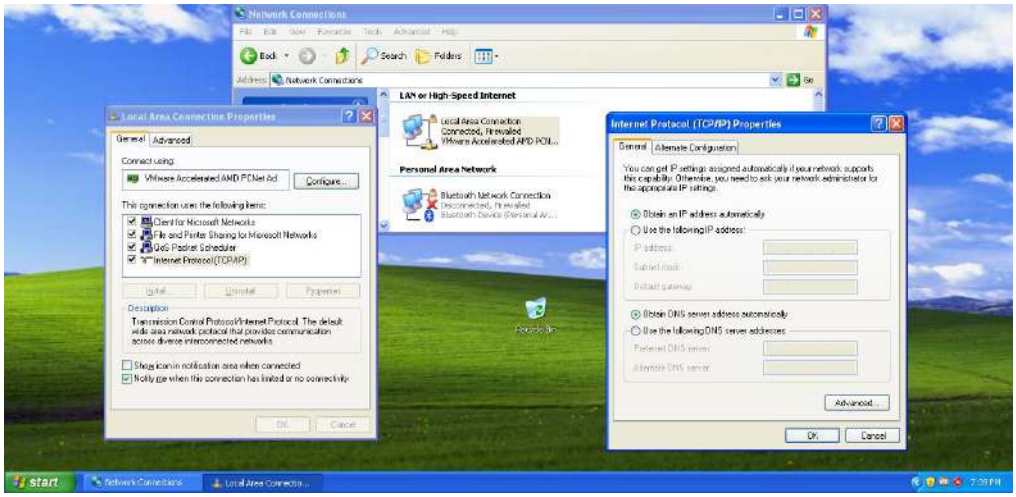

Рис. 118. **Налаштування автоматичного отримання IP-адреси на ВМ з ОС Windows XP Professional**

Перевіряємо отримані РС (ВМ) з ОС *Windows XP Professional* мережеві налаштування (рис. 119).

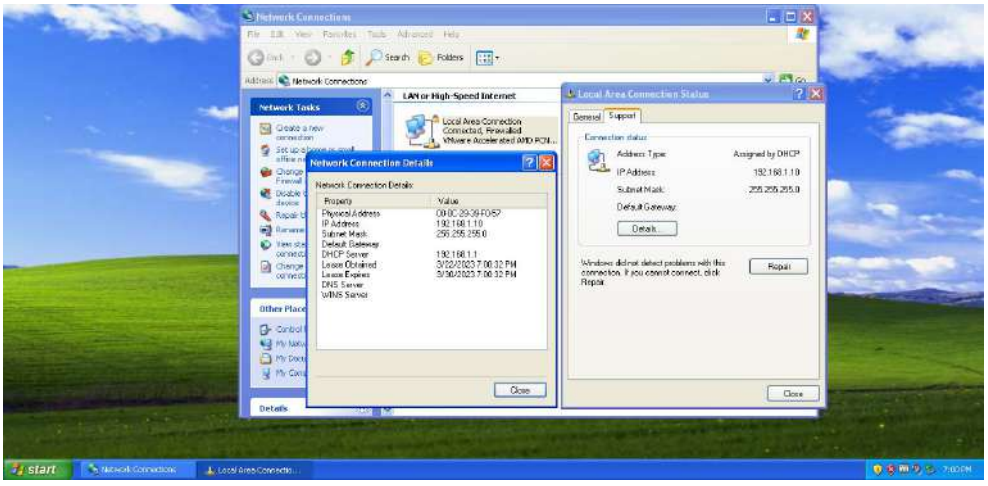

Рис. 119. **Перевірка отриманої IP-адреси та підмережі від DHCP-сервера на ВМ з ОС Windows XP Professional**

За допомогою команд **ipconfig** з ключем **all** та **ping** перевіряємо роботу РС (ВМ) з ОС *Windows XP Professional* з отриманими від DHCP-сервера налаштуваннями (рис. 120).

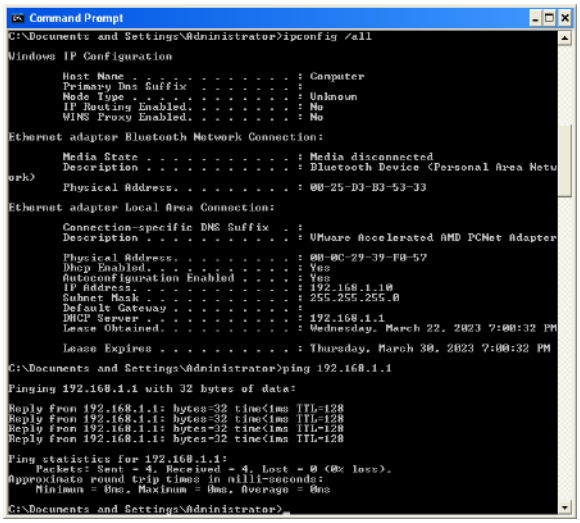

Рис. 120. **Перевірка роботи в мережі PC (ВМ) з ОС Windows XP Professional з отриманими від DHCP-сервера налаштуваннями**

Перевіряємо налаштування DHCP-сервера на PC з ОС *Windows Server 2003 Enterprise Edition* (рис. 121).

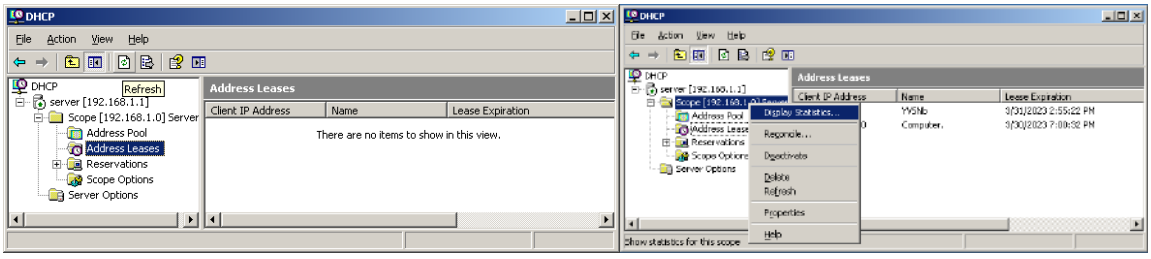

Рис. 121. **Оновлення даних про видані IP-адреси та виклик вікна Display Statistics**

У вікні DHCP вибираємо пункт **Address Leases** та натискаємо кнопку **Refresh**. Дані оновляться. Натискаємо праву кнопку мишки на розділі **Scope [192.168.1.0] Server** та в меню, що відкриється, обираємо пункт **Display Statistics**. Перевіряємо налаштування пунктів *Address Pool* та *Address Leases* вікна DHCP (рис. 122).

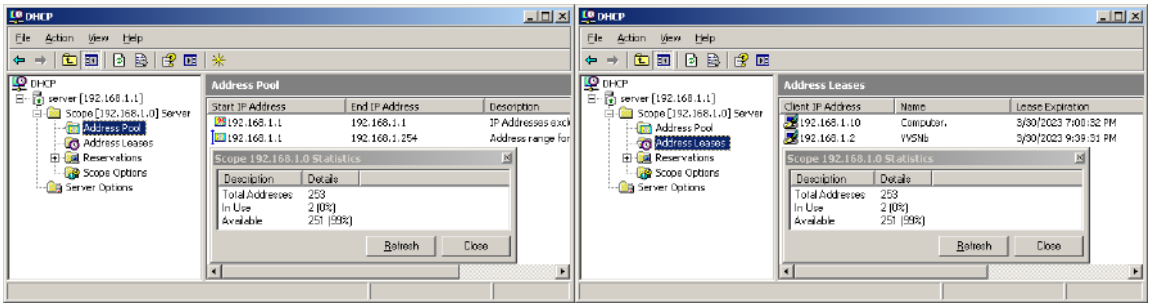

Рис. 122. **Перевірка налаштування загального пулу IP-адрес і орендованих IP-адрес**

У пункті *Reservations* є можливість видавати постійні IP-адреси клієнтам DHCP сервера із загального пулу адрес.

За допомогою команд **ipconfig** з ключем ***/all*** та **ping** проводимо перевірку роботи PC з ОС *Windows Server 2003 Enterprise Edition* з налаштованим DHCP-сервером (рис. 123).

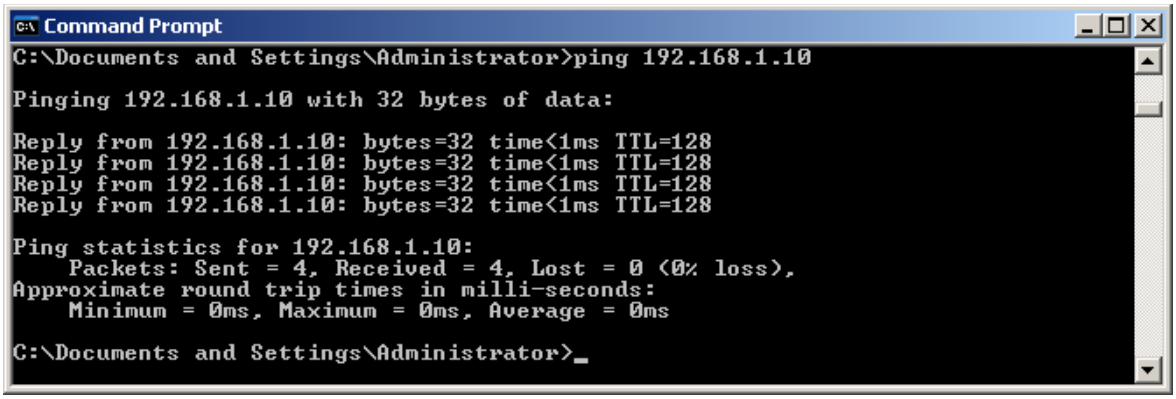

Рис. 123. **Перевірка з PC з Windows Server 2003 Enterprise Edition доступності в мережі PC з Windows XP**

Зміст звіту

1. Назва лабораторної роботи (ЛР), тема, мета й зміст завдань ЛР.
2. Вхідні дані до лабораторної роботи.
3. Навести скриншоти результатів виконання всіх етапів завдань лабораторної роботи.
4. Висновки за результатами виконання ЛР.

Контрольні запитання

1. Яке призначення DHCP-сервера?
2. Для чого визначають виключений діапазон адрес у DHCP-сервері?
3. Для чого використовують резервування IP-адрес?
4. Як виконати налаштування діапазону адрес зони, часу оренди та ін.?
5. Яким чином і де використовують на практиці DHCP-сервер?

Лабораторна робота 3
Конфігурування DNS-сервера засобами Windows Server

Метою лабораторної роботи є конфігурування й перевірка роботи DNS-сервера під час роботи комп'ютерної мережі.

Порядок виконання роботи

Конфігурування й перевірка роботи DNS-сервера

Завантажуємо з гіпервізора ВМ з ОС *Windows Server 2003 Enterprise Edition*. Вибираємо: меню **Start -> Administrative Tool -> Configure Your Server Wizard** (рис. 124).

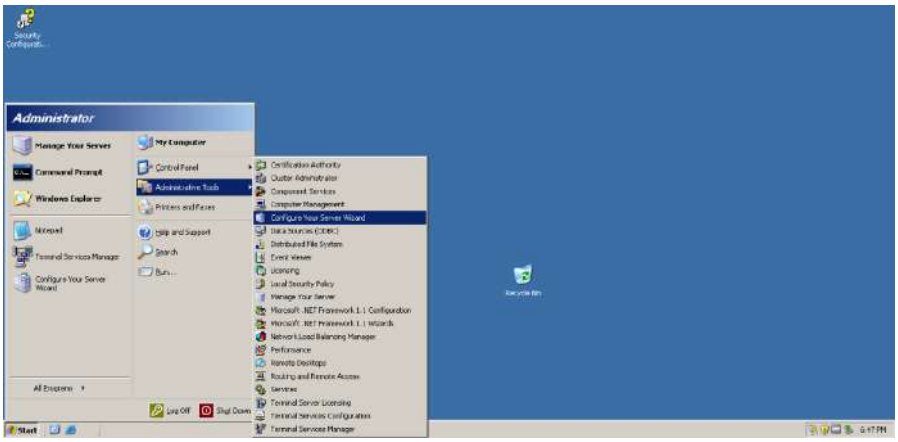

Рис. 124. **Запуск майстра налаштувань Windows Server 2003 Enterprise Edition**

У вікні, що відкриється, вибираємо кнопку **Next** для початку роботи майстра налаштувань (рис. 125).

Рис. 125. **Вікно початку роботи майстра налаштувань сервера**

У наступному вікні вибираємо кнопку **Next** для визначення параметрів мережевих налаштувань (рис. 126).

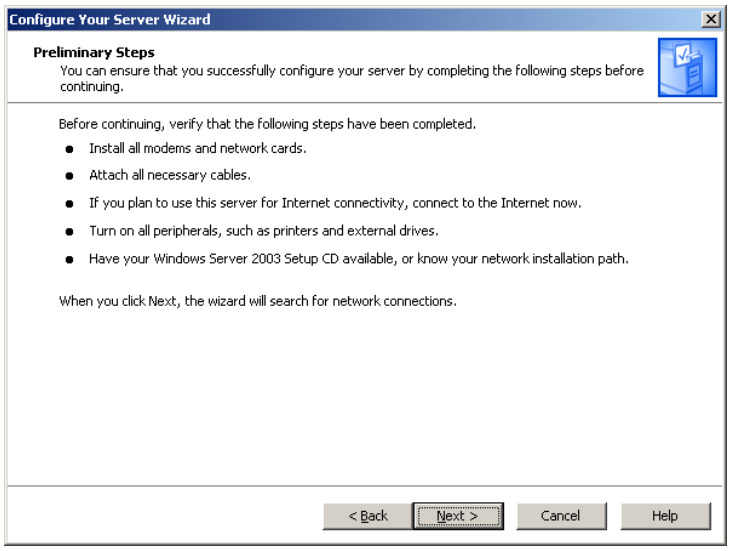

Рис. 126. **Визначення параметрів мережевих налаштувань**

Для налаштування DNS сервера вибираємо пункт **DNS server** і натискаємо кнопку **Next** (рис. 127).

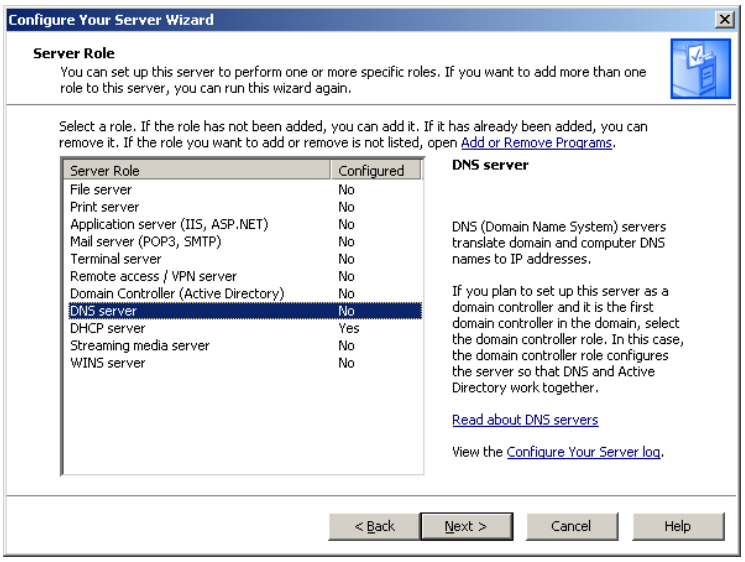

Рис. 127. **Вибір пункту налаштування DNS-сервера**

Починається встановлення DNS-сервера (рис. 128), яке буде складатися з двох етапів:

- установлення програми DNS-сервера (рис. 129);
- запуску майстра налаштування DNS-сервера для налаштування DNS (рис. 130).

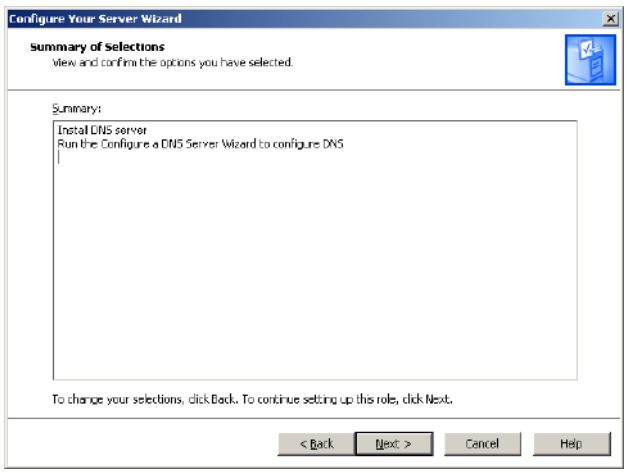

Рис. 128. **Вікно початку встановлення DNS-сервера**

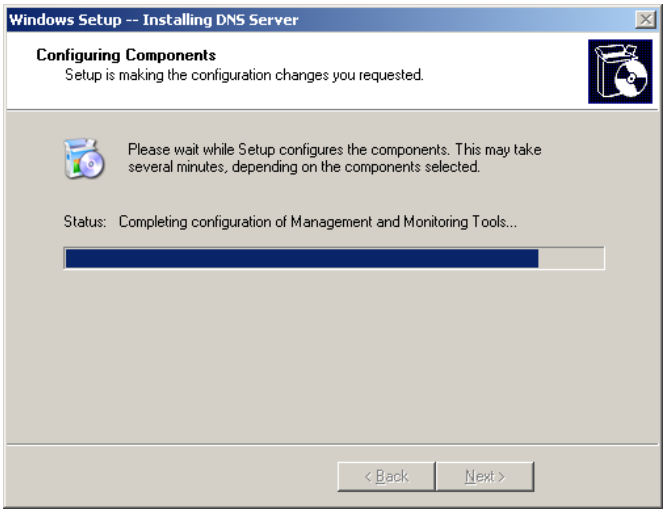

Рис. 129. **Установлення програми DNS-сервера**

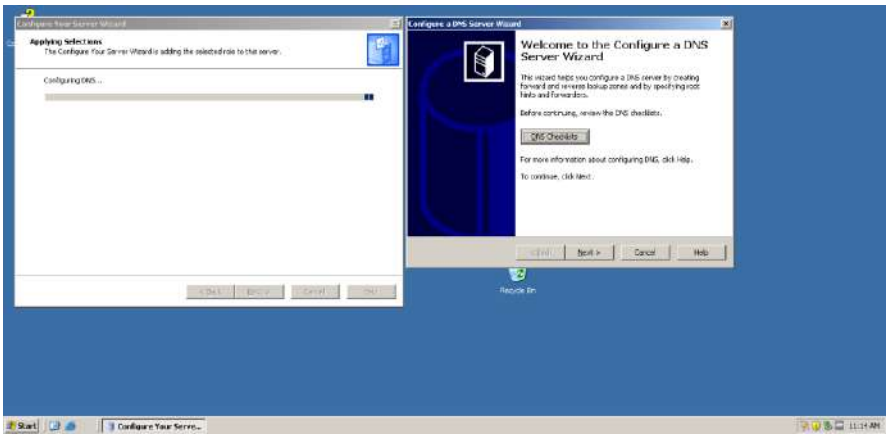

Рис. 130. **Запуск майстра налаштування DNS-сервера**

Переходимо далі, натискаючи кнопки **Next** у кожному з перерахованих вікон. За допомогою майстра налаштувань створюємо зону прямого перегляду (рис. 131).

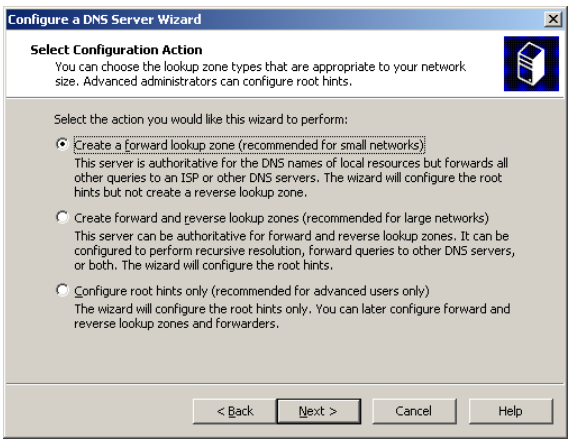

Рис. 131. **Створення зони прямого перегляду**

Вибираємо цей сервер для підтримки зони (рис. 132).

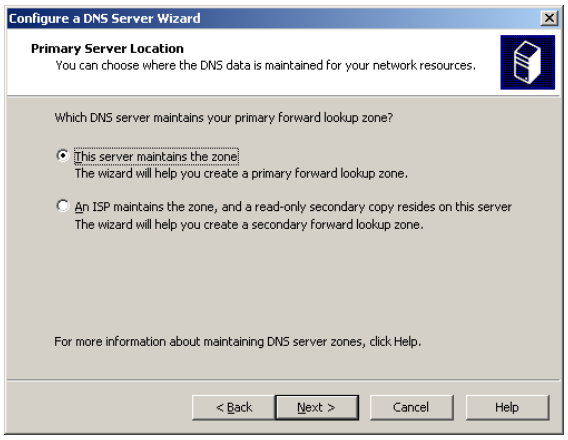

Рис. 132. **Вибір підтримки зони**

Призначаємо ім’я зони. Воно повинно містити **прізвище студента, записане латиницею** (рис. 133).

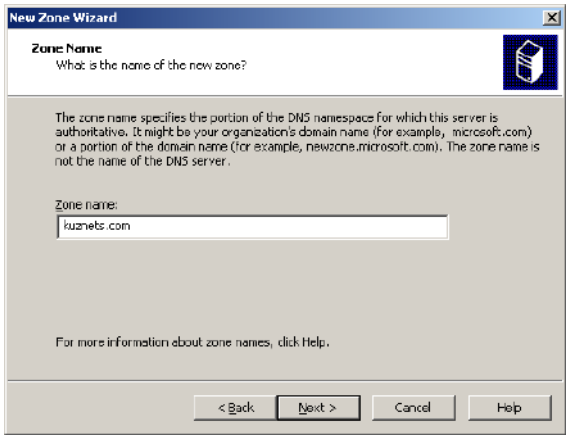

Рис. 133. **Призначення імені зони**

Створюємо новий файл зони (рис. 134).

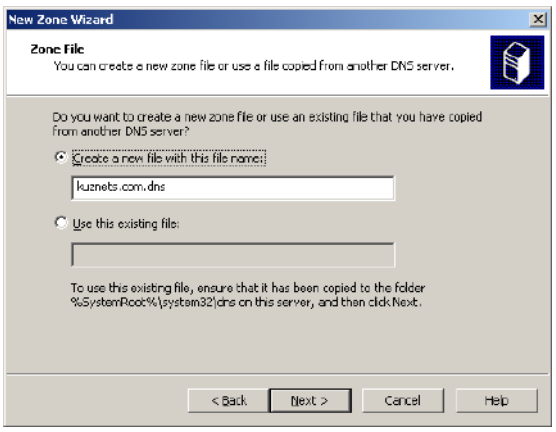

Рис. 134. **Створення нового файлу зони**

Необхідно заборонити динамічне оновлення та пересилання запитів, тому що в мережі не існує інших DNS-серверів (рис. 135 і 136).

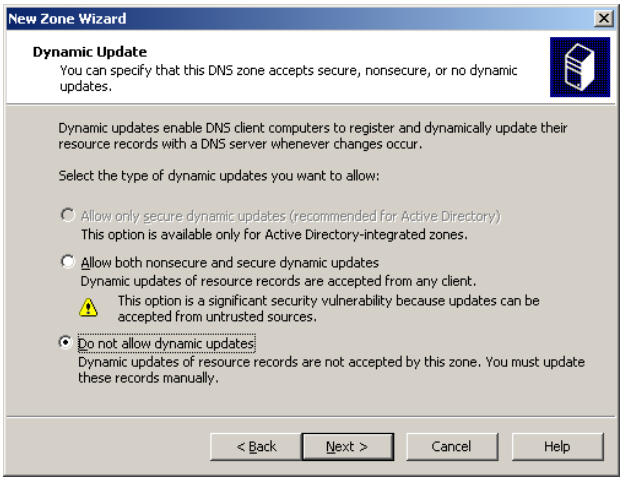

Рис. 135. **Заборона динамічного оновлення**

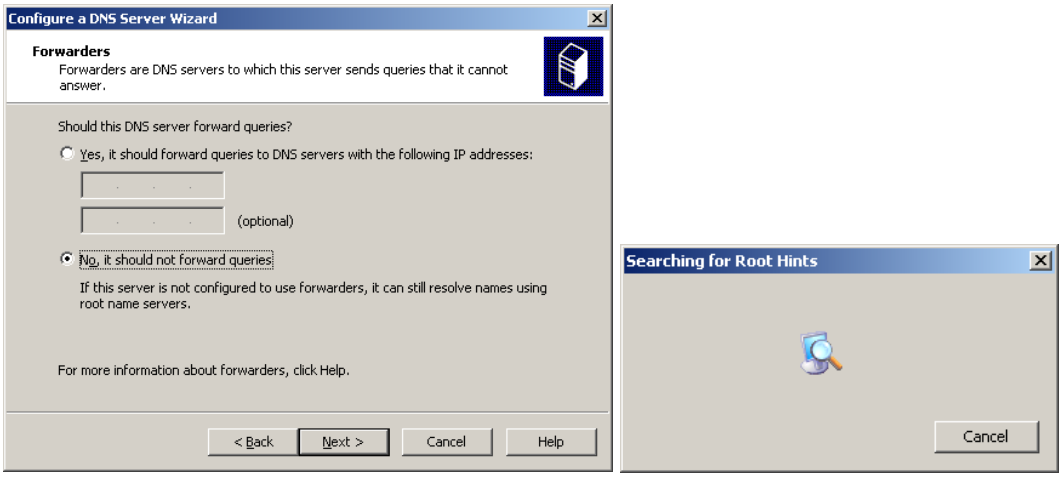

Рис. 136. **Заборона пересилання запитів**

Завершуємо роботу майстра налаштувань DNS-сервера (рис. 137).

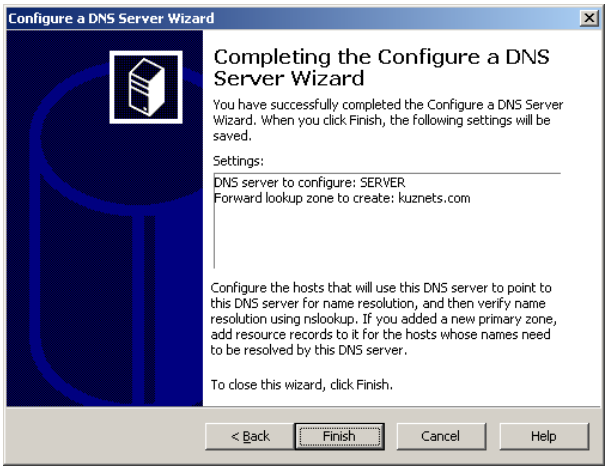

Рис. 137. **Завершення роботи майстра налаштувань DNS-сервера**

Завершуємо роботу майстра налаштування сервера (рис. 138).

Рис. 138. **Завершення роботи майстра налаштувань сервера**

Викликаємо програму *Windows Firewall*: вибираємо меню **Start -> Control Panel -> Windows Firewall** (рис. 139).

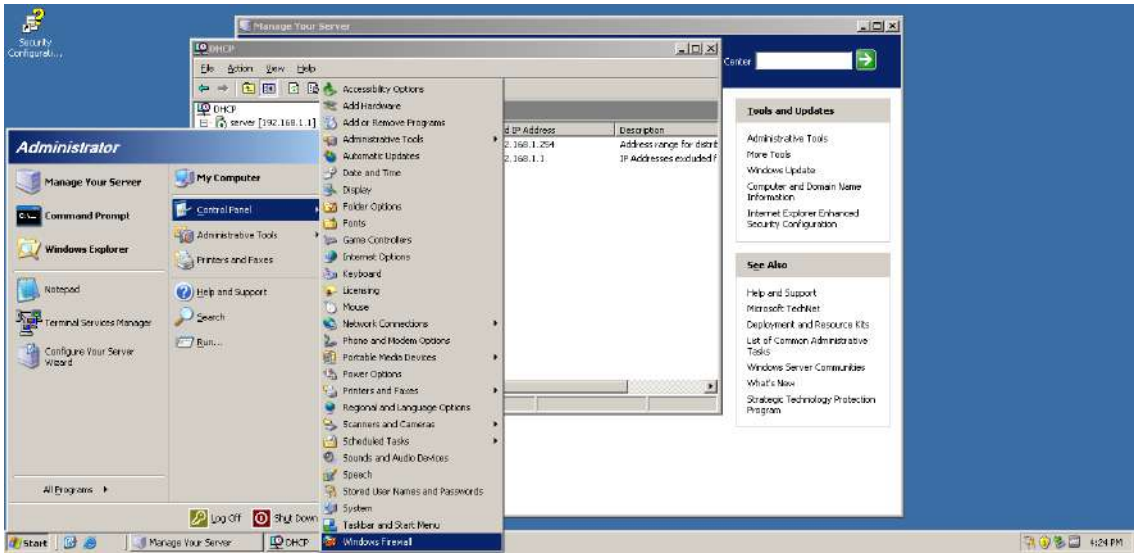

Рис. 139. **Виклик програми Windows Firewall**

Відкриваємо дозвіл на роботу з DNS-сервером за протоколом TCP (рис. 140).

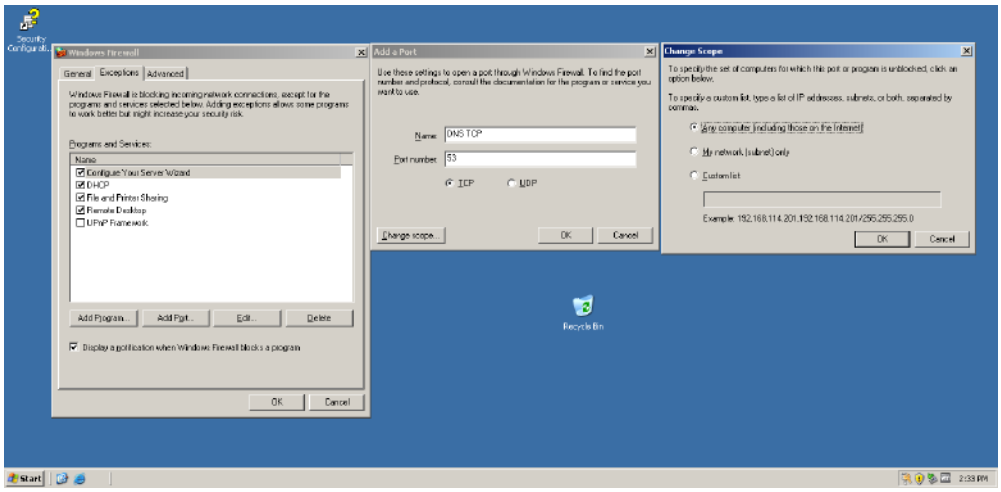

Рис. 140. **Відкриття дозволу на роботу DNS-сервера за протоколом TCP у програмі Windows Firewall**

Для цього у вкладці **Exceptions** вибираємо кнопку **Add Port**. Уводимо назву сервісу, до якого належить порт: **DNS TCP**. Номер порту: **53**. Вибираємо тип протоколу: **TCP**. Перевіряємо, для яких PC відкрито дозвіл, натискаючи кнопку **Change scope**. Повертаємося до вкладки **Exceptions** та відкриваємо дозвіл на роботу з DNS-сервером за протоколом **UDP** (рис. 141). Вибираємо кнопку **Add Port**. Уводимо назву сервісу, до якого належить порт: **DNS UDP**. Номер порту: **53**. Вибираємо тип протоколу: **UDP**. Перевіряємо, для яких PC відкрито дозвіл, натискаючи кнопку **Change scope**.

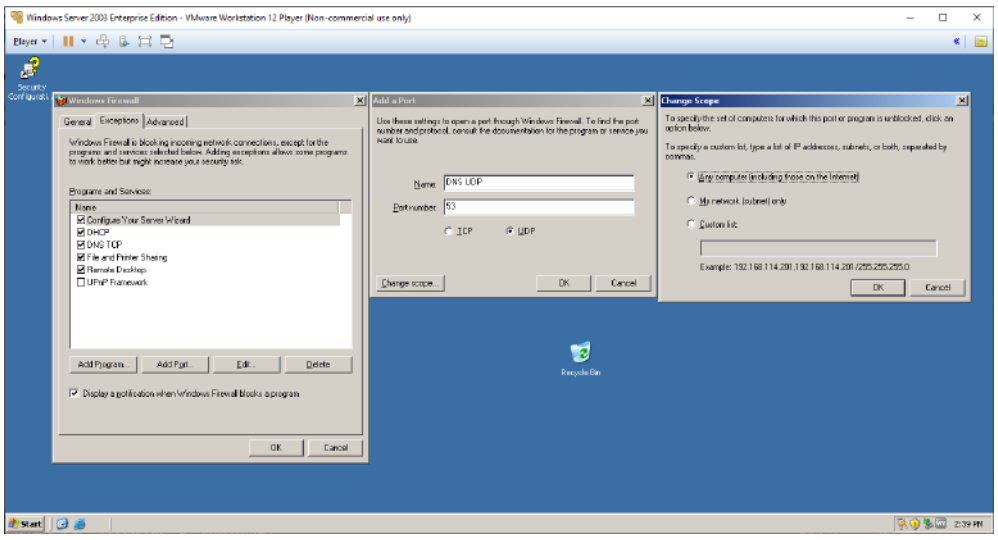

Рис. 141. **Відкриття дозволу на роботу DNS-сервера за протоколом UDP у програмі Windows Firewall**

Після виконання відповідних налаштувань у розділі *Program and Services* з'являться пункти DNS TCP та DNS UDP, дозволяючи доступ до відповідної служби сервера (рис. 142).

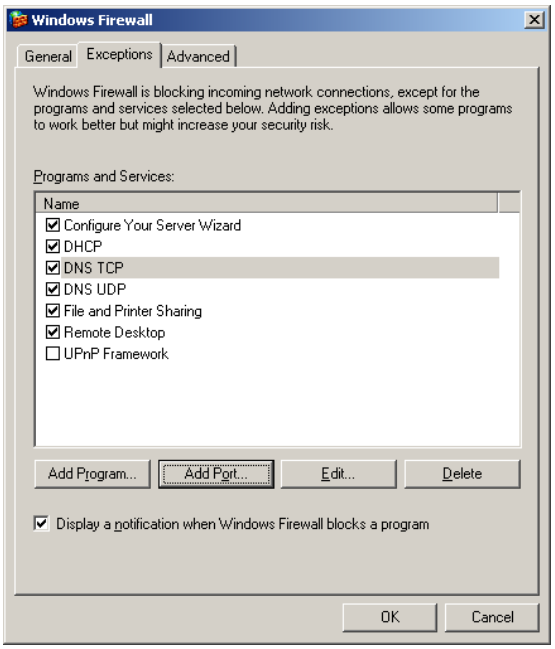

Рис. 142. **Дозвіл на роботу зі службою DNS**

Закриваємо вікно *Windows Firewall* кнопкою **ОК**. Викликаємо програму *Manage Your Server*. Вибираємо: меню **Start -> Manage Your Server** (рис. 143).

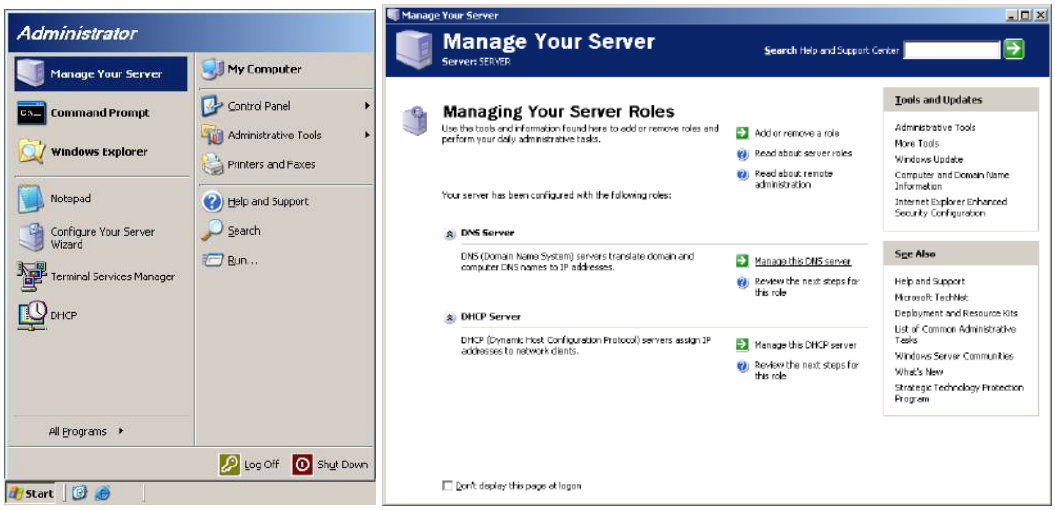

Рис. 143. **Виклик програми Manage Your Server**

Відкриваємо вікно управління DNS-сервером, вибираючи пункт **Manage this DNS server** (рис. 144).

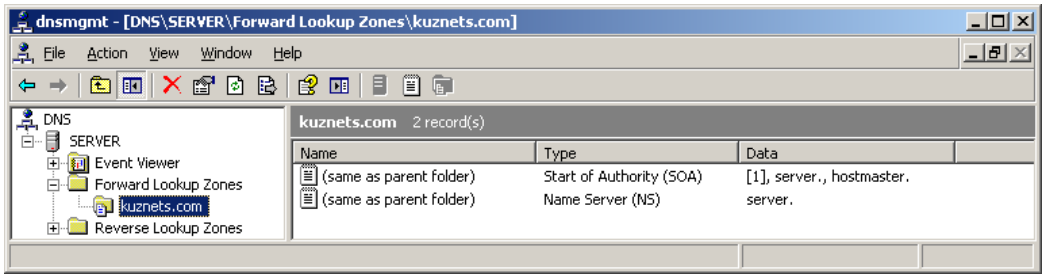

Рис. 144. **Вікно управління DNS-сервером**

Додаємо записи для кореневої РС (ВМ) на ОС *Windows Server 2003 Enterprise Edition* та на РС (ВМ) на ОС *Windows XP Professional* (рис. 145 – 147).

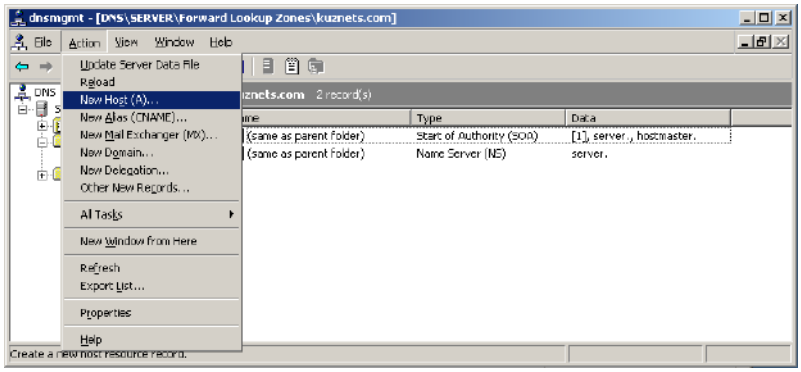

Рис. 145. **Вікно управління DNS-сервером**

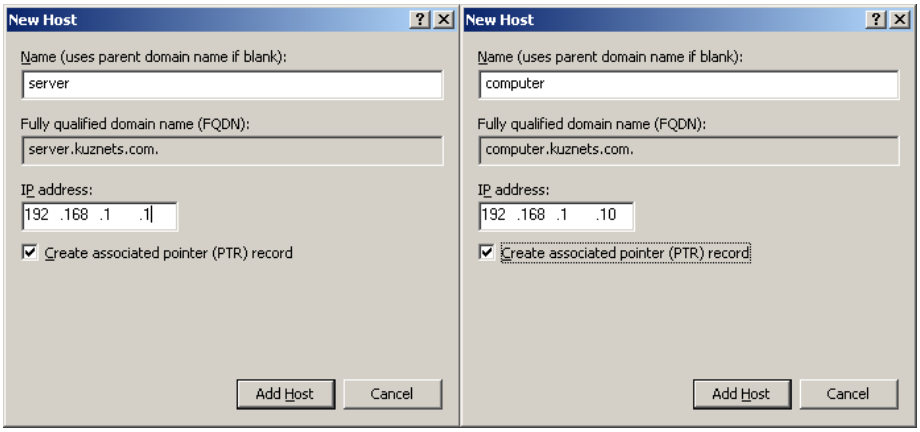

Рис. 146. **Додавання РС**

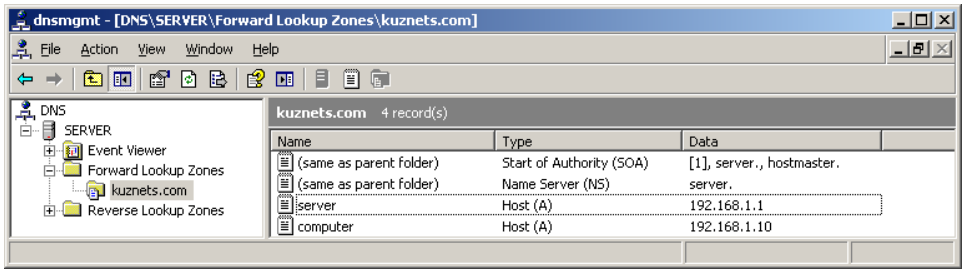

Рис. 147. **Налаштована зона прямого перегляду**

Створюємо зону зворотного перегляду (рис. 148 – 150).

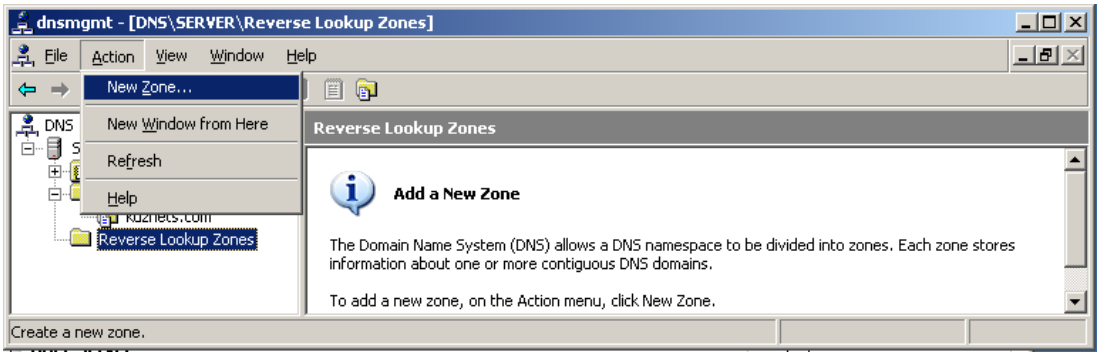

Рис. 148. **Створення нової зони зворотного перегляду**

Рис. 149. **Запуск майстра налаштувань нової зони**

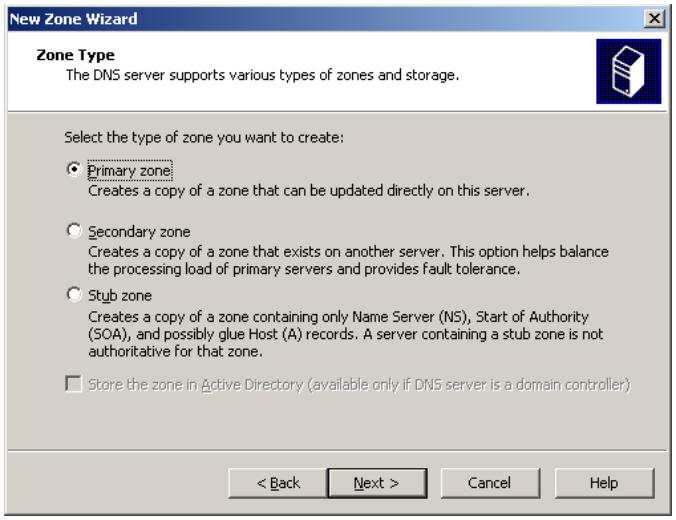

Рис. 150. **Вибір типу зони**

Ідентифікуємо зворотну зону пошуку трьома старшими байтами мережі (IP-адреси мережі) (рис. 151).

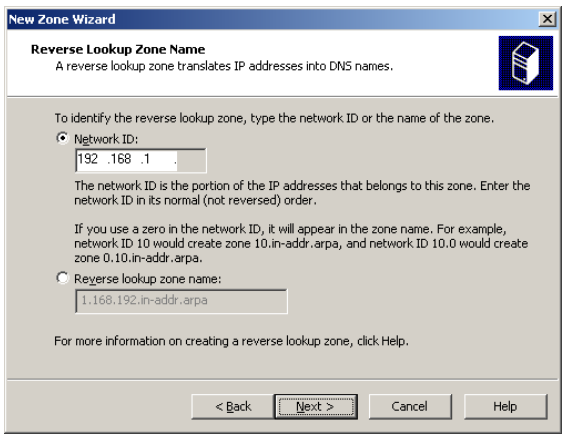

Рис. 151. **Вибір IP-адреси мережі для зворотної зони мережі**

Створюємо файл нової зони (рис. 152).

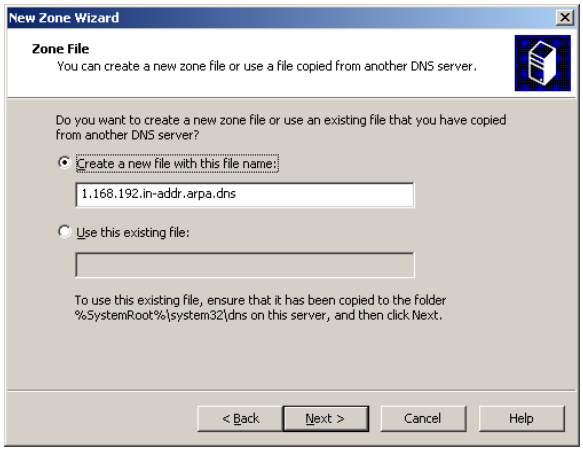

Рис. 152. **Створення імені файлу зони**

Забороняємо динамічне оновлення запису про ресурси для створеної зони та виходимо з майстра налаштувань нової зони (рис. 153 і 154).

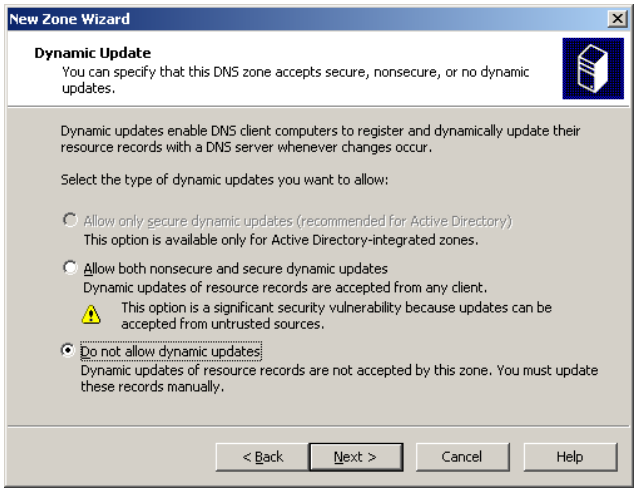

Рис. 153. **Заборона динамічного оновлення для створеної зони**

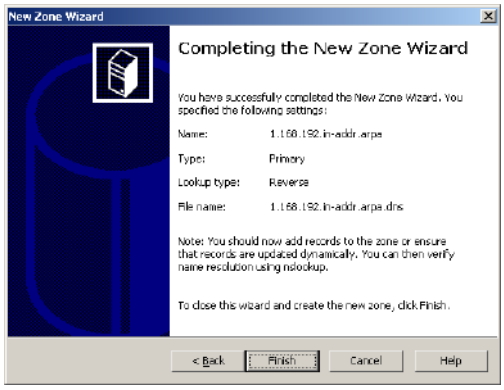

Рис. 154. **Вихід з майстра налаштувань нової зони**

Додаємо записи для кореневої PC (ВМ) *з Windows Server 2003 Enterprise Edition та PC (ВМ) з Windows* XP Professional (рис. 155).

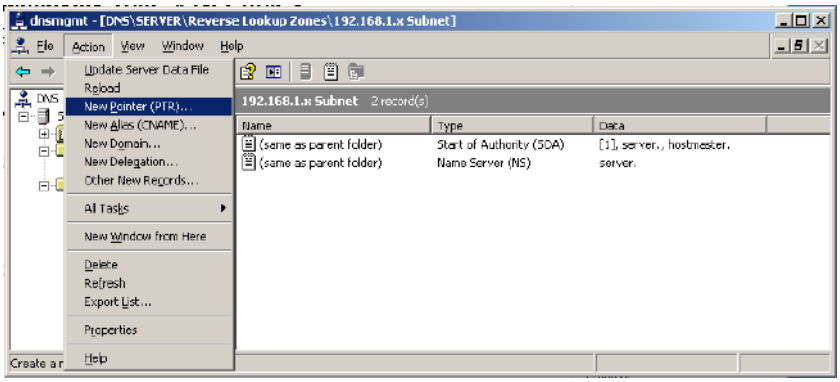

Рис. 155. **Вікно управління DNS-сервером**

Створюємо покажчики для кожної з PC, пов'язуючи їхню IP-адресу, указану в пункті Host IP number, з повним іменем, указаним у пункті *Host name* (рис. 156 і 157). Повне ім'я PC вибираємо, переглядаючи записи, зроблені під час налаштування зони прямого перегляду, у вікні, що відкривається під час натискання на кнопку **Browse**.

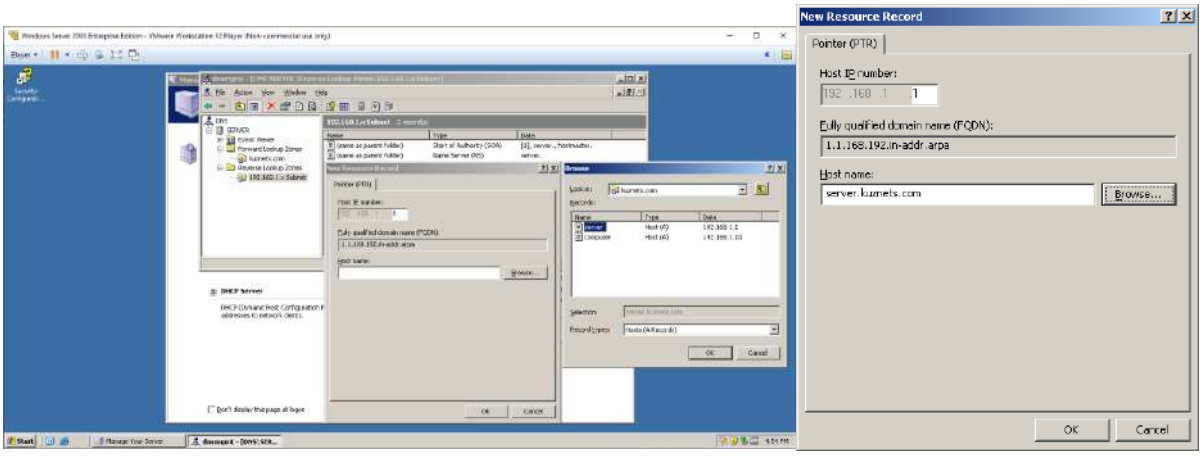

Рис. 156. **Додавання PC (ВМ) з ОС WS 2003 Enterprise Edition**

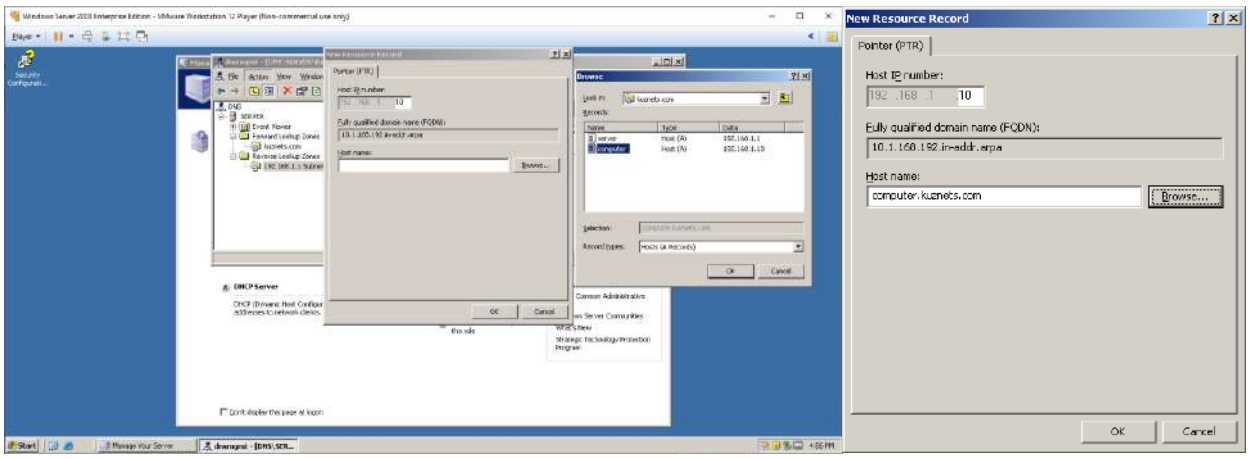

Рис. 157. **Додавання PC (ВМ) з ОС Windows XP Professional**

Перевіряємо налаштування зони зворотного перегляду (рис. 158).

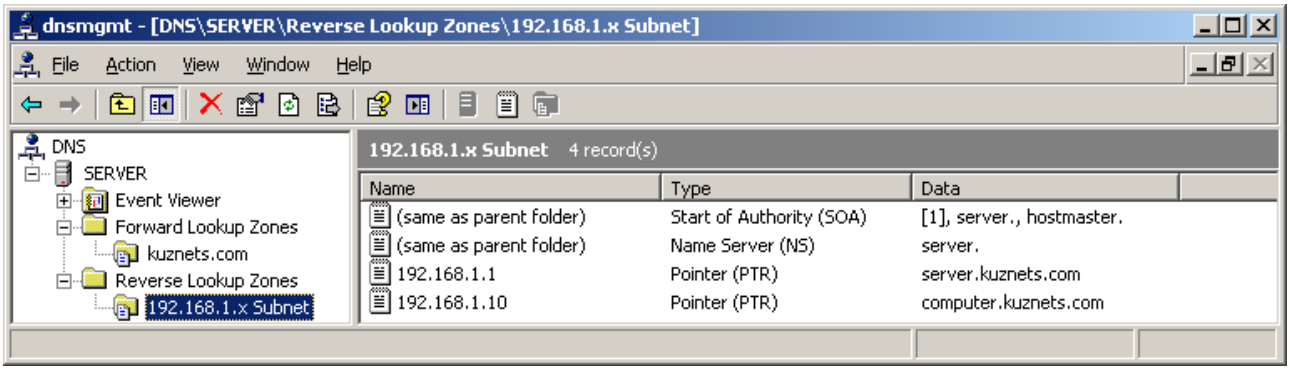

Рис. 158. **Налаштована зона зворотного перегляду**

Перед перевіркою роботи DNS-сервера необхідно виконати його додаткові налаштування таким чином, щоб він видавав PC з *Windows XP Professional*, окрім IP-адреси і маски підмережі, ще й адресу сервера, на якому розгорнуто DNS-сервер. У вікні налаштування DHCP вибираємо пункт **Server Options**, а в меню **Action** – пункт **Configure Option** (рис. 159).

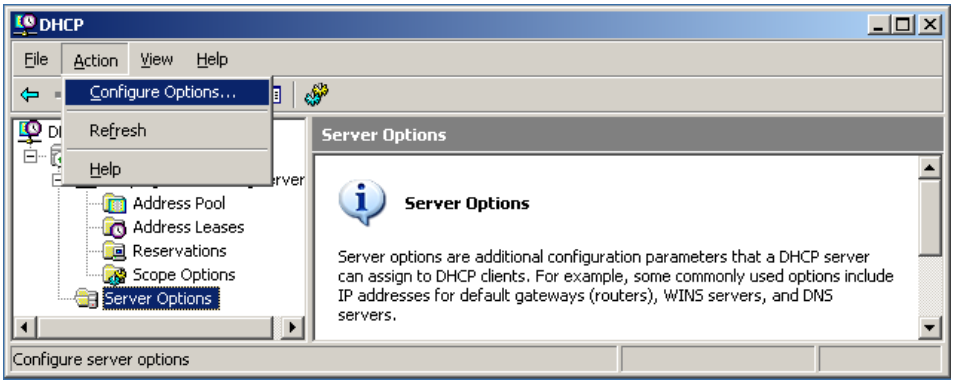

Рис. 159. **Вхід у вікно налаштування DNS-сервера в DHCP**

У вкладці *General* вікна *Server Options* налаштовуємо DNS-сервер (рис. 160).

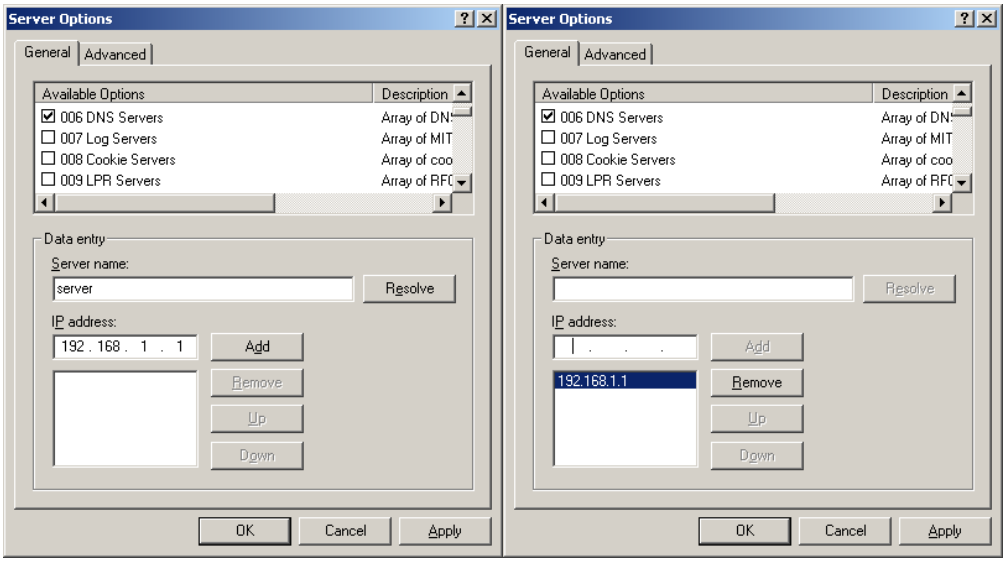

Рис. 160. **Налаштування DNS-сервера в DHCP**

Перевіряємо виконані налаштування (рис. 161).

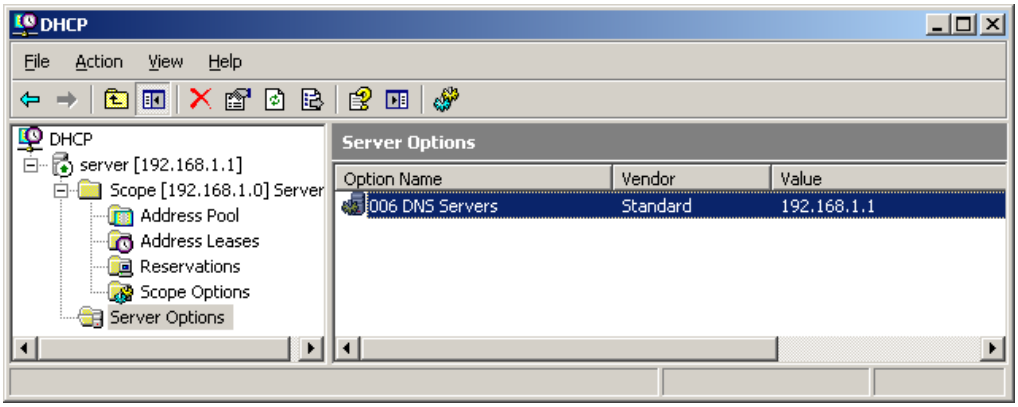

Рис. 161. **Перевірка виконаних налаштувань DNS-сервера в DHCP**

На РС (ВМ) з ОС *Windows XP Professional* перевіряємо отриману інформацію про IP-адресу DNS-сервера (рис. 162). Заходимо у вікно *Network Connections*. Переходимо у вікно *Local Area Connection Status* та вибираємо вкладку **Support**. Натискаємо кнопку **Details**. Відкриється вікно *Network Connections Details*, де перевіряємо пункт **DNS Server**.

Якщо в цьому пункті не вказано ніякої IP-адреси, то натискаємо кнопку **Close** та повертаємося в попереднє вікно. Повторюємо отримання мережевих налаштувань кнопкою *Repair* та повторно перевіряємо пункт **DNS Server**.

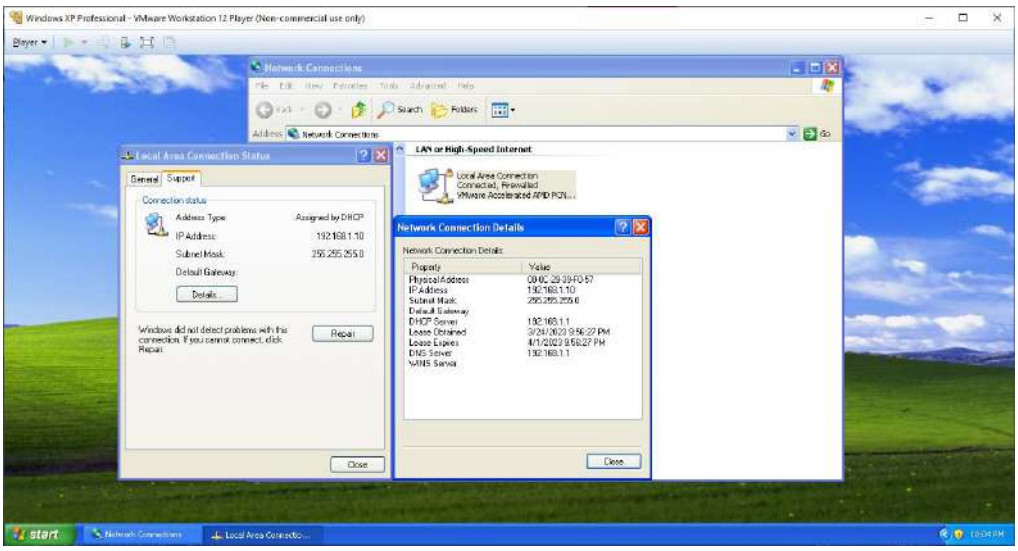

Рис. 162. **Перевірка інформації про IP-адресу DNS-сервера**

Перевіряти роботу DNS-сервера будемо на PC з ОС *Windows XP Professional*. Для перевірки роботи використовуємо команди: **ping** та **nslookup**. Викликаємо вікно **Command Prompt**, у командному рядку якого вводимо команду **nslookup**. У програмі послідовно вводимо IP-адреси та доменні імена PC з ОС *Windows Server 2003 Enterprise Edition* і PC з ОС *Windows XP Professional* (рис. 163).

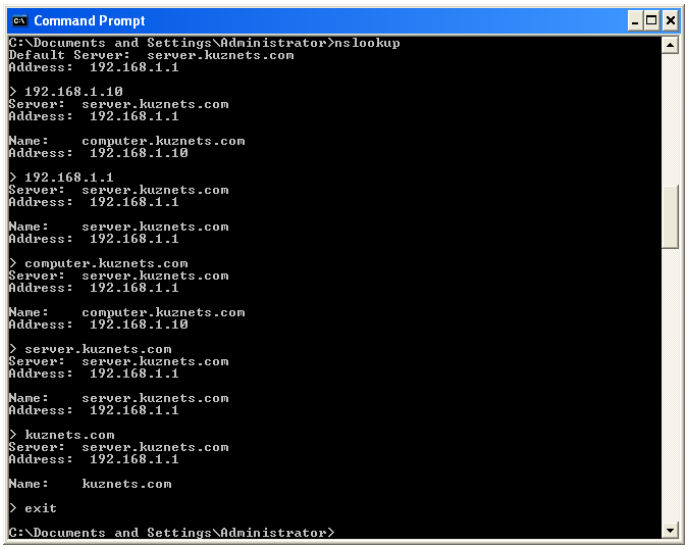

Рис. 163. **Результат виконання команди nslookup**

Проводимо перевірку роботи мережі з використанням DNS-імен за допомогою команди **ping**. Необхідно на PC з ОС *Windows Server 2003 Enterprise Edition* задати ім'я PC з ОС *Windows XP Professional* (рис. 164), а на PC з ОС *Windows XP Professional* задати ім'я PC з ОС *Windows Server 2003 Enterprise Edition* (рис. 165).

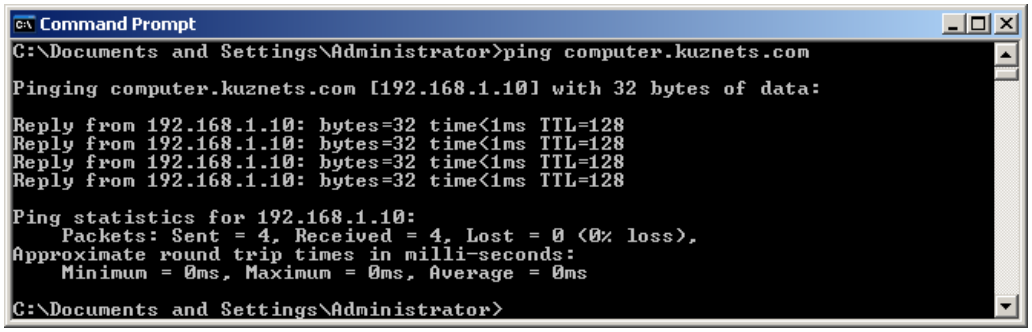

Рис. 164. **Перевірка з'єднання PC з ОС Windows Server 2003 Enterprise Edition та PC з ОС Windows XP Professional командою ping**

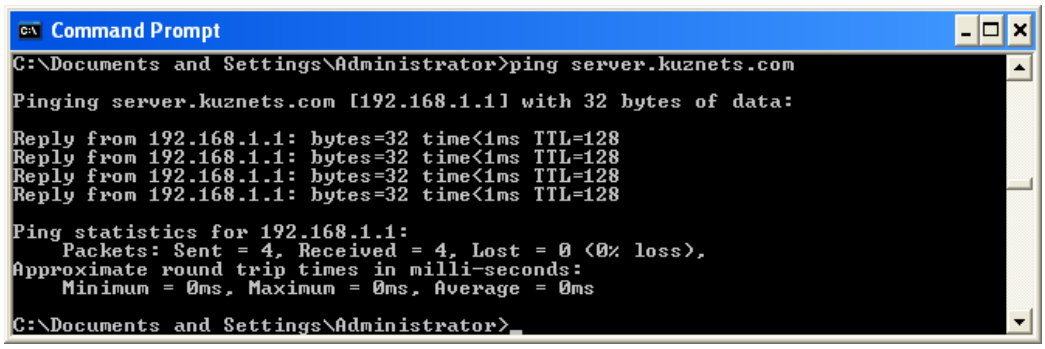

Рис. 165. **Перевірка з'єднання PC з ОС Windows XP Professional та PC з ОС Windows Server 2003 Enterprise Edition командою ping**

Зміст звіту

1. Назва (тема) лабораторної роботи, мета й зміст завдань ЛР.
2. Вихідні дані до ЛР.
3. Навести скриншоти результатів виконання всіх етапів завдань ЛР.
4. Висновки з ЛР.

Контрольні запитання

1. Яке призначення DNS-сервера?
2. Що є прямою зоною DNS-сервера?
3. Що є зворотною зоною DNS-сервера?
4. Яким чином визначають батьківську зону (адресу) під час створення нової прямої зони в DNS-сервері?
5. Яким чином визначають дочірню зону (адресу) під час створення нової прямої зони в DNS-сервері?
6. Яким чином і де використовують на практиці DNS-сервер?
7. Для чого використовують команду **nslookup**?

Лабораторна робота 4
Установка поштового сервера засобами Windows Server

Метою лабораторної роботи є встановлення поштового сервера та створення клієнтських облікових записів засобами *Windows Server 2003 Enterprise Edition.*

Порядок виконання роботи

Для виконання лабораторної роботи (ЛР) будемо використовувати робочу станцію (РС) з ОС *Windows Server 2003 Enterprise Edition*. Завантажуємо з гіпервізора ВМ з *Windows Server 2003 Enterprise Edition*. Вибираємо: меню **Start -> Administrative Tool -> Configure Your Server Wizard** (рис. 166).

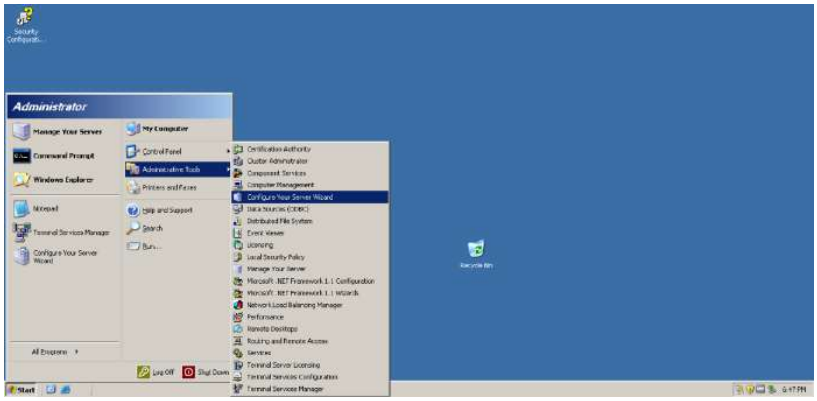

Рис. 166. **Запуск майстра налаштувань Windows Server 2003 Enterprise Edition**

У вікні, що відкриється, вибираємо кнопку **Next** для початку роботи майстра налаштувань (рис. 167).

Рис. 167. **Вікно початку роботи майстра налаштувань сервера**

У наступному вікні вибираємо кнопку **Next** для визначення параметрів мережевих налаштувань (рис. 168).

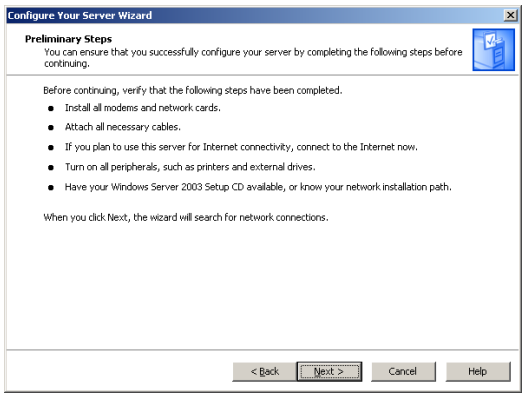

Рис. 168. **Визначення параметрів мережевих налаштувань**

Для налаштування поштового сервера вибираємо пункт **Mail server (POP3, SMTP)** та натискаємо кнопку **Next** (рис. 169).

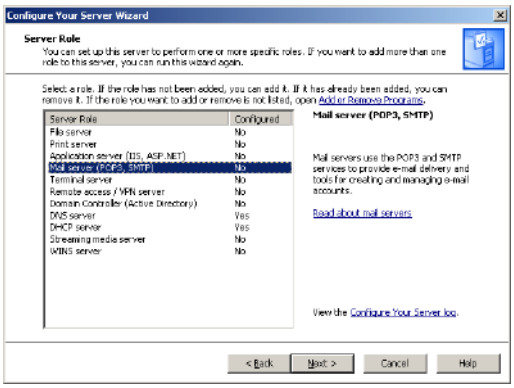

Рис. 169. **Вибір пункту налаштування поштового сервера**

У вікні *Configure POP3 Service*, що з'явиться, вибираємо метод автентифікації: **Local Windows Accounts** та вводимо доменне ім'я сервера електронної пошти: **server.kuznets.com** (рис. 170).

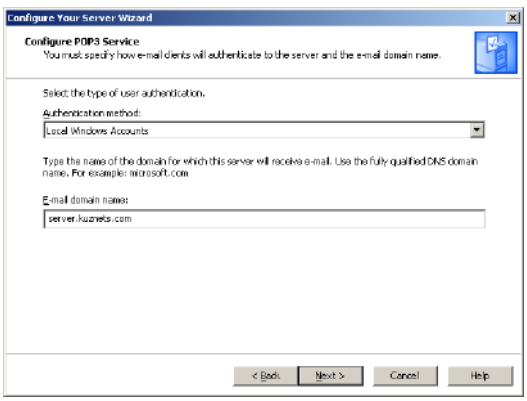

Рис. 170. **Вибір методу автентифікації та введення імені домену**

У вікні *Configure POP3 Service*, що з'явиться, вибираємо метод автентифікації: **Local Windows Accounts** та вводимо доменне ім'я сервера електронної пошти: **server.kuznets.com** (див. рис. 170).

Після натискання кнопки **Next**, з'явиться вікно з вибраними параметрами. Буде встановлено POP3 та SMTP, дозвіл POP3 поштовому клієнту відправляти та отримувати поштові повідомлення (рис. 171).

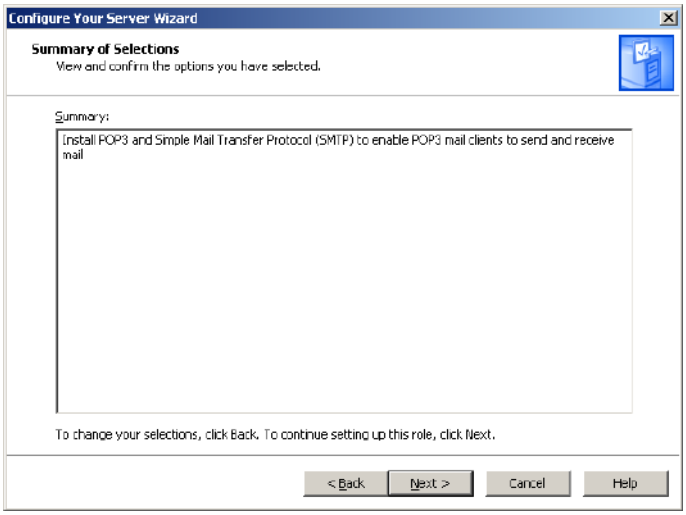

Рис. 171. **Вікно з вибраними параметрами**

Натискаємо кнопку **Next** для початку встановлення (рис. 172).

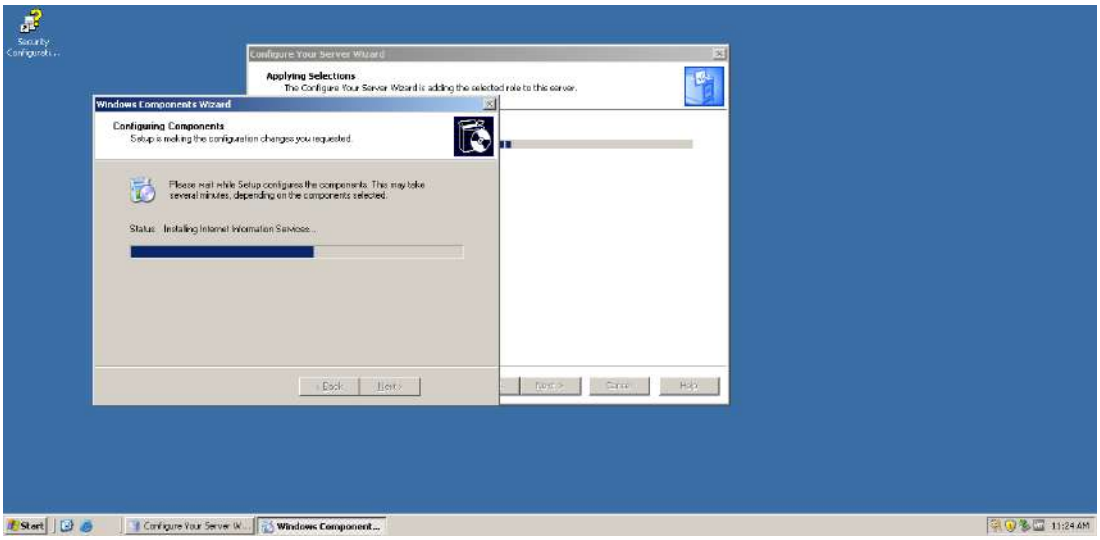

Рис. 172. **Установлення POP3 та SMTP**

Після закінчення встановлення необхідних файлів закриваємо вікно майстра налаштувань сервера, натискаючи кнопку **Finish** (рис. 173).

Рис. 173. **Вікно завершення роботи майстра налаштувань сервера**

Викликаємо програму *Manage Your Server*. Вибираємо: меню **Start -> Manage Your Server** (рис. 174).

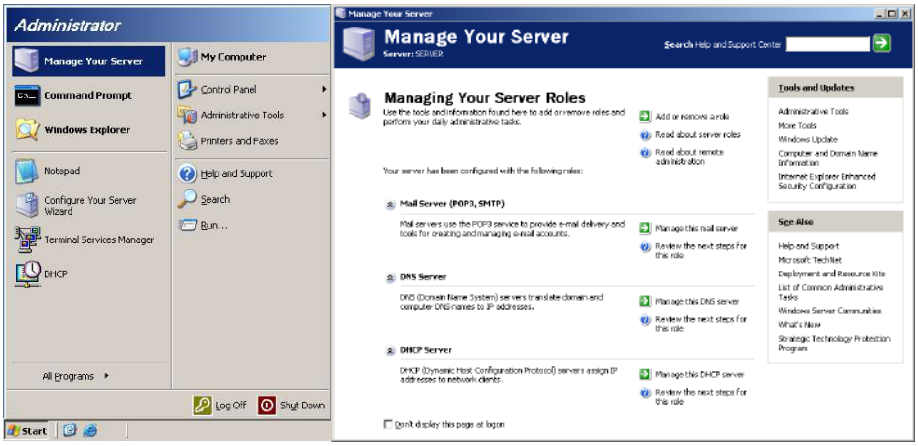

Рис. 174. **Виклик програми Manage Your Server**

Вибираємо пункт **Manage this mail server** у розділі *Mail Server* (POP3, SMTP). У вікні *POP3 Service*, що відкриється, створюємо поштові скриньки, натискаючи кнопку **Add Mailbox** (рис. 175).

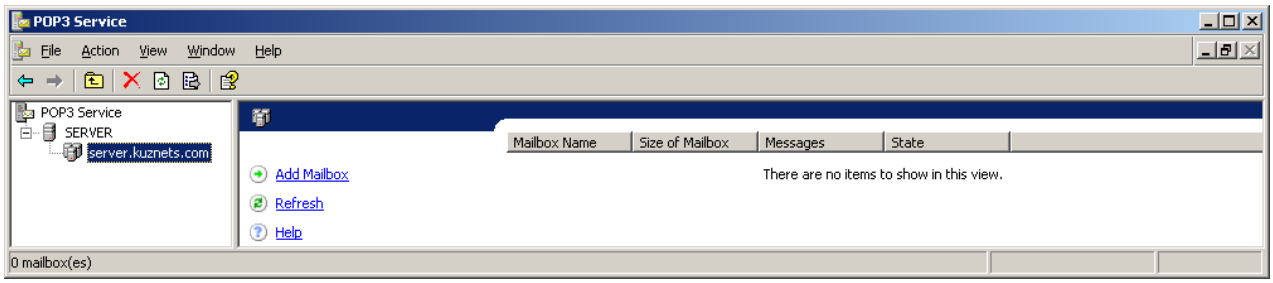

Рис. 175. **Вікно служби POP3**

Уводимо ім'я поштової скриньки **(вибрати прізвище студента латиницею з числом)** та пароль для авторизації користувача (рис. 176).

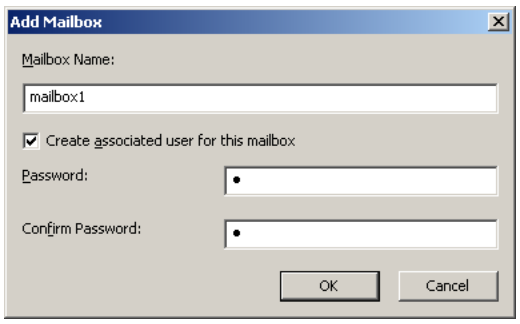

Рис. 176. **Створення поштової скриньки та пароля для авторизації користувача**

Після створення поштової скриньки виводиться підсумкова інформація про створену поштову скриньку (рис. 177).

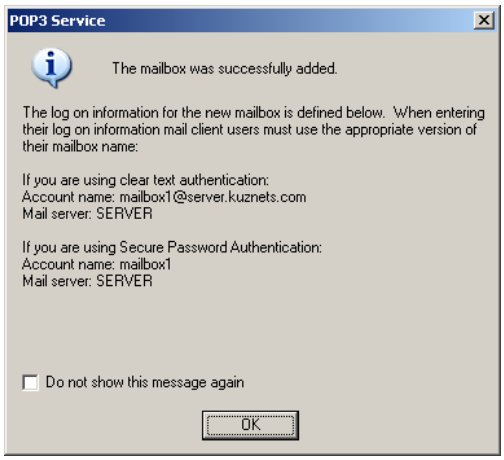

Рис. 177. І**нформація про створену поштову скриньку**

Створюємо три поштові скриньки (облікові записи) на поштовому сервері (рис. 178).

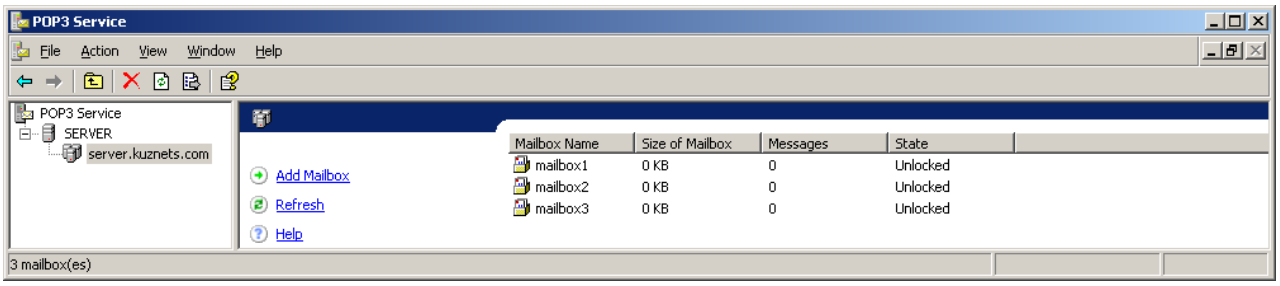

Рис. 178. **Вікно зі створеними обліковими записами користувачів**

Результатом конфігурування поштового сервера є створення облікових записів користувачів для роботи в конкретному домені на поштовому сервері.

Викликаємо програму *Windows Firewal*. Вибираємо меню **Start -> Control Panel -> Windows Firewall**. У вікні, що відкриється, вибираємо вкладку **Advanced** та в розділі *Network Connection Settings* натискаємо кнопку **Settings** (рис. 179).

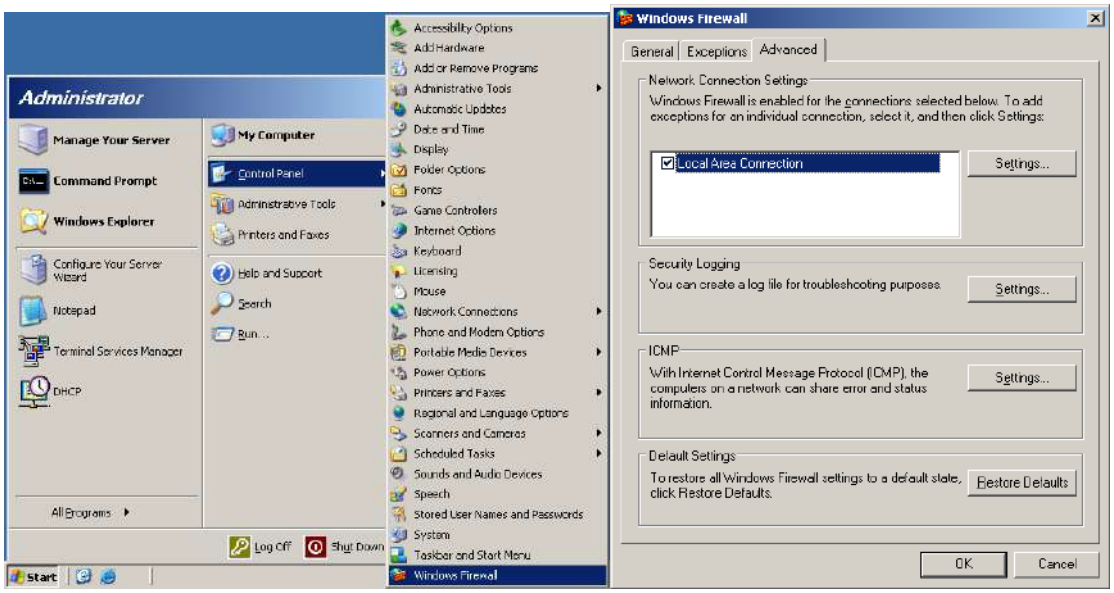

Рис. 179. **Виклик програми Windows Firewall**

У вікні *Advanced Settings* треба поставити галочки в пунктах: **Internet Mail Server (SMTP), Post-Office Protocol Version 3 (POP3)** (рис. 180).

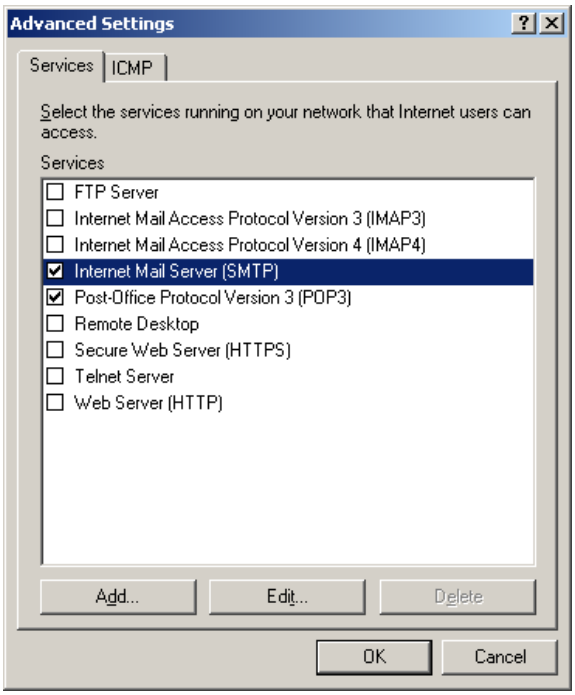

Рис. 180. **Налаштування дозволу на роботу із сервісами**

Перевірка роботи поштового сервера за допомогою поштової програми Outlook Express

Завантажуємо з гіпервізора ВМ з ОС *Windows XP Professional* та вибираємо **вбудовану поштову програму Outlook Express** у меню (рис. 181).

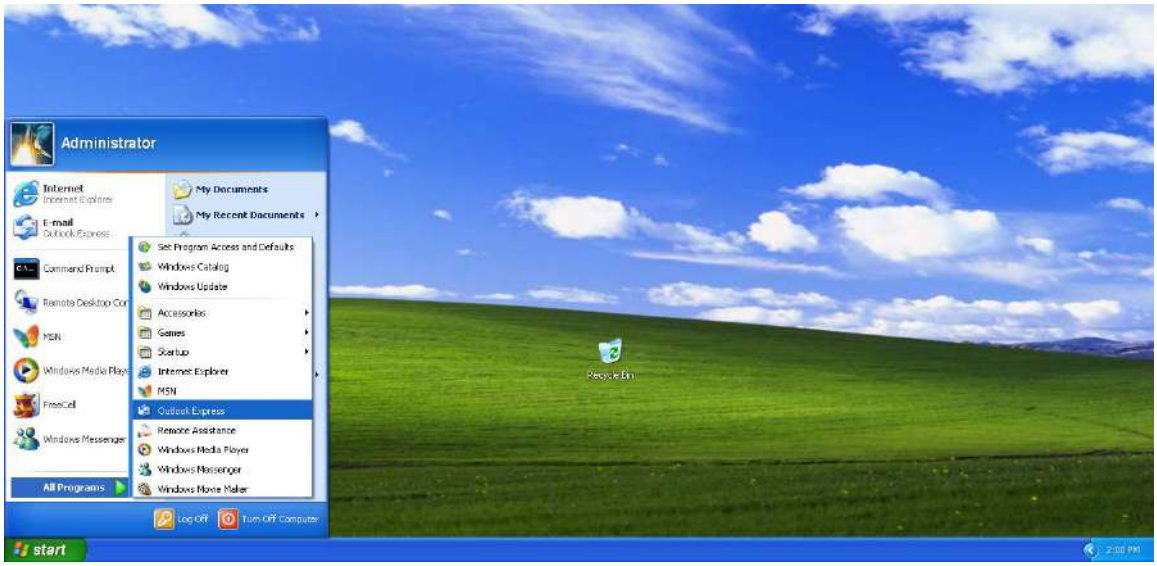

Рис. 181. **Налаштування місця встановлення програми**

На екрані з’явиться майстер нового з’єднання. Натискаємо кнопку **Next**, у наступному вікні вибираємо тип мережевого з’єднання **Connect to the Internet** і натискаємо кнопку **Next** (рис. 182).

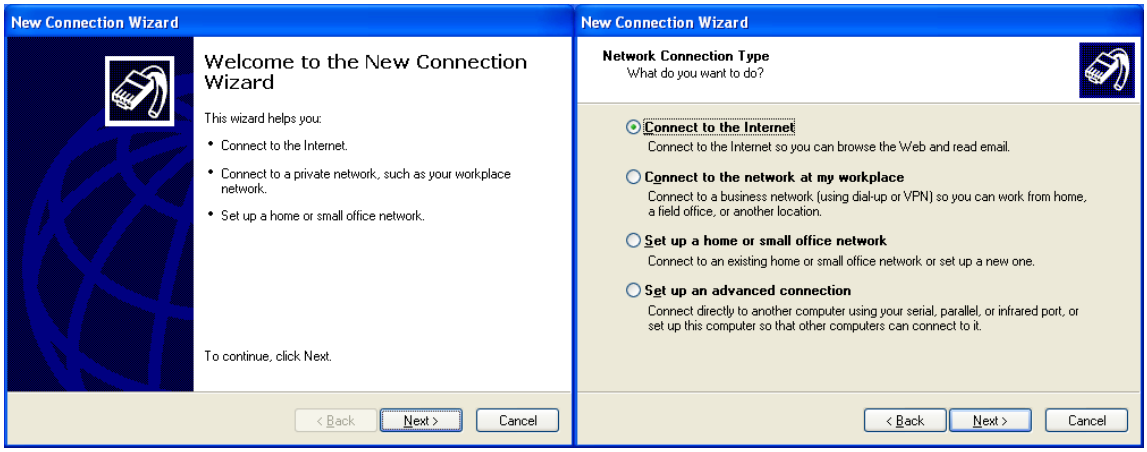

Рис. 182. **Вікно майстра нового з’єднання та вибір типу з’єднання**

У наступному вікні вибираємо, як з’єднатися з мережею. Натискаємо кнопку **Next**. Закінчуємо роботу з майстром нових з’єднань (рис. 183).

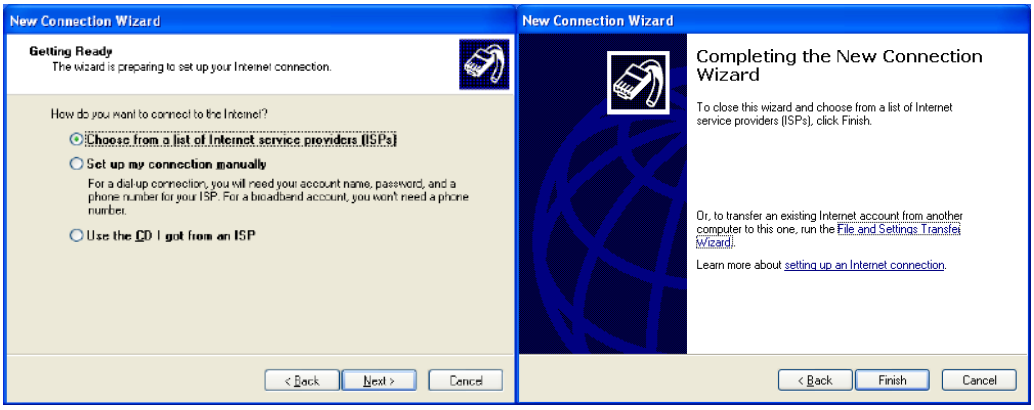

Рис. 183. **Вибір з’єднання з мережею та закриття майстра нових з’єднань**

Закриваємо вікно *Online Services* (рис. 184) та переходимо до вікна майстра з’єднання з інтернетом, де в пункті *Display name* задаємо ім’я власника листа (рис. 185).

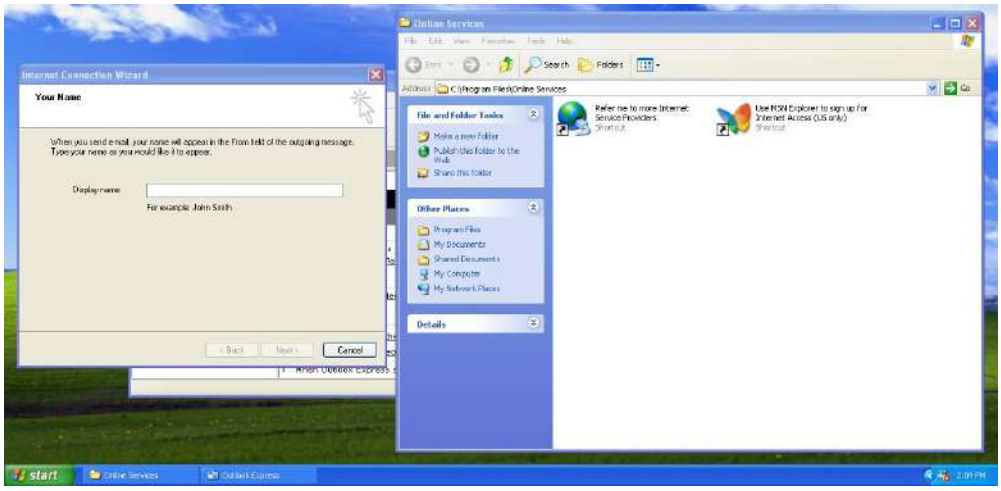

Рис. 184. **Вікно майстра з’єднання з інтернетом**

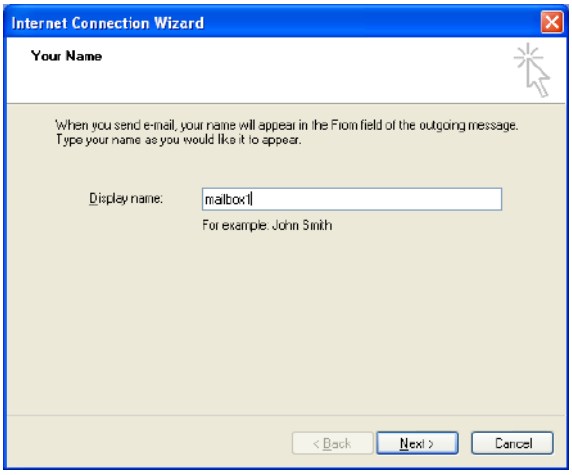

Рис. 185. **Задавання ім’я власника листа**

Задаємо поштову адресу користувача поштової скриньки (рис. 186).

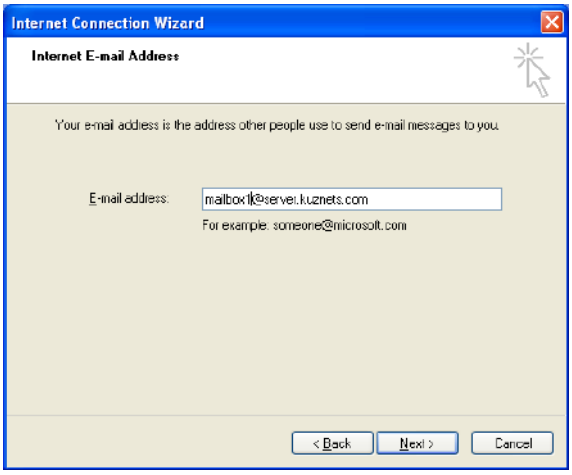

Рис. 186. **Поштова адреса користувача**

Указуємо параметри з'єднання з поштовим сервером (рис. 187).

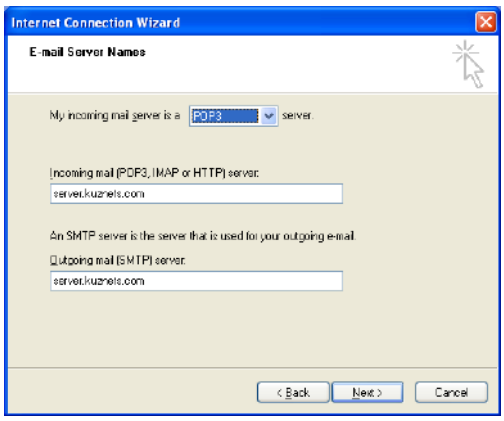

Рис. 187. **Параметри з'єднання з поштовим сервером**

Задаємо ім'я облікового запису *Account name*, пароль *Password* та закінчуємо роботу з майстром з'єднання з інтернетом (рис. 188).

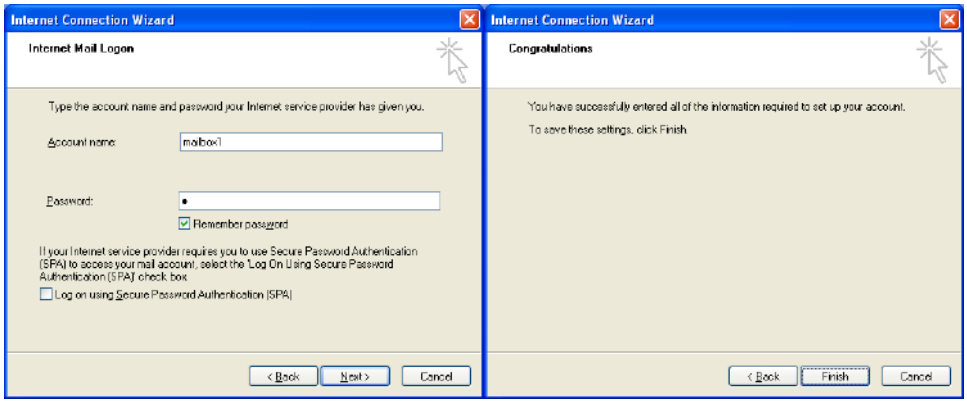

Рис. 188. **Задавання імені облікового запису, пароля та закінчення роботи майстра**

Після закінчення роботи майстра бачимо головний екран програми з налаштованою поштовою скринькою (рис. 189).

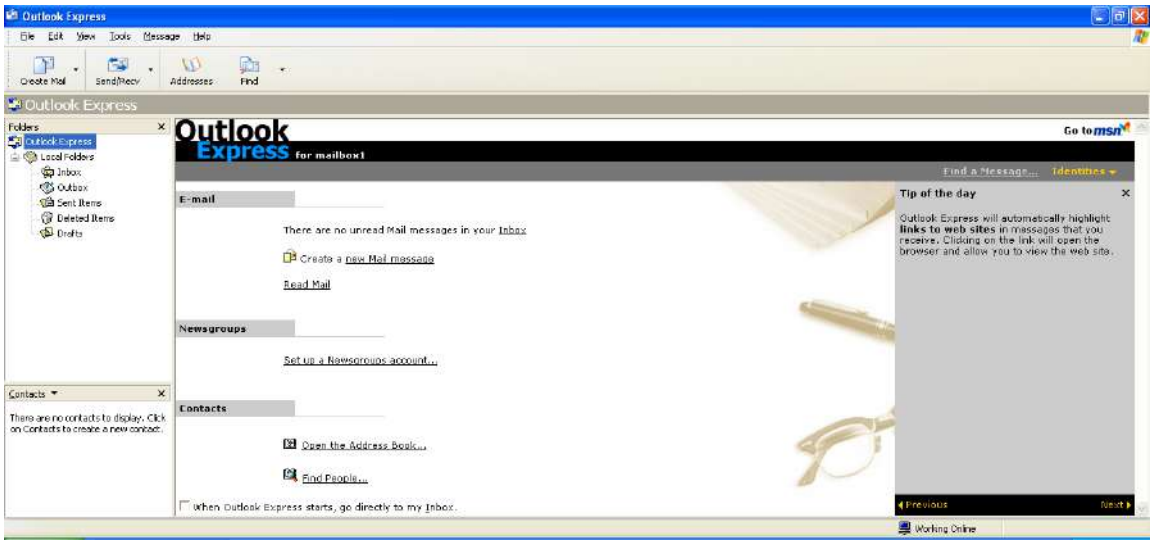

Рис. 189. **Головне вікно програми Outlook Express**

Налаштовуємо **ще дві поштові скриньки**. Для цього вибираємо в програмі пункти меню **Tools -> Accounts**. Відкривається вікно *Internet Accounts*, у якому вибираємо вкладку **Mail** (рис. 190).

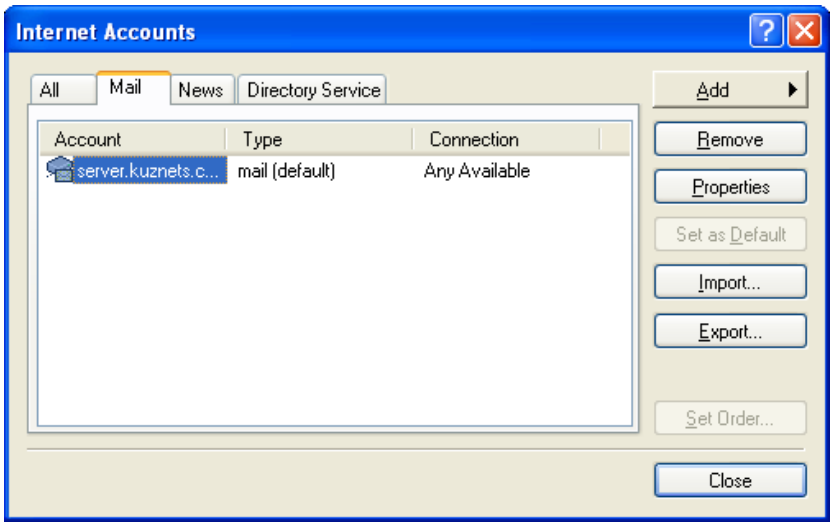

Рис. 190. **Вікно налаштувань Internet Accounts**

Натискаємо кнопку *Add* і в меню, що з'явиться, вибираємо пункт *Mail.* Відкриється вікно майстра з'єднання з інтернетом, таке саме, як і під час налаштування першої поштової скриньки. Налаштовуємо, відповідно, другу та третю поштові скриньки. Після цього вкладка *Mail* вікна *Internet Accounts* набуде такого вигляду (рис. 191).

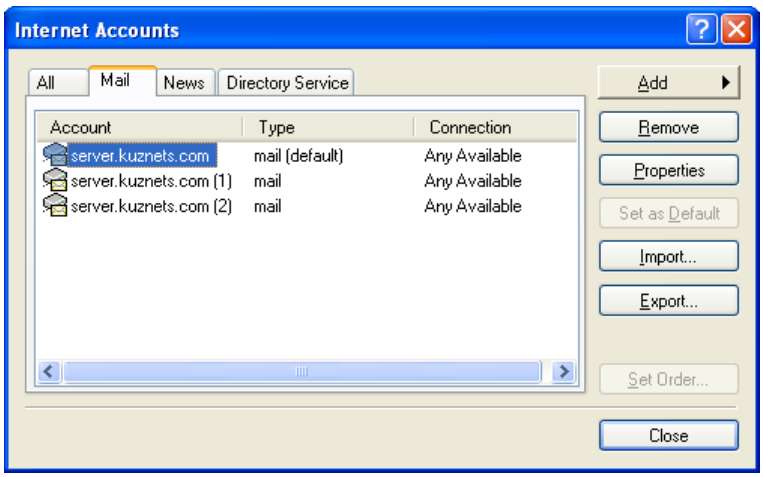

Рис. 191. **Вікно налаштувань Internet Accounts із трьома поштовими скриньками**

Створюємо новий лист у першій скриньці та вказуємо в полях To: і Cc: електронні адреси інших скриньок (рис. 192).

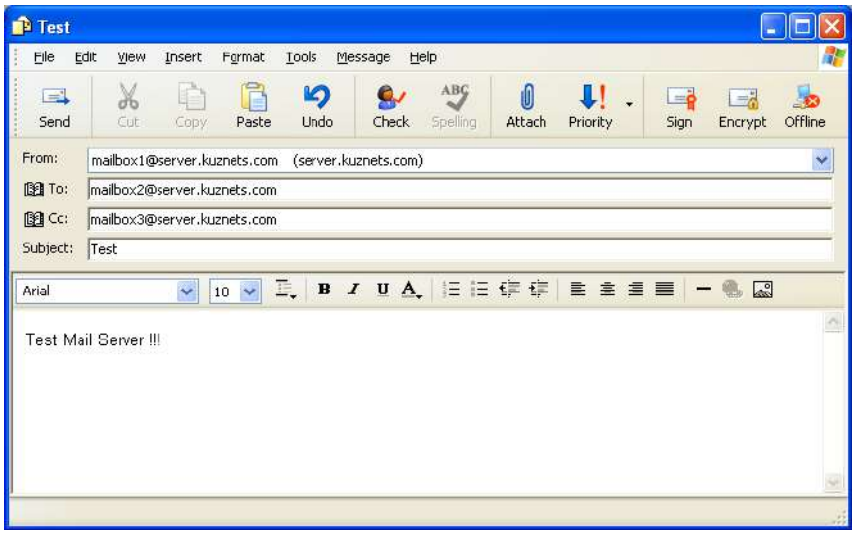

Рис. 192. **Створення поштового листа**

Відправляємо лист і перевіряємо його наявність в обох створених поштових скриньках на поштовому сервері (рис. 193).

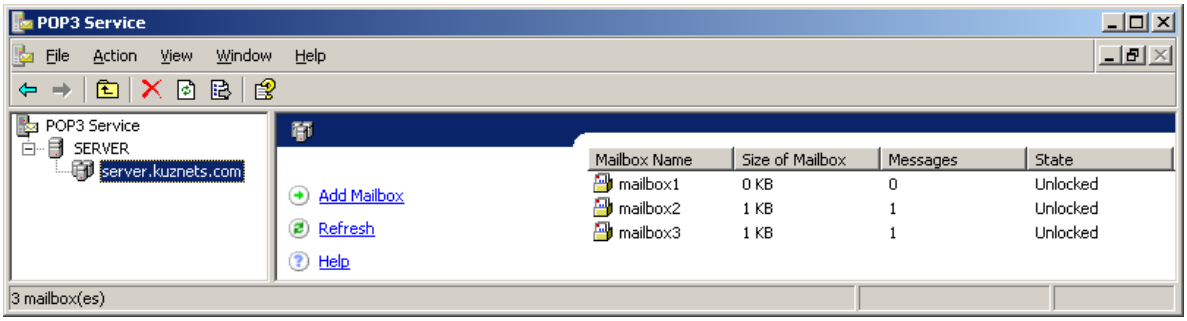

Рис. 193. **Листи на поштовому сервері**

У поштовій програмі *Outlook Express* у меню вибираємо кнопку **Send/Recv** та входимо в обидві поштові скриньки для отримання листів (рис. 194).

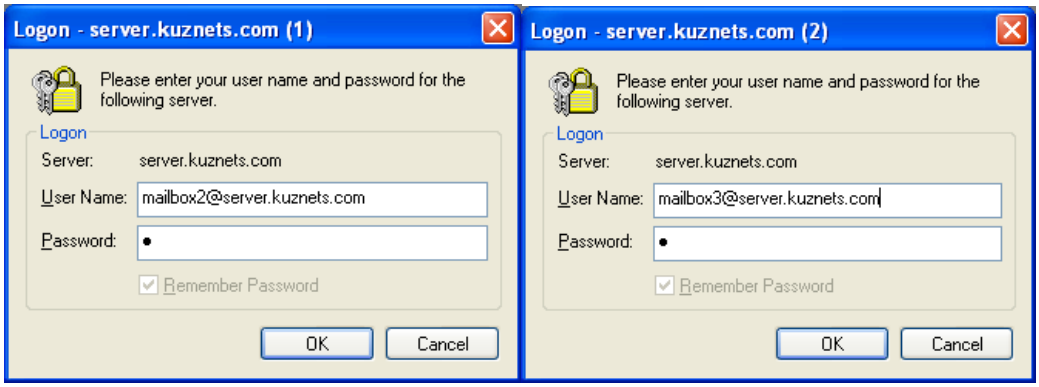

Рис. 194. **Вхід в обидві поштові скрині**

Було отримано два нових листа (рис. 195).

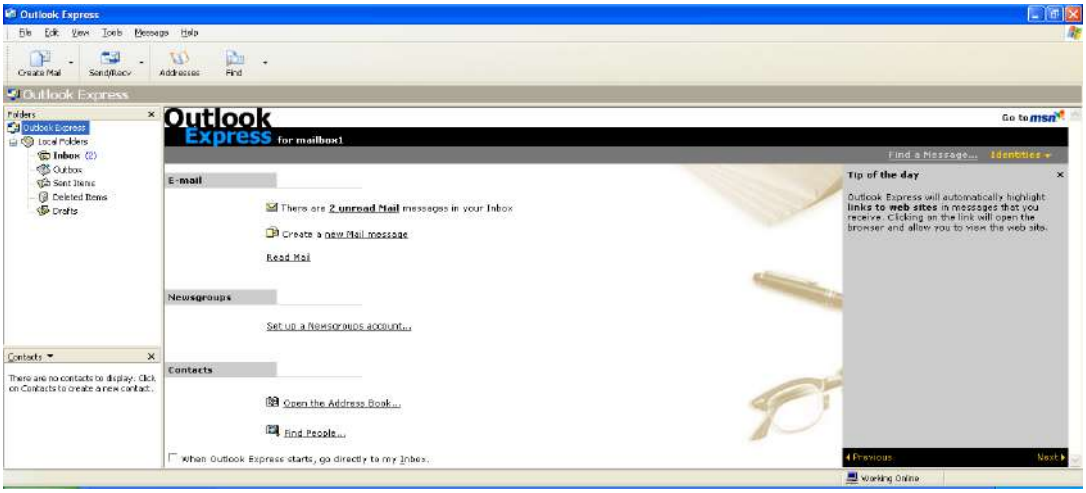

Рис. 195. **Вікно програми з повідомленнями про отримання листа**

Переглядаємо отримані листи (рис. 196).

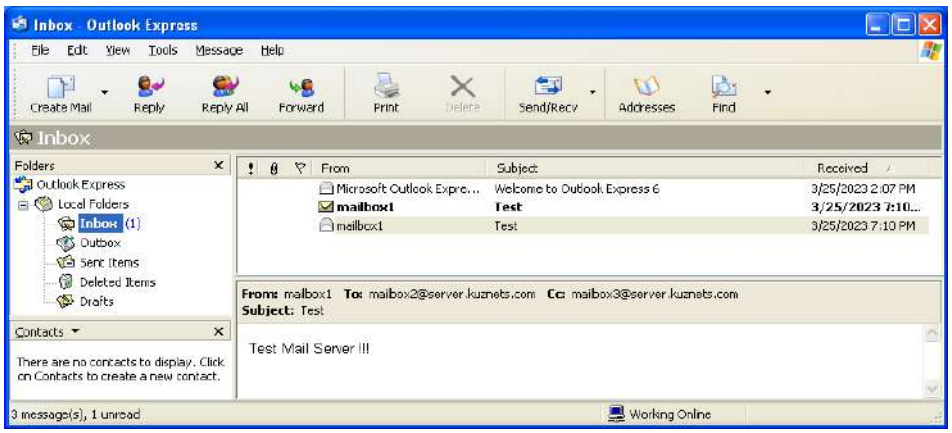

Рис. 196. **Уміст отриманого листа**

Після їх отримання знову перевіряємо поштовий сервер. У вікні *POP3 Service* натискаємо на кнопку **Refresh** для оновлення результатів (рис. 197).

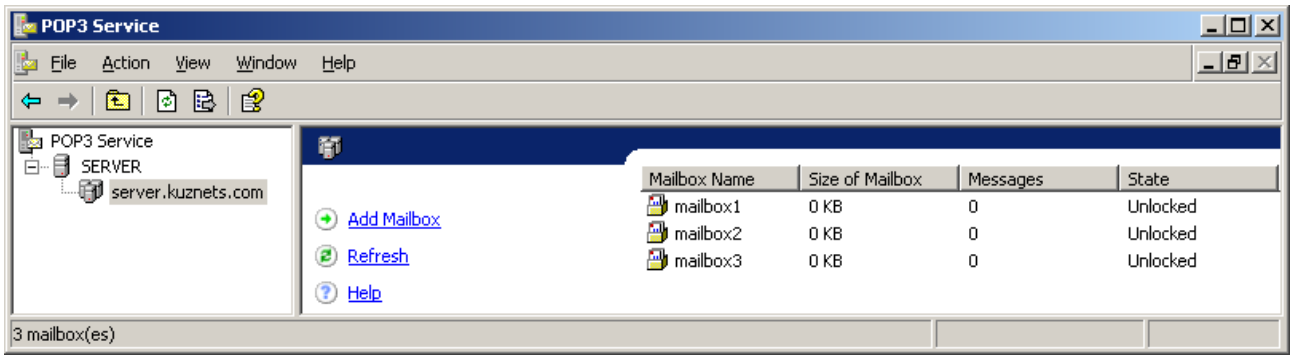

Рис. 197. **Поштові листи, завантажені клієнтом**

На цьому налаштування поштового сервера закінчено.

Зміст звіту

1. Назва лабораторної роботи (ЛР), тема, мета й зміст завдань ЛР.
2. Вхідні дані до лабораторної роботи.
3. Навести скриншоти результатів виконання всіх етапів завдань лабораторної роботи.
4. Висновки за результатами виконання ЛР.

Контрольні запитання

1. Які протоколи застосовують під час роботи поштового сервера *Windows Server 2003 Enterprise Edition*?
2. Що містить конфігурування поштового сервера? Наведіть послідовність завдань?
3. Яким чином додають новий домен у поштовому сервері?
4. Яким чином додають обліковий запис у поштовому сервері?
5. Який поштовий протокол застосовували в програмі *Outlook Express*?
6. Які параметри налаштовує майстер з'єднання з інтернетом?
7. Які порти використовують протоколи POP3 та SMTP?

Лабораторна робота 5
Установка й керування роботою WWW- та FTP-серверів засобами Windows Server

Метою лабораторної роботи є ознайомлення з принципами роботи служб IIS, налаштування роботи WWW- та FTP-серверів у *Windows Server 2003 Enterprise Edition* для публікації (розміщення) вебсайту й забезпечення доступу до його вмісту.

Порядок виконання роботи

Для виконання лабораторної роботи (ЛР) будемо використовувати робочу станцію (РС) з ОС *Windows Server 2003 Enterprise Edition*. Завантажуємо з гіпервізора потрібну віртуальну машину (ВМ). Вибираємо: меню **Start -> Administrative Tool -> Configure Your Server Wizard** (рис. 198).

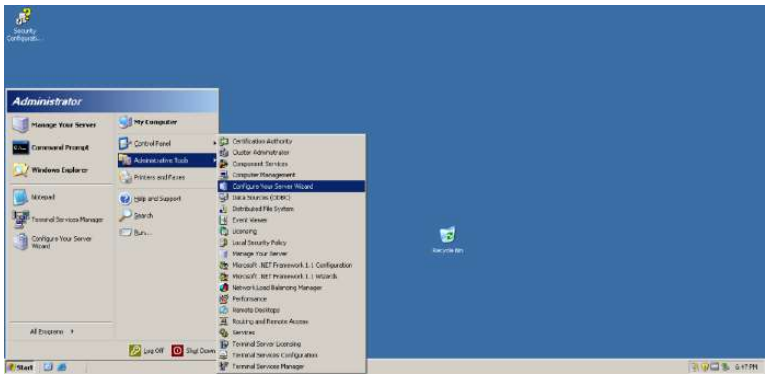

Рис. 198. **Запуск майстра налаштувань сервера**

У вікні, що відкриється, вибираємо кнопку **Next** для початку роботи майстра налаштувань (рис. 199).

Рис. 199. **Вікно початку роботи майстра налаштувань сервера**

У наступному вікні вибираємо кнопку **Next** для визначення параметрів мережевих налаштувань (рис. 200).

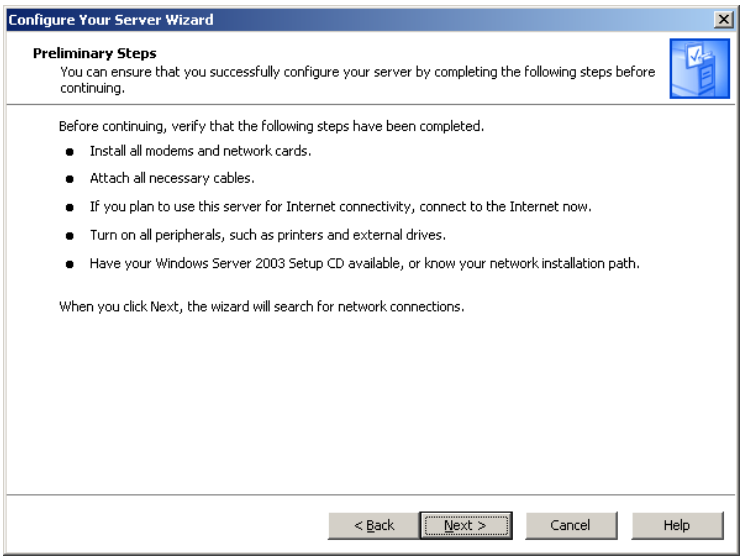

Рис. 200. **Визначення параметрів мережевих налаштувань**

Для налаштування сервера додатків вибираємо пункт **Application server (IIS, ASP.NET)**. Буде встановлено вебсервер у складі *IIS (Internet Information Services*, підтримувані протоколи включають HTTP, HTTPS, FTP, SMTP, POP3). Натискаємо кнопку **Next** (рис. 201).

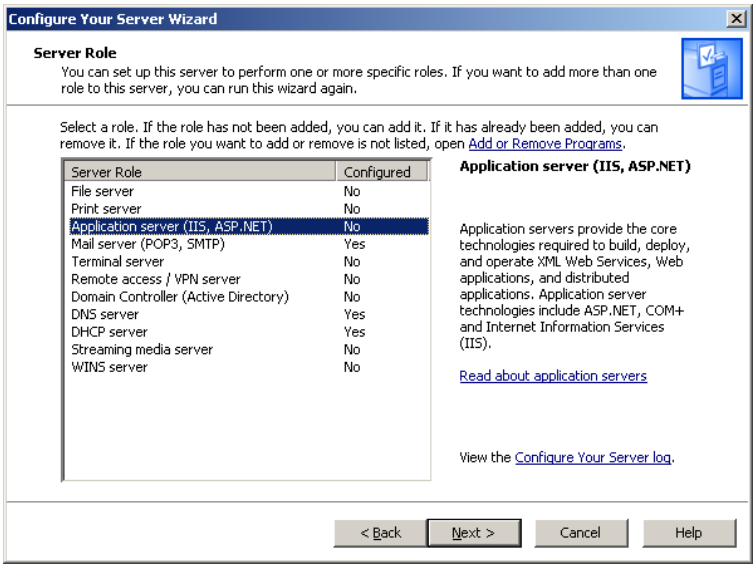

Рис. 201. **Вибір пункту сервера додатків**

Переходимо до вікна, у якому відображені компоненти IIS та компоненти, що підтримують його. Пункти залишаємо не вибраними. Натискаємо кнопку **Next** (рис. 202).

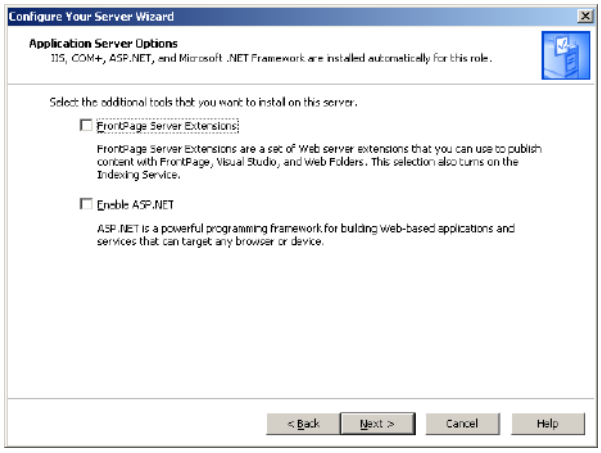

Рис. 202. **Вікно вибору параметрів сервера додатків**

У вікні, що відкриється, перевіряємо вибрані параметри та натискаємо кнопку **Next** (рис. 203).

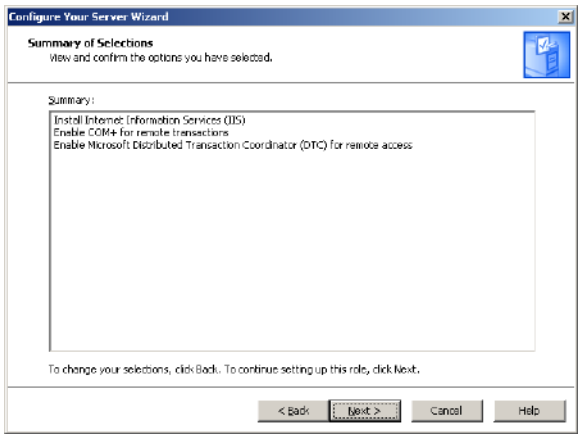

Рис. 203. **Вікно перевірки вибраних параметрів IIS**

Виконується встановлення необхідних для роботи файлів (рис. 204) та завершується робота майстра встановлення сервера додатків (рис. 205).

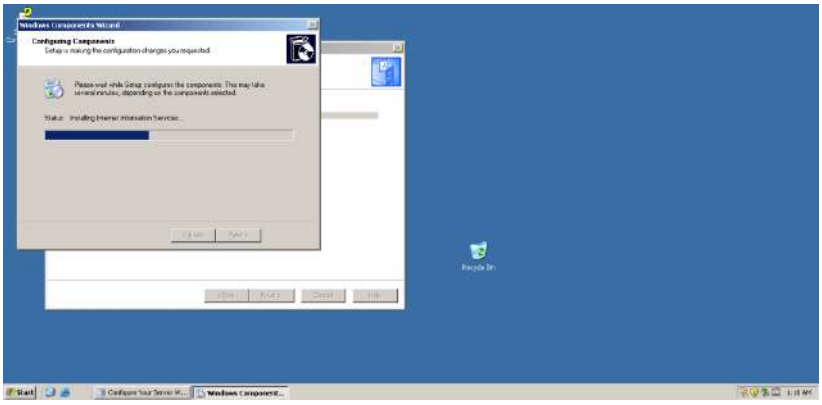

Рис. 204. **Установлення необхідних для роботи файлів**

Рис. 205. **Завершення роботи майстра встановлення сервера додатків**

Вмикаємо FTP сервер. Додаємо службу FTP у IIS. Вибираємо: меню **Start –> Control Panel –> Add or Remove Programs** (рис. 206).

Рис. 206. **Установка та видалення програм**

Далі у вікнах, що відкриваються (рис. 207), вибираємо: **кнопку Add/Remove Windows Components -> пункт Application Server -> кнопку Details -> пункт Internet Information Services (IIS) -> кнопку Details**.

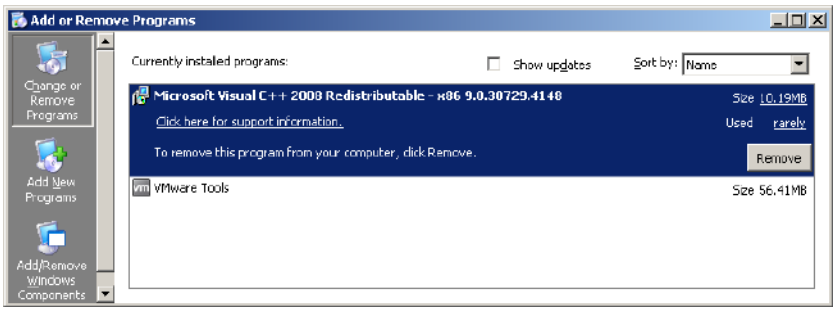

Рис. 207. **Вікно Add and Remove Programs**

У вікні *Internet Information Services (IIS)*, що відкриється, треба поставити галочку в пункті *File Transfer Protocol (FTP) Service* (рис. 208).

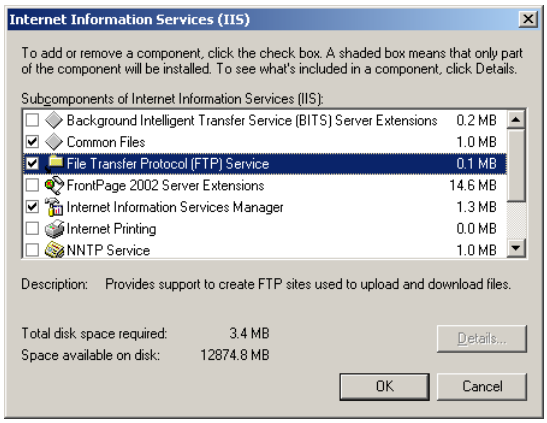

Рис. 208. **Вікно додавання FTP сервісу**

Далі виконуємо налаштування компоненти *Application Server*, натискаючи кнопку **Next** (рис. 209).

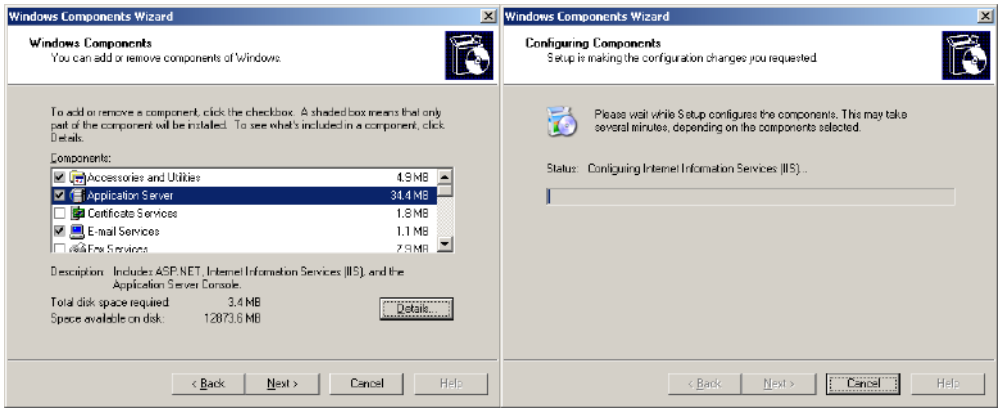

Рис. 209. **Вікно налаштування служби IIS**

Після закінчення налаштувань виходимо з вікна майстра компонент (рис. 210), натискаючи на кнопку **Finish** (рис. 210).

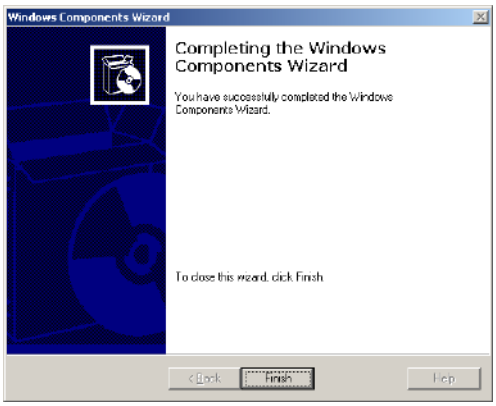

Рис. 210. **Вікно завершення майстра компонент**

Викликаємо програму *Manage Your Server*. Вибираємо: меню **Start -> Manage Your Server** (рис. 211).

Рис. 211. **Виклик програми Manage Your Server**

Вибираємо пункт **Manage this application server** у розділі *Application Server* та переходимо у вікно *Application Server* (рис. 212).

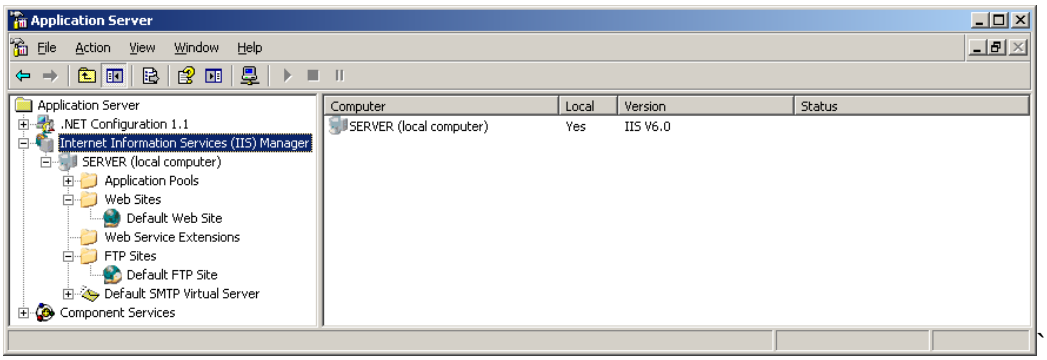

Рис. 212. **Вікно керування сервером додатків**

На питання про блокування програми у відповідь натискаємо кнопку **Unblock** (рис. 213).

Рис. 213. **Розблокування програми управління у Windows Firewall**

У разі необхідності виконуємо запуск компонент **Default Web Site** та **Default FTP Site**.

Створюємо в корені диска **C папку** з назвою **Site**, яка буде містити файли, що передаються за допомогою FTP-сервера (рис. 214).

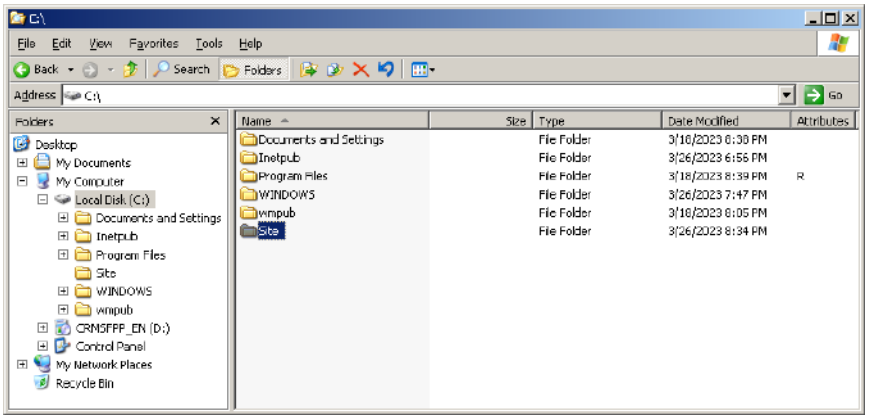

Рис. 214. **Створена папка Site**

Відкриваємо пункт меню **Properties** пункту **Default FTP Site** і у вікні, що відкриється, вибираємо розділ **Home Directory**. У рядку *Local path* указуємо локальний шлях до створеної папки та дозволяємо запис у неї (рис. 215).

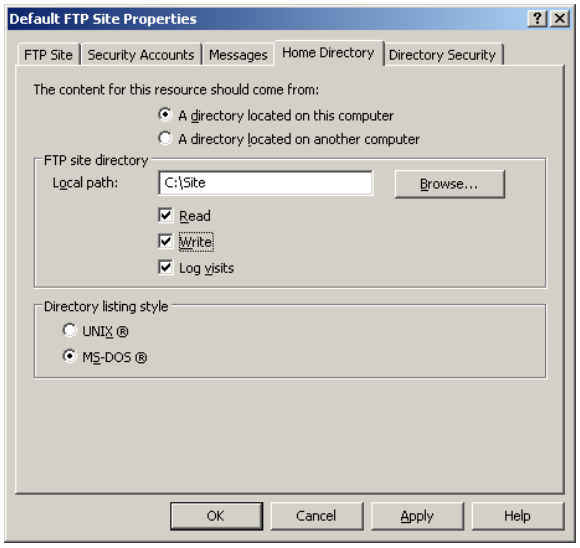

Рис. 215. **Налаштування домашнього каталога для FTP-сервера**

Викликаємо програму *Windows Firewall*. Вибираємо: меню **Start -> Control Panel -> Windows Firewall**. У вікні, що відкриється, вибираємо вкладку **Advanced** і в розділі *Network Connection Settings* натискаємо кнопку **Settings** (рис. 216).

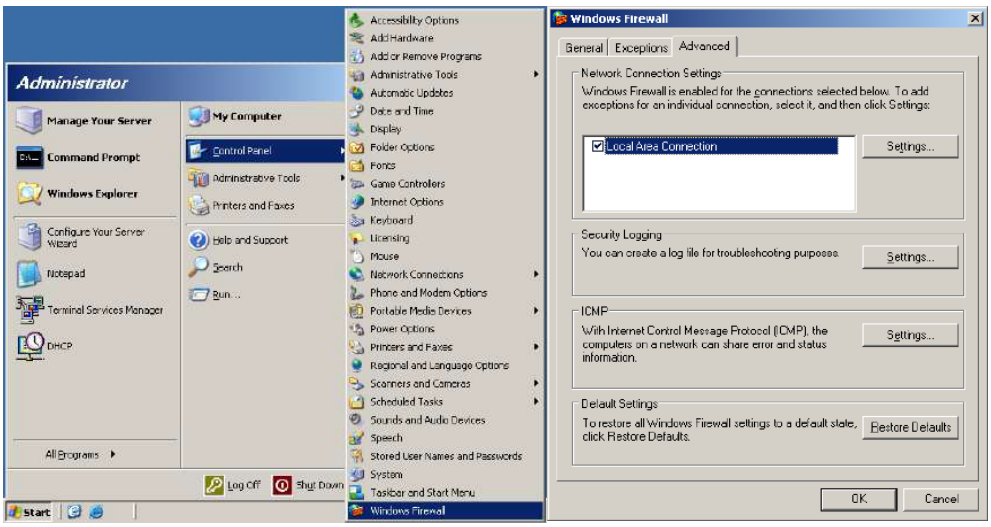

Рис. 216. **Виклик програми Windows Firewall**

У вікні *Advanced Settings* поставити галочки в пунктах: **FTP Server, Secure Web Server (HTTPS), Web Server (HTTP)** (рис. 217).

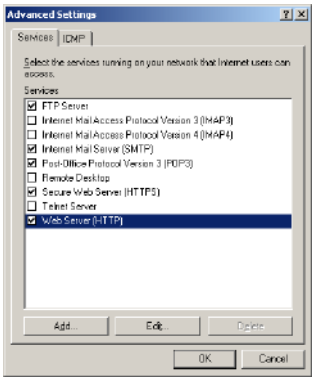

Рис. 217. **Налаштування дозволу на роботу із сервісами**

Завантажуємо ВМ з ОС *Windows XP Professional* та запускаємо *Internet Explorer*. В адресному рядку треба ввести адресу у форматі **ftp://ім'я_сервера,** де **ім'я_сервера –** це server.kuznets.com, або IP-адреса FTP сервера (Windows Server) (рис. 218).

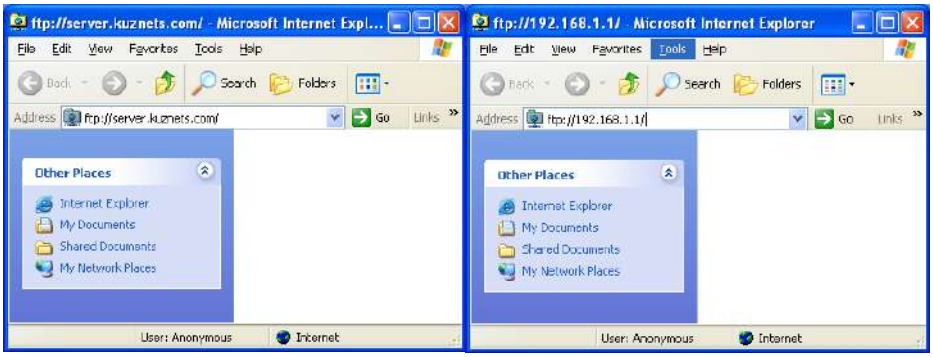

Рис. 218. **Internet Explorer з відкритою FTP-папкою**

Створюємо файл з іменем **My.html** та вмістом, як на рисунку (рис. 219).

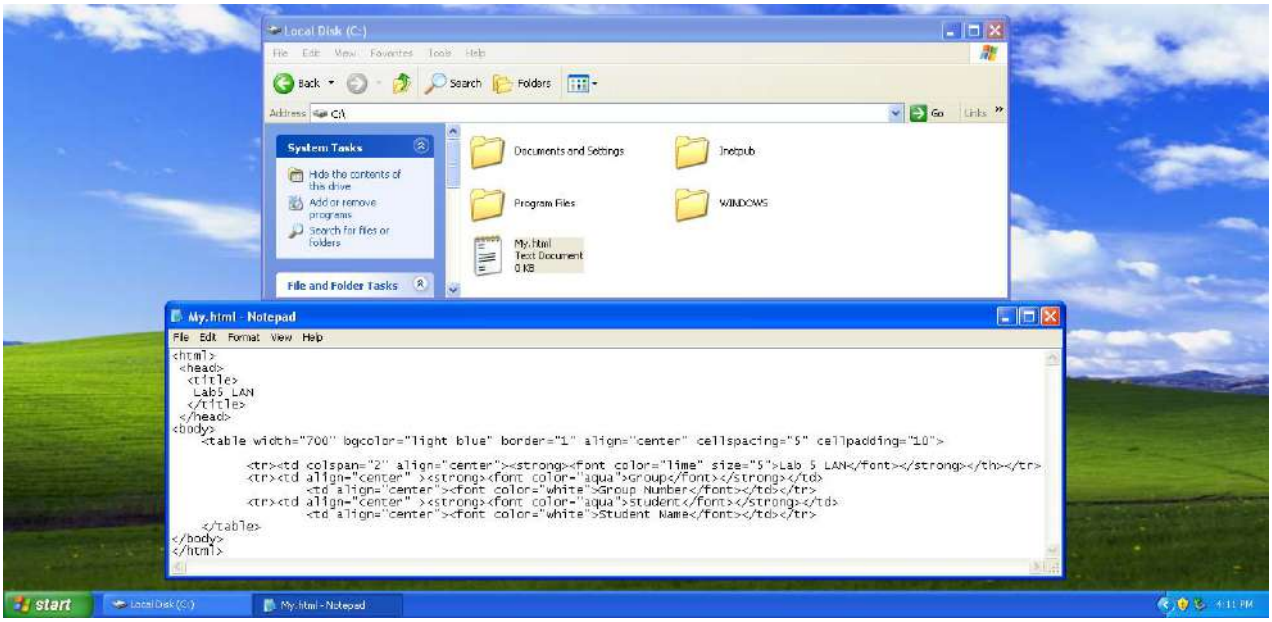

Рис. 219. **Файл My.html та його вміст**

У файлі потрібно замінити **Group number** на номер групи студента і **Student name** – на прізвище студента.

Пересилаємо створений файл на FTP-сервер (рис. 220).

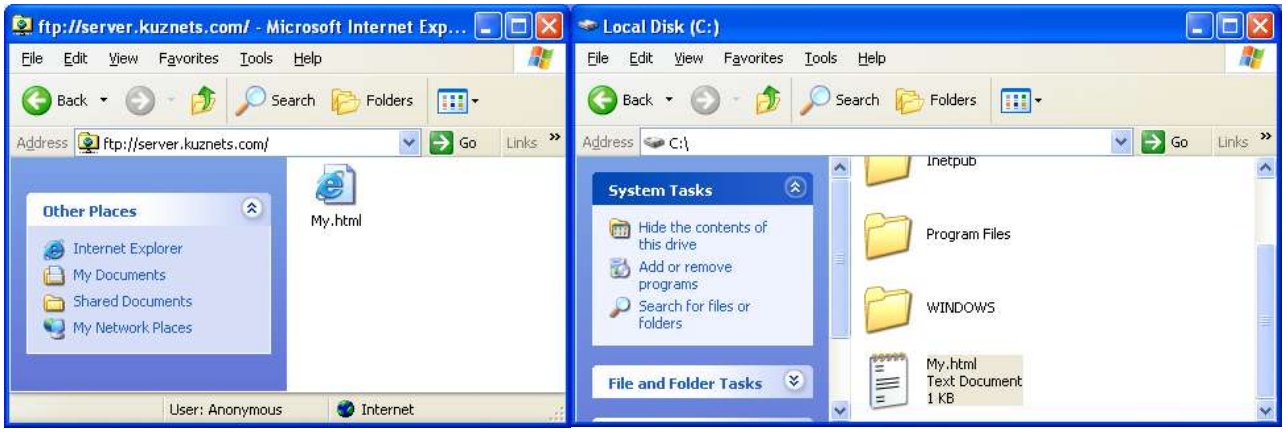

Рис. 220. **Пересилання файлу на сервер**

Повертаємося на PC з ОС *Windows Server 2003 Enterprise Edition* та виконуємо конфігурування вебсайту.

Викликаємо програму *Manage Your Server*. Вибираємо: меню **Start -> Manage Your Server** (рис. 221).

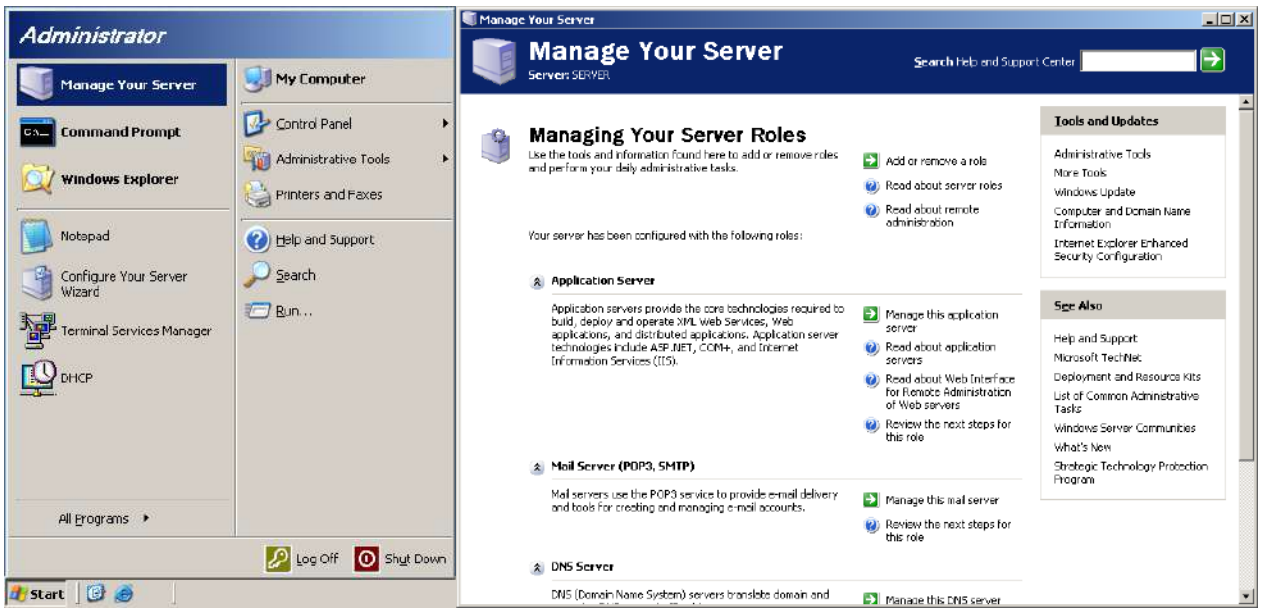

Рис. 221. **Виклик програми Manage Your Server**

Вибираємо пункт **Manage this application server** у розділі *Application Server* та переходимо у вікно *Application Server* (рис. 222).

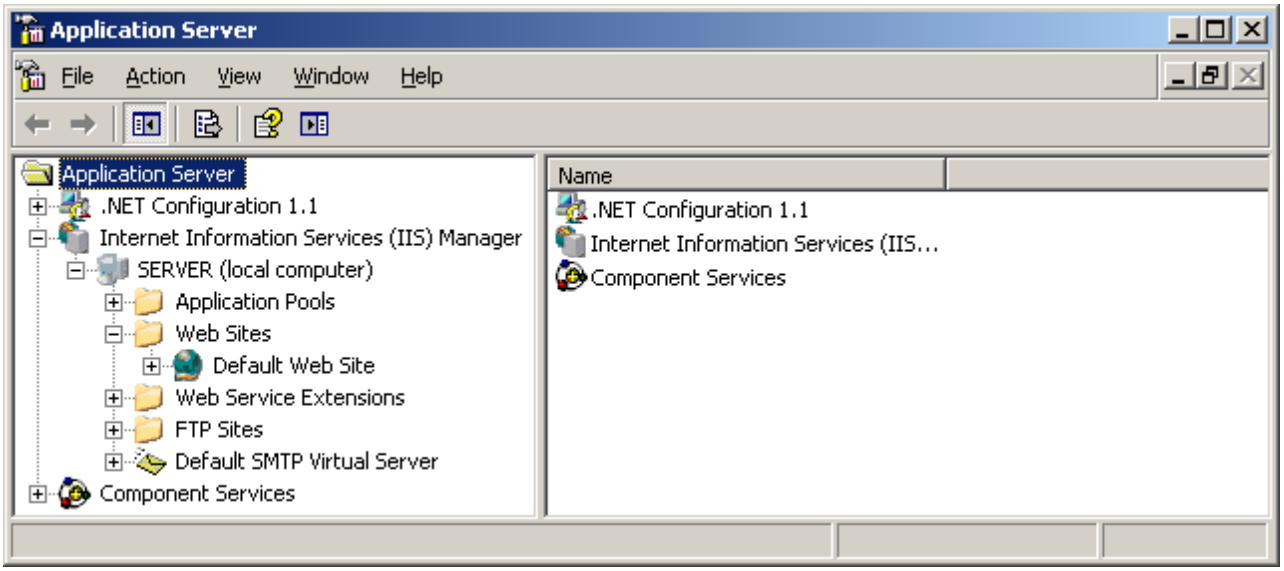

Рис. 222. **Вікно керування сервером додатків**

Переходимо до налаштувань *Default Web Site*. Входимо у вікно *Default Web Site Properties*, вибираючи розділ *Properties* у меню. Переходимо на розділ *Home Directory*.

У рядку *Local path* указуємо локальний шлях до папки *Site* і режим *Read* (рис. 223).

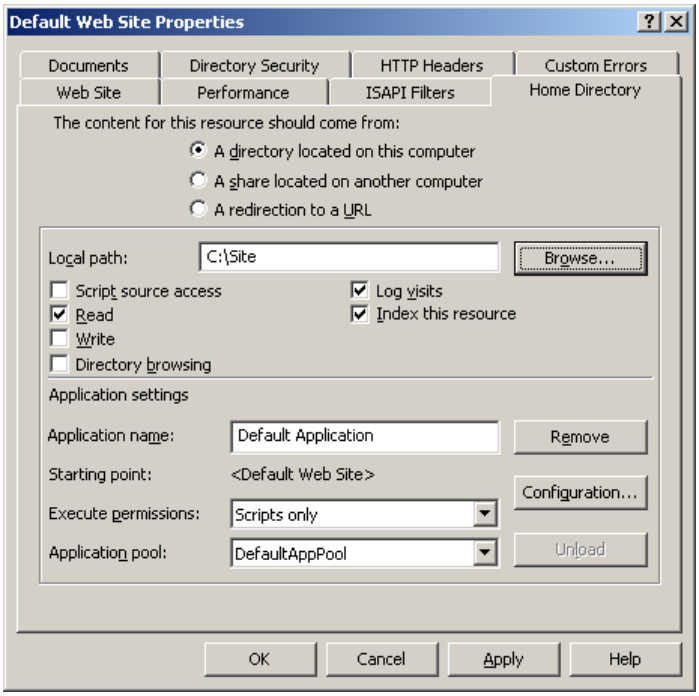

Рис. 223. **Вибір локального шляху до папки сайту**

Щоб сайт під час старту запускав необхідний файл, потрібно додати його ім'я в розділ *Enable default content page* вкладки *Documents* (рис. 224).

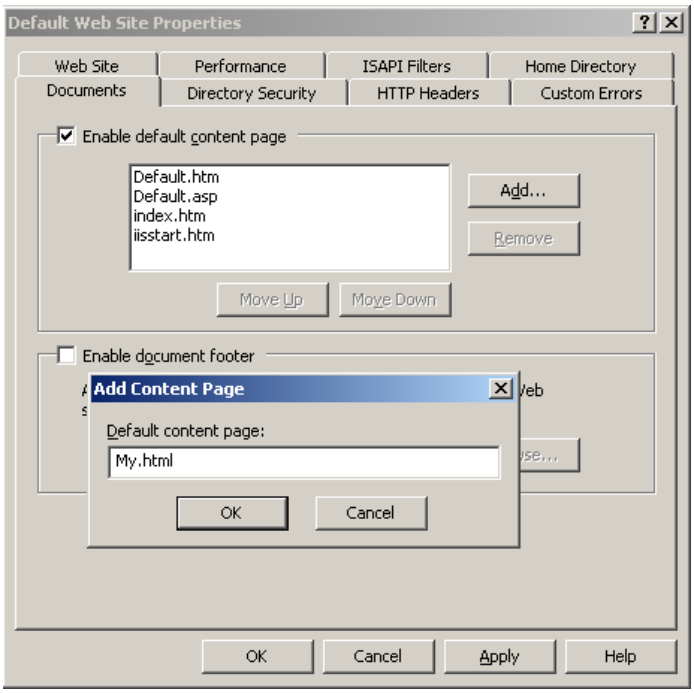

Рис. 224. **Вибір стартової сторінки сайту**

Переходимо на PC з ОС *Windows XP Professional* та перевіряємо роботу сайту, відкривши його в *Internet Explorer* (рис. 225).

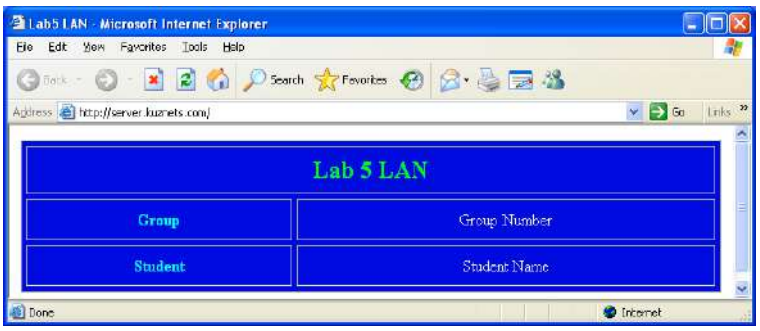

Рис. 225. **Перевірка роботи сайту у Windows XP Professional**

Розміщення другого сайту на вебсервері

У РС з ОС *Windows XP Professional* створюємо другий файл з іменем **My1.html** та вмістом, як показано на рис. 226.

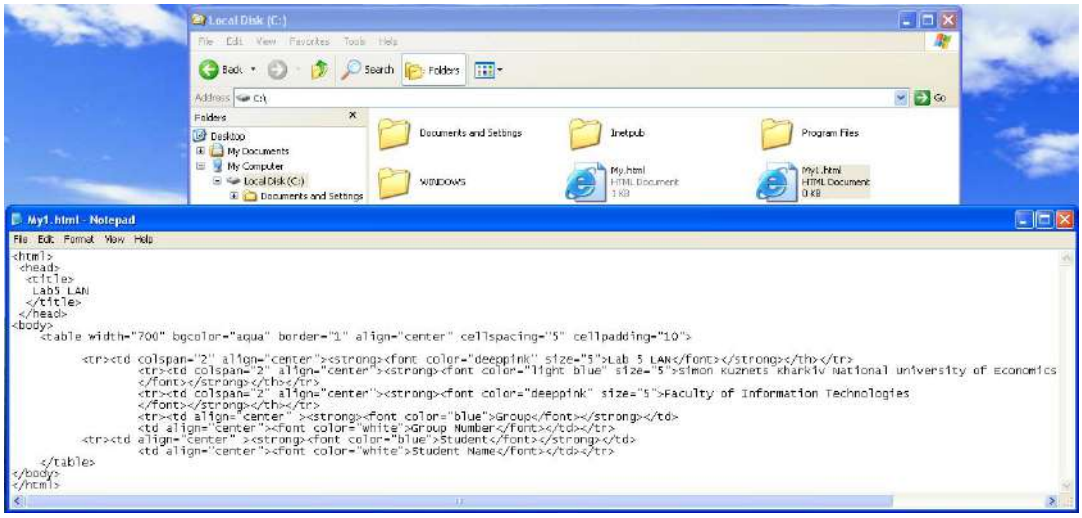

Рис. 226. **Файл My1.html та його вміст**

За допомогою FTP-сервера завантажуємо його на сервер (рис. 227).

Рис. 227. **Пересилання файлу на сервері**

У РС з ОС *Windows Server 2003 Enterprise Edition* переходимо до вікна керування сервером додатків *Application Server*.

На *Web Sites* створюємо додатковий сайт (рис. 228).

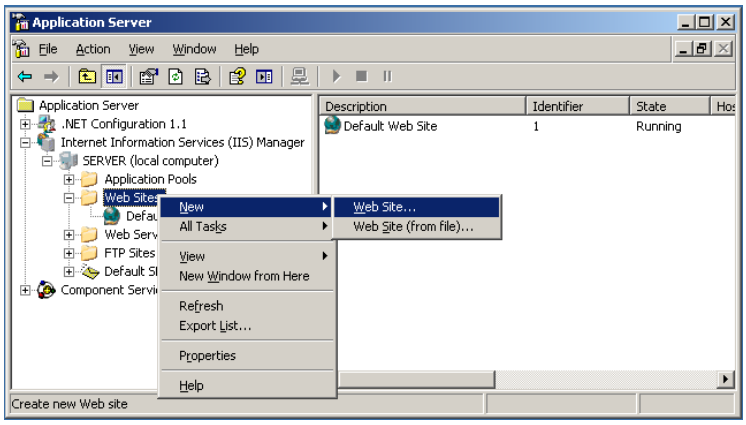

Рис. 228. **Створення додаткового вебсайту**

Робимо налаштування в майстрі створення сайту (рис. 229).

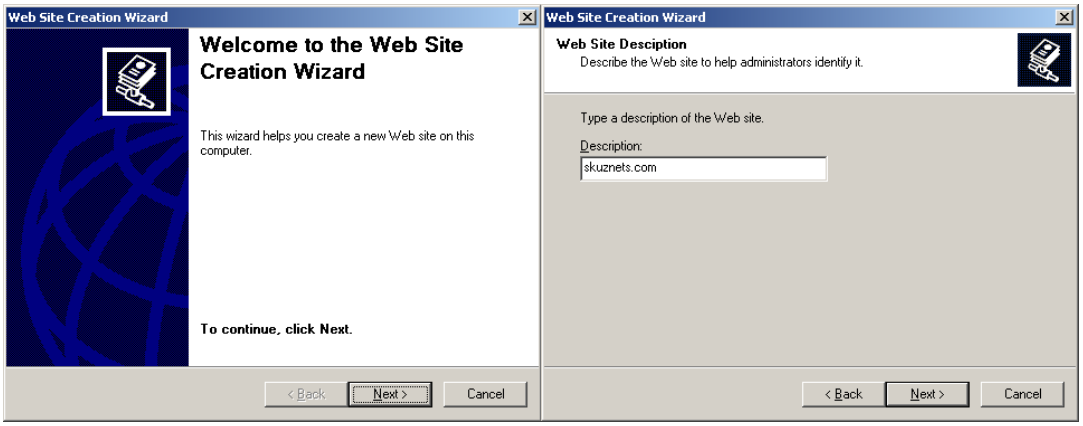

Рис. 229. **Запуск майстра створення сайту та задавання імені вузла**

У заголовку вузла прописуємо ім’я сайту та його папку (рис. 230).

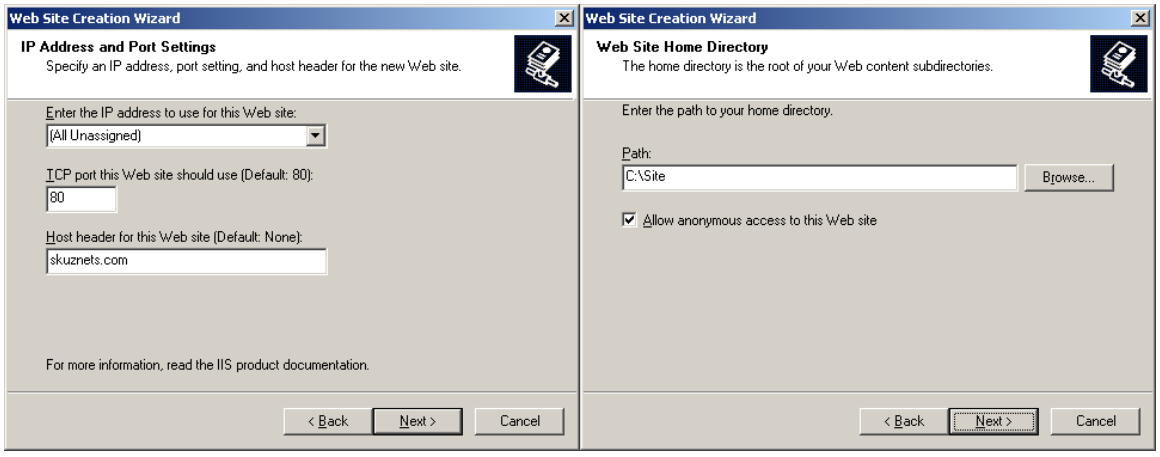

Рис. 230. **Налаштування сайту та папки його розташування на сервері**

Указуємо тип доступу до сайту (*Read*) та завершуємо роботу майстра налаштувань (рис. 231).

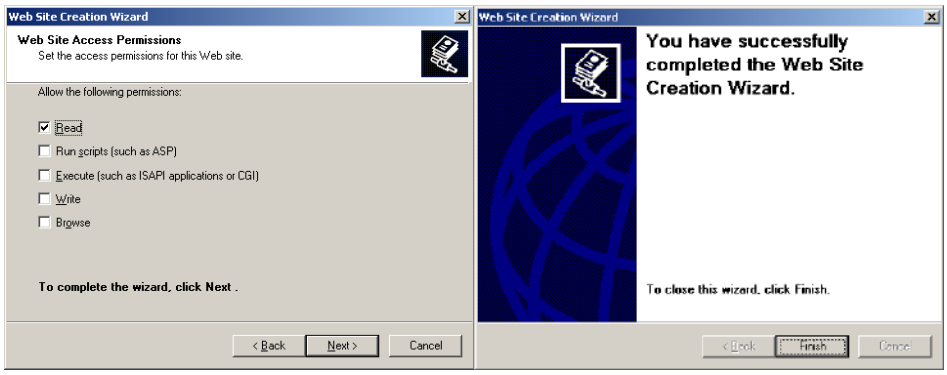

Рис. 231. **Тип доступу до сайту та завершення роботи майстра**

Виконуємо перевірку налаштувань для другого сайту (рис. 232).

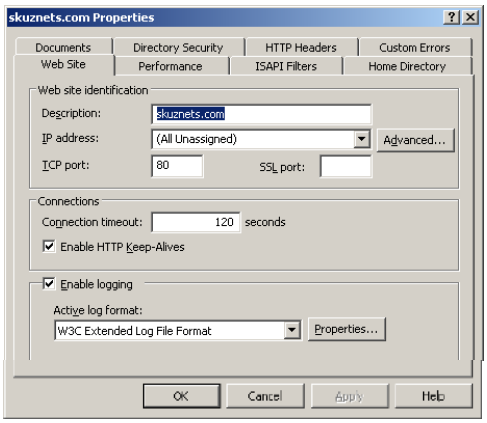

Рис. 232. **Параметри другого сайту**

Перевіряємо параметри ідентифікації сайту, натискаючи кнопку **Advanced -> Edit** (рис. 233).

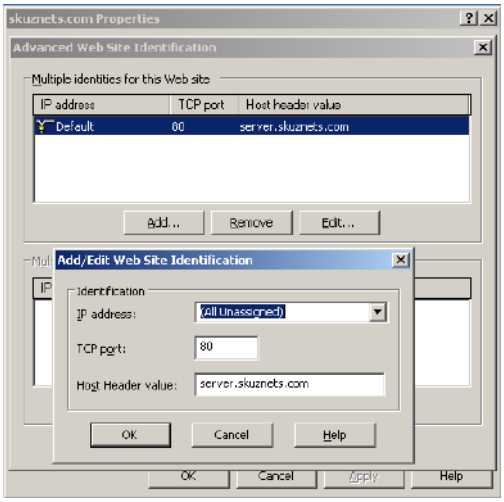

Рис. 233. **Параметри ідентифікації другого сайту**

Додаємо ім’я файлу My1.html, що містить стартову сторінку другого сайту (рис. 234).

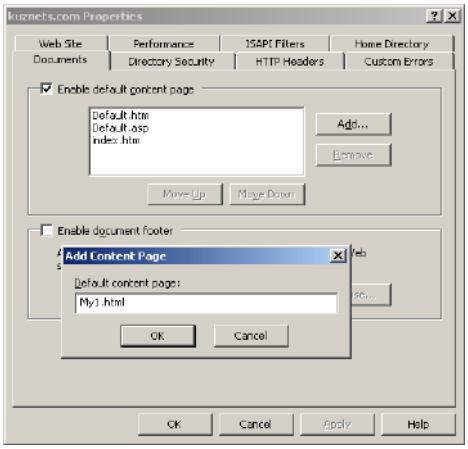

Рис. 234. **Стартова сторінка другого сайту**

У налаштуваннях *Default Web Site* додаємо заголовок server.kuznets.com, який містить DNS-ім’я (рис. 235).

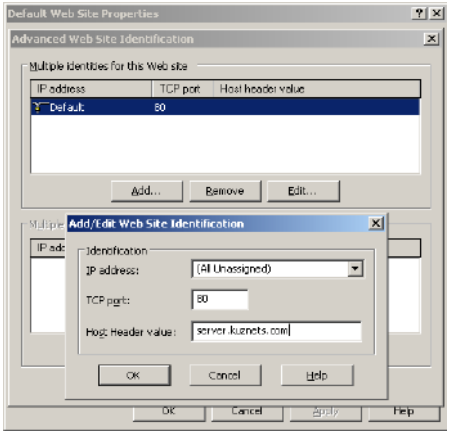

Рис. 235 . **Вікно ідентифікації Default Web Site**

Обираємо у вікні *Manage Your Server* пункт **Manage this DNS server**. У вікні DNS (*dnsmgmt*), що відкриється, створюємо додаткову (нову) зону для другого сайту (рис. 236).

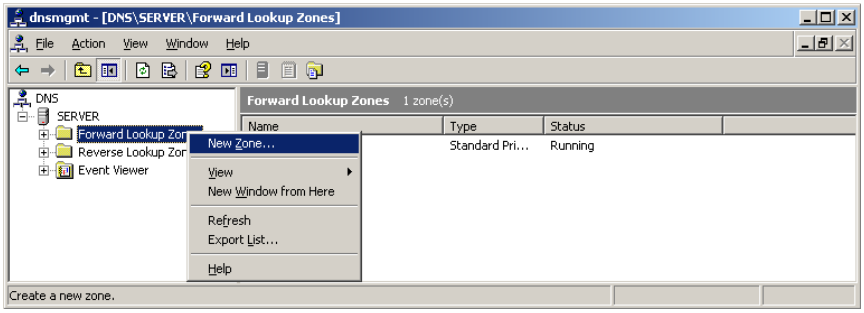

Рис. 236. **Створення додаткової зони для другого сайту**

Виконуємо налаштування майстра створення нової зони (рис. 237).

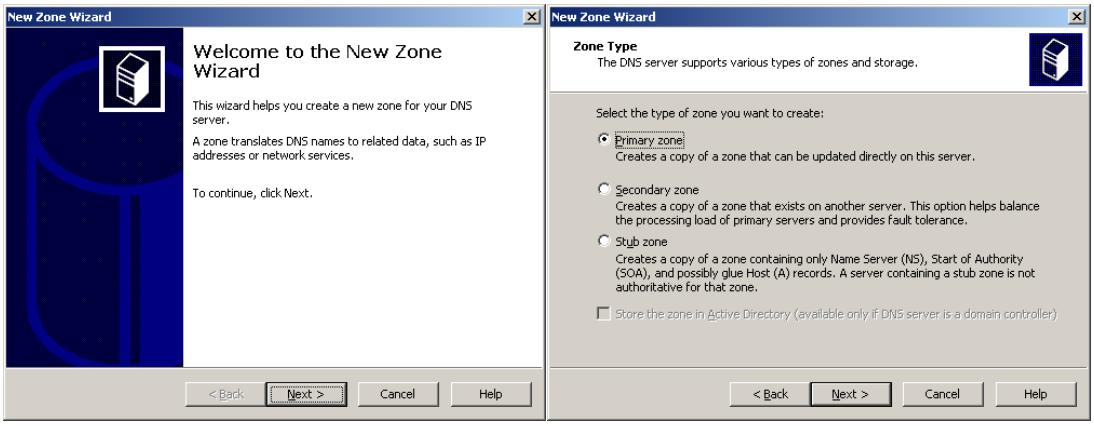

Рис. 237. **Вікно майстра та створення нової основної зони**

Задаємо ім’я зоні та створюємо новий файл зони (рис. 238).

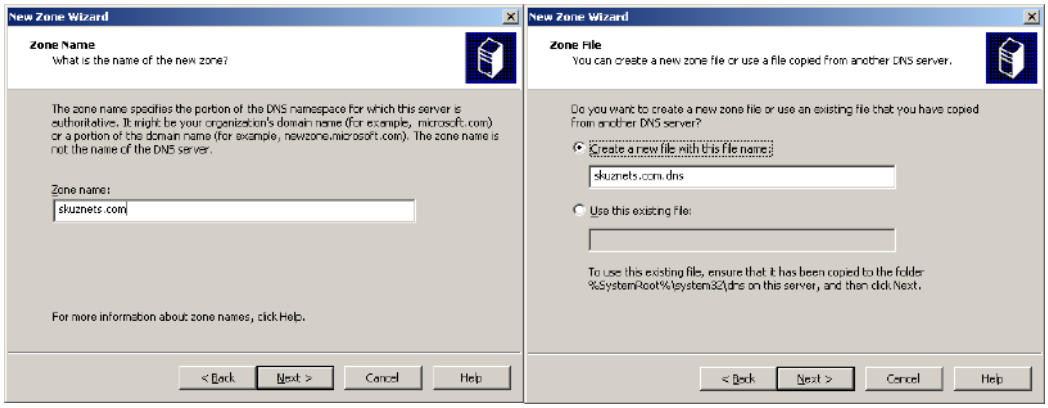

Рис. 238. **Привласнення імені зоні та створення нового файлу**

Відключаємо динамічне оновлення зони та закінчуємо роботу майстра налаштувань нової зони (рис. 239).

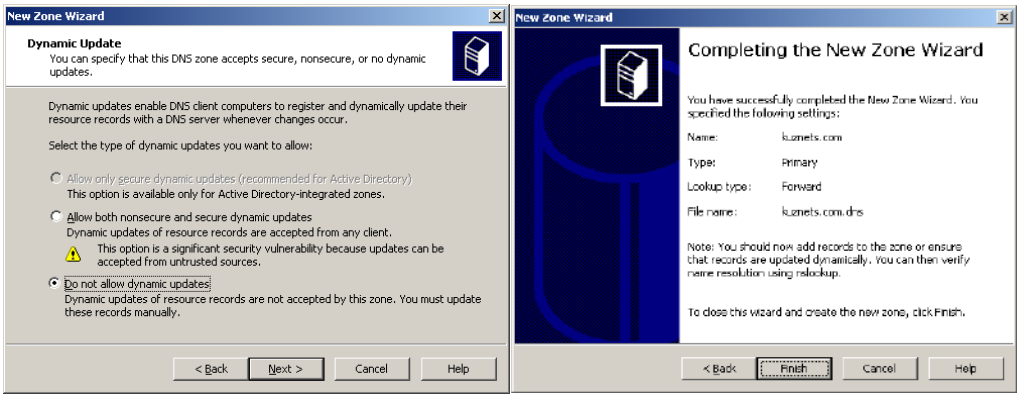

Рис. 239. **Відключення динамічного оновлення та завершення роботи майстра налаштувань нової зони**

Створюємо нову PC (рис. 240).

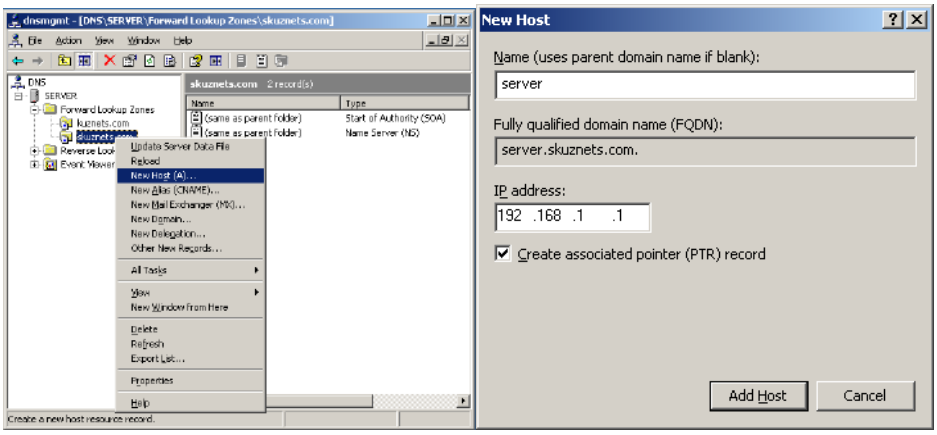

Рис. 240. **Налаштування нової PC**

Перевіряємо налаштування обох зон прямого перегляду (рис. 241).

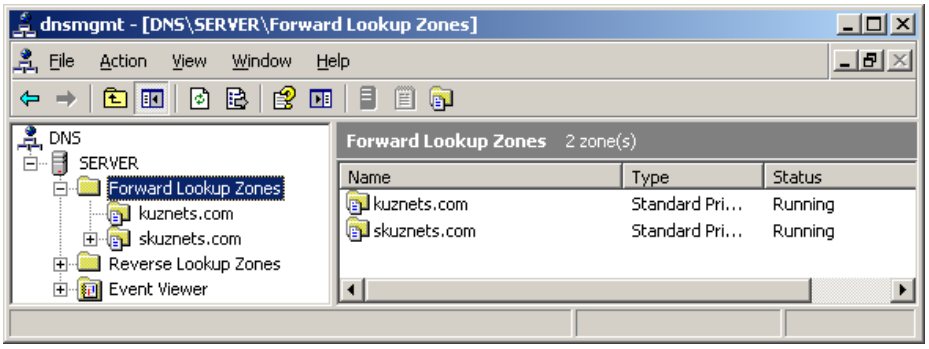

Рис. 241. **Перевірка налаштування зон прямого перегляду**

Виконуємо перевірку роботи обох сайтів на PC з ОС *Windows XP Professional* (рис. 242).

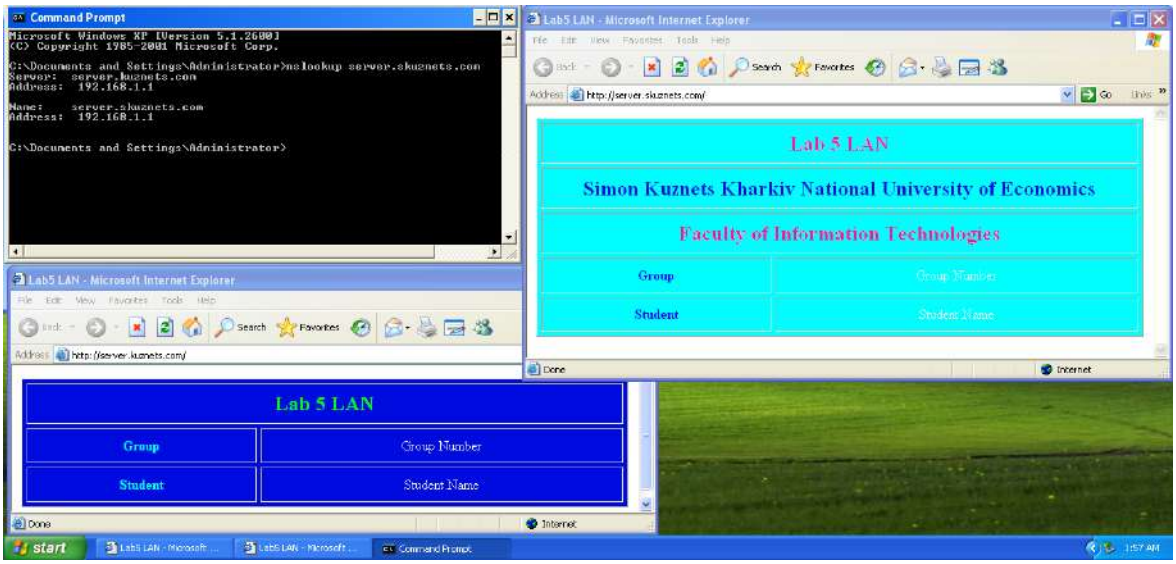

Рис. 242. **Перевірка роботи обох сайтів**

Для забезпечення доступу до сайтів з використанням префікса WWW необхідно в DNS сервері додати запис типу **CNAME** у кожній зоні прямого перегляду (рис. 243). Для цього у вікні *dnsmgmt* в меню *Action* вибираємо пункт *New Alias* (*CNAME*) для обох зон прямого перегляду.

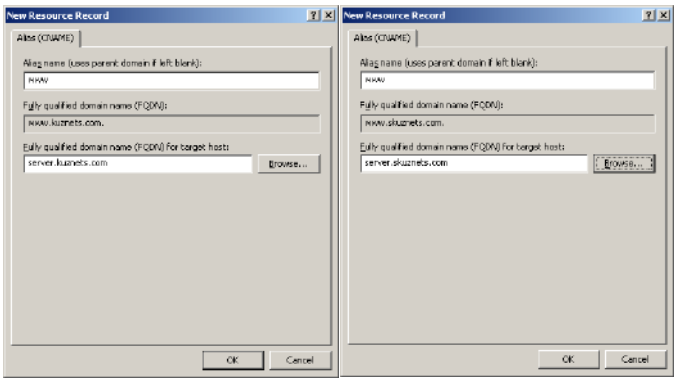

Рис. 243. **Налаштування використання префікса WWW в обох зонах**

Створені записи типу CNAME в обох зонах прямого перегляду (рис. 244).

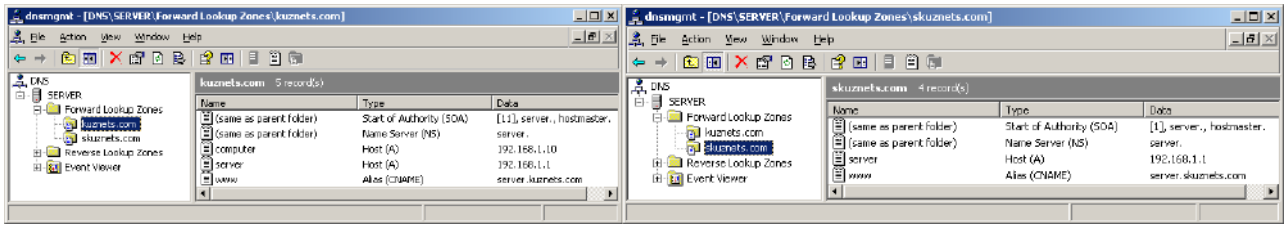

Рис. 244. **Створення записів типу CNAME в обох зонах**

У налаштуваннях сайтів додаємо необхідні записи (рис. 245 і 246).

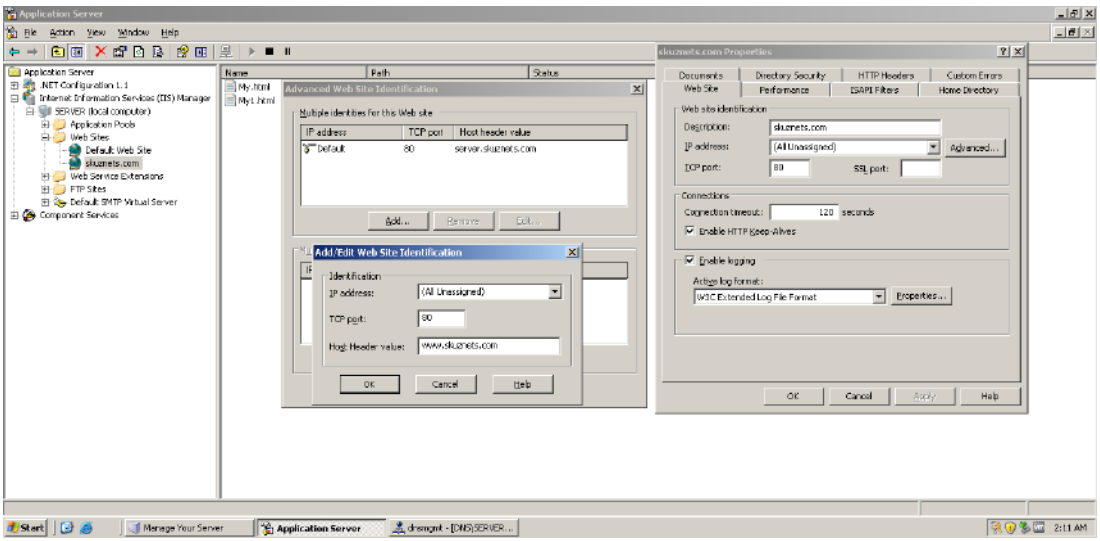

Рис. 245. **Налаштування ідентифікатора сайту www.skuznets.com**

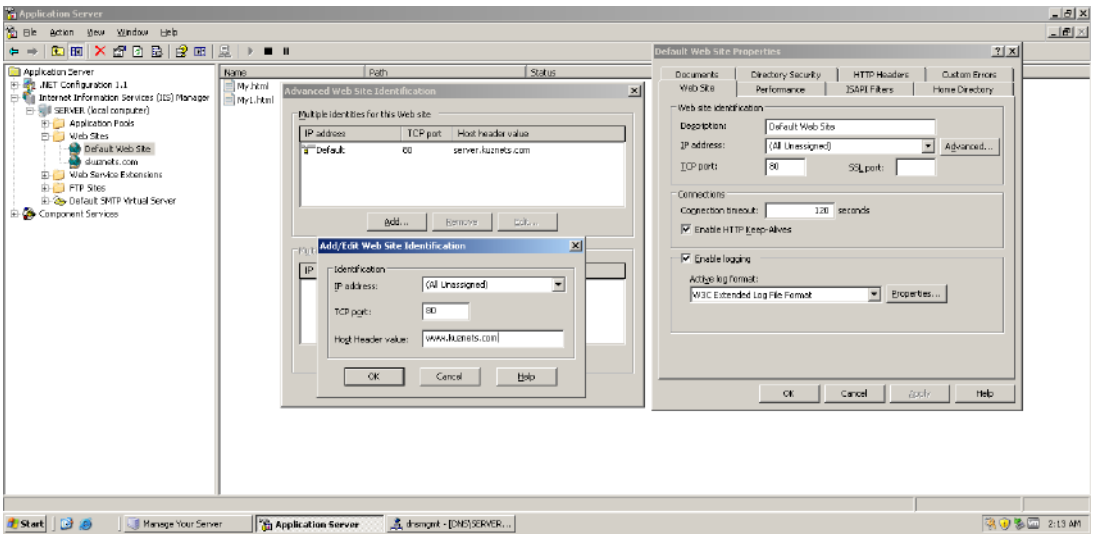

Рис. 246. **Налаштування ідентифікатора сайту www.kuznets.com**

Перевіряємо роботу сайтів із префіксом WWW на PC з *Windows XP Professional* (рис. 247).

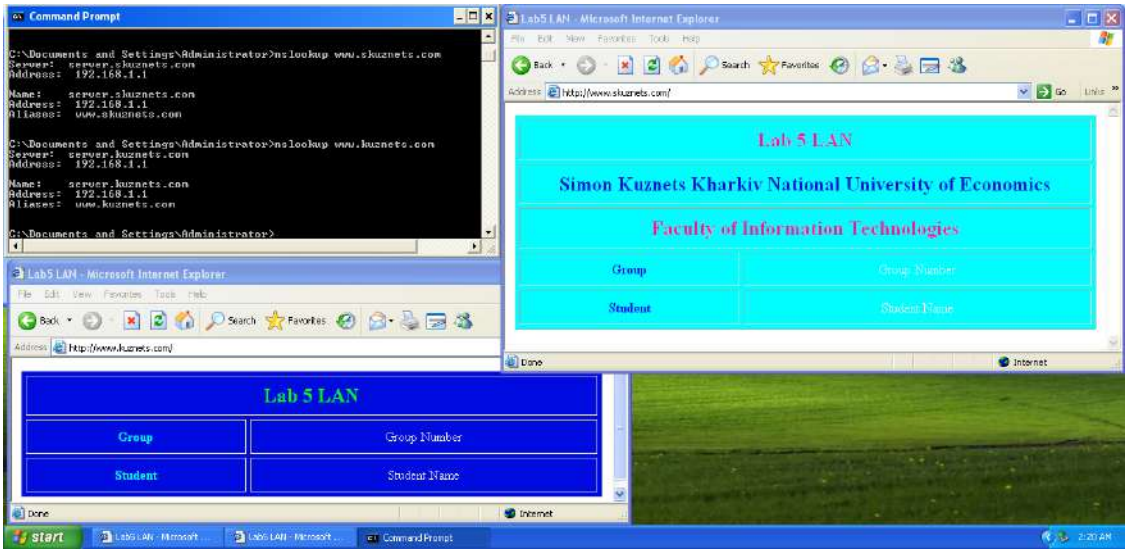

Рис. 247. **Перевірка роботи сайтів із префіксом WWW**

Вікно налаштувань вебсайтів (рис. 248).

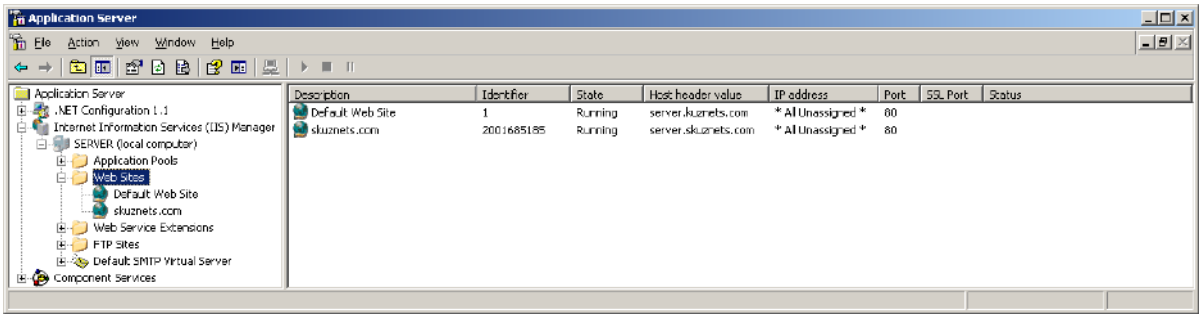

Рис. 248. **Налаштування вебсайтів**

На цьому створення вебсайтів та FTP-сервера закінчено.

Зміст звіту

1. Назва (тема) лабораторної роботи (ЛР), мета й зміст завдань лабораторної роботи.
2. Вихідні дані до лабораторної роботи.
3. Навести скриншоти результатів виконання всіх етапів завдань лабораторної роботи.
4. Висновки з лабораторної роботи.

Контрольні запитання

1. Яким чином зробити доступ до домашньої сторінки за певною адресою?
2. Для чого потрібно додавати нову адресу під час роботи із сервером додатків?
3. Які операції можна виконувати під час роботи з вебвузлом?
4. Яким чином зробити доступ до сайту з ім’ям, наприклад, *iis.com*?
5. Для чого в роботі встановлюють службу FTP?
6. Яким чином вибирають параметри сервера додатків?
7. Як забезпечити роботу сайту з використанням префікса WWW?

Лабораторна робота 6
Дослідження роботи мережевого симулятора Packet Tracer. Налаштування статичної маршрутизації в Packet Tracer

Метою лабораторної роботи є закріплення і поглиблення знань щодо методів моделювання роботи складних та локальних мереж за допомогою симулятора *Packet Tracer*, дослідження характеристик активного та пасивного мережевого устаткування.

6.1. Загальні відомості

Адресація в локальних мережах

MAC-адреса

MAC-адреса – це унікальний шістнадцятковий серійний номер, що призначають кожному мережевому пристрою для ідентифікації його в мережі. Для мережевих пристроїв (так само, як і для більшості інших мережевих типів) цю адресу встановлюють під час виготовлення, хоча зазвичай, вона може бути змінена за допомогою відповідної програми.

Кожна мережева карта має унікальну MAC-адресу, таким чином вона може ексклюзивно забирати з мережевого кабелю пакети, призначені для неї. Якщо MAC-адреса не є унікальною, то не існує способу провести відмінність між двома станціями. Пристрої в мережі переглядають мережевий трафік і шукають свою MAC-адресу в кожному пакеті, щоб визначити, повинні вони декодувати цей пакет чи ні. Є спеціальні способи для широкомовного розсилання повідомлень кожному пристрою.

MAC-адреси мають довжину 6 байтів, їх записують шістнадцятковим числом у вигляді 12:34:56:78:90:AB (двокрапок може не бути, але їх наявність робить адресу більш читабельною).

IP-адреса

IP-адреса вузла розділяється на дві частини: **IP-адресу мережі** й **IP-адресу вузла** в цій мережі.

IP-адреса мережі може бути вибрана адміністратором довільно або призначена за рекомендацією спеціального підрозділу **Internet (Internet Network Information Center, InterNIC)**, якщо мережа повинна працювати як складова частина **Internet**. Зазвичай постачальники послуг інтернету отримують діапазони адрес у підрозділів **InterNIC**, а потім розподіляють їх між своїми абонентами.

Номер вузла в протоколі IP призначають незалежно від локальної адреси вузла.

Необхідно відразу з'ясувати основний принцип IP-адресації – IP-адреси призначають **мережевим інтерфейсам вузлів** складної мережі, а не вузлам складної мережі.

Як правило, багато (якщо не більшість) комп'ютерів у IP-мережі мають єдиний мережевий інтерфейс (і як наслідок – одну IP-адресу). Але

комп’ютери й інші пристрої можуть мати декілька (якщо не більше) **мережевих інтерфейсів** – і кожен інтерфейс матиме свою власну IP-адресу. Пристрій із шістьма активними інтерфейсами (наприклад, маршрутизатор) матиме шість IP-адрес – по одній на кожен інтерфейс у кожній мережі, до якої він підключений.

Іноді говорять про IP-адресу як про адресу вузла-користувача складної мережі-хоста. Але це не зовсім точне визначення. Певний хост може мати декілька IP-адрес. У принципі багато (якщо не більшість) пристроїв у мережі "Інтернет" має тільки один інтерфейс і означає одну IP-адресу. Отже, IP-адреса визначає однозначно мережу і вузол, який підключено до цієї мережі. Варто розглянути структуру IP-адреси.

IP-адреса має довжину 4 байти (по 8 бітів) (IPv4), це дає в сукупності **32 біти** доступної інформації. 32-бітова розрядність IP-адреси призводить до того, що числа виходять великими, навіть якщо вони подані в десятковій системі числення. Тому для читабельності IP-адресу записують у вигляді чотирьох чисел, розділених точками. Наприклад, **128.10.2.30** – десяткова форма подання адреси – чотири (десяткових) числа, розділених крапками (.), а **10000000 00001010 00000010 00011110** – двійкова форма подання цієї ж адреси – чотирма 8-розрядними числами (октетами).

*Оскільки кожне з чотирьох чисел – це десяткове подання 8-бітового байта, то кожне число може набувати значень від **0 до 255***.

Тут потрібно зазначити, що десяткову форму запису IP-адреси використовують в основному в операційних системах як найбільш зручну під час налаштування. Окрім двійкової форми, часто застосовують шістнадцяткову форму запису IP-адреси: **C0.94.1.3**.

Використання 32-розрядних двійкових чисел дозволяє створювати 4 294 967 296 унікальних IP-адрес – більш ніж достатньо для будь-якої приватної інтрамережі (хоча мережа "Інтернет" уже почала відчувати нестачу унікальних IP-адрес).

6.2. Організація самостійної роботи студентів

Під час підготовки до виконання лабораторної роботи необхідно:

1. Ознайомитися з основами роботи IP-мереж.

2. Вивчити теоретичні матеріали з питань маршрутизації в комп’ютерних мережах.

3. Відповісти на контрольні запитання.

6.3. Опис лабораторної установки

Лабораторну роботу виконують на персональному комп'ютері з операційною системою *Windows* і пакетом *Packet Tracer* (завантажити з офіційного сайту).

6.4. Порядок виконання роботи

Частина 1. Ознайомлення з програмою Packet Tracer.

1. Запустити програму **Packet Tracer**, використовуючи: меню **Пуск**. Інтерфейс виглядає таким чином (рис. 249).

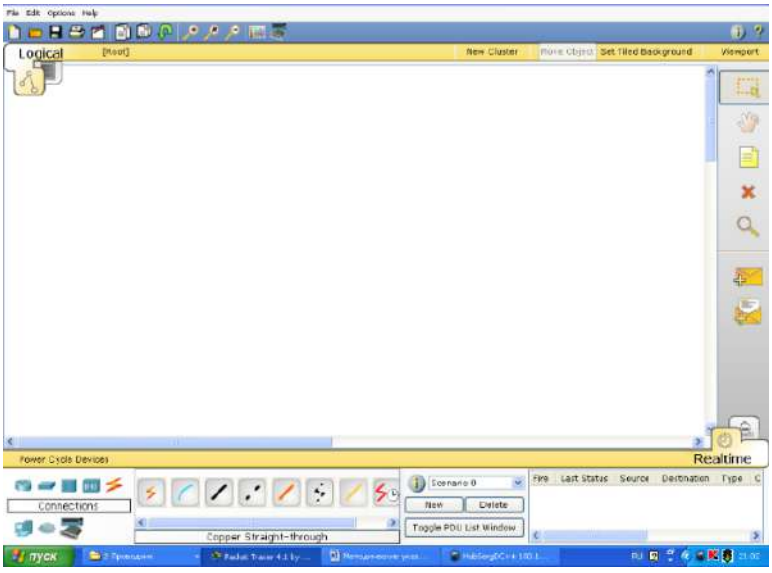

Рис. 249. **Інтерфейс програми**

Він складається з:

- **Робочого поля** – поля, у якому розміщується проєкт, що розробляють. Може перебувати у двох станах: **Real Time** – «розроблення проєкту», **Simulation** – «режим симуляції роботи проєкту».
- **Меню**.
- **Панелі пристроїв** – знаходиться внизу вікна програми. Містить: вибір виду мережевого пристрою *Routers* (маршрутизатор), *Hubs* (концентратор тощо) і вибір з'єднання мережевих пристроїв (вита пара,

коаксіальний кабель та ін.). Перенесення необхідного пристрою на робочу зону здійснюють за допомогою лівої кнопки мишки. З'єднання пристрою з пристроєм здійснюють за допомогою послідовного натискання на пристрої, які потрібно з'єднати, лівою кнопкою мишки і вибору відповідного порту або роз'єму. Для правильного з'єднання роз'єми двох пристроїв повинні сходитися.

- **Панелі сценаріїв** – знаходиться внизу вікна програми, містить усі сценарії та процеси, які працюють в момент, і дозволяє керувати ними.

2. Зібрати проєкт (рис. 250), який містить: **чотири ПК типу PC-PT**, **концентратор (*Hub-PT*)**. Кожен ПК має бути сполучений з концентратором за допомогою витої пари ***(Copper Straight – Through)***.

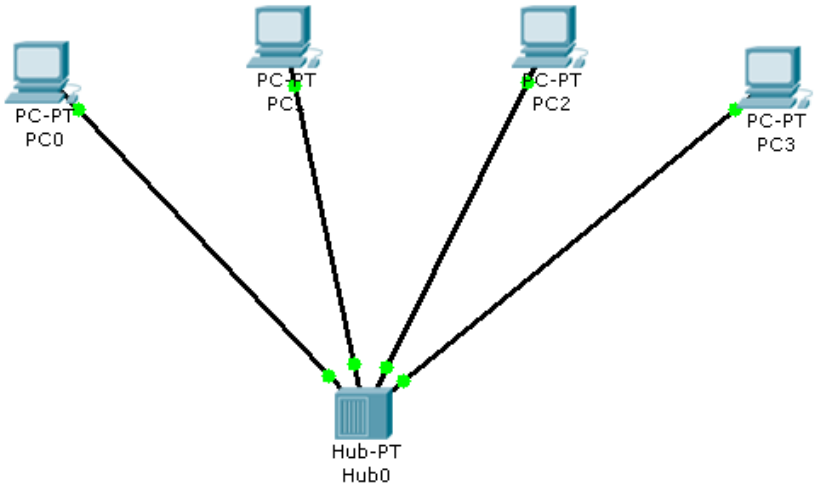

Рис. 250. **Топологія 1**

3. Зберегти проєкт і його скриншот.

4. Кожному ПК присвоїти унікальну **IP-адресу** (IPv4).

Для його призначення необхідно зайти в меню конфігурації ПК шляхом одноразового клацання по ньому лівою кнопкою мишки і вибору вкладки **Config/Interface** (рис. 251).

У полі ***ip address*** слід увести відповідну адресу, а в полі ***Subnet Mask*** – маску, що відповідає цій адресі, або через вкладки **Desktop/Ip configuration** (рис. 252).

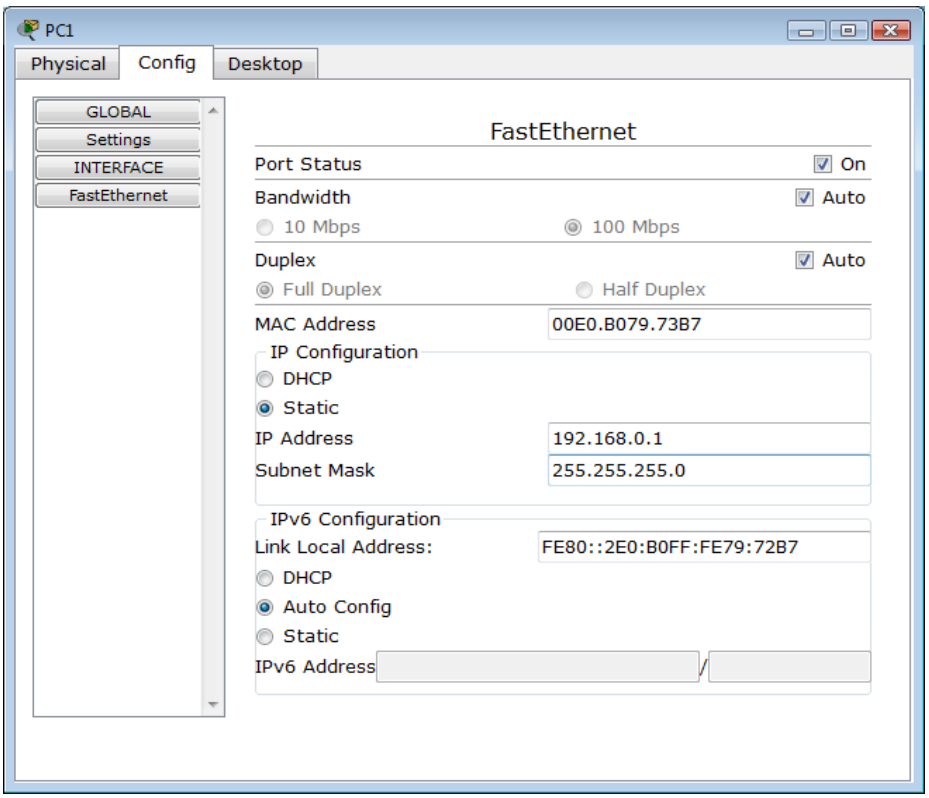

Рис. 251. **Призначення адреси локальній машині**

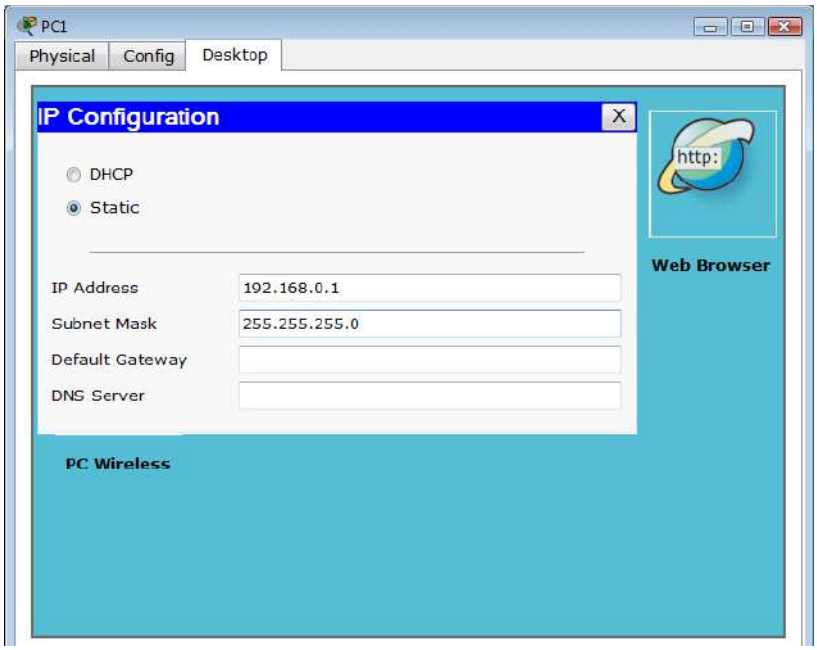

Рис. 252. **Призначення адреси локальній машині через вкладку "Робочий стіл"**

Значення IP-адреси для кожної машини (ПК) наведено в табл. 2.

Таблиця 2

Значення IP-адреси для кожної машини

Назва	IP-адреса
PC0	192.168.0.1
PC1	192.168.0.2
PC2	192.168.0.3
PC3	192.168.0.4

Значення маски для адреси: 255.255.255.0.

5. Перевірити працездатність отриманої мережі. Це роблять шляхом посилання мережевих запитів **(ICMP-пакетів)** від одного ПК до іншого. Для привласнення такого пакета ПК використовують кнопку **ADD SIMPLE PDU** в правій частині робочого вікна (рис. 253). Після цього потрібно клацнути лівою кнопкою мишки на локальну машину-джерело, а потім – на машину-отримувача. Перевірити працездатність мережевого шляху ***PC0*** і ***PC3***.

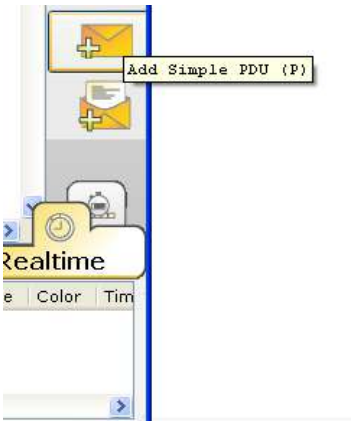

Рис. 253. **Привласнення *ICMP*-пакета ПК**

Результатом правильної роботи запиту посилання мережевих запитів **(*ICMP-пакетів*)** від одного ПК до іншого є поява в правому нижньому вікні повідомлення (рис. 254).

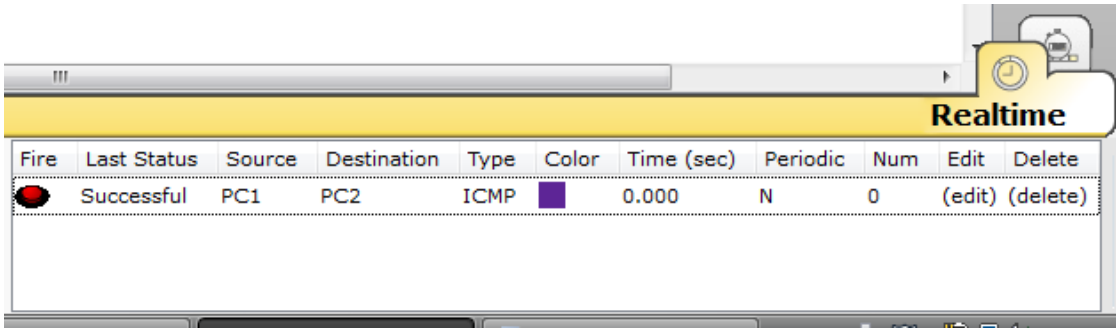

Рис. 254. **Результат запиту ICMP-пакетів**

6. Перейти в режим **Simulation** (рис. 255) і за допомогою кнопки *Even List* викликати вікно відображення подій у мережі ***Simulation Panel***.

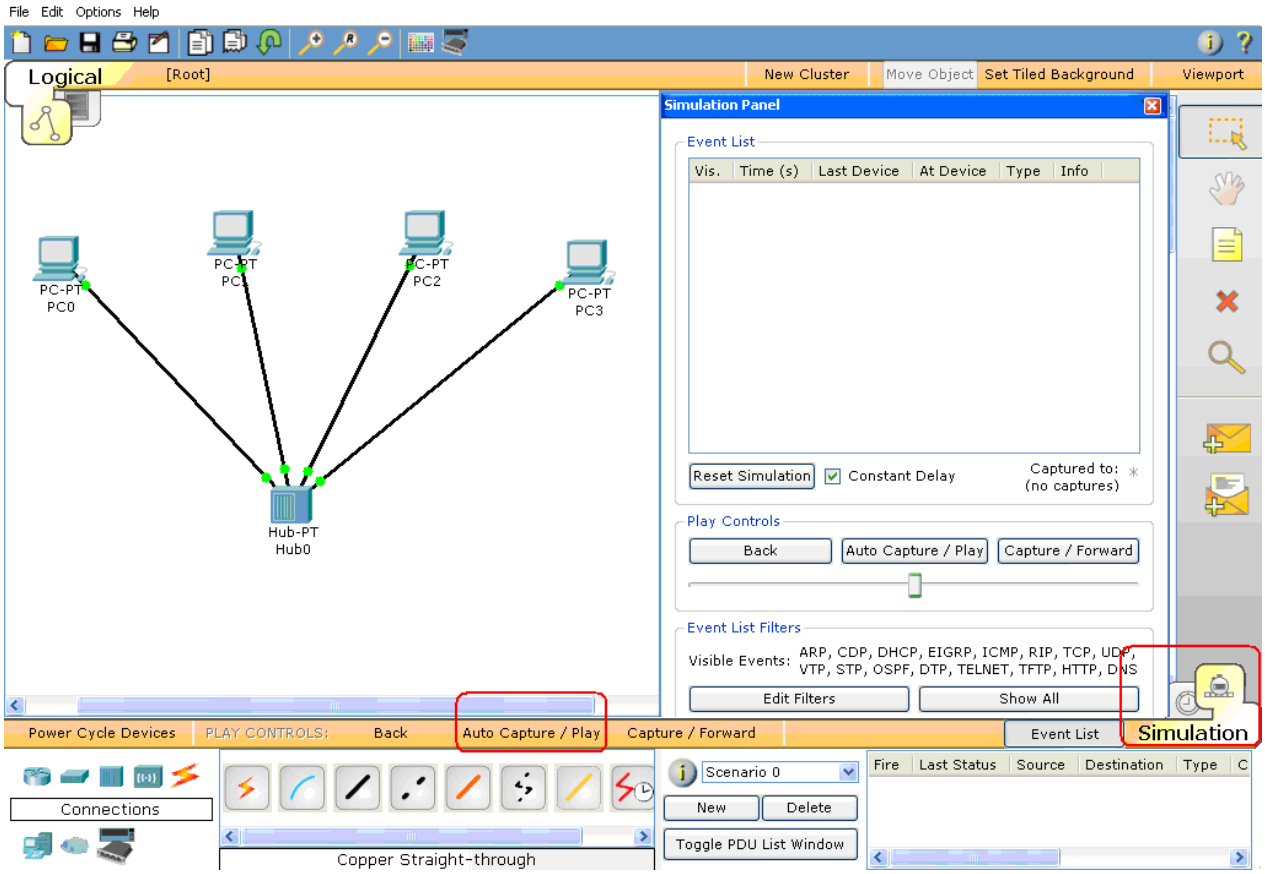

Рис. 255. **Режим симуляції**

7. Використовуючи кнопку **Auto Capture/Play**, запустити симуляцію роботи ***ICMP-пакетів***. Простежити просування пакетів мережею і зберегти цей скриншот.

8. Простежити за порядком і шляхом дотримання пакетів у вікні ***Simulation Panel*** (рис. 256). Відмітити періодичність посилання пакетів і їх поширення в мережі та зберегти цей скриншот.

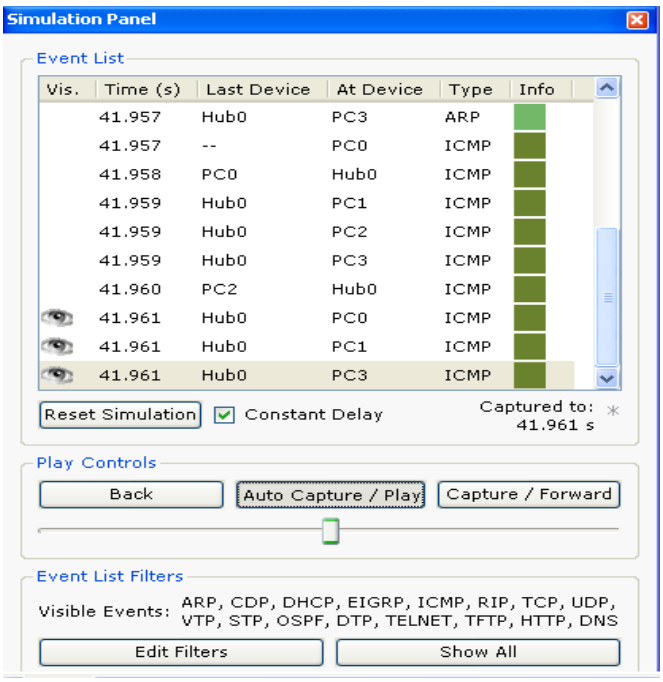

Рис. 256. **Вид панелі *Simulation Panel***

9. Проглянути інформацію про пакети з вікна **Simulation Panel** і їх відповідність моделі OSI шляхом подвійного клацання на пакеті у вікні (рис. 257). Ознайомитися зі вмістом пакета і проаналізувати його призначення (рис. 258). Проаналізувати процес установлення зв’язку між двома ПК та зберегти результати у вигляді скриншоту.

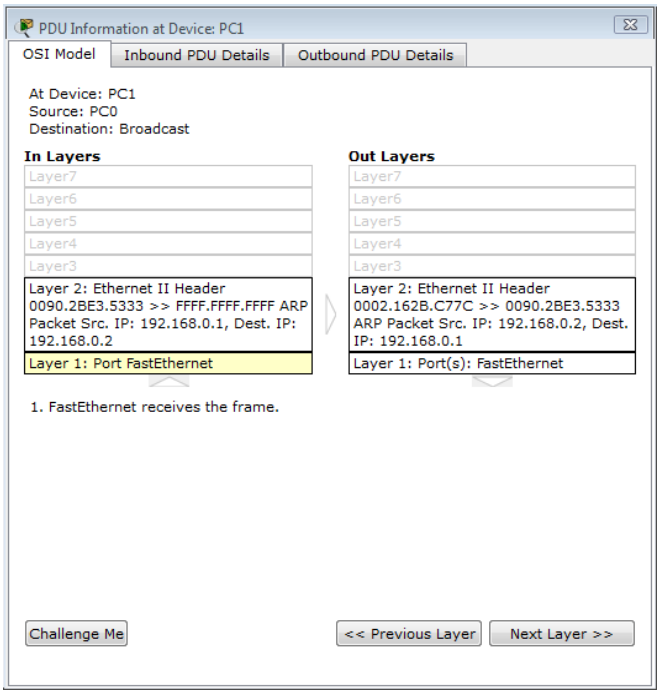

Рис. 257. **Відповідність пакета моделі OSI пакету протоколу ARP**

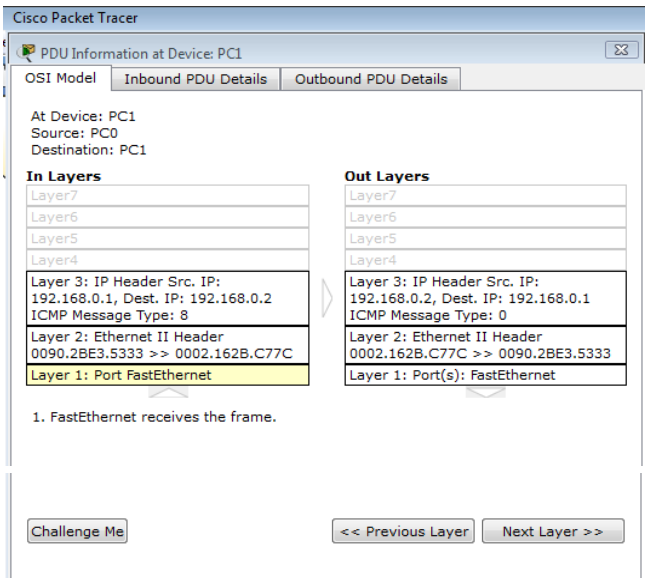

Рис. 258. **Відповідність пакета моделі OSI пакету протоколу ICMP**

Частина 2. Дослідження статичної маршрутизації

1. Зібрати проєкт (рис. 259), який містить: **три ПК типу PC-PT, три маршрутизатори (*Router*-PT)**.

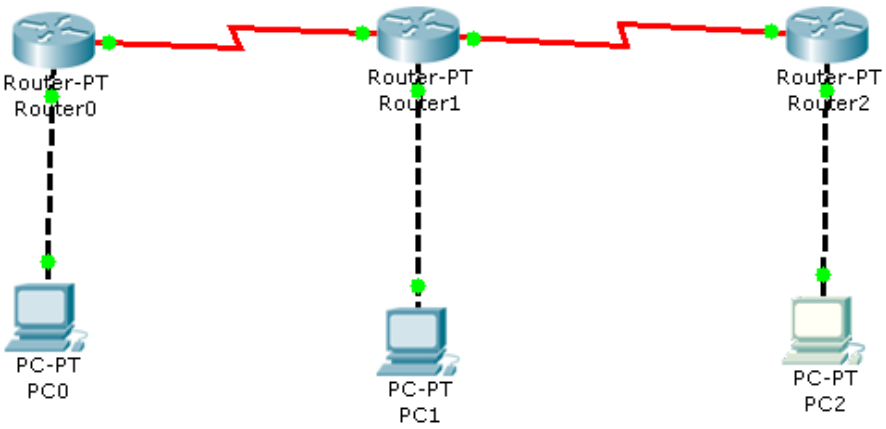

Рис. 259. **Досліджувана топологія мережі 1**

Кожен ПК має бути сполучений з маршрутизатором за допомогою кросового кабелю **(Copper Cross-over)** з використанням портів ***FastEthernet***.

Маршрутизатори з'єднати в топологію «шина» за допомогою спеціальних низькошвидкісних ***Serial***-портів і кабелю ***Serial DCE Copper***.

2. Кожному ПК присвоїти унікальну ***IP-адресу***. Адреси наведено в табл. 3.

Таблиця 3

Значення унікальних IP-адрес

Назва	IP-адреса
PC0	192.168.1.10
PC1	192.168.3.10
PC2	192.168.5.10

Значення маски для адрес: 255.255.255.0.

3. Маршрутизатор є активним мережевим пристроєм, тобто в цьому пристрої є функція перетворення мережевих адрес, яка використовує таблицю маршрутизації. За допомогою маршрутизатора можна об'єднувати різні підмережі, що мають різні IP-адреси. На відміну від комутаторів, портам маршрутизатора призначають унікальні IP-адреси (інтерфейси).

Приклад побудови мережі з трьома ПК і трьома маршрутизаторами.

Є три підмережі (клас С), у яких знаходяться три персональні комп'ютери: перша підмережа – ***x.x. 1.x***, друга, – ***x.x. 3.x***, третя, – ***x.x. 5.x.*** Завдання маршрутизатора – перенаправляти потоки даних у підмережах. Для цього потрібно задати IP-адреси вхідним ***(FastEthernet)*** і вихідним ***(Serial)*** портам маршрутизатора. Ці адреси наведено в табл. 4.

Таблиця 4

IP-адреси вхідним і вихідним портам

Router 0	
Fast Ethernet 0/0	192.168.1.1
Serial	192.168.2.1
Router 1	
Fast Ethernet 0/0	192.168.3.1
Serial 1	192.168.2.2
Serial 2	192.168.4.1
Router 2	
Fast Ethernet 0/0	192.168.5.1
Serial 1	192.168.4.2

Значення маски для адрес: 255.255.255.0.

Маршрутизатору, згідно з адресами підмереж, які він обслуговує, призначають відповідні інтерфейси. Для перегляду інтерфейсів необхідно навести курсор на потрібний маршрутизатор (рис. 260).

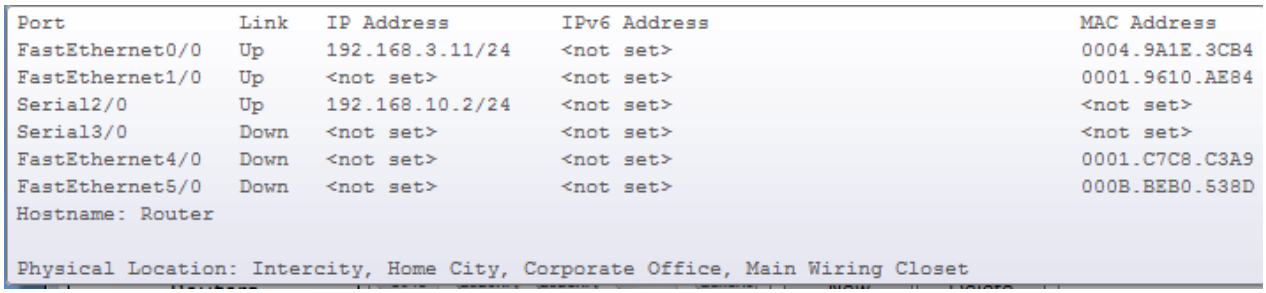

Рис. 260. **Значення IP-адрес інтерфейсів маршрутизатора**

IP-адреси для портів маршрутизатора вводять у вкладці ***Config/Interface***. Слід також простежити, щоб статус робочого порту був активний (рис. 261).

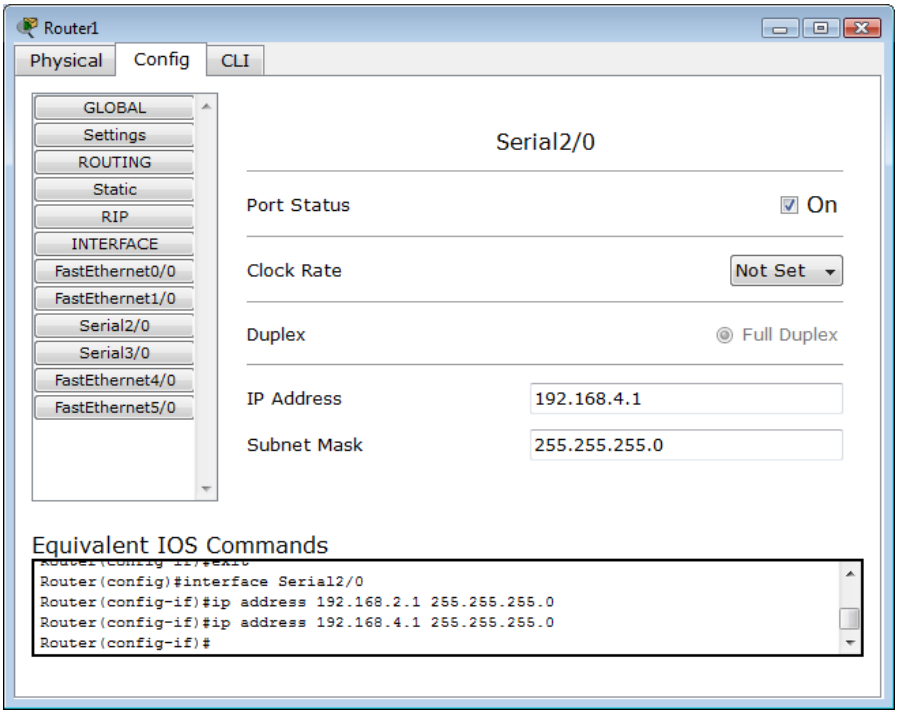

Рис. 261. **Визначення параметрів одного з робочих портів маршрутизатора**

4. Проставити для кожного ПК шлюз за замовчуванням. Це роблять у вкладці ***Config/Global***. Для кожного ПК шлюзом за замовчуванням є адреса порту маршрутизатора ***FastEthernet***, з яким він сполучений. Ця дія сполучає локальну машину з активним мережевим пристроєм, у цьому випадку – з маршрутизатором.

5. Перевірити зв’язок між кожним ПК і маршрутизатором, використовуючи етапи, описані в пп. 5 – 9 частини 1.

6. Для кожного маршрутизатора призначити **статичні маршрути**, які зв’язуватимуть цей маршрутизатор з іншими підмережами. Для цього використовують вкладку конфігурації маршрутизатора **Config/Static**. Приклад призначення маршрутів для **Router 0** наведено на рис. 262.

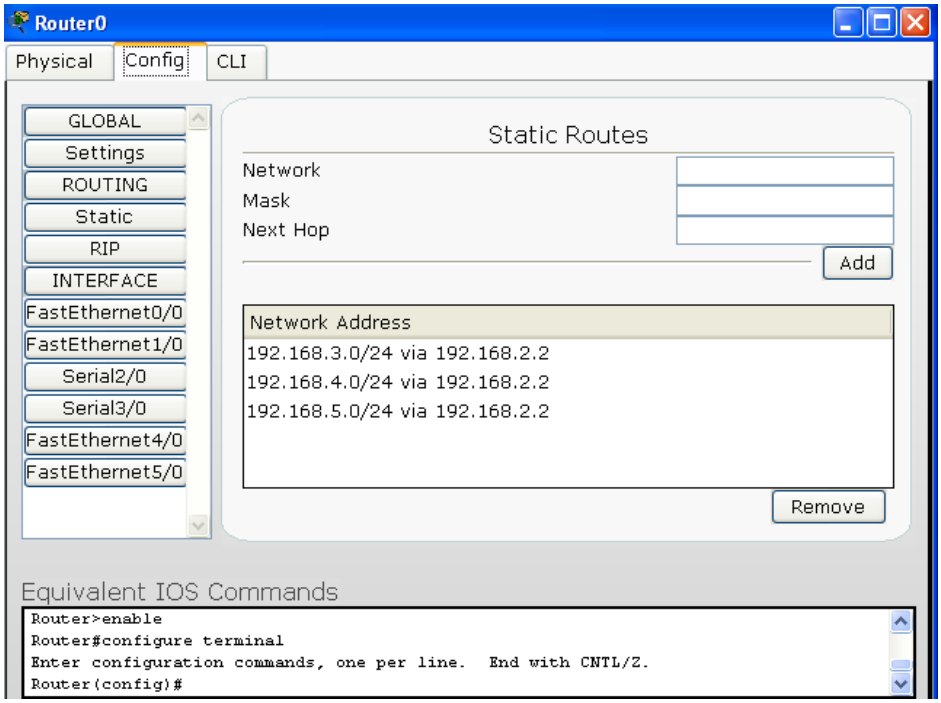

Рис. 262. **Призначення статичних маршрутів**

Потрібну підмережу задають у вкладці **Network**, маску підмережі – у **Mask**; порт, через який роблять доступ до підмережі, прописують у вкладці **Next Hop**.

Наприклад, відповідно до рис. 263, у маршрутизаторі **Router 0** прописано три статичні маршрути – у підмережах 192.168.3.0, 192.168.4.0 і 192.168.192.5.0. Це означає, що цей маршрутизатор дозволяє перенаправляти потоки інформації з підмережі 192.168.1.0, де знаходиться **PC0**, в інші підмережі: 192.168.3.0 – підмережу **PC1**, 192.168.4.0 – підмережу між **Router 1** і **Router 2** та 192.168.5.0 – підмережу **PC2**. Аналогічним чином призначити статичні маршрути для інших маршрутизаторів.

7. Використовуючи пп. 5 – 9 частини 1, перевірити працездатність зв’язку між **PC0-PC1**, **PC1-PC2**, **PC0-PC2**. Зберегти результати перевірки у вигляді скриншотів.

8. Створити новий проєкт. У цьому проєкті на двох **Switch** створити підмережі, що складаються з трьох ПК. Маршрутизатори з'єднують з комутаторами за допомогою витої пари (**Copper Straight – through**).

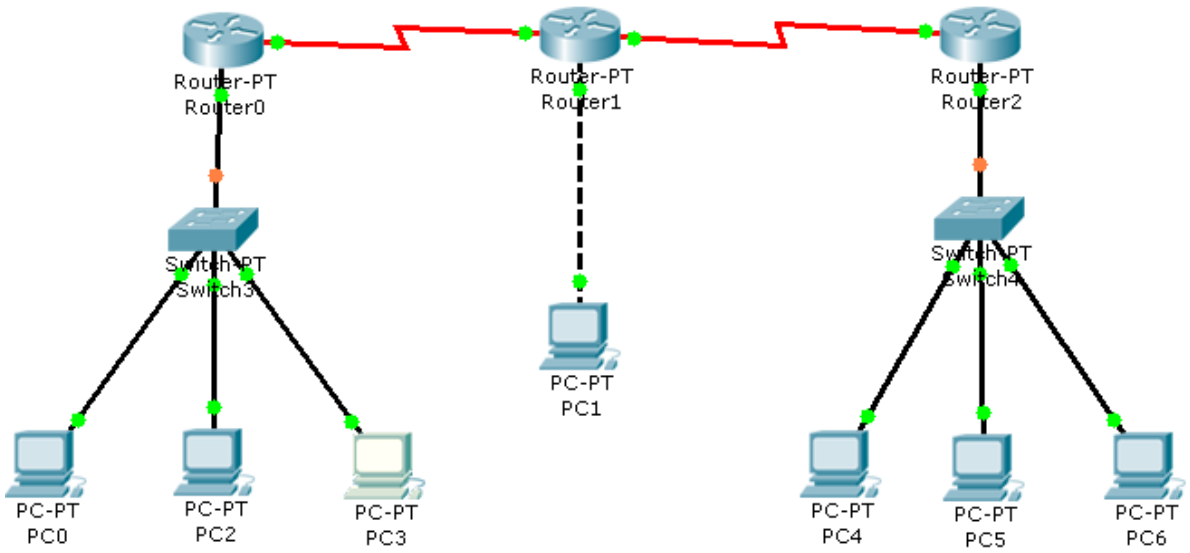

Рис. 263. **Досліджувана топологія мережі 2**

9. Кожному ПК присвоїти унікальну IP-адресу згідно з табл. 5.

Таблиця 5

Унікальні IP-адреси ПК

Назва	IP-адреса
PC0	192.168.1.10
PC2	192.168.1.11
PC3	192.168.1.12
PC1	192.168.3.10
PC4	192.168.5.10
PC5	192.168.5.11
PC6	192.168.5.12

Значення маски для IP-адрес: 255.255.255.0.

Адреси портів маршрутизатора наведено в табл. 6.

Таблиця 6

Адреси портів маршрутизатора

Router 0	
Fast Ethernet 0/0	192.168.1.1
Serial	192.168.2.1
Router 1	
Fast Ethernet 0/0	192.168.3.1
Serial 1	192.168.2.2
Serial 2	192.168.4.1
Router 2	
Fast Ethernet 0/0	192.168.5.1
Serial 1	192.168.4.2

Значення маски для IP-адрес: 255.255.255.0.

10. Визначити для кожного ПК шлюз за замовчуванням.

11. Використовуючи пп. 5 – 9 частини 1, перевірити працездатність зв'язку між **PC0-PC4**, **PC2-PC5**, **PC3-PC0**. Виокремити особливості встановлення зв'язку між прикордонними вузлами. Зберегти результати перевірки у вигляді скриншоту.

12. Виконати індивідуальне завдання відповідно до таких варіантів (табл. 7).

Під час виконання варіанта необхідно в кожну з підмереж включати не менше трьох PC.

У процесі виконання завдань варіанта потрібно:

1. Вибрати базову мережу.

2. Навести для кожної з масок підмереж діапазони адрес, що виділяють для PC. Звести отримані результати в таблицю (приклад наведено нижче).

3. Розробити проєкт відповідно до пп. 1 – 11 згідно з індивідуальним варіантом табл. 7.

Таблиця 7

Варіанти індивідуальних завдань

№ варіанта	Клас мережі	Маска мережі
1	B	20, 22, 23
2	C	24, 25, 29
3	B	17, 18, 19
4	C	24, 26, 28
5	B	16, 17, 20
6	C	25, 29, 30
7	B	20, 21, 23
8	C	26, 28, 30
9	B	18, 19, 21
10	C	26, 29, 30
11	B	16, 18, 20
12	C	24, 26, 30
13	B	16, 19, 22
14	C	27, 28, 29
15	B	17, 19, 21
16	B	20, 21, 23
17	C	26, 29, 30
18	B	16, 17, 20
19	C	23, 24, 25
20	B	20, 21, 23
21	B	15, 18, 20
22	C	24, 26, 30
23	B	20, 22, 23
24	C	25, 26, 27
25	B	20, 21, 23

Приклад таблиці для розроблення проєкту моделі

Таблиця даних для розроблення проєкту згідно з варіантом.

Мережа 1

Клас мережі, маска	**IP-адреса мережі (базова)**		
Мережа 1	Адреса маршрутизатора	Перша адреса хоста	Остання адреса хоста
Підмережа 1	Адреса		
Адреси хостів підмережі 1			
Підмережа 2	Адреса		
Адреси хостів підмережі 2			
Підмережа ... n ...	Адреса		
Адреси хостів підмережі … n ...			

Мережа 2

Клас мережі, маска	**IP-адреса мережі (базова)**		
Мережа 2	Адреса маршрутизатора	Перша адреса хоста	Остання адреса хоста
Підмережа 1	Адреса		
Адреси хостів підмережі 1			
Підмережа 2	Адреса		
Адреси хостів підмережі 2			
Підмережа ... n ...	Адреса		
Адреси хостів підмережі … n ...			

Мережа 3

Клас мережі, маска	IP-адреса мережі (базова)		
Мережа 3	Адреса маршрутизатора	Перша адреса хоста	Остання адреса хоста
Підмережа 1	Адреса		
Адреси хостів підмережі 1			
Підмережа 2	Адреса		
Адреси хостів підмережі 2			
Підмережа ... n ...	Адреса		
Адреси хостів підмережі … n ...			

Зміст звіту

1. Назва (тема) лабораторної роботи (ЛР), мета й зміст завдань лабораторної роботи.
2. Вихідні дані до лабораторної роботи.
3. Навести скриншоти результатів виконання всіх етапів завдань лабораторної роботи.
4. Висновки з лабораторної роботи.

Контрольні запитання

1. Що таке IP-адреса? Назвіть її функції.
2. Що таке MAC-адреса? Назвіть її функції.
3. У чому полягають функції ARP-пакета?
4. У чому полягають функції ICMP-пакета?
5. Перерахуйте види статичних маршрутів. Охарактеризуйте їхні переваги, недоліки та сфери використання.

Рекомендована література

Основна

1. Волосюк Ю. В. Комп’ютерні мережі : курс лекцій / Ю. В. Волосюк. – Миколаїв : МНАУ, 2019. – 203 с.
2. Городецька О. С. Комп’ютерні мережі : навч. посіб. / О. С. Городецька, В. А. Гикавий, О. В. Онищук. – Вінниця : ВНТУ, 2018. – 129 с.
3. Задерейко О. В. Комп’ютерні мережі : навч. посіб. / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса : ОЮА, 2022. – 249 с.
4. Карпенко М. Ю. Конспект лекцій з курсу "Комп’ютерні мережі" (для студентів усіх форм навчання спеціальностей 122 – Комп’ютерні науки, 151 – Автоматизація та комп’ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / М. Ю. Карпенко, Н. В. Макогон. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с.
5. Комп’ютерні мережі : підручник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін. – Вінниця : ВНТУ, 2020. – 378 с.
6. Stevens W. Unix development of network applications / W. Stevens. – New Jersey : Wiley, 2020. – 1038 p.

Додаткова

7. Лунтовський А. Проектування та дослідження комп’ютерних мереж / А. Лунтовський, І. Мельник. – Львів : Університет "Україна", 2020. – 362 с.
8. Отрох С. І. Комп’ютерні мережі. Комп’ютерний практикум : навч. посіб. для студентів спеціальності 122 "Комп’ютерні науки" / С. І. Отрох,

Н. М. Аушева, І. І. Гусєва, В. О. Кузьміних. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 127 с.

9. Сучасні інформаційні технології та системи : монографія / Н. Г. Аксак, Л. Е. Гризун, О. В. Щербаков та ін. ; за заг. ред. В. С. Пономаренка. – Харків : ХНЕУ ім. С. Кузнеця, 2022. – 270 с.

10. Цвіркун Л. І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 "Інформаційні технології" : у 2 ч. / Л. І. Цвіркун, Я. В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т "Дніпровська політехніка". – Дніпро : НТУ "ДП", 2018. – Ч. 1. – 60 с.

11. Цвіркун Л. І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 "Інформаційні технології" : у 2 ч. / Л. І. Цвіркун, Я. В. Панферова ; М-во освіти і науки України ; Нац. техн. ун-т "Дніпровська політехніка". – Дніпро : НТУ "ДП", 2018. – Ч. 2. – 39 с.

Інформаційні ресурси

12. Навчальний курс Computer networks [Електронний ресурс]. – Режим доступу : https://nesoacademy.org/cs/06-computer-networks.

13. Персональна навчальна система "Комп’ютерні мережі" [Електронний ресурс]. – Режим доступу : https://pns.hneu.edu.ua/course/view.php?id=7309.

14. Проектування безпроводових комп’ютерних мереж [Електронний ресурс] : навч. посіб. / А. В. Лемешко, Л. А. Кирпач, Д. В. Сорокін та ін. – Київ : ДУТ, 2021. – 147 с. – Режим доступу : https://dut.edu.ua/uploads/l_2224_69488065.pdf.

15. Packet Tracer 8.2.1 і всі попередні версії [Електронний ресурс]. – Режим доступу : https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html/.

16. Survey and Performance Evaluation of the Upcoming Next Generation WLAN Standard-IEEE 802.11 ax [Electronic resource] / Qiao Qu, Bo Li, Mao Yang et al. – Access mode : https://arxiv.org/ftp/arxiv/papers/1806/1806.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

КОМП’ЮТЕРНІ МЕРЕЖІ

Лабораторний практикум
для студентів спеціальності 122 "Комп’ютерні науки"
освітньої програми "Комп’ютерні науки"
першого (бакалаврського) рівня

Самостійне електронне текстове мережеве видання

Укладачі: **Мінухін** Сергій Володимирович
Коцюба Василь Петрович
Савін Юрій Вікторович

Відповідальний за видання *Д. О. Бондаренко*

Редактор *В. О. Дмитрієва*

Коректор *Н. Г. Войчук*

План 2023 р. Поз. № 96 ЕВ. Обсяг 122 с.

Видавець і виготовлювач – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб’єкта видавничої справи до Державного реєстру
ДК № 4853 від 20.02.2015 р.