

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

МЕРЕЖІ ОБМІНУ ДАНИМИ. КОМП'ЮТЕРНИЙ ПРАКТИКУМ

*Рекомендовано Методичною радою КПІ ім. Ігоря
Сікорського як навчальний посібник для студентів,
які навчаються за спеціальністю 151 «Автоматизація та комп'ютерно-
інтегровані технології»*

Київ

КПІ ім. Ігоря Сікорського

2021

Мережі обміну даними. Комп'ютерний практикум [Електронний ресурс]: навч. посіб. для студ. спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / КПІ ім. Ігоря Сікорського; уклад.: А. О. Абрамова. – Електронні текстові дані (1 файл: 4,52 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 141 с.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 9 від 01.11.2021 р.) за поданням Вченої ради інженерно-хімічного факультету (протокол № 2 від 09.12.2021)

Електронне мережне навчальне видання

МЕРЕЖІ ОБМІНУ ДАНИМИ КОМП'ЮТЕРНИЙ ПРАКТИКУМ

Укладачі: *Абрамова Алла Олександрівна, к.т.н.*

Відповідальний
редактор *Абрамова Алла Олександрівна, к.т.н.*

Рецензенти: *Джигирей І.М., к.т.н., доц.*

Навчальний посібник розроблено відповідно до програми підготовки бакалаврів за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології». Навчальний посібник призначений для виконання лабораторних робіт з дисципліни «Мережі обміну даними», що викладається згідно з учбовим планом бакалаврської підготовки інженерно-хімічного факультету. Дана дисципліна призначена для ознайомлення майбутніх фахівців хімічної промисловості з функціонуванням, керуванням комп'ютерними мережами зв'язку та роботою в них. Представлені матеріали мають за мету закріплення знань та набуття вміння користування необхідними базовими навичками в галузі комп'ютерних мереж, серед яких функціонування, експлуатація та адміністрування мережі, які вони зможуть використовувати в подальшому процесі навчання.

© КПІ ім. Ігоря Сікорського, 2021

Зміст

Вступ.....	6
ПРАКТИЧНА РОБОТА 1.....	7
ОСВОЄННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ NETCRACKER.....	7
1.1 Теоретичні відомості	7
1.2 Порядок виконання роботи	15
1.3 Оброблення та аналізування результатів. Оформлення звіту.	25
1.4 Контрольні питання	25
ПРАКТИЧНА РОБОТА № 2.....	26
МОДЕЛЮВАННЯ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖІ.....	26
2.1 Теоретичні відомості	26
2.2 Порядок виконання роботи	28
2.3 Оброблення та аналізування результатів. Оформлення звіту.	31
2.4 Контрольні питання	31
ПРАКТИЧНА РОБОТА № 3.....	32
СТВОРЕННЯ МОДЕЛІ У NETCRACKER.....	32
3.1 Теоретичні відомості	32
3.2 Порядок виконання	46
3.3 Оброблення та аналізування результатів. Оформлення звіту.	49
3.4 Контрольні питання	49
ПРАКТИЧНА РАБОТА № 4.....	50
ВИВЧЕННЯ ОБЛАДНАННЯ ТА КАБЕЛЬНОЇ СИСТЕМИ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ. ЕТАЛОННА МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ	50
4.1 Теоретичні відомості	50
4.2 Порядок виконання	58
4.3 Оброблення та аналізування результатів. Оформлення звіту.	62
4.4 Контрольні питання	62
ПРАКТИЧНА РОБОТА №5.....	63
СТВОРЕННЯ БАГАТОРІВНЕВОГО ПРОЕКТУ	63
5.1 Теоретичні відомості	63
5.2 Порядок виконання	65
5.3 Оброблення та аналізування результатів. Оформлення звіту.	70
5.4 Контрольні питання	71

ПРАКТИЧНА РОБОТА 6.....	72
ДОСЛІДЖЕННЯ РОБОТИ МЕРЕЖЕВОГО СИМУЛЯТОРА PASCET TRACER. НАЛАШТУВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ В PASCET TRACER	72
6.1 Теоретичні відомості	72
6.2 Порядок виконання роботи	81
6.3 Оброблення та аналізування результатів.	93
6.4 Контрольні питання	93
ПРАКТИЧНА РОБОТА №7.....	95
ДІАГНОСТИКА IP-ПРОТОКОЛУ.....	95
7.1 Теоретичні відомості	95
7.2 Порядок виконання	102
7.3 Оброблення та аналізування результатів. Оформлення звіту.....	103
7.4 Контрольні питання	103
ПРАКТИЧНА РОБОТА 8.....	104
КОНФІГУРУВАННЯ DHCP-СЕРВЕРА	104
8.1 Теоретичні відомості	104
8.2 Порядок виконання роботи	107
8.3 Оброблення та аналізування результатів. Оформлення звіту.	117
8.4 Контрольні питання	117
ПРАКТИЧНА РОБОТА 9.....	118
КОНФІГУРУВАННЯ DNS-СЕРВЕРА.....	118
9.1 Теоретичні відомості	118
9.2 Порядок виконання роботи	124
9.3 Оброблення та аналізування результатів. Оформлення звіту.	138
9.4 Контрольні питання	139
Список рекомендованої літератури	140

Вступ

Проблема передачі інформації від одного комп'ютера на інший існувала з моменту появи комп'ютерів. Для її вирішення використовувалися різні підходи. Найбільш поширений, в недавньому минулому, «кур'єрський» підхід полягав у копіюванні інформації на змінний носій і перенесенні до місця призначення і повторне копіювання. В даний час подібні способи переміщення інформації поступаються місцем мережним технологіям обміну даними. Вивченню принципів, способів та апаратного оформлення такого обміну присвячена дана дисципліна.

Метою даної дисципліни є вироблення у студентів знань та навичок в галузі комп'ютерних мереж обміну даними, серед яких функціонування, експлуатація та адміністрування мережі, які вони зможуть використовувати в подальшому процесі навчання.

Предметом вивчення дисципліни є мережеві протоколи, стандарти, канали передачі даних, обладнання мереж обміну даними.

У процесі вивчення дисципліни студент оволодіє методами та підходами до аналізування, визначення характеристик та організації каналів передачі інформації при використанні мереж обміну даними.

Дисципліна «Мережі обміну даними» викладається згідно з учбовим планом бакалаврської підготовки інженерно-хімічного факультету й призначена ознайомити майбутніх фахівців з функціонуванням, керуванням комп'ютерними мережами зв'язку та роботою в них.

ПРАКТИЧНА РОБОТА 1

ОСВОЄННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ NETCRACKER

Мета та основні завдання роботи: вивчити роботу графічного інтерфейсу NetCracker, ознайомитись з головними можливостями даної програми і загальними принципами моделювання мережі в ній.

Вивчити та стисло описати у протоколі практичної роботи:

- основні елементи інтерфейсу NetCracker;
- налаштування системи NetCracker;
- головні можливості NetCracker.

1.1 Теоретичні відомості

NetCracker® – програмний пакет, розроблений компанією NetCracker Technology, дозволяє створювати проекти обчислювальних мереж різної складності топології і проводити їх аналіз використовуючи технологію імітаційного моделювання.

Область застосування пакету NetCracker – створення проекту мережевого рішення, тестування цього рішення і документування остаточного варіанту. База даних обладнання допускає, хоча і з деякими обмеженнями, додавання нового обладнання з характеристиками, які задаються користувачем. Ця можливість, зокрема, в достатній мірі компенсує відсутність обладнання GigaBit Ethernet, яке користувач може створити самостійно.

NetCracker дозволяє оцінювати якісно можливість перевантаження устаткування і каналів передачі даних, знаходити «вузькі місця» мережевого проекту. Також необхідно враховувати, що вимоги пакету до продуктивності процесора ростуть у міру збільшення числа заданих потоків даних і на машинах, наприклад, Celeron-500 МГц симуляція проекту з числом потоків 15 вже може давати збої, а для нормальної роботи вимагає, щонайменше, Celeron - 800 МГц.

Крім того, пакет робить можливим познайомитися з практикою створення

найрізноманітніших мережевих рішень майже «вживу» без дорогої тестової лабораторії. Ця можливість, надзвичайно корисна на лабораторних заняттях з мережних технологій, адміністрування та проектування мереж.

Програма NetCracker призначена для проектування і моделювання комп'ютерних мереж. Для проектування структури мережі програма надає можливість вибору необхідного обладнання з вбудованою бази даних, а також додавання в базу даних і конфігурації нового обладнання різних типів. Користувач розміщує обрані компоненти на складальному полі, задає структуру і тип зв'язків між ними, визначає тип програмного забезпечення і характер трафіку між вузлами мережі. Надалі є можливість вказати перелік аналізованих характеристик і вид відображення статистичної інформації і виконати імітаційне моделювання спроектованої мережі.

На рис. 1.1 наведено типовий вигляд вікна програми NetCracker. Панель перегляду компонент, наявних у базі даних, розташовується звичайно в лівій частині вікна і вмикається за допомогою команди **View→ Bars→ Browser Pane**. Панель містить кілька закладок:

- Закладка **Project Hierarchy** призначена для відображення структури документів створюваного проекту мережі.
- Закладка **Devices** призначена для відображення бази даних пристроїв.

Перелік пристроїв має кілька видів відображення:

- **Types** (Типи) – пристрої в списку групуються за типами. Потім у кожній групі можуть виділятися підтипи пристроїв за функціональними ознаками. Після цього пристрою розділяються по виробникам.
- **Vendors** (Продукенти) – пристрої в списку групуються за виробником. Потім у кожній групі виділяються підгрупи, що відповідають типу пристроїв.
- **User** (Користувальницькі) – пристрої, визначені користувачем. У свою чергу також можуть групуватися за типами або виробником.
- **Compatible Devices** призначена для відображення списку сумісних пристроїв.

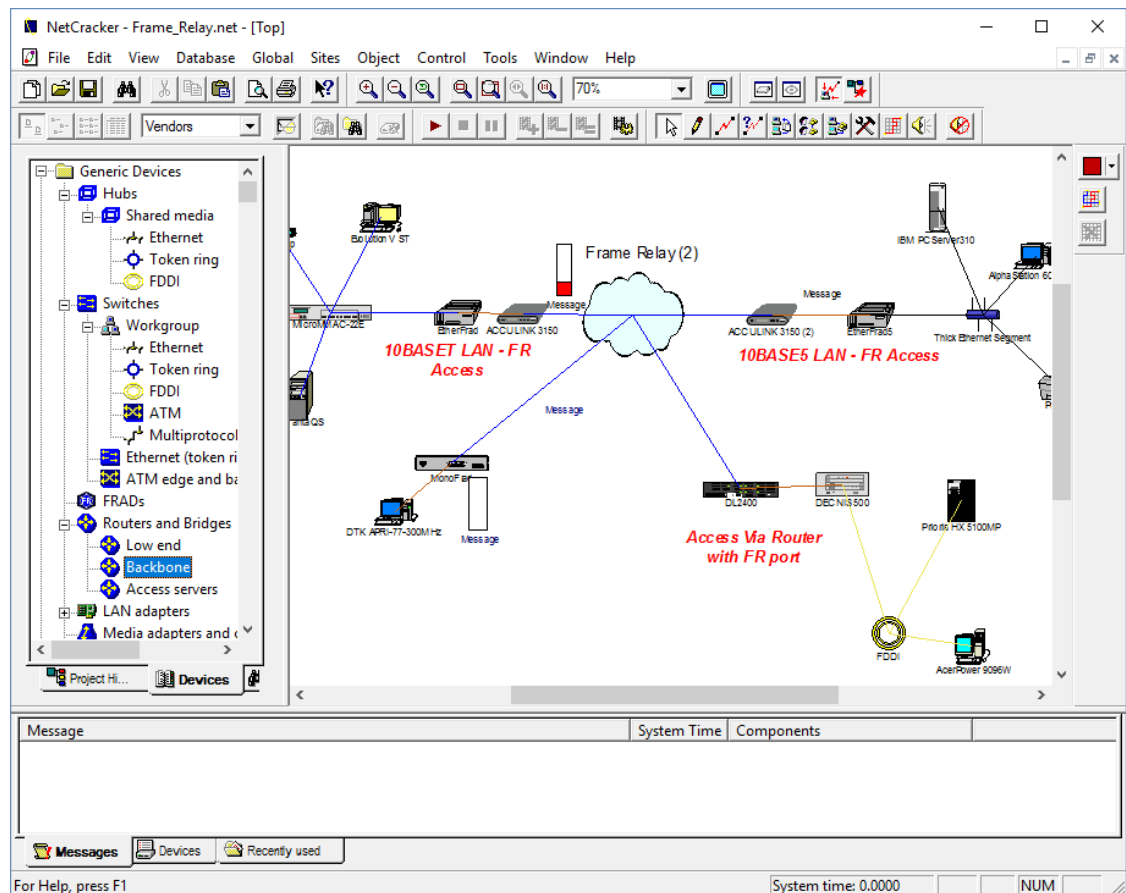


Рис. 1.1. Зовнішній вигляд інтерфейсу NetCracker Pro

У нижній частині вікна програми зазвичай розташовується панель пристроїв, яка може бути відображена за допомогою команди **View**→**Bars**→**Image Pane**. Дана панель призначена для відображення пристроїв з вибраної групи.

У правій верхній частині головного вікна програми розташовується основне вікно, яке представляє собою складальне поле. У ньому необхідно розміщувати використовувані компоненти при проектуванні структури мережі.

Для завдання структури мережі необхідно розмістити в складальному полі використовувані пристрої і з'єднати їх лініями зв'язку. Для розміщення пристрою в складальному полі необхідно, користуючись панеллю перегляду списку пристроїв, вибрати відповідний клас і тип пристрою. Після цього потрібно вибрати пристрій в панелі пристроїв, перетягнути його в складальне

поле і розмістити в потрібному місці. Для дублювання розміщеного пристрою потрібно вибрати потрібний пристрій і виконати команду **Edit→ Duplicate**. Команда **Edit→ Replicate** дозволяє розмістити в складальному полі потрібну кількість пристроїв. Для цього в діалоговому вікні потрібно вказати кількість пристроїв і натиснути кнопку Replicate. Перемикач Organize дозволяє вибрати найбільш зручний варіант розміщення пристроїв у складальному полі. Для видалення пристрою з набірного поля необхідно вибрати пристрій і виконати команду Delete з меню Edit або з контекстного меню.

Для відображення реальної структури мережі організації бажано використовувати такі класи компонент, як City (Місто), Building (Будівля), Campus (Університет), Floor (Поверх) і Room (Кімната). Кожен з цих об'єктів має своє складальне поле, розкрити яке можна за допомогою команди Expand з меню Object або з контекстного меню. У новому вікні, що відкривається при виконанні даної команди, можна побудувати ту частину мережі, яка відповідає даному об'єкту.

При виборі різних пристроїв, що використовуються для побудови мережі, перш за все слід враховувати такі параметри:

- необхідна кількість портів;
- необхідний тип портів;
- пропускну здатність;
- підтримувані транспортні протоколи ;
- підтримувані протоколи маршрутизації ;
- кількість слотів.

Багато пристроїв вимагають установки певних компонентів для виконання ними необхідних функцій. Так, наприклад, багато робочих станцій поставляються без мережевих карт. У такому випадку, їх потрібно встановити.

Для цього треба знайти потрібний пристрій, і перетягнути його на потрібний об'єкт. Слід враховувати кількість слотів і їх тип при встановленні додаткового обладнання. Наприклад, якщо пристрій не містить портів MCA, то встановити в нього мережеву карту, розраховану на шину MCA, буде

неможливо. Також, якщо у пристрої немає вільних слотів, встановити в нього що-небудь буде скрутно. Для перегляду і редагування параметрів пристроїв використовуються команди **Properties**, **Open**, **Configuration**, **Configure Ports** з меню **Object** або команди **Configuration** і **Properties** з контекстного меню.

Для створення зв'язків між пристроями (а точніше між їх інтерфейсами або портами) необхідно скористатися кнопкою **Link Devices** на панелі режимів покажчика миші (включається командою **View**→**Bars**→**Modes**). Після вибору даної кнопки необхідно вказати один із з'єднуювальних пристроїв і, не відпускаючи кнопку миші, розтягнути зв'язок до другого пристрою. Після цього з'являється діалогове вікно **Link Assistant**, в якому проводиться подальше конфігурування параметрів з'єднання. Спочатку надається можливість визначити сполучаються порти пристроїв і пов'язати їх, виконавши клацання по кнопці **Link**. Після цього стає доступною секція **Link Settings**, в якій настраюються параметри даного з'єднання, наприклад, використовуваний протокол (Ethernet 10Base-T), тип середовища передачі (Twisted Pair - кручена пари), пропускна здатність середовища (10 Мб / с), довжина з'єднання (до 100 м). У більшості випадків ці параметри фіксовані і змінюватися не можуть, хоча іноді є можливість вибору з декількох значень. Наприклад, при з'єднанні двох оптоволоконних модемів пропускна здатність може бути обрана зі списку значень: T3, E3, DSn, Ocn, STSn, STMn (для аналогового модему: 2400, 9600, 14400, 28800 і т. д.). Тип з'єднання в даному випадку єдиний – frame relay (ретрансляція кадрів). Передає середовище теж фіксована – fiber-optic cable (оптоволокно). При з'єднанні пристроїв, що мають порт ISDN, список типів з'єднань дещо ширше – ISDN BRI, ISDN PRI, point-to-point leased line (виділена лінія), dial-up analog line (аналогова телефонна лінія). Після завдання структури мережі і топології зв'язків визначається склад і розташування використовуваного програмного забезпечення. Для цього необхідно в списку компонентів вибрати категорію **Network and enterprise software**, в ній знайти необхідне програмне забезпечення і помістити його на відповідний об'єкт в мережі.

Надалі визначається трафік між вузлами мережі. Для завдання трафіку необхідно скористатися кнопкою **Set Traffic** на панелі режимів покажчика миші для переходу у відповідний режим. Після цього необхідно послідовно вибирати пари абонентських станцій (АС) мережі, між якими буде заданий трафік. Порядок клацань на АС визначає напрямок передачі – спочатку зазначається джерело, потім приймач. У результаті з'являється діалогове вікно **Profiles**, що дозволяє задати тип і основні характеристики трафіку. Тип трафіку вибирається зі списку **Profiles List**, причому вказується за принципом "запити клієнта до сервера", тобто в якості приймача може виступати тільки та АС, на якій функціонує відповідне програмне забезпечення (HTTP / FTP Server, SQL server, File Server). Деякі типи трафіку складають виключення з даного правила, наприклад, Small office, LAN peer- to- peer traffic, InterLAN traffic та ін Для завдання характеристик трафіку між зазначеними АС необхідно натиснути кнопку **Advanced**. У діалоговому вікні **Traffic from** (АС-джерело) to (АС-приймач) задаються закон розподілу і діапазон значень для розміру запиту (Transaction Size) та інтервалу між запитами (Time Between Transactions), а також тип протоколу прикладного рівня (Application Layer Protocol). При необхідності додати новий тип трафіку, видалити або змінити параметри існуючих типів слід скористатися кнопками Add, Remove, Edit і Rename діалогового вікна Profiles. Колір, яким при моделюванні будуть відображатися пакети, що належать даному типу трафіку, відображається у стовпці Color. Характеристики типів трафіку, використовувані за замовчуванням, можна змінити також і за допомогою команди **Global→ Profiles**. Також є можливість використовувати команду **Global→ Data Flow** для конфігурування потоків даних у мережі.

Для вказівки аналізованих характеристик слід скористатися командою **Statistics** з контекстного меню або **Define Statistics** з меню **Object**. У діалоговому вікні **Statistical Items** можна задати тип характеристики та спосіб відображення статистичної інформації в процесі моделювання. Це діалогове вікно буде різним для різних типів об'єктів, тобто може змінюватися перелік

характеристик, а також деякі способи відображення інформації можуть бути недоступні. Для одного об'єкта (вибраного пристрою, з'єднання або потоку даних) можна вибирати кілька способів відображення інформації (індикатор, число, графік).

Після цього вже можна виробляти імітаційне моделювання роботи мережі. Для управління процесом моделювання використовуються команди пункту меню **Control**. Команда **Start** використовується для запуску, **Pause** для призупинення і **Stop** для повної зупинки процесу моделювання. Команди **Simulation Faster** і **Simulation Slower** призначені для зміни швидкості моделювання, тоді як команди **Animation Faster**, **Animation Slower**, **Animation Default** призначені для зміни швидкості візуалізації процесу. Команда **Animation Setup** дозволяє в діалоговому режимі вибрати найбільш підходящі параметри для інтенсивності, швидкості та розміру пакетів і дзвінків. Деякі з перерахованих команд можна виконати за допомогою кнопок, розташованих на панелях інструментів **Zoom** і **Control**.

Для перегляду узагальнених результатів моделювання використовується команда **Associated Data Flow** з меню **Object** або з контекстного меню. В результаті виконання даної команди у вікні відображається статистика по процентному співвідношенню кількості пакетів для вхідних (**Incoming Traffic**) і вихідних з'єднань (**Outgoing Traffic**).

За допомогою команд, що містяться в пункті меню **Tools**→ **Reports**, можна створити звіти, узагальнюючі результати виконаної роботи.

Типи мереж Ethernet

1. *FastEthernet* - це мережа Ethernet, призначена для передачі даних зі швидкістю 100 Мбіт / с. Мережа може бути побудована на основі витої пари або оптоволоконного кабелю. Більшість підключених до мережі пристроїв, наприклад ноутбуки або мережеві камери, оснащені інтерфейсом Ethernet 100BASE-TX / 10BASE-T, часто званим інтерфейсом 10/100, який підтримує як швидкість передачі даних 10 Мбіт / с, так і Fast Ethernet. Тип витої пари, що

підтримує протокол Fast Ethernet, називається Cat-5.Gigabit Ethernet - призначений для передачі даних зі швидкістю 1 000 Мбіт / с (1 Гбіт / с), можна реалізовувати її на основі кручених пари або оптоволоконного кабелю. Дана технологія стає дуже популярною. Очікується, що Gigabit Ethernet незабаром замінить технологію Fast Ethernet і стане фактично стандартом. Кабель Cat-5e підтримує передачу даних за технологією Gigabit Ethernet, в ньому всі чотири пари кручених проводів використовуються для досягнення великих швидкостей передачі даних. Для мережевих відеосистем рекомендується використовувати кабель категорії Cat-5e і пізніших. Більшість інтерфейсів сумісні з Ethernet 10 і 100 Мбіт / с і часто називаються інтерфейсами 10/100/1000.

2. *10 Gigabit Ethernet* - це технологія останнього покоління, що дозволяє передавати дані на швидкості 10 Гбіт / с (10 000 Мбіт / с), можливе використання оптоволоконного кабелю або виті пари. Для зв'язку на відстані до 10 000 м можна використовувати стандарти 10GBASE-LX4, 10GBASE-ER і 10GBASE-SR на основі оптоволоконного кабелю. При використанні виті пари необхідний кабель дуже високої якості (Cat-6а або Cat-7). Стандарт Ethernet зі швидкістю передачі 10 Гбіт / с в основному використовується для магістральних з'єднань при роботі з високопродуктивними додатками, які вимагають великих швидкостей передачі даних.

Робочі станції в ROOM 31,32 з'єднані топологією "Шина", яка являє собою загальний кабель (т. званий шина або магістраль), до якого приєднані всі робочі станції. На кінцях кабелю знаходяться термінатори, для запобігання відображення сигналу.

Топологія шина передбачає використання одного кабелю, до якого підключаються всі комп'ютери мережі. Повідомлення, що відправляється будь-якою робочою станцією поширюється на всі комп'ютери мережі. Кожна машина перевіряє, кому адресоване повідомлення, - якщо повідомлення адресоване їй, то обробляє його. Приймаються спеціальні заходи для того, щоб при роботі із загальним кабелем комп'ютери не заважали один одному передавати і приймати дані.

Шина самою своєю структурою припускає ідентичність мережного устаткування комп'ютерів, а також рівноправність всіх абонентів. При такому з'єднанні комп'ютери можуть передавати інформацію тільки по черзі, послідовно - тому що лінія зв'язку єдина. В іншому випадку пакети переданої інформації будуть спотворюватися в результаті взаємного накладання.

У топології «шина» відсутній центральний абонент, через якого передається вся інформація, що збільшує надійність «шини». Додавання нових абонентів у «шину» досить просте і зазвичай можливо навіть під час роботи мережі. У більшості випадків при використанні «шини» потрібно мінімальна кількість сполучного кабелю в порівнянні з іншого топологією. Правда, потрібно врахувати, що до кожного комп'ютера (крім двох крайніх) підходять два кабелі, що не завжди зручно.

Мережевий комутатор (switch) - пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. Комутатор працює на каналному (другому) рівні моделі OSI. Комутатори були розроблені з використанням мостових технологій і часто розглядаються як багатопортові мости.

1.2 Порядок виконання роботи

Запустіть з стартового меню програму NetCracker. Натисніть на кнопку ОК у відповідь на можливе повідомлення про те, що база даних знаходиться в режимі читання «2read-only mode». Цей режим звичайно пов'язаний із заборонаю на запис, встановленим системним адміністратором для файлів пакета і не дозволить створювати свої пристрої і зберігати їх в бібліотеках пакета.

Головне вікно програми зображено на (рис. 1.2). Воно складається з браузера устаткування зліва, робочого вікна праворуч і головного меню вгорі.

Ознайомтеся з вмістом головного меню програми, вибираючи основні пункти: File, Edit, View, DataBase і ін.

Відкрийте (рис. 1.3) файл-приклад проекту мережі NetCracker Professional 4.1 з підкаталогу Samples каталогу установки програми: **File** → **Open**.

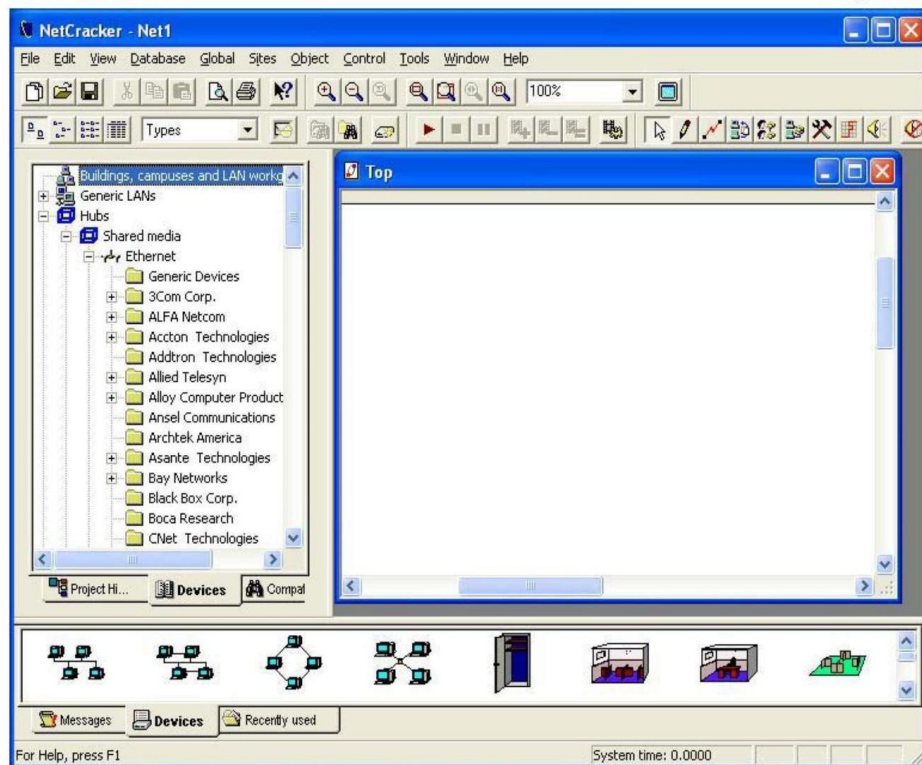


Рис. 1.2. Головне вікно NetCracker

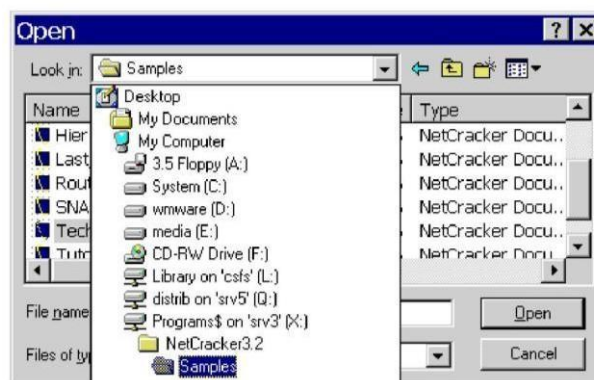


Рис. 1.3. Відкриття файлу-прикладу

Виберіть файл Techno.net, натиснувши кнопку Open або подвійним клацанням лівої кнопки миші. Проект мережі завантажиться в робоче вікно (рис. 1.4).

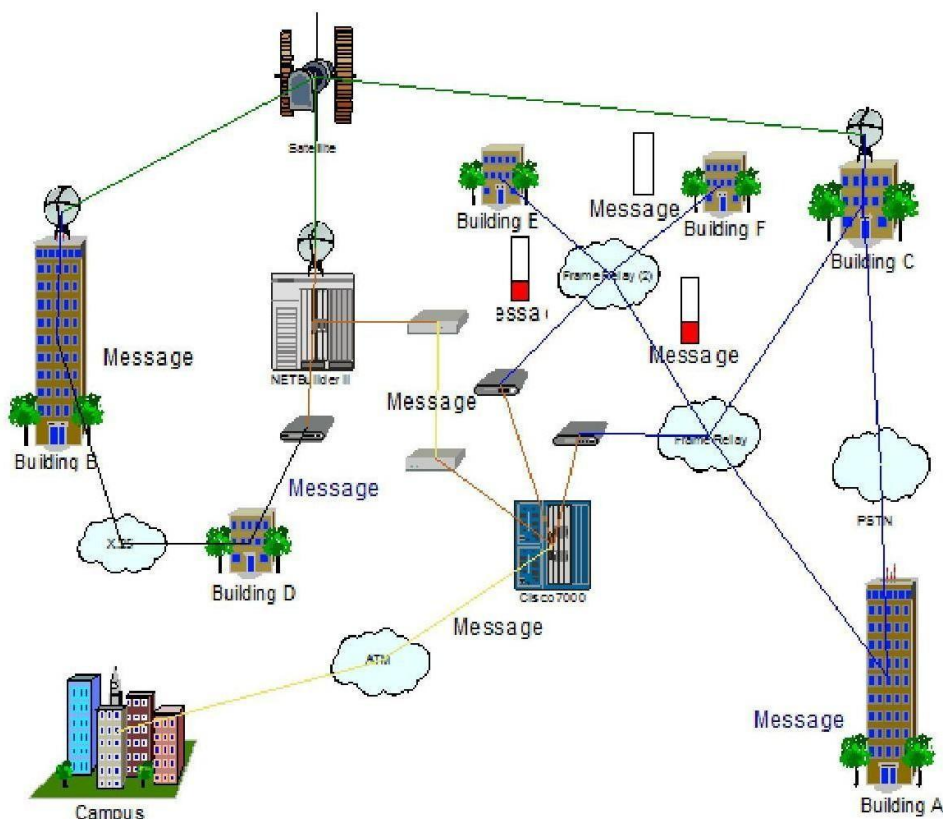


Рис. 1.4. Проект мережі Масштаб перегляду можна регулювати кнопками Zoom.

За допомогою лінійки прокрутки ознайомтеся з вмістом браузера обладнання (закладка Devices). Групи пристроїв, помічені в вузлах знаком «+», розкриваються на складові.



Сортування обладнання, що міститься в БД:

DataBase → **Hierarchy** → **Types** (сортування за типами обладнання)

DataBase → **Hierarchy** → **Vendors** (сортування по фірмам-виробникам)

Наприклад, необхідно в мережевому проекті сервер компанії Cray Research C916. Для цього в розділі Supercomputers виберемо групу з обладнанням компанії Cray Research, а в нижньому вікні Devices - сервер C916. Подвійне клацання лівою кнопкою миші викличе сторінку властивостей сервера і

відобразить повний набір його технічних характеристик.

Використовуючи DataBase toolBar, можна здійснювати перегляд складу групи, пошук і створення нового обладнання:



Рис.1.5. Панель DataBase toolBar

Пошук обладнання проводиться також з розділу меню DataBase, наприклад, так: **DataBase → Find → Condition = Description → includes → Frame Relay**. Результати пошуку будуть відображатися на закладці браузера обладнання «Compatible Devices». Перейти до звичайного режиму браузера можна вибравши закладку «Devices». Часто не потрібно використовувати в проекті обладнання конкретних виробників, тоді можна скористатися

«узагальненими» пристроями з розділу **DataBase → Hierarchy → Vendors → Generic Devices**.

У відкритому файлі-проект мережі можна переглянути і змінити характеристики обладнання, включеного в проект. Наприклад, у Вас відкритий в даний момент файл Techno.net. Двічі клацніть мишкою по маршрутизатора Cisco 7000, в результаті з'явиться вікно конфігурації Cisco 7000 (рис. 1.6).

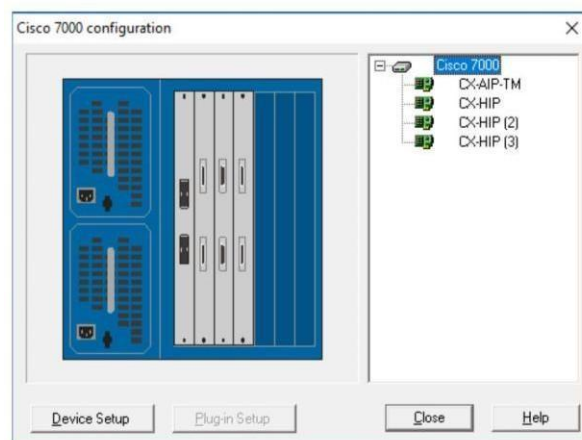


Рис. 1.6. Вікно конфігурації Cisco 7000

При натисканні кнопки Device Setup з'являється вікно з описом властивостей Cisco 7000. Якщо потрібна інформація про пристрої, якими укомплектований маршрутизатор Cisco 7000 з проекту Techno.net, потрібно вибрати назву пристрою і натиснути кнопку PluginSetup. Такого ж ефекту можна досягти, вибравши назву пристрою і натиснувши праву кнопку миші,

потім в контекстному меню вибрати Properties (тут можна також і прослухати назву пристрою по-англійськи Say description). Наприклад, подивимося властивості ATM Interface Processor TAXI multi-mode (рис. 1.7).

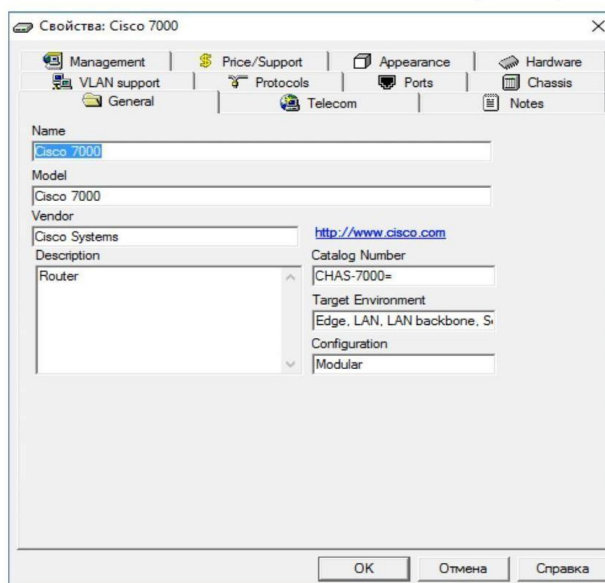


Рис. 1.7. Властивості ATM Interface Processor TAXI multi-mode

Пройдіть по закладках і ознайомтеся з міститься інформацією про вибраному пристрої. Всі пристрої, наявні в базі даних NetCracker, з браузера устаткування (сторінка Devices) можна перетягувати в робоче поле свого проекту, утримуючи ліву кнопку миші.

З'єднання пристроїв

Пристрої з'єднуються за допомогою майстра з'єднань «Link Assistant». Серед NetCracker перевіряє тип інтерфейсів пристроїв і з'єднує лише сумісні. Наприклад, в персональних комп'ютерах (**LanWorkstations** → **PCs** → **GenericDevices** → **PC**) в початковому стані є тільки послідовні COM-порти, тому для з'єднання їх з мережевим обладнанням потрібно встановити мережеву карту.

Створіть новий проект **File** → **New**. Знайдіть комп'ютер в БД обладнання (**LanWorkstations** → **PCs** → **GenericDevices** → **PC**) і перенесіть методом Drag-and-Drop іконку PC в основне вікно проекту TOP. Потім знайдіть мережеву карту в БД обладнання (**LANadapter** → **Ethernet** → **GenericDevices** →

FastEthernet). Перенесіть іконку "FastEthernetAdapter" методом Drag-and-Drop на комп'ютер PC. Для мереж Ethernet можна вибрати і готовий «мережевий комп'ютер» EthernetWorkstation (**LANworkstation** → **Workstations** → **GenericDevices** → **EthernetWorkstation**).

Додайте в основне вікно ще один такий комп'ютер і комутатор FastEthernet (**Switches** → **Workgroup** → **Ethernet** → **GenericDevices** → **EthernetSwich**) і з'єднайте два комп'ютери через комутатор:

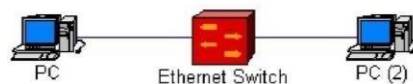


Рис. 1.8. Мережа

Порядок з'єднання такий:

1. Вибрати в панелі інструментів інструмент «Link devices»:



Рис. 1.9. Інструмент «Link devices»

2. Переконайтеся, що модулі (комп'ютери, комутатори, концентратори), які ви плануєте поєднати, мають сумісні мережеві порти, наприклад, **Fast Ethernet**. Це можна зробити вибравши «Properties» в контекстному меню пристрою, а потім закладку «Ports».

В даному випадку пристрої PC не мають даного входу, додаємо **Lan**



adapter ---Ethernet **Ethernet adapter** . Обираємо і перетягуємо на пристрій PC та PC(2).

3. Клацнути лівою кнопкою миші спочатку по джерелу, потім по прийомнику

даного з'єднання.

4. Натиснути в діалозі «Link Assistant» на кнопку «Link», а також задати тип, довжину і інші характеристики середовища (довжина лінії не враховується при симуляції передачі даних в мережі).

5. Закрити діалог, натиснувши на кнопку «Close».

Створення нових пристроїв (Device Factory)

Незважаючи на велику кількість пристроїв в базі даних середовища NetCracker, іноді необхідне устаткування відсутнє. При наявності доступу по запису до файлів баз даних програми NetCracker (звичайний шлях C: \ Program Files \ NetCracker \ DDB \) можна створити нове обладнання. Майстер Device Factory запускається з меню DataBase. Нове обладнання створюється на основі існуючих шаблонів. На рис. 1.10 показаний вибір шаблону для GigaBit Ethernet комутатора.

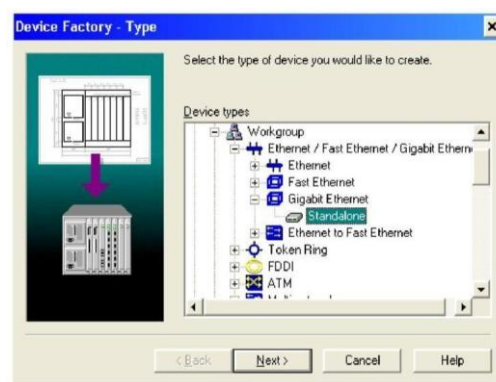


Рис. 1.10. Вибір шаблону для GigaBit Ethernet комутатора

Потім послідовно вибираються додаткові властивості, такі як (наприклад, для комутаторів): назва нового пристрою, групи / кількість портів (на рисунках обрано назву GigaBit Switch, добавлена одна група з 24 портів),

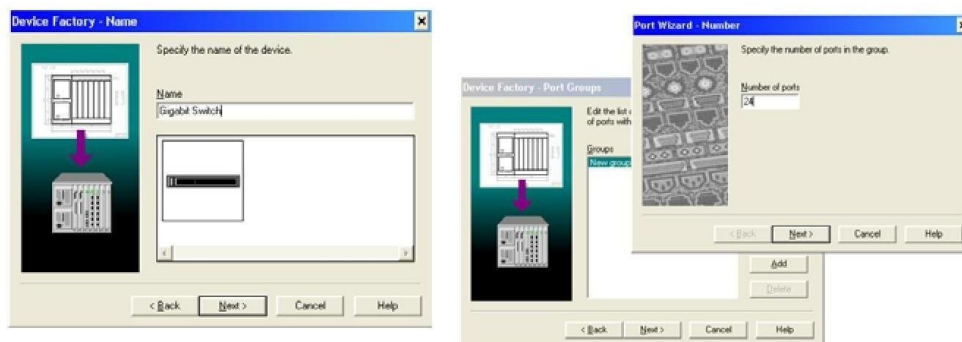


Рис. 1.11. Вибір додаткових властивостей
сигнальні стандарти (100Base-TX, 1000Base-T) для них:

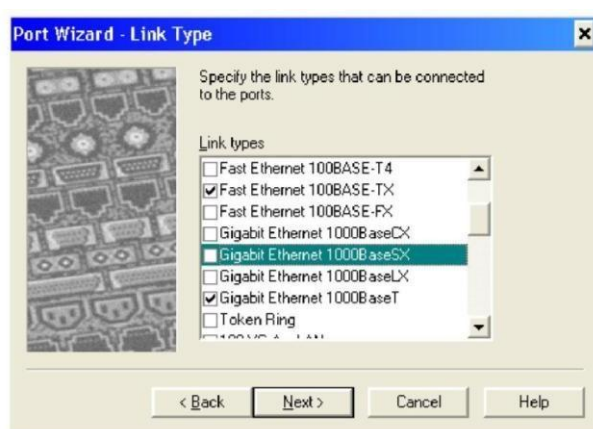


Рис. 1.12. Вибір сигнальних стандартів і тип фізичного середовища:

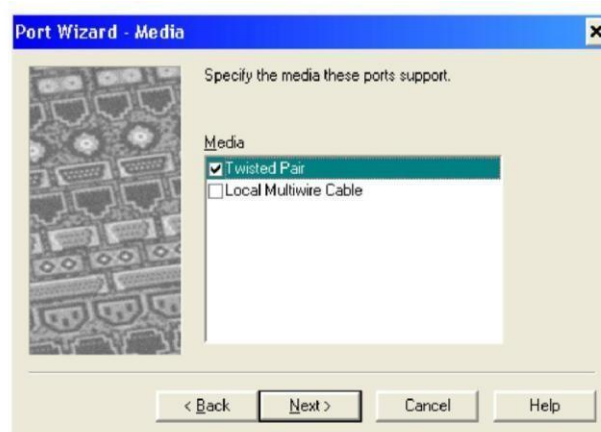


Рис. 1.13. Вибір типу фізичного середовища

В результаті отримано нове призначене для користувача пристрій «GigaBit Switch» з 24 портами, що підтримують стандарти 100Base-TX, 1000Base-T. Новий пристрій буде доступний при виборі в панелі інструментів бази даних «User». Параметри пристрою, за замовчуванням певним шаблоном (в

даному випадку GigaBit Ethernet Standalone), вимагають перевірки. Наприклад, в шаблоні для гігабітного комутатора задано аномально велике значення затримки (Telecom → Latency) - 0.1 с. З такою затримкою будуть 100% -ві втрати даних, що проходять через цей пристрій. Типове значення затримки для даного виду обладнання близько 0.1 мкс, тобто на 6 порядків менше.

Завдання трафіку

Перш за все, при завданні трафіку потрібно враховувати процесорні можливості комп'ютера. Так, при потоках трафіку і включеній анімації для стійкої роботи програми потрібно процесор не нижче Celeron-800. Перевірте конфігурацію свого комп'ютера: **My Computer** → **Properties**. Трохи полегшити задачу для комп'ютера можна скасувавши візуалізацію переданих даних:

Global → **Data Flow** → **Uncheck All** → **Close**. При цьому зберігається можливість спостерігати результати моделювання, одержувані через індикатори статистики.

Трафік в моделюється мережі задається за допомогою майстра, що викликається кнопкою панелі інструментів «Set traffic». Порядок завдання трафіку такий:

1. Вибрати в панелі інструментів інструмент «Set traffic»:



Рис. 1.14. Інструмент «Set traffic»

2. Клацнути лівою кнопкою миші спочатку по модулю-джерела трафіку, потім по модулю-приймача трафіку.
3. Наведіть курсор миші на один із стандартних профілів трафіків, наприклад, «InterLAN traffic». Потім правою кнопкою миші і в контекстному меню виберіть даний профіль трафіку (пункт Select). При виборі профілю можна змінювати характеристики профілю (кнопка Edit), задаючи статистику

розмірів дейтаграм «Transaction size», статистику моментів приходу дейтаграм, пауза «Time Between transactions», а також протокол рівня додатка «Application Layer Protocol». Натиснувши на кнопку Add, можна створити свій профіль трафіку з певними Вами характеристиками. Трафік отримає ім'я Traffic (номер), яке можна змінити вибравши в контекстному меню дорожнього руху пункт Rename (спробуйте це зробити).

4. Можна переглянути потоки даних в мережі **Global** → **Data Flow**. Тут же можна відредагувати (в тому числі і видалити) властивості потоків і профілів трафіків. Враховуйте максимальні пропускні спроможності каналів передачі даних і не перевантажуйте їх надмірно. Помічено, що при перевантаженні на порядок індикатори статистики середовища NetCracker дають невірні (довільні) дані.

При призначенні клієнт-серверного трафіку можна змінювати характеристики відповідей сервера, задаючи статистику розмірів дейтаграм

«Transaction size», статистику моментів приходу дейтаграм / пауз «Time Between transactions», а також протокол рівня додатка «Application Layer Protocol».

Звіти

В процесі розробки варіанту проекту мережі можна отримати в NetCracker звіти про склад проекту, наприклад:

Tools → Reports → Bill of Material

Можна отримати звіт про номенклатуру обладнання, що входить в проект мережі, ціни кожної одиниці обладнання, загальною ціни проекту:

Tools → Reports → Device Summary

або специфікацію усіх одиниць обладнання. Подібні специфікації можна згенерувати і по окремих класах обладнання (наприклад, Workstations, Servers, Hubs, і т. д.). Отримані таким чином звіти можна роздрукувати або зберегти в файл, скориставшись панеллю меню по роботі зі звітами (рис. 1.15).



Рис. 1.15. Панель меню по роботі із звітами

При виборі опції «Зберегти» з'являється вікно Export (Рис. 1.16), в якому можна визначити формат звіту і місце його зберігання (файл на диску або відправка поштою).

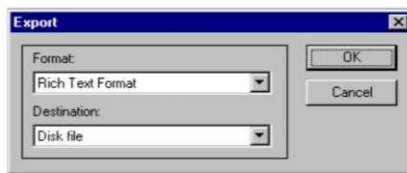


Рис. 1.16. Вікно Export

Закрийте проект Techno.net, вибравши **File** → **Close**. У діалоговому вікні з питанням want to save the file? Дайте відповідь NO.

1.3 Оброблення та аналізування результатів. Оформлення звіту.

При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

1.4 Контрольні питання

- 1) Які завдання проектування і дослідження мереж можуть бути вирішені з використанням пакета NetCracker?
- 2) Які основні можливості пакету NetCracker Pro?
- 3) З яких елементів складається інтерфейс NetCracker Pro?
- 4) Для яких цілей служить браузер пристроїв? Робоча зона? Панель зображень?
- 5) Які засоби NetCracker дозволяють кількісно оцінювати рівень завантаженості конкретного каналу зв'язку?
- 6) Як створити новий пристрій ?
- 7) Що таке трафік, як його змінити?
- 8) Як створити звіт про склад проекту?

ПРАКТИЧНА РОБОТА № 2

МОДЕЛЮВАННЯ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖІ

Мета та основні завдання роботи: ознайомитись з можливостями NetCracker щодо аналізу трафіків в мережі за допомогою моделювання процесів передачі даних.

Вивчити та стисло описати у протоколі практичної роботи:

- систему імітаційного моделювання Netcracker;
- роботу анімації NetCracker.

2.1 Теоретичні відомості

Система моделювання Netcracker є на сьогоднішній день однією з найпопулярніших систем моделювання обчислювальних мереж. База даних містить тисячі пристроїв різних виробників. У Netcracker є можливість задавати параметри пристроїв, наприклад тип процесора, довжину піній зв'язку, а також створювати багаторівневі мережеві проекти, ставити свої типи трафіку. Можна додавати у базу даних свої пристрої, попередньо вибираючи конфігурацію. У Netcracker забезпечується діалог контролю з'єднань двох точок обчислювальної мережі із зазначенням наявних протоколів мережевих пристроїв.

Система імітаційного моделювання мереж Netcracker Professional 4.1 дозволяє точно прогнозувати продуктивність локальних, глобальних і корпоративних мереж. Netcracker пропонує використовувати простий і інтуїтивно зрозумілий спосіб конструювання моделі мережі, заснований на застосуванні готових базових блоків, відповідних добре знайомим мережевим пристроїв, таким як комп'ютери, маршрутизатори, комутатори, мультиплексори і канали зв'язку.

Користувач застосовує техніку drag-and-drop для графічного зображення модельованої мережі з бібліотечних елементів. Потім система Netcracker виконує детальне моделювання отриманої мережі, відображаючи результати

динамічно у вигляді наочної мультиплікації результуючого трафіку. Іншим варіантом завдання топології модельованої мережі є імпорт топологічної інформації з систем управління і моніторингу мереж. Після закінчення моделювання користувач отримує в своє розпорядження наступні характеристики продуктивності мережі:

- Прогнозовані затримки між кінцевими і проміжними вузлами мережі, пропускні спроможності каналів, коефіцієнти використання сегментів, буферів і процесорів.
- Піки і спади трафіку як функцію часу, а не як усереднені значення.
- Джерела затримок і вузьких місць мережі.

NetCracker здатний до обчислення і відображення різноманітної статистичної інформації, пов'язаної з мережевою активністю. Будь-який пристрій, з'єднання або потік даних можуть мати статистику. Статистична інформація може бути відображена в формі чисел, графіка, або гістограми.

Щоб відобразити статистику для будь-якого об'єкта, виділіть об'єкт і клацніть на ньому правою кнопкою миші, виберіть команду Статистика (*Statistics*) з локального меню або відкрийте об'єктне меню і виберіть команду *Define Statistics*. Відкриється діалог. Виберіть інформацію, яку хочете відображати і закрийте діалог. Графіки і текстові вікна можуть бути змінені для зручного перегляду.

Щоб змінити розмір або колір тексту, клацніть правою кнопкою на текстовому блоці, виберіть команду *Properties*, і використовуйте діалог щоб форматувати ваш індикатор.

У NetCracker Ви можете досліджувати, як потік даних спрямований в комплексній трафік мережі. Ви можете також змушувати трафік / виклик бути спрямованими за неправильною адресою, ламаючи або відновлюючи компонент або, змінюючи алгоритми прокладки траєкторії моделі.

Щоб Ламати і Відновлювати компоненти виберіть компонент, і використовуйте один з наступних методів:

- У локальному меню, виберіть команду *Break* або *Restore*.

- В меню *Object*, виберіть команду *Break* або *Restore*.

Ви можете також використовувати інструмент з панелі **Sites→Modes**.

Щоб змінити алгоритм прокладки траєкторії моделі в меню **Global**, потім в блоці діалогу **Model Settings**, обрати вкладку **Protocols** для зміни алгоритму прокладки траєкторії.

Data Flow dialog (Об'єктний потоковий діалог даних), який ідентифікує початок координат і адресатів всіх потоків даних до або від цього об'єкта. Якщо тип трафіку не було визначено для відібраного об'єкта, то відображається **Message dialog** (Діалог повідомлень).

Ця команда може бути застосована тільки тоді, коли відібраний об'єкт - генератор трафіку.

Анімація NetCracker заснована на дії мережі.

Відкрийте блок діалогу *Animation Setup*, використовуючи один з наступних методів:

- Натисніть кнопку *Animation Setup* на панелі *Animation*.
- Виберіть *Animation Setup* з меню *Control*.

Зробити анімацію швидше або повільніше можна використовуючи один з наступних методів:

- На панелі *Animation* натисніть *Faster* або *Slower*.
- Корегуйте швидкості : Діалог Установки Анімація і / або Запит або

Діалог Установки Анімація

Щоб змінити число пакетів / викликаючи в секунду (інтенсивність)
Корегуйте інтенсивності в вікні діалогу *Animation Setup*.

2.2 Порядок виконання роботи

1. Запустіть з стартового меню програму NetCracker. Відкрийте файл - приклад проекту Router.net.

Перевірте значення затримки перехідного періоду (**Global→Model Settings → Simulation → Warm-Up period**), значення затримки має бути нульовим.

2. Натисніть на кнопку «старт» 

на панелі управління



Далі відобразиться схема (рис. 2.1).

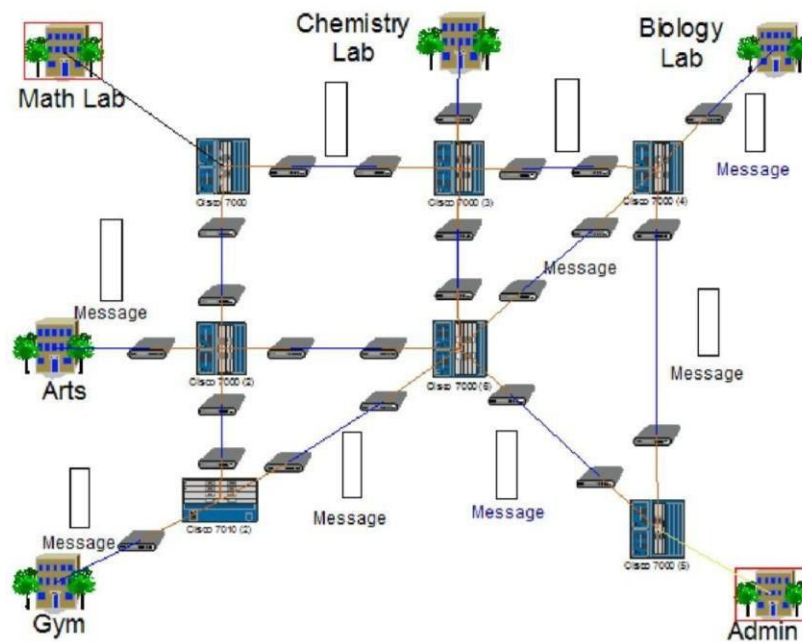


Рис. 2.1. Проект Router.net

1. Задайте статистичні індикатори Average Workload (середнє навантаження), Average Utilization (середнє завантаження / використання). Для цього виділіть канал MathLaB – Cisco7000, клацнувши лівою кнопкою миші по лінії каналу, і в контекстному меню (клацання правою кнопкою миші) виберіть Statistics. Позначте відповідні індикатори. У властивостях індикаторів можна встановити одиницю вимірювання і розмір шрифту. Запам'ятайте значення цих двох індикаторів.

2. Зупиніть симулятор і змініть середнє паузи між пакетами (Time Between Transactions) для трафіку **Global** → **DataFlow** → **Steve** → **Chris** → **Edit** → **InterLAN traffic** → **Edit** зі значення 0.008 сек на значення 0.08 сек. Запустіть знову симулятор і подивіться свідчення встановлених індикаторів.

Параметрами анімації можна керувати за допомогою меню **Control** → **Animation Setup**

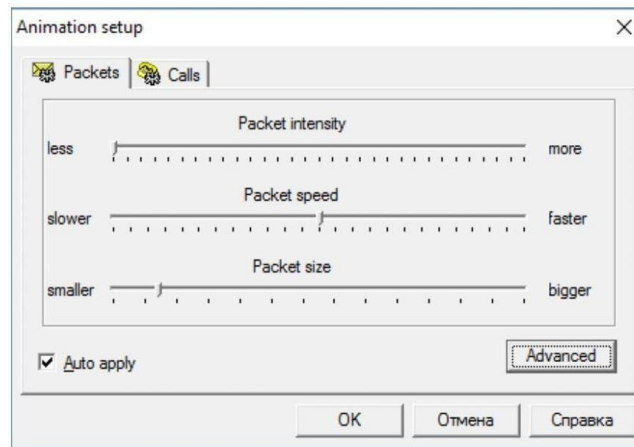


Рис. 2.2. Налаштування анімації

3. Змініть параметри і натисніть на кнопку ОК. Зверніть увагу на зміни в роботі мережі проекту. Розгляньте роботу мережі більш детально. Для цього клацніть лівою кнопкою миші на відкритому проекті, на будівлі, зазначеному як **Math Lab**. Переміщатися по ієрархії мережі можна і на закладці браузера обладнання «Project Hierarchy».

NetCracker дозволяє планувати виділення IP-адрес. Планувальник запускається: **Tools** → **IP Planner** ... Виділення адрес можливо тільки для окремих фізичних сегментів, що формуються парою Hub і порт Switch. У проекті Router.net розподіл може виглядати, наприклад, так.

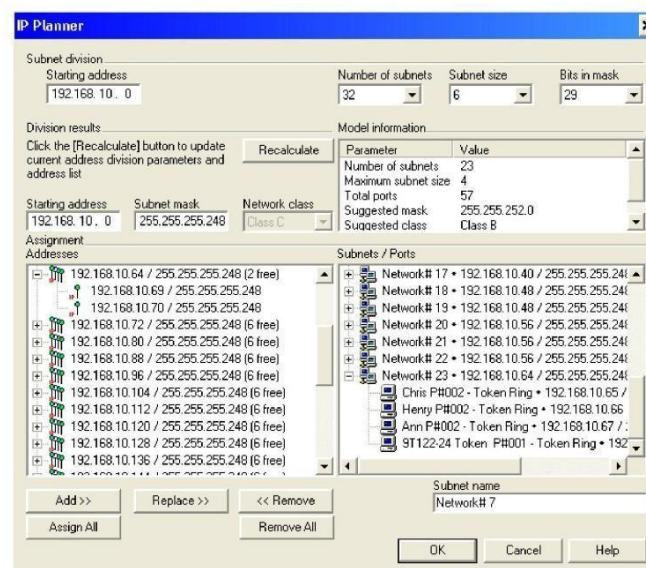


Рис. 2.3. Планувальник IP-адрес

2.3 Оброблення та аналізування результатів. Оформлення звіту.

При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

2.4 Контрольні питання

- 1) Як досліджується потік даних, що спрямований в комплексній трафік мережі?
- 2) Як змінити алгоритм прокладки траєкторії моделі?
- 3) Як корегується швидкість анімації?
- 4) Як перевірити значення затримки перехідного періоду?
- 5) Яким чином здійснюється планування виділення IP-адрес у NetCracker?

ПРАКТИЧНА РОБОТА № 3

СТВОРЕННЯ МОДЕЛІ У NETCRACKER

Мета та основні завдання роботи: отримання практичних навичок роботи з NetCracker, самостійне створення моделі мережі, завдання трафіків і отримання результатів моделювання. Знайомство з поширеними (шаблонними) конфігураціями мереж.

Вивчити та стисло описати у протоколі практичної роботи:

- типові топології NetCracker;
- структуризація локальної мережі;
- мережне комунікаційне обладнання.
-

3.1 Теоретичні відомості

В невеликих мережах (10-30 комп'ютерів) найчастіше використовується певна типова топологія:

- Загальна шина (Ethernet). Зірка (Ethernet).
- Кільце (TokenRing, FDDI).

Всі ці топології мають властивості однорідності – тобто всі комп'ютери у мережі мають однакові права на доступ до інших комп'ютерів. Однорідність структури спрощує нарощення числа комп'ютерів, полегшує обслуговування та експлуатацію мережі.

При розбудові великих мереж виникають певні проблеми:

- Обмеження на довжину ліній між вузлами. Обмеження на кількість вузлів.
- Обмеження на інтенсивність трафіку.

Для вирішення цих проблем використовують спеціальні методи структуризації мереж та спеціальне обладнання:

- Повторювачі (repeater).
- Концентратори (concentrator, hub).
- Мости (bridge).

- Комутатори (switch).
- Маршрутизатори (router).
- Шлюзи (gateway).

Таке обладнання називається комунікаційним, бо воно призначено для об'єднання окремих сегментів мережі до єдиного цілого.

Структуризація локальної мережі

Тут слід розрізняти:

- Топологію фізичних зв'язків, тобто фізичну структуру мережі.
- Топологію логічних зв'язків, тобто логічну структуру мережі.

Конфігурація фізичних зв'язків визначається електричними з'єднаннями комп'ютерів, і може бути представлена у вигляді графу, де вузлами є комп'ютери та комунікаційне обладнання, а ребрами є відрізки кабелю, що з'єднують ці вузли (рис. 3.1).

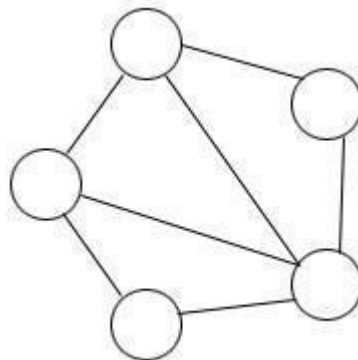


Рис. 3.1. Конфігурація фізичних зв'язків

Логічні зв'язки – це шляхи просування інформаційних потоків по мережі. Вони утворюються за рахунок відповідного налаштування комунікаційного обладнання.

В певних випадках фізична і логічна топології мережі можуть збігатися (рис. 3.2), а в деяких випадках – не збігатися (рис. 3.3).

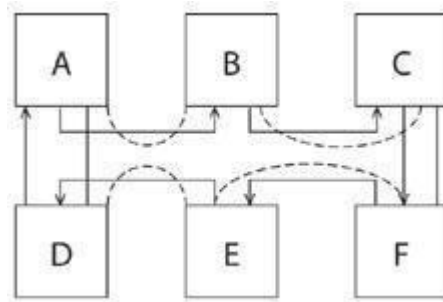


Рис. 3.2. Фізичне «кільце» та логічне «кільце»

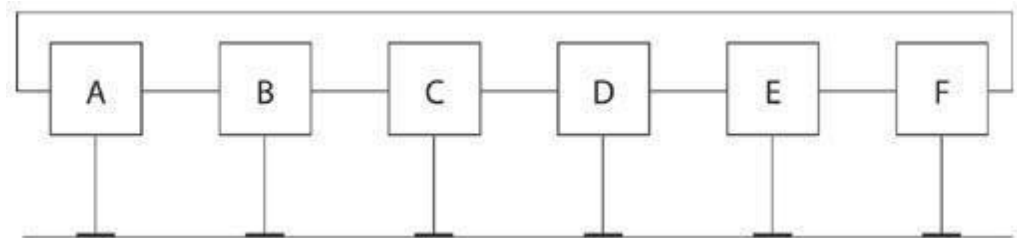


Рис. 3.3. Фізична «загальна шина» та логічне «кільце»

Фізична структуризація локальної мережі

Основними засобами фізичної структуризації локальної мережі є **повторювачі** (repeater) та **концентратори** (concentrator) чи **хаби** (hub).

Повторювач є найпростішим комунікаційним пристроєм, що використовується для фізичного з'єднання різних сегментів кабелю локальної мережі, з метою збільшення загальної довжини мережі. В повторювачі є лише два порти, і сигнал з одного порту перескеровується на інший.

Концентратором називається повторювач, який спроможний з'єднати кілька сегментів. Пристрій має більшу кількість портів, а сигнали, що надійшли на один порт скеровуються на всі інші порти. Концентратори є необхідними пристроями практично у всіх базових мережних технологіях.

Логічна структуризація мережі у роздільному середовищі

Фізична структуризація мережі не дозволяє вирішувати певні проблеми, такі як:

- Дефіцит пропускної здатності.
- Неможливість використання в різних частинах мережі ліній зв'язку з

різною пропускнуою здатністю.

- Типові фізичні топології («загальна шина», «кільце», «зірка») для обміну даними мають лише одне роздільне середовище, що об'єднує всі мережні пристрої. Наприклад, в мережі «загальна шина» взаємодія двох комп'ютерів займає шину на весь час обміну, тому при збільшенні кількості комп'ютерів зменшується продуктивність та швидкодія мережі.
- Часто типові топології виявляються неадекватними до структури інформаційних потоків великої мережі.

Логічна структуризація мережі – це процес розділення загального роздільного середовища (мережа) на логічні сегменти, які представляють самостійні роздільні середовища (сегменти мережі) з меншою кількістю вузлів.

За правильної логічної структуризації мережі її продуктивність суттєво підвищується, оскільки комп'ютери одного відділу не очікують в той час, як комп'ютери іншого відділу передають дані. Також, логічна структуризація допускає наявність різної пропускнуої здатності в різних сегментах мережі.

Поширення трафіку, що призначений для комп'ютерів певного сегменту мережі лише у межах цього сегменту називається **локалізацією трафіку**.

Для логічної структуризації використовують:

- Мости.
- Комутатори.
- Маршрутизатори.
- Шлюзи.

Мережне комунікаційне обладнання Повторювач (repeater)

Основною функцією повторювача є повторення сигналів, що надходять до його порту. Повторювач відновлює і підсилює електричні характеристики сигналів та їх синхронність, і за рахунок цього з'являється можливість збільшувати загальну довжину кабелю між віддаленими вузлами в мережі (рис. 3.4).

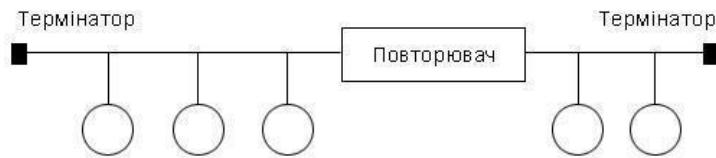


Рис. 3.4. Об'єднання фізичних сегментів за допомогою повторювача

Концентратор (concentrator), хаб (hub)

Концентратором або хабом називають багатопортовий повторювач. Він виконує не лише функцію повторення сигналів, але і виконує функції об'єднання комп'ютерів мережі. Практично у всіх сучасних мережних стандартах концентратор є необхідним елементом мережі, що сполучає окремі комп'ютери у мережу.

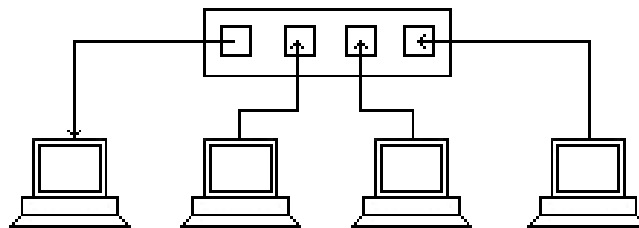


Рис. 3.5. Мультиплексування потоків у концентраторі

Функції, що виконує концентратор наближені до функцій мультиплексора (рис. 3.5). Ядром концентратора є процесор.

В концентраторі сумарна пропускна здатність вхідних каналів є вищою за пропускну здатність вихідного каналу. Оскільки потоки вхідних даних в концентраторі є більшими за вихідний потік, то головним його завданням є концентрація даних. У разі, коли число блоків даних, що поступають на входи концентратора, перевищують його можливості, тоді концентратор ліквідовує частину цих блоків.

Яку б складну структуру не утворювали концентратори, всі комп'ютери, що під'єднані до них утворюють єдиний логічний сегмент, в якому люба пара взаємодіючих комп'ютерів повністю блокує можливість обміну даними для

інших комп'ютерів цього сегменту.

Виробники концентраторів реалізують в своїх пристроях різні набори додаткових функцій, але найчастіше зустрічаються наступні:

- Об'єднання сегментів з різними фізичними середовищами (наприклад коаксіальний кабель, скручена пара, оптоволоконний кабель) до єдиного логічного сегменту.
- Автосегментація портів – автоматичне від'єднання порту при його некоректній поведінці (пошкодження кабелю, інтенсивна генерація пакетів помилкової довжини тощо).
- Підтримка між концентраторами резервних зв'язків, які будуть задіяні у разі відмови основних зв'язків.
- Захист даних, що передаються по мережі від несанкціонованого доступу.
- Сучасні концентратори мають порти для під'єднання до різних локальних мереж.
- Підтримка засобів управління мережами.

Концентратори та повторювачі є мережними пристроями, що діють на фізичному рівні мережної моделі OSI. Відрізки кабелю, що об'єднують два комп'ютери або два інших мережних пристрої, називаються фізичними сегментами, тому концентратори і повторювачі, які використовуються для долучення нових фізичних сегментів є засобами фізичної структуризації мережі.

Міст (bridge)

Перші пристрої, що дозволяли об'єднувати кілька мереж, були двохпортовими і отримали назву **мостів**. З розвитком даного типу обладнання, вони стали багатопортовими і отримали назву **комутаторів**. Певний час обидва поняття існували одночасно, а пізніше замість терміну «міст» стали застосовувати «комутатор».

Міст, а також його швидший аналог – комутатор, поділяє загальне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання кількох фізичних сегментів (відрізків кабелю) за допомогою одного чи кількох концентраторів (рис. 3.6).

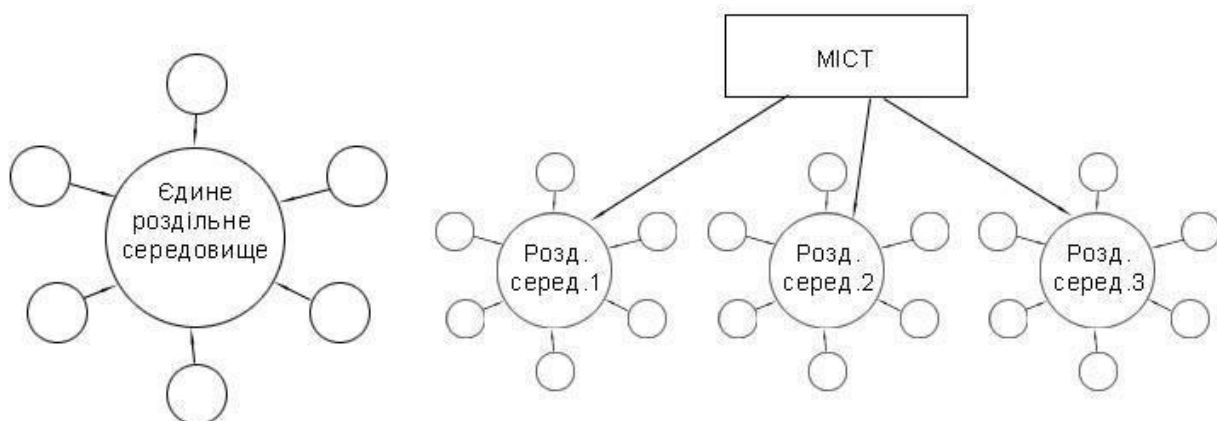


Рис. 3.6. Об'єднання логічних сегментів мережі за допомогою мосту

Кожен логічний сегмент підключається до окремого порту моста. Після надходження кадру на певний порт, міст повторює цей кадр, але не на всіх портах, як це робить концентратор, а лише на тому порту, до якого під'єднано сегмент, що містить комп'ютер-одержувач.

Тим самим міст ізолює трафік одного сегменту від трафіку іншого, і підвищує загальну продуктивність мережі. Локалізація трафіку не лише економить пропускну здатність, але і зменшує можливість несанкціонованого доступу до даних, оскільки кадри не виходять за межі свого сегменту і їх складніше перехопити зловмисникові.

Для локалізації трафіку мости використовують апаратні адреси комп'ютерів.

Будь-який пакет обробляється наступним чином:

1. Міст витягує зі службової інформації пакету MAC-адресу відправника і шукає його в таблиці адрес абонентів, які відносяться до даного порту. Якщо такої адреси в таблиці немає, то вона туди додається. Таким чином, автоматично формується таблиця адрес всіх абонентів кожного сегменту, що під'єднані до портів моста.

2. Міст витягує зі службової інформації пакету MAC-адресу одержувача і шукає його в таблицях адрес, що відносяться до всіх портів.

- Якщо пакет адресовано в сегмент, з якого він надійшов, то він не ретранслюється на інші порти.
- Якщо пакет є широкомовним або груповим, то він ретранслюється у всі порти окрім того, з якого надійшов пакет.
- Якщо пакет адресовано для одного абонента, то він ретранслюється лише в той порт, до якого приєднано сегмент з цим абонентом.
- Якщо адресу приймача не виявлено в жодній з таблиць адрес, то пакет надсилається до всіх портів, окрім того, з якого він надійшов (як широкомовний).

Таблиці адрес абонентів мають обмежений розмір, тому вони формуються так, щоб мати можливість автоматичного оновлення свого вмісту. Адреси абонентів, які довго не надсилають пакетів, за певний час (за стандартом IEEE 802.1D - 5 хвилин) витираються з таблиці. Це гарантує, що адреса абонента, якого від'єднано від мережі або перенесено до іншого сегменту, не займатиме зайвого місця в таблиці.

Одночасно міст може ретранслювати тільки один пакет. Всі функції моста виконуються послідовно одним центральним процесором. Саме тому, міст працює повільніше, ніж комутатор.

Мости не мають механізмів управління потоками блоків даних. Тому, може статися, що вхідний потік блоків виявляється більшим, ніж вихідний. У цьому випадку міст може не впоратися з обробкою вхідного потоку, і його буфери будуть переповнюватися. Щоб цього не відбулося, надмірні блоки викидаються.

Мости можуть підтримувати обмін між сегментами з різною швидкістю передачі, а також забезпечувати сполучення напівдуплексних і дуплексних сегментів.

Оскільки, точна топологія зв'язків між логічними сегментами мосту є невідомою, він може правильно працювати лише в тих мережах, в яких

міжсегментні зв'язки не утворюють замкнутих контурів (петель).

Отже, мости мають абсолютно певне призначення. По-перше, вони призначені для з'єднання мережних сегментів, що мають різні фізичні середовища, наприклад для з'єднання сегменту з оптоволоконним кабелем і сегменту з коаксіальним кабелем. По-друге, мости можуть бути використані для зв'язку сегментів, що мають різні протоколи нижніх рівнів (фізичного і канального).

Комутатор (switch)

Комутатор за функціональністю є подібним до моста і відрізняється від моста в основному вищою продуктивністю. Часто термін «комутатор» використовується у вузькому сенсі, позначаючи конкретний тип пристрою (рис. 3.7).

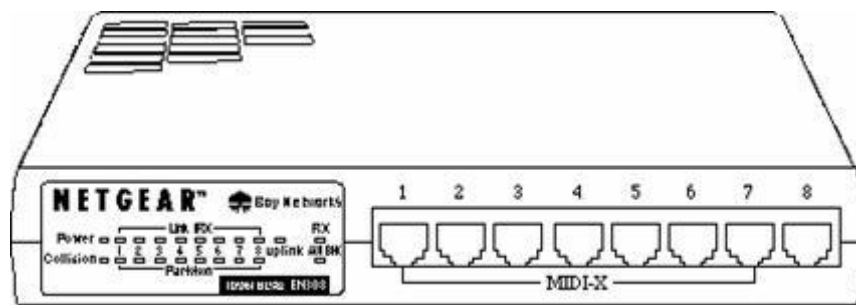


Рис. 3.7. Комутатор

Кожен порт комутатора оснащено спеціальним процесором, який обробляє кадри за алгоритмом моста незалежно від процесорів інших портів. Міст в кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між всіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно.

Мости з'явилися в ті часи, коли мережу ділили на невелику кількість сегментів, а міжсегментний трафік був невеликим. Мережу найчастіше ділили на два сегменти, тому і термін був вибраний відповідний - міст. Для обробки потоку даних з середньою інтенсивністю 1 Мбит/с мосту цілком вистачало продуктивності одного процесорного блоку.

При зміні ситуації в кінці 80-х - початку 90-х років - появи швидких протоколів, продуктивних персональних комп'ютерів, мультимедійної інформації, розділенні мережі на велику кількість сегментів - класичні мости перестали справлятися з роботою. Обслуговування потоків кадрів між кількома портами за допомогою одного процесорного блоку вимагало значного підвищення швидкодії процесора і було досить дорогим рішенням.

Ефективнішим виявилось рішення, яке і «породило» комутатори: для обслуговування потоку, що надходить на кожен порт, в пристрій ставився окремий спеціалізований процесор, який реалізовував алгоритм моста. По суті, комутатор - це мультипроцесорний міст, що здатний паралельно просувати кадри відразу між всіма парами своїх портів.

Коли стало економічно виправдано використовувати окремі спеціалізовані процесори на кожному порту комунікаційного пристрою, комутатори локальних мереж цілком витіснили мости.

За рахунок цього загальна продуктивність комутатора, зазвичай, є вищою за продуктивність традиційного моста, що має один процесорний блок.

В комунікаційній мережі комутатор є системою ретрансляції - системою, що призначена для передачі даних або перетворення протоколів. Комутація здійснюється тут без жодної обробки даних. Комутатор не має буферів і не може накопичувати дані. Тому, при використанні комутатора швидкості передачі сигналів в каналах мають збігатися. Канальні процеси, що реалізуються комутатором, виконують спеціальні інтегральні схеми.

Спочатку, комутатори використовувалися лише в територіальних мережах. Потім вони з'явилися і в локальних мережах, наприклад, комутатори приватних установ. Пізніше з'явилися комутовані локальні мережі. Їх ядром стали комутатори локальних мереж.

Комутатор може об'єднувати сервери і бути основою для об'єднання кількох робочих груп. Він скеровує пакети даних між вузлами локальної мережі. Кожен комп'ютер сегменту отримує доступ до каналу передачі даних без конкуренції і бачить лише той трафік, який курсує в його сегменті.

Функції комутатора локальної мережі:

- Забезпечення наскрізної комутації. Наявність засобів маршрутизації.
- Підтримка простого протоколу управління мережею.
- Імітація моста або маршрутизатора. Організація віртуальних мереж.
- Швидкісна ретрансляція блоків даних.

Відповідно до базової еталонної моделі OSI мости та комутатори описуються протоколами фізичного і канального рівнів. Мости та комутатори перетворюють фізичний (1A, 1B) і канальний (2A, 2B) рівні різних типів (рис. 3.8).

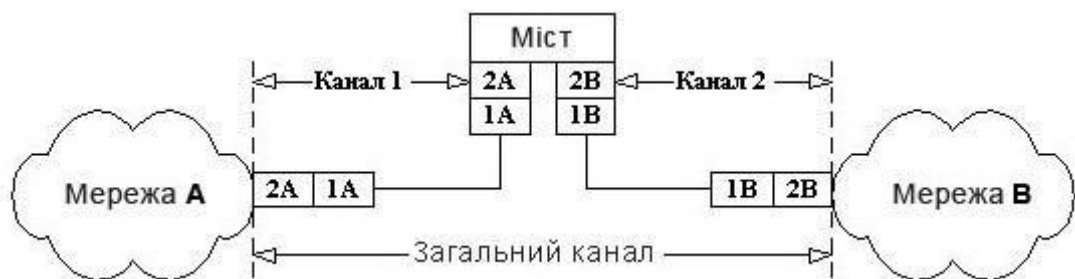


Рис. 3.8. Робота комутаторів на фізичному та канальному рівнях

Обмеження, що пов'язані із застосуванням мостів і комутаторів за топологією зв'язків та інших привели до того, що в переліку комунікаційних пристроїв з'явився ще один пристрій – маршрутизатор.

Маршрутизатор (router)

Маршрутизатор – система ретрансляції, що сполучає дві комунікаційні мережі або їх частини. Маршрутизатори працюють на третьому (мережному) рівні моделі OSI, що спілкується з протоколами вищих рівнів. **Маршрутизатори, як і мости або комутатори ретранслюють пакети з однієї частини мережі в іншу.** Спочатку маршрутизатор від комутатора відрізнявся тільки тим, що на комп'ютері, який об'єднує дві чи більше мереж, було встановлено інше програмне забезпечення.

На тепер між маршрутизатором і комутатором існують принципові відмінності:

- Маршрутизатори працюють не з фізичними адресами пакетів (MAC-адресами), а з логічними мережними адресами (IP-адресами).
- Маршрутизатори ретранслюють не всю інформацію, що приходить, а лише ту, яка адресована до них особисто, і відкидають (не ретранслюють) широкомовні пакети.
- Маршрутизатори на відміну від мостів і комутаторів не є прозорими для абонентів.

Головною відмінністю є те, що маршрутизатори підтримують мережі з великою кількістю можливих маршрутів та шляхів передачі інформації, так звані комірчасті мережі (*meshed networks*). Приклад такої мережі показаний на рис.3.9. Комутатори ж вимагають, щоб в мережі не було петель, щоб шлях поширення інформації між двома будь-якими абонентами був єдиним.

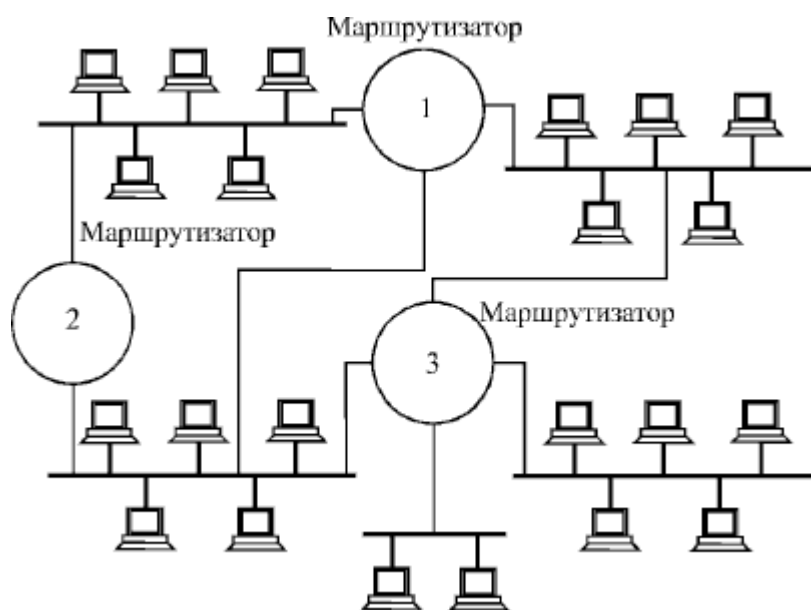


Рис. 3.9. Комірчаста мережа з маршрутизаторами

Маршрутизатори є складнішими за мости і комутатори і, відповідно, дорожчими. Маршрутизаторами складніше управляти, вони є повільнішими за комутатори. Проте, вони забезпечують найглибше розділення мережі на частини.

Якщо концентратори лише повторюють всі пакети (фізичний рівень моделі OSI), що поступили на них, комутатори і мости ретранслюють тільки

міжсегментні і широкомовні пакети (канальний рівень), то маршрутизатори сполучають окремі автономні мережі, що не впливають одна на одну, зберігаючи при цьому можливість передачі інформації між ними (мережний рівень).

Розмір мережі, що під'єднується до маршрутизатора практично нічим не обмежено: ні допустимими розмірами зони конфліктів, ні допустимою кількістю широкомовних пакетів, ні можливими для комутаторів і мостів різноманітними перевантаженнями. При цьому легко забезпечуються альтернативні, дублюючі шляхи поширення інформації для збільшення надійності зв'язку.

Для вибору маршруту кожен маршрутизатор формує в своїй пам'яті таблиці даних, які містять:

- Номери всіх мереж, що під'єднані до даного маршрутизатора.
- Список всіх сусідніх маршрутизаторів.
- Список MAC-адрес і IP-адрес всіх абонентів мереж, які під'єднані до маршрутизатора. Цей список автоматично оновлюється, як і у разі мостів та комутаторів.

Крім того, список всіх доступних маршрутизаторів повинен бути у кожного абонента мережі. Маршрутизатори обробляють адресну інформацію, що міститься у службовій інформації пакету. Вона містить номер мережі, і саме ці мережі сполучає маршрутизатор.

Кожен абонент, перш ніж відправити пакет, визначає, чи може він скерувати його безпосередньо до одержувача чи йому потрібно скористатися послугами маршрутизатора. Якщо номер власної мережі відправника збігається з номером мережі отримувача, то пакет передається безпосередньо, без маршрутизації. Якщо одержувач знаходиться в іншій мережі, то пакет передається до маршрутизатора, який скеровує його у потрібну мережу. При цьому виходить, що пакет в цілому адресовано до маршрутизатора (як до одного з абонентів власної мережі), а вкладена в ньому інформація адресована для абонента з іншої мережі, для якого вона, власне, і призначена.

Маршрутизатор аналізує IP-адресу, що міститься у складі пакету, і перетворює пакет, що надійшов по одній з мереж, у пакет, що призначений для іншої мережі. У полі адреси пакету він ставить MAC-адресу одержувача і свою MAC-адресу, як відправника пакету. У відповідь пакет аналогічно має пройти через посередника – маршрутизатор.

Потужний маршрутизатор є дорогим пристроєм, він складний в налаштуванні та експлуатації. Тому використовувати його слід у випадках, коли це дійсно необхідно, наприклад, коли застосування комутаторів і мостів не дозволяє подолати перевантаження мережі.

Шлюзи (gateway)

Шлюз є системою ретрансляції, що забезпечує взаємодію інформаційних мереж. Шлюз дозволяє об'єднувати мережі, що побудовані на істотно різних програмних і апаратних платформах. Наприклад, шлюз може дозволити користувачам, що працюють в мережі Unix, взаємодіяти з користувачами мережі Windows. Традиційно в Інтернеті терміни «шлюз» і «маршрутизатор» використовуються як синоніми.

Шлюзи оперують на верхніх рівнях моделі OSI (сеансовому, представницькому і прикладному) і представляють найбільш розвинений метод об'єднання мережних сегментів і комп'ютерних мереж. Необхідність в мережних шлюзах виникає при об'єднанні двох мереж, що мають різну архітектуру.

В якості шлюзу, зазвичай, використовується виділений комп'ютер, на якому запущено програмне забезпечення шлюзу і проводяться перетворення, що дозволяють взаємодіяти кільком системам в мережі.

Іншою функцією шлюзів є перетворення протоколів. При отриманні повідомлення IPX/SPX для клієнта TCP/IP шлюз перетворює повідомлення у протокол TCP/IP.

Шлюзи є складнішими у встановленні та налаштуванні і працюють повільніше, ніж маршрутизатори.

3.2 Порядок виконання

1. Отримати у викладача варіант завдання. Ознайомитися з описом завдання і в NetCracker зібрати мережу із заданою топологією і специфікаціями.
2. Поставити мережевий трафік згідно із завданням.
3. Вивести статистику основних каналів передачі даних. Запустити модель і визначити, чи є перевантаження устаткування або зв'язків. Показати результати викладачеві або зробити знімок екрана, експорт мережі в JPG-файл.

Загальні рекомендації

1. Застосовуйте пристрої з розділів Generic Devices. Наприклад, комп'ютери (LANworkstations → Workstations → Generic devices → Ethernet Workstation), хаби (HuBs → Shared Media → Ethernet → Generic devices → Fast Ethernet HuB), комутатори (Switches → Workgroup → Ethernet → Generic devices → Ethernet Switch), маршрутизатори (Router and Bridges → BackBone → BackBone router).
2. Умовні позначення: хаби (hubs), комутатори (switches), маршрутизатори (routers).
3. Якщо в завданні потрібно обладнання з інтерфейсами GigaBit Ethernet (1GBps), його доведеться або створити за допомогою Device → Device Factory. *Якщо інше не зазначено в описі завдання або на малюнку, використовуйте інтерфейси і обладнання Fast Ethernet, сигнальний стандарт 100Base-TX і кабель «кручена пара».*
4. Використання значень за замовчуванням для статистичних характеристик трафіків, визначених в усіх готових профілях: LAN peer-to-peer, Small InterLAN та інших, якщо в завданні не наводяться характеристики цих трафіків або не потрібно їх зміна, підбір.

Завдання

1. Створіть проект мережі з топологією і складом устаткування згідно Рис. 3.10 з використанням Fast Ethernet adapter. Задайте трафік з профілем LAN peer-to-peer між усіма робочими станціями і клієнт-серверний трафік File server's client від кожної робочої станції до сервера.

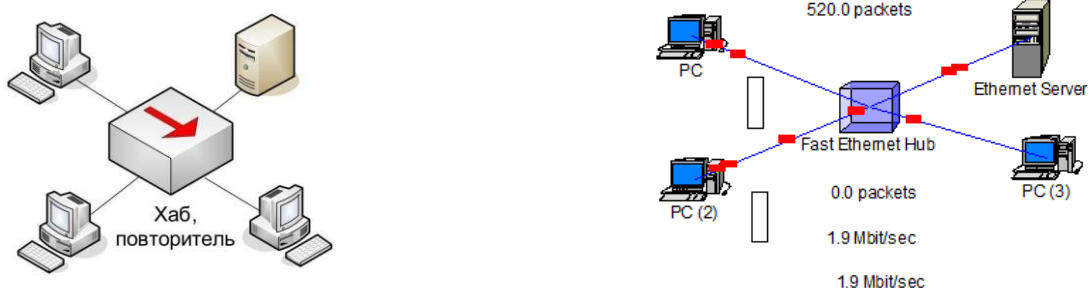


Рис. 3.10. Топологія «шина в точці» (англ. Bus-in-a-point)

2. Створіть проект мережі з топологією і складом устаткування згідно рис. 3.11 з використанням Fast Ethernet adapter. Задайте трафік з профілем LAN peer-to-peer між усіма робочими станціями.

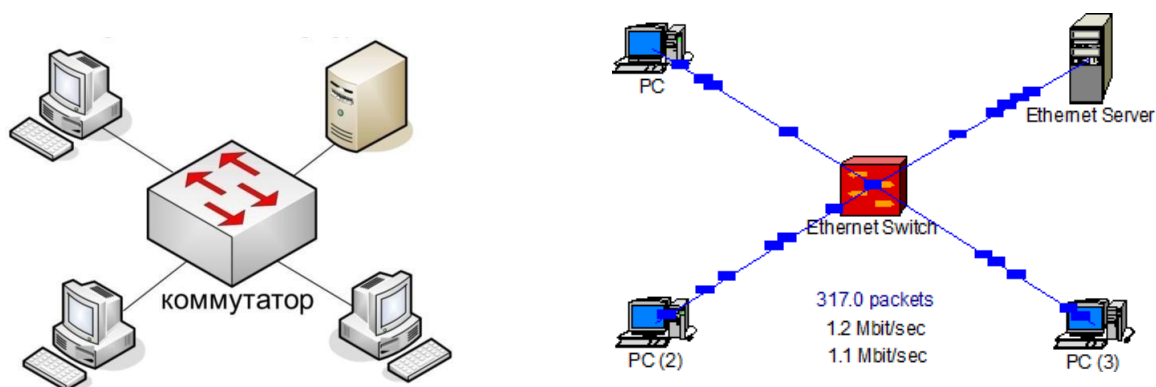


Рис. 3.11. Топологія «зірка» (англ. star)

3. Створіть проект мережі з топологією і складом устаткування згідно рис. 3.12 з використанням Fast Ethernet adapter. Задайте трафік з профілем LAN peer-to-peer між усіма робочими станціями.

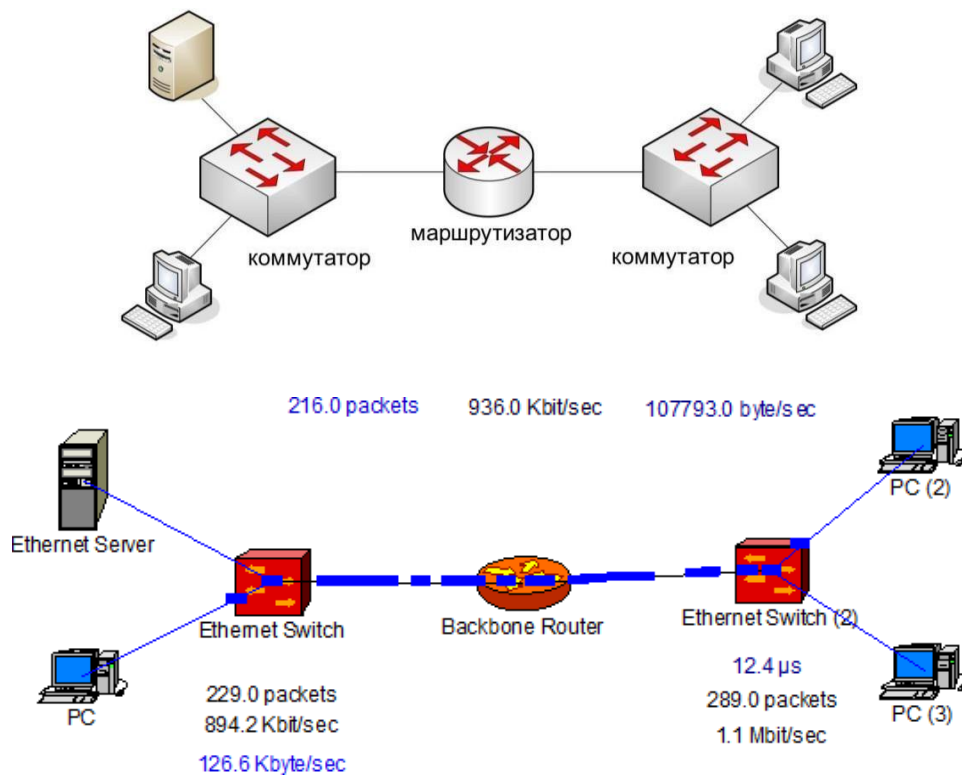
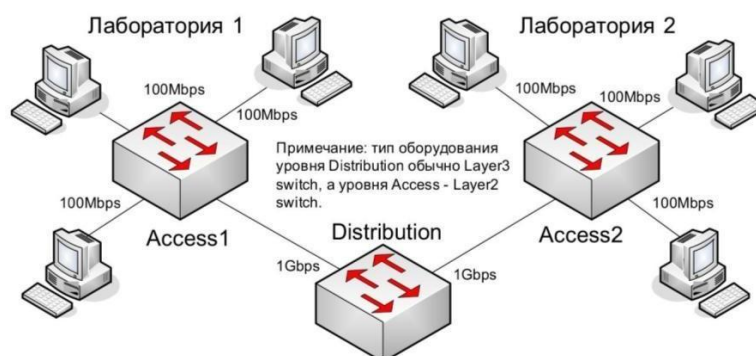


Рис. 3.12. Ієрархічна (неплоска) мережа

4. Створіть проект мережі з топологією і складом устаткування згідно рис. 3.13. Задайте трафік з профілем LAN peer-to-peer між комп'ютерами Лабораторії N 1. Задайте трафік з профілем LAN peer-to-peer між комп'ютерами Лабораторії N 2. Задайте трафік з профілем InterLAN між трьома парами комп'ютерів (комп'ютери пари належать різним лабораторіям).



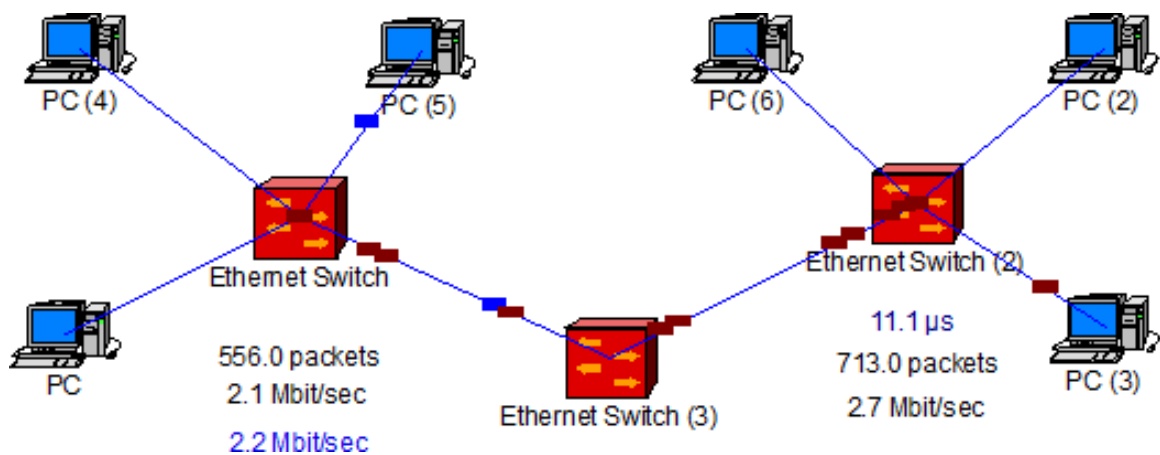


Рис. 3.13. Топологія «сніжинка» (англ. snow-flake)

3.3 Оброблення та аналізування результатів. Оформлення звіту.

При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

3.4 Контрольні питання

1. Які пристрої є основними засобами фізичної структуризації локальної мережі?
2. Який пристрій використовується для об'єднання кількох логічних сегментів мережі?
3. Який пристрій є багатопроцесорним?
4. Який пристрій використовується для об'єднання кількох мереж з різними топологіями?
5. Який пристрій забезпечує взаємодію мереж, що побудовані на істотно різних програмних і апаратних платформах?
6. На якому рівні стеку протоколів оперують шлюзи?
7. Протоколи якого рівня втілено у концентратори та повторювачі?
8. Яка істотна відмінність є між мостом та комутатором?

ПРАКТИЧНА РАБОТА № 4

ВИВЧЕННЯ ОБЛАДНАННЯ ТА КАБЕЛЬНОЇ СИСТЕМИ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ. ЕТАЛОННА МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ

Мета та основні завдання роботи: ознайомитись з багаторівневою організацією мережевої взаємодії систем та з основними апаратними засобами локальних обчислювальних мереж, отримати навички вибору обладнання та кабельної системи для побудови локальної обчислювальної мережі.

Вивчити та стисло описати у протоколі практичної роботи:

- еталонна модель взаємодії відкритих систем;
- рівні моделі OSI.

4.1 Теоретичні відомості

Еталонна модель взаємодії відкритих систем.

На початку 80-х років ряд міжнародних організацій по стандартизації - ISO, ITU-T і деякі інші - розробили модель, яка зіграла значну роль у розвитку мереж. Ця модель називається еталонною моделлю взаємодії відкритих систем (Open System Interconnection, OSI) або моделлю OSI. Модель OSI визначає різні рівні взаємодії систем, дає їм стандартні імена і вказує, які функції повинен виконувати кожен рівень. Модель OSI була розроблена на основі великого досвіду, отриманого при створенні комп'ютерних мереж, в основному глобальних, у 70-і роки. Повний опис цієї моделі займає більше 1000 сторінок тексту. У моделі OSI засоби взаємодії діляться на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережевий, каналний і фізичний. Кожен рівень має справу з одним певним аспектом взаємодії мережевих пристроїв. Модель OSI описує тільки системні засоби взаємодії, що реалізуються операційною системою, системними утилітами, системними апаратними засобами. Модель не включає засоби взаємодії

додатків кінцевих користувачів. Свої власні протоколи взаємодії додатку реалізують, звертаючись до системних засобів. Додаток може взяти на себе функції деяких верхніх рівнів моделі OSI. Наприклад, деякі СУБД мають вбудовані засоби віддаленого доступу до файлів. У цьому випадку програму, виконуючи доступ до віддалених ресурсів, не використовує системну файлову службу; він обходить верхні рівні моделі OSI і звертається напряму до системних засобів, відповідальних за транспортування повідомлень по мережі, які розташовуються на нижніх рівнях моделі OSI.

Рівні моделі OSI

Фізичний рівень (Physical layer) має справу з передачею бітів по фізичних каналах зв'язку, таких, наприклад, як коаксіальний кабель, кручена пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як смуга пропускання, перешкодозахищеність, хвильовий опір і інші. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад, крутість фронтів імпульсів, рівні напруження або струму сигналу, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи роз'ємів і призначення кожного контакту. Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом. Прикладом протоколу фізичного рівня може служити специфікація 10-BaseT технології Ethernet, яка визначає як використовуваного кабелю неекрановану виту пару категорії 3 із хвильовим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів, манчестерський код для представлення даних в кабелі, а також деякі інші характеристики середовища і електричних сигналів.

Канальний рівень

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, в яких лінії зв'язку використовуються (розділяються) навперемінно декількома парами взаємодіючих комп'ютерів,

фізичне середовище передачі може бути зайнята. Тому одним із завдань канального рівня (Data Link layer) є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення і корекції помилок. Для цього на каналному рівні біти групуються в набори, звані кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру, вміщуючи спеціальну послідовність біт в початок і кінець кожного кадру, для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить по мережі, одержувач знов обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр вважається правильним і приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка. Канальний рівень може не тільки виявляти помилки, але і виправляти їх за рахунок повторної передачі пошкоджених кадрів. Необхідно відзначити, що функція виправлення помилок не є обов'язковою для канального рівня, тому в деяких протоколах цього рівня вона відсутня, наприклад, в Ethernet і Frame Relay. У протоколах канального рівня, що використовуються в локальних мережах, закладена певна структура зв'язків між комп'ютерами і способи їх адресації. Хоча канальний рівень і забезпечує доставку кадру між будь-якими двома вузлами локальної мережі, він це робить тільки в мережі з абсолютно певною топологією зв'язків, саме тією топологією, для якої він був розроблений. До таких типових топологій, що підтримуються протоколами канального рівня локальних мереж, відносяться загальна шина, кільце і зірка, а також структури, отримані з них за допомогою мостів і комутаторів. Прикладами протоколів канального рівня є протоколи Ethernet, Token Ring, FDDI, 100VG-AnyLAN. У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами і маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережесистемних адаптерів і їх драйверів. У глобальних мережах, які рідко володіють регулярною топологією, канальний рівень часто забезпечує обмін даними тільки між двома сусідніми

комп'ютерами, сполученими індивідуальною лінією зв'язку. Прикладами протоколів "точка- точка» (як часто називають такі протоколи) можуть служити широко поширені протоколи PPP і LAR-B. У таких випадках для доставки повідомлень між кінцевими вузлами через всю мережу використовуються засоби мережевого рівня. Саме так організовані мережі X.25. Іноді в глобальних мережах функції каналного рівня в чистому вигляді виділити важко, оскільки в одному і тому ж протоколі вони об'єднуються з функціями мережевого рівня. Прикладами такого підходу можуть служити протоколи технологій ATM і Frame Relay. У цілому каналний рівень являє собою вельми могутній і закінчений набір функцій по пересилці сполучень між вузлами мережі. У деяких випадках протоколи каналного рівня виявляються самодостатніми транспортними засобами і можуть допускати роботу понад них безпосередньо протоколів прикладного рівня або додатків, без залучення засобів мережевого і транспортного рівнів. Наприклад, існує реалізація протоколу управління мережею SNMP, безпосередньо без Ethernet, хоч стандартно цей протокол працює на основі мережевого протоколу IP і транспортного протоколу UDP. Природно, що застосування такої реалізації буде обмеженим - вона не підходить для складних мереж різних технологій, наприклад Ethernet і X.25, і навіть для такої мережі, в якій у всіх сегментах застосовується Ethernet, але між сегментами існують петлевидні зв'язки. А от у двохсегментній мережі Ethernet, об'єднаній мостом, реалізація SNMP над каналним рівнем буде цілком працездатна. Проте для забезпечення якісного транспортування повідомлень в мережах будь-яких топологій і технологій функцій каналного рівня виявляється недостатньо, тому в моделі OSI рішення цієї задачі покладається на два наступних рівні - мережевий і транспортний.

Мережевий рівень

Мережевий рівень (Network layer) служить для утворення єдиної транспортної системи, що об'єднує декілька мереж, причому ці мережі можуть використати абсолютно різні принципи передачі повідомлень між кінцевими вузлами і володіти довільною структурою зв'язків. Функції мережевого рівня

досить різноманітні. Протоколи канального рівня локальних мереж забезпечують доставку даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією, наприклад топологією ієрархічної зірки. Це дуже жорстке обмеження, яке не дозволяє будувати мережі з розвиненою структурою, наприклад, мережі, що об'єднують декілька мереж підприємства в єдину мережу, або високонадійні мережі, в яких існують надмірні зв'язки між вузлами. Можна було б ускладнювати протоколи канального рівня для підтримки петлевидних надлишкових зв'язків, але принцип поділу обов'язків між рівнями приводить до іншого розв'язку. Щоб з одного боку зберегти простоту процедур передачі даних для типових топологій, а з іншого допустити використання довільних топологій, вводиться додатковий мережевий рівень. На мережевому рівні сам термін мережа наділяють специфічним значенням. У даному випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї з стандартних типових топологій і використовують для передачі даних один з протоколів канального рівня, визначений для цієї топології. Усередині мережі доставка даних забезпечується відповідним канальним рівнем, а ось доставкою даних між мережами займається мережевий рівень, який і підтримує можливість правильного вибору маршруту передачі даних навіть у тому випадку, коли структура зв'язків між складовими мережами має характер, відмінний від прийнятого в протоколах канального рівня. Мережі з'єднуються між собою спеціальними пристроями, званими маршрутизаторами. Маршрутизатор - це пристрій, який збирає інформацію про топологію міжмережових з'єднань і на її підставі пересилає пакети мережевого рівня в мережу призначення. Щоб передати повідомлення від відправника, що знаходиться в одній мережі, одержувачу, що знаходиться в іншій мережі, треба здійснити деяку кількість транзитних передач між мережами, або хопів (від hop - стрибок), кожний раз вибираючи відповідний маршрут. Таким чином, маршрут являє собою послідовність маршрутизаторів, через які проходить пакет. Проблема вибору найкращого шляху називається

маршрутизацією, і її розв'язання є однією з головних задач мережевого рівня. Ця проблема ускладнюється тим, що найкоротший шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту; воно залежить від пропускнуої спроможності каналів зв'язку і інтенсивності трафіку, яка може змінюватися з плином часу. Деякі алгоритми маршрутизації намагаються пристосуватися до зміни навантаження, в той час як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися і за іншими критеріями, наприклад надійності передачі. У загальному випадку функції мережевого рівня ширше, ніж функції передачі повідомлень по зв'язках з нестандартною структурою, які розглянуті на прикладі об'єднання декількох локальних мереж. Мережевий рівень вирішує також задачі узгодження різних технологій, спрощення адресації у великих мережах і створення надійних і гнучких бар'єрів на шляху небажаного трафіка між мережами. Блок даних мережевого рівня прийнято називати пакетами (packets). При організації доставки пакетів на мережному рівні використовується поняття «номер мережі». У цьому випадку адреса одержувача складається з старшої частини - номера мережі і молодшої - номера вузла в цій мережі. Всі вузли однієї мережі повинні мати одну і ту ж старшу частину адреси, тому терміну "мережа" на мережевому рівні можна дати і інше, більш формальне визначення: мережа - це сукупність вузлів, мережева адреса яких містить один і той же номер мережі. На мережевому рівні визначаються два види протоколів. Перший вид - мережеві протоколи (routed protocols) - реалізують просування пакетів через мережу. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережевого рівня. Однак часто до мережевого рівня відносять і інший вид протоколів, званих протоколами обміну маршрутної інформацією або просто протоколами маршрутизації (routing protocols). За допомогою цих протоколів маршрутизатори збирають інформацію про топологію міжмережевих з'єднань. Протоколи мережевого рівня реалізуються програмними модулями операційної системи, а також програмними і апаратними засобами

маршрутизаторів. На мережевому рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, використовуваного на мережному рівні, на локальну адресу мережі. Такі протоколи часто називають протоколами дозволу адрес - Address Resolution Protocol, ARP. Іноді їх відносять не до мережевого рівня, а до канального, хоча тонкощі класифікації не змінюють їх суті. Прикладами протоколів мережевого рівня є протокол міжмережевої взаємодії IP стека TCP / IP і протокол міжмережевого обміну пакетами IPX стека Novell.

Транспортний рівень

На шляху від відправника до одержувача пакети можуть бути спотворені або загублені. Хоча деякі додатки мають власні засоби обробки помилок, існують і такі, які вважають за краще відразу мати справу з надійним з'єднанням. Транспортний рівень (Transport layer) забезпечує додаткам або верхнім рівням стека - прикладному і сеансовому - передачу даних з тим ступенем надійності, яка їм потрібна. Модель OSI визначає п'ять класів сервісу, що надаються транспортним рівнем. Ці види сервісу відрізняються якістю наданих послуг: терміновістю, можливістю відновлення перерваного зв'язку, наявністю коштів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне - здатністю до виявлення і виправлення помилок передачі, таких як спотворення, втрата і дублювання пакетів. Вибір класу сервісу транспортного рівня визначається, з одного боку, тим, якою мірою завдання забезпечення надійності вирішується самими додатками і протоколами більш високої, ніж транспортний, рівнів, а з іншого боку, цей вибір залежить від того, наскільки надійною є система транспортування даних в мережі, забезпечується рівнями, розташованими нижче транспортного - мережним, канальним і фізичним. Так, наприклад, якщо якість каналів передачі зв'язку є дуже високою і імовірність виникнення помилок, не виявлених протоколами більш низьких рівнів, невелика, то розумно скористатися одним з полегшених сервісів транспортного рівня, не обтяжених численними перевірками, квотуванням і

іншими прийомами підвищення надійності. Якщо ж транспортні засоби нижніх рівнів спочатку дуже ненадійні, то доцільно звернутися до найбільш розвинутого сервісу транспортного рівня, який працює, використовуючи максимум засобів для виявлення і усунення помилок, - за допомогою попереднього встановлення логічного з'єднання, контролю доставки повідомлень по контрольних сумах і циклічній нумерації пакетів, встановлення тайм-аутів доставки і т. п. Блок даних транспортного рівня прийнято називати дейтаграммами (datagram).

Як правило, всі протоколи, починаючи з транспортного рівня і вище, реалізуються програмними засобами кінцевих вузлів мережі - компонентами їх мережових операційних систем. Як приклад транспортних протоколів можна привести протоколи TCP і UDP стека TCP / IP і протокол SPX стека Novell. Протоколи нижніх чотирьох рівнів узагальнено називають мережовим транспортом або транспортною підсистемою, оскільки вони повністю вирішують задачу транспортування повідомлень із заданим рівнем якості в складових мережах з довільною топологією і різними технологіями. Інші три верхніх рівні вирішують завдання надання прикладних сервісів на основі транспортної підсистеми.

Сеансовий рівень

Сеансовий рівень (Session layer) забезпечує управління діалогом: фіксує, яка зі сторін є активною в даний момент, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки, а не починати все з початку. Насправді деякі докладання використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто об'єднують з функціями прикладного рівня і реалізують в одному протоколі.

Представницький рівень

Представницький рівень (Presentation layer) має справу з формою подання переданої по мережі інформації, не змінюючи при цьому її змісту. За рахунок

рівня уявлення інформація, що передається прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть подолати синтаксичні відмінності в представленні даних або ж відмінності в кодах символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватися шифрування і дешифрування даних, завдяки якому секретність обміну даними забезпечується відразу для всіх прикладних служб. Прикладом такого протоколу є протокол Secure Socket Layer (SSL), який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP / IP. Прикладний рівень Прикладний рівень (Application layer) - це насправді просто набір різноманітних протоколів, за допомогою яких користувачі мережі отримують доступ до ресурсів, що, таким як файли, принтери або гіпертекстові Webсторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, звичайно називається повідомленням (message).

Існує дуже велика різноманітність служб прикладного рівня, наприклад, кілька найбільш поширених реалізації файлових служб: NCP в операційній системі Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP і TFTP, що входять в стек TCP / IP.

4.2 Порядок виконання

1. Отримати у викладача варіант завдання. Ознайомитися з описом завдань і в NetCracker зібрати мережу із заданою топологією і специфікаціями.
2. Поставити мережевий трафік згідно із завданнями.
3. Провести імітаційне моделювання роботи мережі і зібрати статистику: середнє завантаження вузлів, каналів передачі даних; середня затримка; кількість прийнятих, відкинутих пакетів.
4. У відповідний розділ бази даних компонент додати опис нового елемента із зазначеними характеристиками (табл. 4.1 – 4.4).

Варіанти та приклад виконання завдання 1

Таблиця 4.1 – Варіанти до завдання 1

№ варіанту	Тип адаптеру	Тип концентратору	Тип комутатору
1	1	1	1
2	2	2	2
3	3	3	1
4	4	1	2
5	5	2	1
6	1	3	2
7	2	1	1
8	3	2	2

Таблиця 4.2 – Типи мережевих адаптерів(*LAN adapters* → *Ethernet*)

№	Виробник	Модель	Максимальна відстань до концентратору, м
1	D-Link Systems	DFE-530TX	100
2	Intel	EtherExpress PRO/100+TX Adapter	100
3	IBM	EtherJet PC Card Adapter	100
4	3Com Corp.	Fast EtherLink XL 10/100 PCI (3C905B-TX)	100
5	3Com Corp.	Fast EtherLink III 10/100 PCI (3C595-T)	100

Таблиця 4.3 – Типи концентраторів (*Hubs* → *Shared media* → *Ethernet*)

№	Виробник	Модель	Тип портів	Кількість портів	Швидкість передачі, Мб/с
1	D-Link Systems	10/100 MB DUAL-SPEED HUB DFE-916x (Master)	Ethernet, TX	16	10/100
2	Archtek America	SmartLink 16-Port 10Base-T Ethernet Hub	Ethernet, TX	16	10/100
3	Allied Telesyn	CentreCOM 100Base-TX 8-Port Fast Ethernet Hub, Europe	Ethernet, TX	8	10/100

Таблиця 4.4 – Типи комутаторів (*Switches* → *Workgroup* → *Ethernet*)

№	Виробник	Модель	Тип портів	Кількість портів	Швидкість передачі, Мб/с
1	Allied Telesyn	16-port 10/100TX unmanaged fast ethernet switch	Ethernet, TX	16	10/100
2	Cisco Systems	Catalyst 3512 XL (Standard Edition)	Ethernet, TX	12	10/100

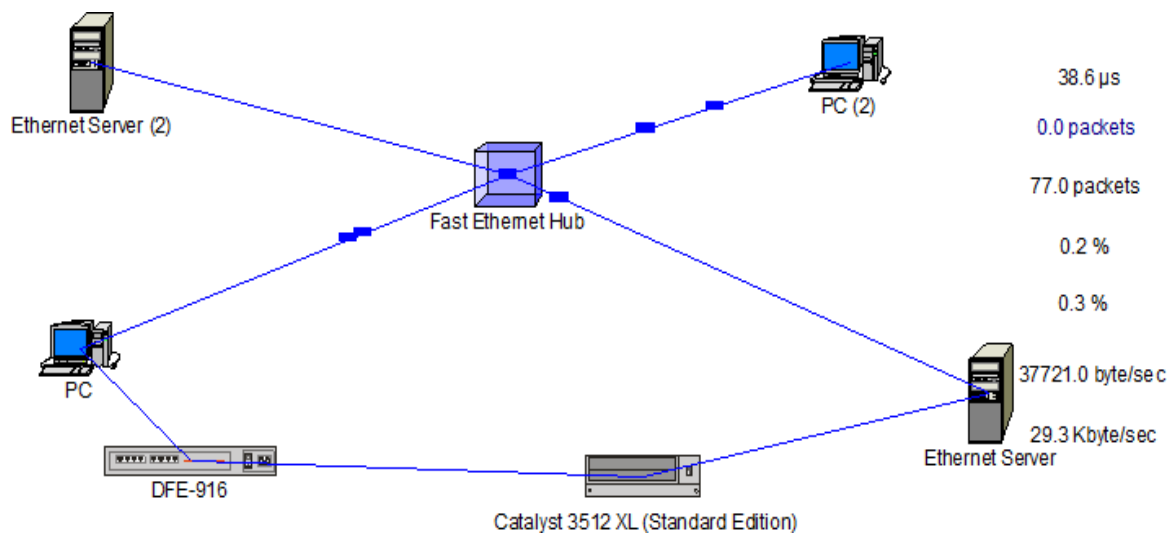


Рис.4.1. Приклад виконання завдання 1

Варіанти та приклад виконання завдання 2

- Кількість робочих станцій $N_{PC} = N_B + 2$;
- Кількість серверів $N_C = N_B + 1$;
- N_B – номер варіанту (порядковий номер студента в журналі групи).
- Тип трафіку: *LAN peer-to-peer traffic; FTP; E-Mail (SMTP); HTTP*.

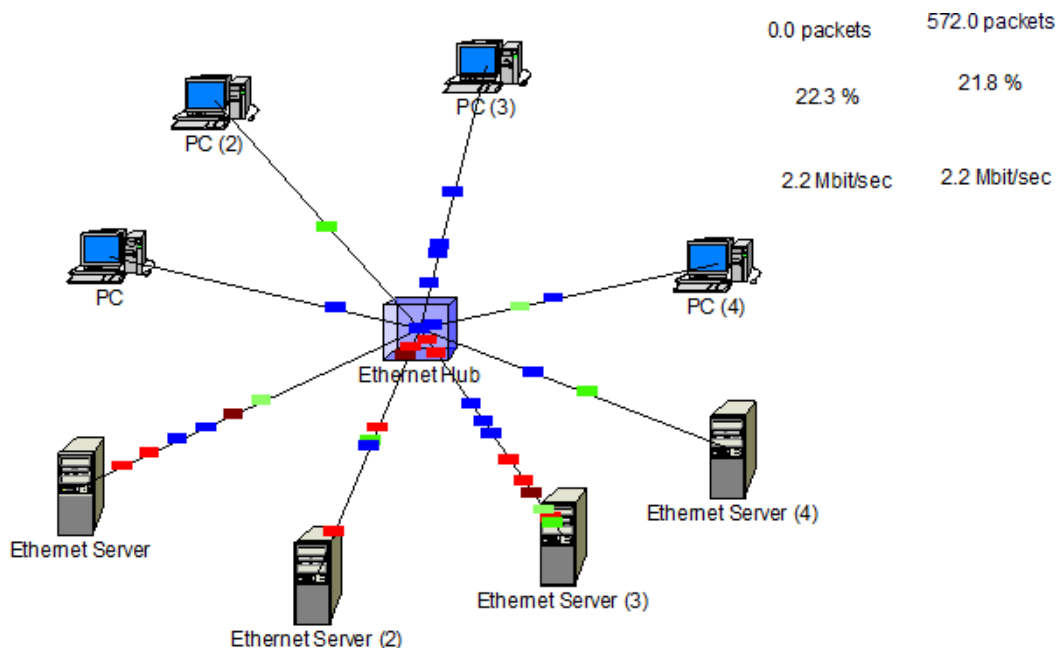


Рис.4.2. Приклад виконання завдання 2

4.3 Оброблення та аналізування результатів. Оформлення звіту.

При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

4.4 Контрольні питання

1. Охарактеризуйте еталонну модель взаємодії відкритих систем.
2. Охарактеризуйте фізичний та канальний рівні моделі OSI.
3. Охарактеризуйте мережевий та транспортний рівні моделі OSI.
4. Охарактеризуйте сеансовий та представницький рівні моделі OSI.
5. Охарактеризуйте прикладний рівень моделі OSI.
6. Що таке мережевий адаптер та повторювач? Надайте їх основні характеристики.
7. Що таке концентратор та міст? Надайте їх основні характеристики.
8. Що таке комутатор? Надайте його основні характеристики.

ПРАКТИЧНА РОБОТА №5

СТВОРЕННЯ БАГАТОРІВНЕВОГО ПРОЕКТУ

Мета та основні завдання роботи: вивчити можливості NetCracker у створенні багаторівневого проекту.

Вивчити та стисло описати у протоколі практичної роботи:

- технологію клієнт – сервер;
- переваги та недоліки мережі клієнт – серверної архітектури.

5.1 Теоретичні відомості

Технологія клієнт – сервер, яка широко застосовується при роботі з базами даних в мережі, відома вже давно і найчастіше застосовувалась у великих організаціях. Сьогодні, з розвитком INTERNET, ця технологія все частіше приваблює погляди розробників програмного забезпечення, оскільки в світі нагромаджено величезну кількість інформації по різноманітних питаннях і найчастіше ця інформація зберігається в базах даних.

Архітектура мережі визначає основні елементи мережі, характеризує її загальну логічну організацію, технічне забезпечення, програмне забезпечення, описує методи кодування. Архітектура також визначає принципи функціонування та інтерфейс користувача.

Архітектура клієнт – сервер (client-server architecture) – це концепція інформаційної мережі, в якій основна частина її ресурсів зосереджена в серверах, обслуговуючих своїх клієнтів. Розглянута архітектура визначає два типи компонентів: сервери і клієнти.

Сервер – це об'єкт, що дає сервіс іншим об'єктам мережі за їх запитам.

Сервіс – це процес обслуговування клієнтів.

Сервер працює за завданнями клієнтів і управляє виконанням їх завдань. Після виконання кожного завдання сервер посилає отримані результати клієнту, який послав це завдання. Сервісна функція в архітектурі клієнт – сервер описується комплексом прикладних програм, відповідно до якого

виконуються різноманітні прикладні процеси.

Процес, який викликає сервісну функцію за допомогою певних операцій, називається клієнтом. Ним може бути програма або користувач.

Клієнти – це робочі станції, які використовують ресурси сервера і надають зручні інтерфейси користувача. Інтерфейси користувача це процедури взаємодії користувача з системою або мережею.

Клієнт є ініціатором і використовує електронну пошту або інші сервіси сервера. У цьому процесі клієнт запитує вид обслуговування, встановлює сеанс, отримує потрібні йому результати і повідомляє про закінчення роботи.

У мережах з виділеним файловим сервером на виділеному автономному ПК встановлюється серверна мережева операційна система. Цей ПК стає сервером. Програмне забезпечення (ПЗ), встановлене на робочій станції, дозволяє їй обмінюватися даними з сервером. Найбільш поширені мережеві операційна системи:

- NetWare фірми Novel;
- Windows NT фірми Microsoft;
- UNIX фірми AT &T;
- Linux.

Крім мережевої операційної системи необхідні мережні прикладні програми, що реалізують переваги, надані мережею.

Мережі на базі серверів мають кращі характеристики і підвищену надійність. Сервер володіє головними ресурсами мережі, до яких звертаються інші робочі станції.

У сучасній клієнт – серверній архітектурі виділяється чотири групи об'єктів: клієнти, сервери, дані і мережеві служби. Клієнти розташовуються в системах на робочих місцях користувачів. Дані в основному зберігаються в серверах. Мережеві служби є спільно використовуваними серверами і даними. Крім того служби керують процедурами обробки даних. Мережі клієнт – серверної архітектури мають наступні переваги:

- Дозволяють організовувати мережі з великою кількістю робочих

станцій.

- Забезпечують централізоване управління обліковими записами користувачів, безпекою та доступом, що спрощує мережне адміністрування.
- Ефективний доступ до мережевих ресурсів.
- Користувачеві потрібен один пароль для входу в мережу і для отримання доступу до всіх ресурсів, на які поширюються права користувача.

Поряд з перевагами мережі клієнт – серверної архітектури мають і ряд недоліків:

- Несправність сервера може зробити мережу непрацездатною, як мінімум втрату мережевих ресурсів.
- Вимагають кваліфікованого персоналу для адміністрування.
- Мають вищу вартість мереж і мережевого обладнання.

5.2 Порядок виконання

1. Запустіть NetCracker Professional.
2. Відкрийте файл NetCracker Professional (*Tutor.NET*).
3. Максимізуйте вікно сайту.
4. Відкрийте *Project Hierarchy*. Проект показаний як ієрархічна структура. Кожен рівень має відповідний символ розкриття.
5. Знайдіть об'єкт-контейнер *Building* (будівля) в лівому верхньому кутку



і двічі клацніть на ньому. Building

Вікно сайту *Building* стане поточним вікном.

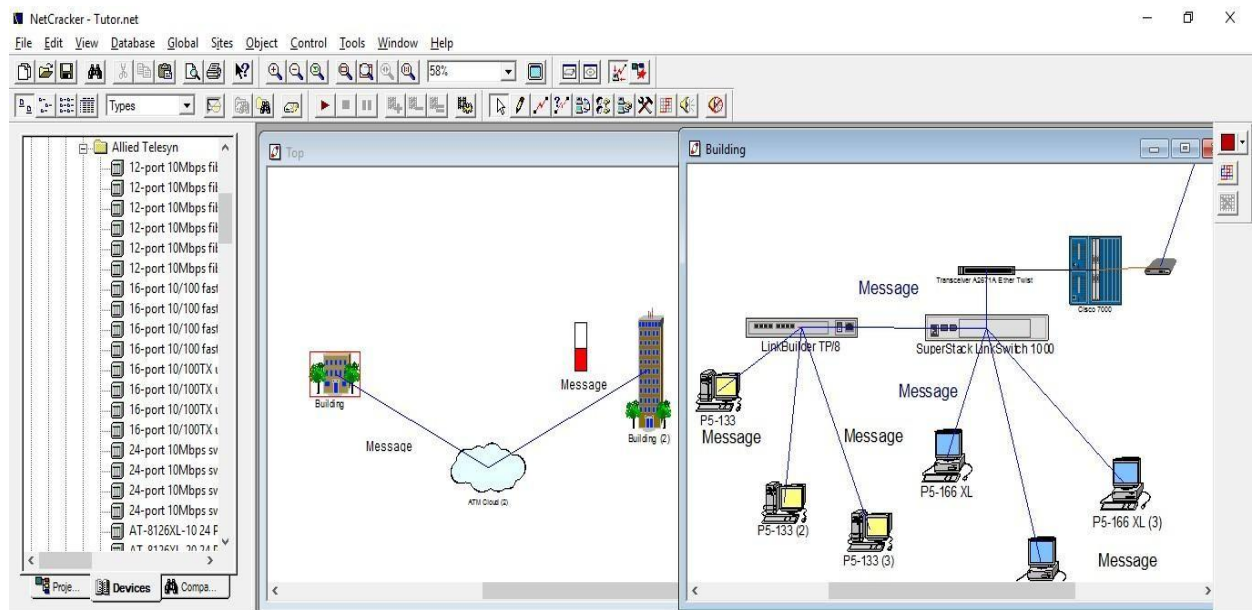


Рис.5.1. Багаторівневий проект Tutor.NET

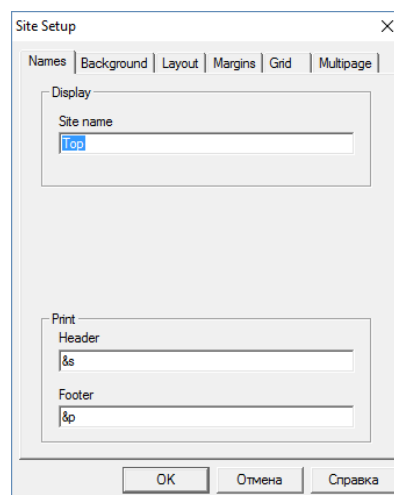
1. Для повторного відкриття вікна *Top* з вікна *Building* двічі клацніть на іконці з'єднання.

2. Перейменуємо вікно проекту.

а. Спочатку зробимо поточним вікно *Top*.

б. Тепер викличемо діалог *Site Setup* наступним чином:

У меню *Sites menu*, виберіть команду *Site Setup*. З'явиться вікно діалогу *Site Setup*.



с. Виберіть закладку *Names*. Перейдіть до імені (Top) і введіть "*The MacNally Corporation*".

д. Перейменуйте *Building* в "*The MacNally Building*" нові імена тут же з'являються в ієрархічній структурі проекту.

3. Використовуємо інструменти малювання для анотування проекту.
- a. Зробіть поточним *MacNally Building* і знайдіть іконку конектора.
 - b. На панелі режимів натисніть кнопку *Draw mode*.
 - c. На панелі інструментів клацніть кнопку малювання ліній. Використовуйте лінії для малювання стрілки, що вказує в правий кут вікна сайту. Поверніться до звичайного режиму, клацнувши на стрілці в панелі режимів.

d. Змініть колір лінії за допомогою меню **Object** → **Styles**

e. Для того, щоб позначити іконку конектора зробіть наступне:

- ✓ Включіть режим малювання,
- ✓ На панелі малювання виберіть **Text**,
- ✓ Обведіть область, в якій буде розташовуватися текст




Рис.5.2. Панель малювання

f. Напишіть "Зв'язок з *MacNally Corporation*" і натисніть Enter.

g. Поверніться до звичайного режиму.

4. Підсвітити трафік, використовуючи *Trace mode*.

a. Запустимо анімацію.

b. На панелі режимів натисніть кнопку  трасування, клацніть на робочій станції (P5-166 XL (3)) справа на сайті *MacNally Building*, потім клацніть на станції зліва (P5-133 XL (3)). Зв'язок між ними забарвиться в червоний колір.

5. Підсвітіть шлях від пристрою з одного сайту до пристрою, що належить іншому сайту.

6. Зупиніть анімацію.

7. Закрийте проект, попередньо зберігши його ..

8. Створіть новий проект.

9. У браузері пристроїв знайдіть *Buildings, campuses and LAN workgroups*.

10. Перенесіть один з об'єктів *Building* на робочу область.

11. Розкрийте будівлю, для чого клацніть на ньому правою кнопкою миші і в контекстному меню виберіть команду **Expand**. Ви створили підрівень основного сайту.

12. Наповнимо будинок використовуючи архітектуру "клієнт-сервер".

Будемо використовувати сконфігуровані пристрої.

У браузері розкрийте **LAN workstations**. Ви побачите список загальних пристроїв (рис. 5.3)

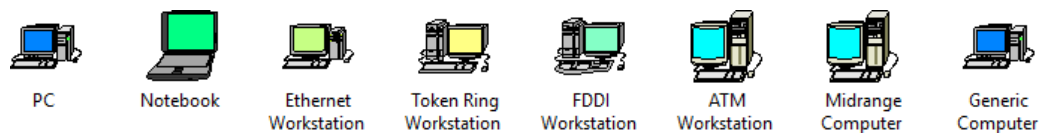


Рис.5.3. Пристрої загального призначення

a. Виберіть і перетягніть **Ethernet workstation** в вікно *Building*.

b. У меню *Edit* виберіть *Duplicate*.

c. У **Devices** розкрийте **Switches**, розкрийте **Workgroup**, розкрийте **Ethernet**, і клацніть на папці **Generic devices**. Ethernet switch з'явиться в панелі зображень



d. Перенесіть комутатор в вікно сайту *Building*.

e. Клацніть на кнопці

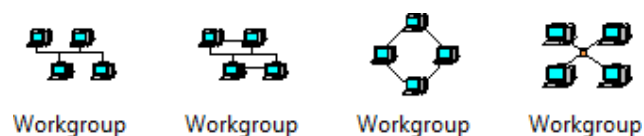
f. Клацніть на робочій станції і протягнете зв'язок до комутатора.

g. Зв'яжіть також комутатор з другої робочої станцією

h. Зробіть поточним вікно сайту *Top*.

i. Виберіть Buildings, campuses і LAN workgroups в браузері пристроїв.

Виберіть



робочу групу

j. Виберіть і перенесіть робочу групу у вікно сайту *Top*

k. З'єднайте робочу групу і *Building*.

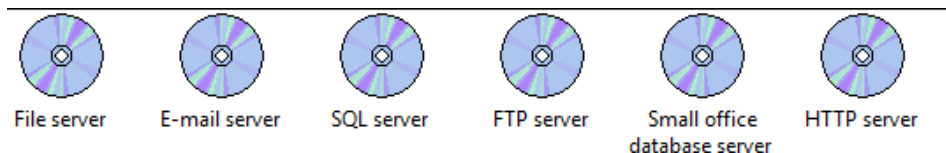
Увага! Пунктирна лінія вказує на те, що ці відносини не повна!

l. Двічі клацніть на *Building*. Вікно сайту *Building* стане поточним.

m. Виберіть кнопку встановлення зв'язків. У вікні сайту *Building* клацніть на іконці **Ethernet Switch**, потім клацніть на іконці **Workgroup**. З'явиться діалог Асистента зі зв'язків та оберіть *Link* для завершення зв'язку.


13. Зробимо з однієї з робочих станцій сервер наступним чином ::

a. У браузері пристроїв знайдіть розділ "*Network and enterprise software*" і розкрийте його. Клацніть на "*Server software*". З'являться доступні типи серверів



b. Перенесіть **E-mail server** на одну з робочих станцій.

14. Встановимо клієнт-серверний трафік:


a. У вікні сайту будівлі виберемо режим установки трафіку оберемо *Set traffic*  клацніть на робочій станції без серверного програмного забезпечення, потім на робочій станції з серверним програмним забезпеченням.

b. оберіть *E-mail* в якості типу трафіку.

15. Визначимо інший трафік:

a. У вікні сайту *Top* щелкнем робочу групу *Workgroup*, потім у вікні сайту *Building* оберемо робочу станцію без серверного програмного забезпечення.

b. Виберемо *Small office environment* як тип трафіку.

c. Запустимо анімацію 

16. Збережемо проект.

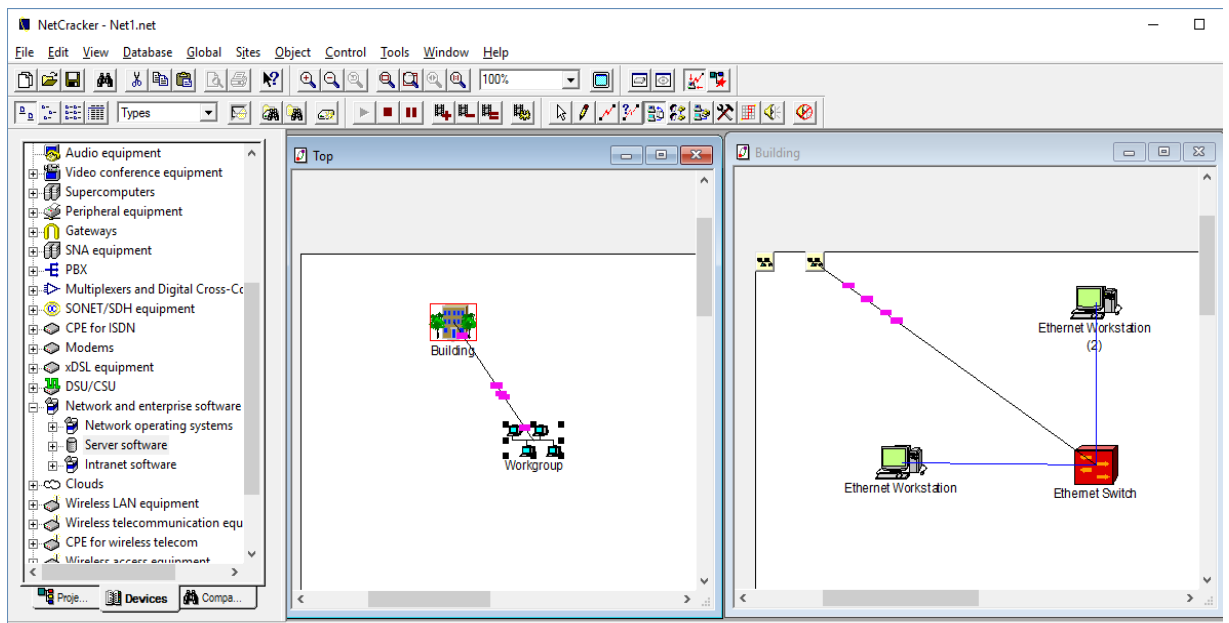


Рис. 5.4. Приклад багаторівневого проекту

Варіанти завдань

№ варіанту	Кількість робочих станцій з E-mail server	Кількість робочих станцій без E-mail server
1	2	1
2	1	2
3	1	1
4	2	2
5	1	3
6	2	3
7	2	4
8	1	4

5.3 Оброблення та аналізування результатів. Оформлення звіту.

При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

5.4 Контрольні питання

- 1) Що представляє собою архітектура мережі ?
- 2) Що таке «технологія клієнт – сервер»?
- 3) Що таке «клієнт мережі»?
- 4) Які переваги мережі клієнт – серверної архітектури?
- 5) Які недоліки мережі клієнт – серверної архітектури?
- 6) Які групи об'єктів сучасної клієнт – серверної архітектури ви знаєте?
- 7) Що таке сервер і як він працює?
- 8) Що таке клієнт і як він працює?

ПРАКТИЧНА РОБОТА 6

ДОСЛІДЖЕННЯ РОБОТИ МЕРЕЖЕВОГО СИМУЛЯТОРА PACKET TRACER. НАЛАШТУВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ В PACKET TRACER

Мета та основні завдання роботи: отримання практичних навичок роботи з симулятором Cisco packet tracer, самостійне створення моделі локальної мережі, дослідження характеристики пасивного мережевого устаткування.

Вивчити та стисло описати у протоколі практичної роботи:

- описати інтерфейс програми;
- організація мережі;
- мережне комунікаційне обладнання.

6.1 Теоретичні відомості

Адресація в локальних мережах

MAC-адреса

MAC-адреса — це унікальний шістнадцятковий серійний номер, що призначається кожному мережевому пристрою для ідентифікації його в мережі. Для мережевих пристроїв (так само, як і для більшості інших мережевих типів) ця адреса встановлюється 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 пакети з мережевого кабелю, призначені для неї. Якщо MAC-адреса не є єдиною, то не існує способу провести відмінність між двома станціями. Пристрої в мережі переглядають мережевий трафік і шукають свій MAC-адрес в кожному пакеті, щоб визначити, чи повинні вони декодувати цей пакет, чи ні. Існують спеціальні способи для широкомовної розсилки повідомлень кожному пристрою. MAC-адреси мають довжину 6 байт і зазвичай записуються шістнадцятковим числом у вигляді 12:34:56:78:90:AB (двокрапки можуть бути відсутніми, але їх наявність робить адресу більше читабельною).

IP-адреса

IP-адреса розділяється на дві частини: **номери мережі** і **номера вузла**. Номер мережі може бути вибраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу **Internet (Internet Network Information Center, InterNIC)**, якщо мережа повинна працювати як складова частина **Internet**. Зазвичай постачальники послуг **Інтернет** отримують діапазони адрес у підрозділів **InterNIC**, а потім розподіляють їх між своїми абонентами.

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

Необхідно відразу утямити основний принцип IP-адресації – IP-адреси призначаються мережевим інтерфейсам вузлів складеної мережі, а не вузлам складеної мережі. Що це означає?

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. Так, пристрій з 6 активними інтерфейсами (наприклад, маршрутизатор) матиме 6 IP-адрес – по одному на кожен інтерфейс у кожній мережі, до якої він підключений.

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

IP-адреса має довжину 4 байти (по 8 біт), 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 формі числення. Тому для читабельності, IP-адреса записується у вигляді чотирьох чисел, розділених крапками.

Наприклад, **128.10.2.30** – десяткова форма подання адреси-4 (десятикових)

числа, розділених (.) крапками.

А **10000000 00001010 00000010 00011110** – двійкова форма подання цієї ж адреси. Чотири 8-ми розрядних числа (октету)

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

Тут потрібно відмітити: десяткова форма запису IP-адреси використовується в основному в операційних системах як найбільш зручна під час налаштування. Окрім двійкової форми, часто зустрічається шістнадцятикова форма запису IP-адреси: **C0.94.1.3**.

Для зведення: використання 32-розрядних двійкових чисел дозволяє створювати 4 294 967 296 унікальних IP-адрес — більш ніж достатньо для будь-якої приватної інтрамережі (хоча мережа Internet скоро може почати випробовувати нестачу унікальних адрес, але про це пізніше).

Опис програми Cisco packet tracer

Packet Tracer - це інструмент від компанії Cisco, який дозволяє моделювати реальні комп'ютерні мережі. Нижче зображено вікно програми:

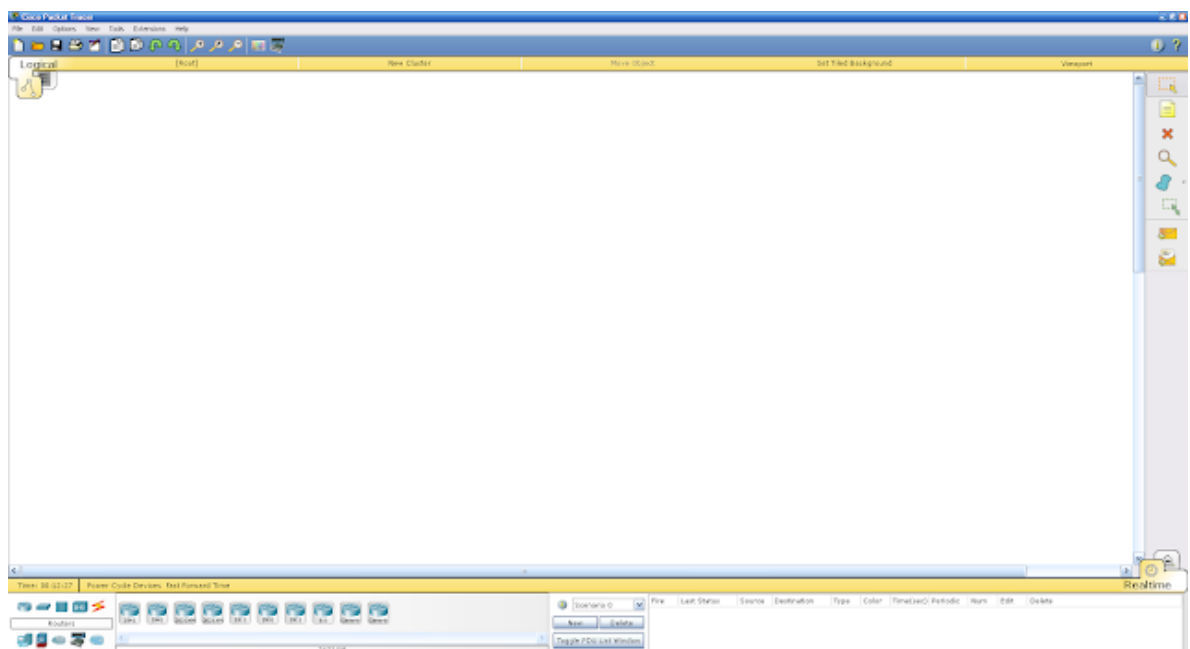


Рис. 6.1. Головне вікно програми

У верхній частині знаходиться головне меню. Воно містить такі кнопки: File, Edit, Options, View, Tools, Extensions, Help.



Рис.6.2. Головне меню

Категорія File містить стандартні пункти, такі як: створити новий файл, відкрити файл, зберегти файл, надрукувати файл, вийти.

Категорія Edit містить пункти: копіювати, вставити, скасувати попередню дію, виконати попередню дію.

Категорія Options містить пункти: налаштування користувача, користувацький профіль, налаштування алгоритмів, показати журнал логів.

Категорія View містить пункти: збільшення розміру схеми, відображення панелей.

В категорії Tools містяться пункти: панель малювання, діалог пристроїв. Категорія Extensions включає пункти: майстер активності, мультикористувач, ІРС, скриптинг (конфігурування скриптів та інтерфейсів), очистка терміналу, агент мультикористувача локальної мережі, агент мультикористувача глобальної мережі, UPnP мультикористувач. Під головним меню розташовується панель з найпотрібнішими і найбільш часто вживаними елементами головного меню.



Рис.6.3. Найуживаніші елементи головного меню

Цими елементами є: створити файл, відкрити файл, зберегти, надрукувати, майстер активності, копіювати, вставити, скасувати попередню дію, виконати попередню дію, збільшити зображення, відновити зображення, зменшити зображення, панель малювання, діалог пристроїв. Ще нижче розташовується перемикач між логічною та фізичною організацією мережі.

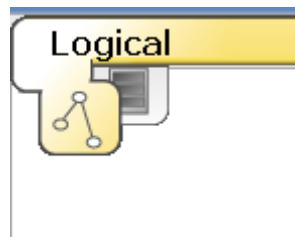


Рис.6.4. Перемикач між логічною та фізичною організацією мережі

При зміні на фізичну організацію мережі, порожній бланк замінюється на фізичну карту, на яку можна додавати міста, будівлі, шафи, встановлювати фон. Натомість у логічній організації можна додавати кластери.

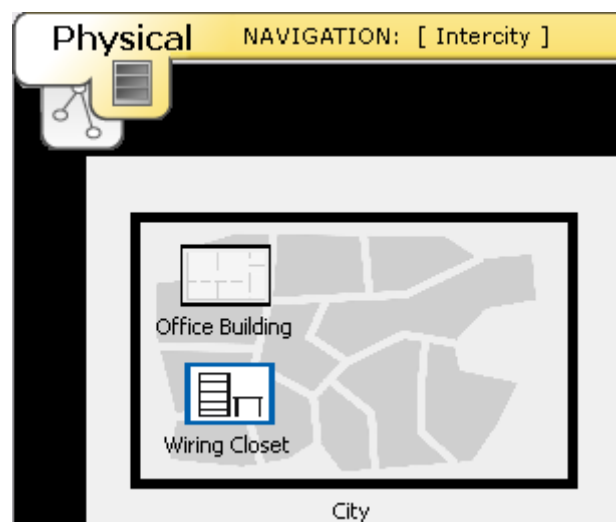


Рис. 6.5.Зміна організації мережі

З правої сторони знаходиться панель інструментів. На ній містяться кнопки: виділення елементів, додавання нотатки, видалення елементу, інспектування, малювання полігону, зміна розміру фігури і формування довільних пакетів.

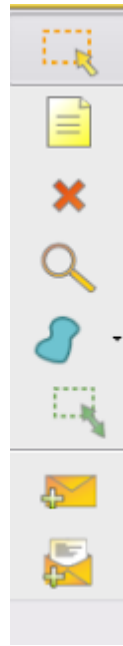


Рис.6.6. Панель інструментів

Знизу зправа міститься перемикач між реальним режимом і режимом моделювання. У режимі моделювання всі пакети, що пересилаються всередині мережі, відображаються в графічному вигляді. Ця можливість дозволяє мережевим спеціалістам наочно демонструвати, за якою інтерфейсом в даний момент рухається пакет, який протокол використовується тощо.

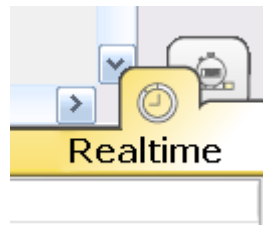


Рис.6.7. Перемикач між реальним режимом і режимом моделювання

Знизу зліва міститься панель з пристроями. На ній містяться різновиди хабів, світів, роутерів, бездротових девайсів, з'єднань, кінцевих пристроїв, безпеки, емуляція глобальної мережі, з'єднання мультитюзера, кастомні пристрої.



Рис.6.8. Панель з пристроями

Над панеллю вказується час роботи над проектом. По сусідству з панеллю знаходиться блок сценаріїв, в якому можна додавати, редагувати та видаляти сценарії мережі.

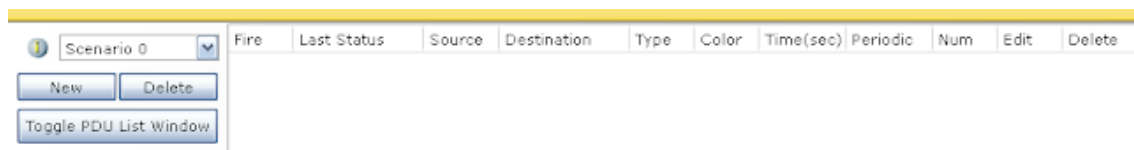


Рис.6.9. Блок сценаріїв

Додавати елементи на робочу схему можна простим перетягуванням з панелі пристроїв. Двічі натиснувши на назву пристрою можна її змінити. Один раз натиснувши на пристрій отримаємо фізичне зображення пристрою.

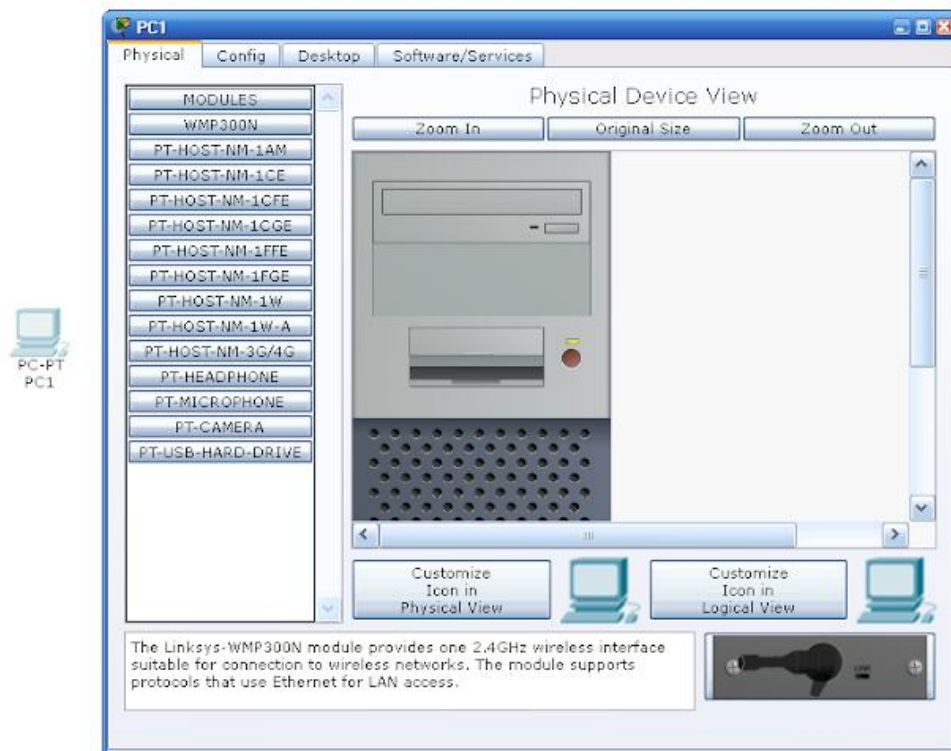


Рис.6.10. Фізичне зображення пристрою

Також шляхом перетягування можна додавати і видаляти фізичні компоненти. Також можна натискати кнопки. Наприклад, таким чином можна змінити конфігурацію комп'ютера до такого вигляду:



Рис.6.11. Зміна конфігурації комп'ютера

В інших категоріях можна налаштовувати пристрій, заходити на робочий стіл, налаштовувати програмне забезпечення і сервіси.

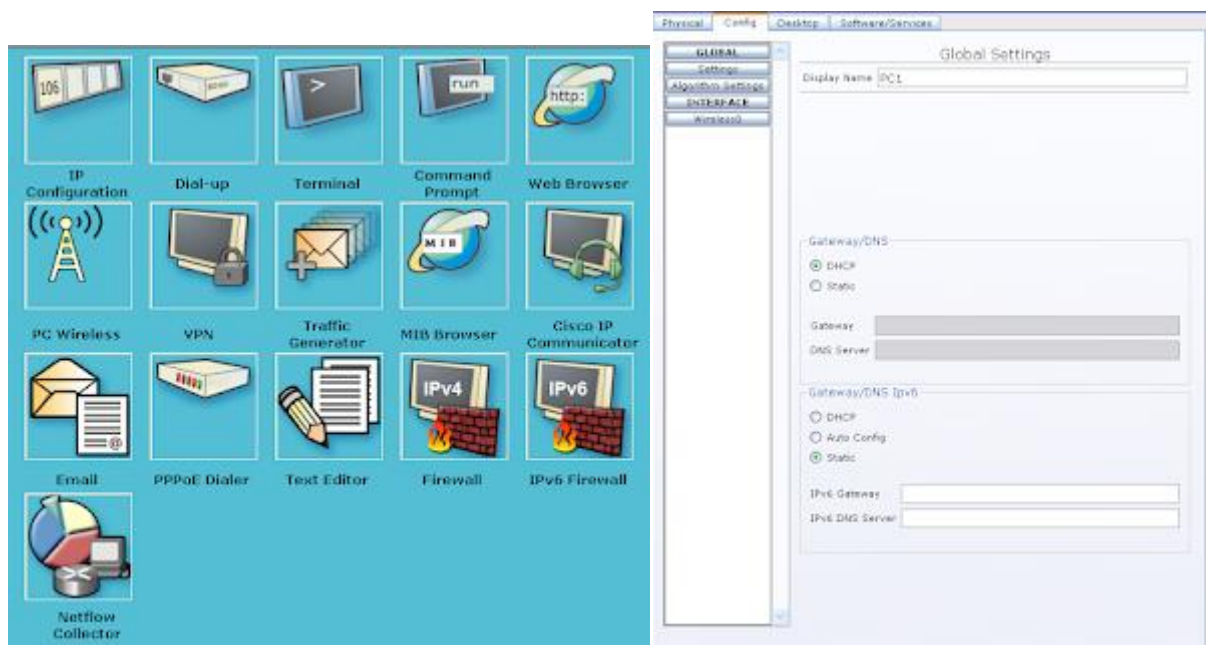


Рис.6.12. Налаштування програмного забезпечення і сервіси

Пристрої можна з'єднувати за допомогою пункту з'єднань на панелі пристроїв. Обираємо потрібне з'єднання, натискаємо на перший пристрій, в отриманому контекстному меню обираємо порт і під'єднуємо до іншого пристрої, також обираючи порт.



Рис.6.13.З'єднання пристроїв

В якості з'єднань можуть виступати:



- автоматичний тип - при даному типі з'єднання PacketTracer автоматично вибирає найбільш бажаний тип з'єднання для вибраних пристроїв
- консоль - консольні з'єднання
- мідь Пряме - з'єднання через мідний кабель типу вита пара, обидва кінці кабелю обтягуються в однаковій розкладці. Підійде для наступних сполучень: комутатор - комутатор, комутатор - маршрутизатор, комутатор - комп'ютер та ін.
- мідь кроссовер - з'єднання через мідний кабель типу вита пара, кінці кабелю обтягуються як кросовер. Підійде для з'єднання двох комп'ютерів.
- оптика - з'єднання за допомогою оптичного кабелю, необхідне для об'єднання пристроїв, що мають оптичні інтерфейси.
- телефонний кабель - звичайний телефонний кабель, може знадобитись для підключення телефонних апаратів.
- коаксіальний кабель - з'єднання пристроїв за допомогою коаксіального кабелю.

6.2 Порядок виконання роботи

Частина 1. Ознайомлення з програмою Packet Tracer 5.

- Запустити програму Packet Tracer 5, використовуючи меню Пуск.
- Інтерфейс виглядає таким чином (рис.6.14). Він складається з: Робоче поле – поле, в якому розміщується проект, що розробляється. Може знаходитися в двох станах: Real Time – "розробка проекту", Simulation – "режим симуляції роботи проекту".
- Меню.
- Панель пристроїв – знаходиться внизу вікна програми. Містить: вибір виду мережевого пристрою Routers (маршрутизатор), Hubs (концентратор) т. д) і вибір з'єднання мережевих пристроїв (вита пара, коаксіальний кабель і т. д). Перенесення необхідного пристрою на робочу область здійснюється за допомогою лівої кнопки мишки. З'єднання пристрою з пристроєм здійснюється за допомогою послідовного натиснення на пристрої, які необхідно з'єднати, лівою кнопкою миші вибору відповідного порту або роз'єму. Для правильного з'єднання роз'єми двох пристроїв повинні співпадати.

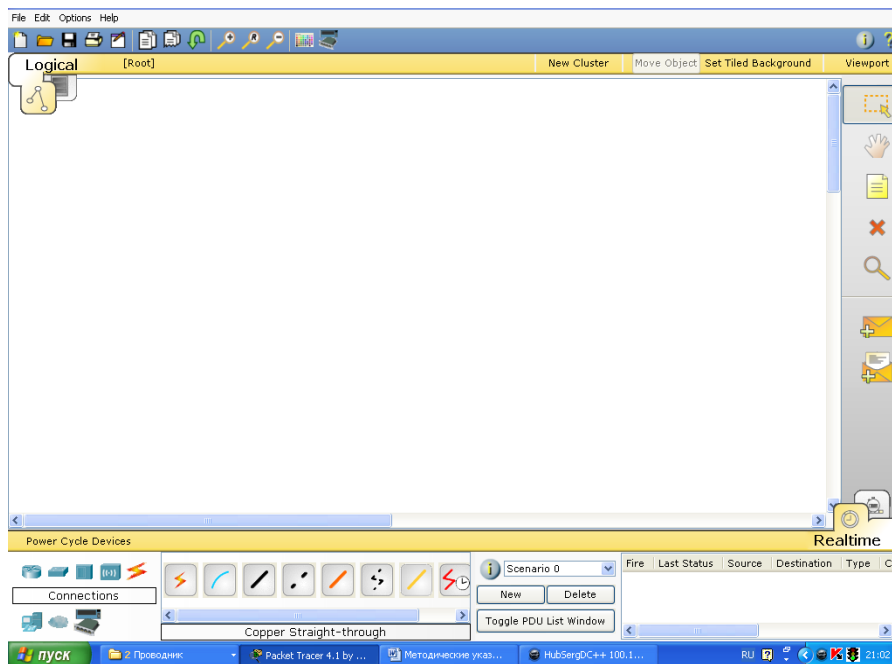


Рис. 6.14. Інтерфейс робочої програми

- **Панель сценаріїв** – знаходиться внизу вікна програми, містить усі

працюючі в даний момент сценарії і процеси, дозволяє управляти ними.

1. Зібрати наступний проект (рис 6.15), який містить: **4 ПК типу PC-PT, Концентратор (Hub-PT)**. Кожен комп'ютер має бути сполучений з концентратором за допомогою витії пари (**Copper Straight – Through**).

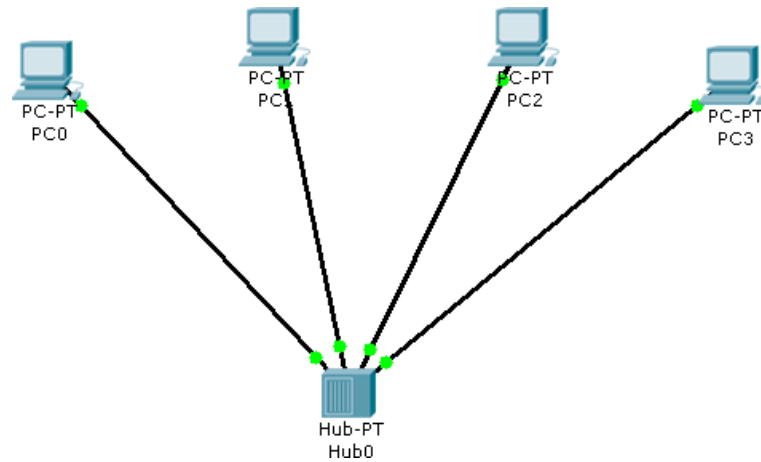


Рис. 6.15. Топологія 1

2. Зберегти проект і його скріншот.

3. 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**. У полі **ip address** необхідно ввести відповідну адресу, а в полі **SubnetMask** — що відповідає цій адресі — маску (рис. 6.16) або через вкладки **Desktop/Ip configuration** (рис. 6.4).

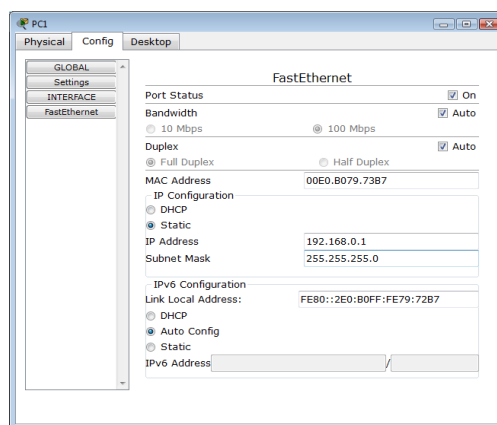


Рис. 6.16. Призначення адреси локальній машині

Значення IP-адреси для кожної машини наведені в табл. 6.1.

Таблиця 6.1.

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.

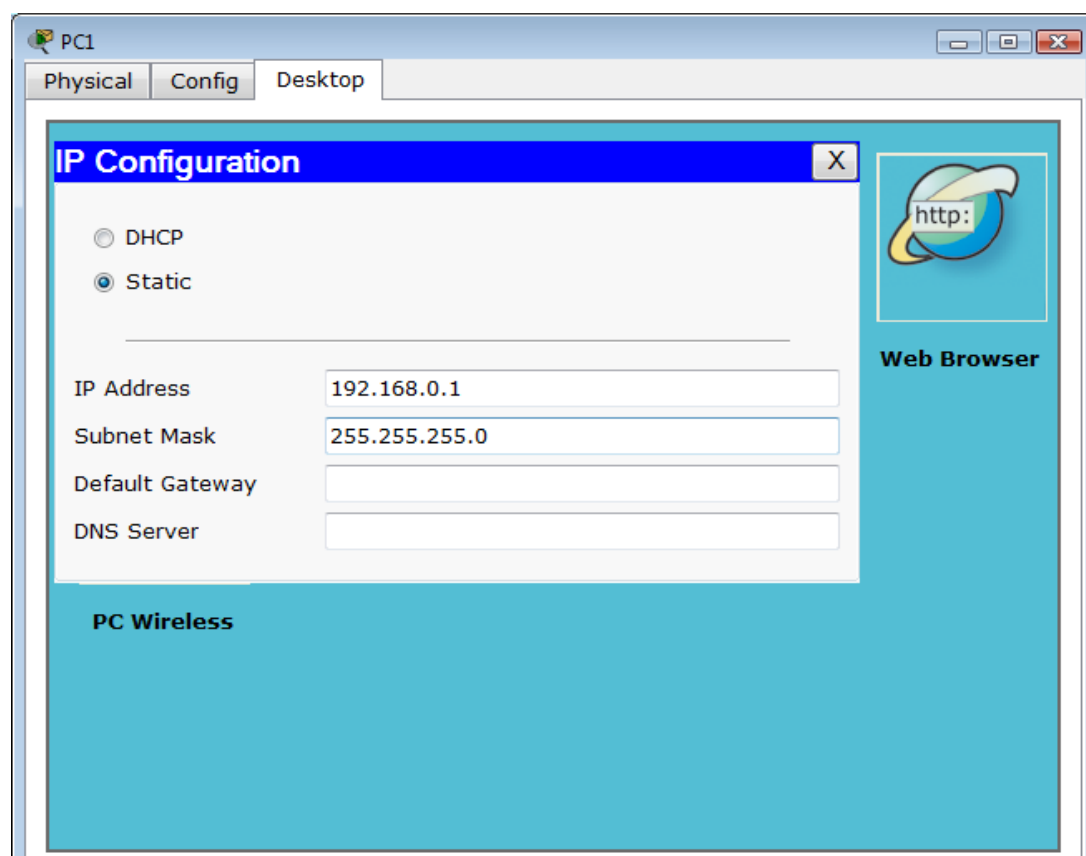


Рис. 6.17. Призначення адреси локальній машині через вкладку Робочий стіл

4. Перевірити працездатність отриманої мережі. Це робиться шляхом посилення мережевих запитів (*ICMP-пакетів*) від одного ПК до іншого. Для привласнення такого пакета ПК використайте кнопку **ADD SIMPLE PDU** в правій частині робочого вікна (рис. 6.18). Після цього клацніть лівою кнопкою

мишки на локальну машину-джерело, потім — на машину-одержувача. Перевірити працездатність мережевого шляху *PC0* і *PC3*.

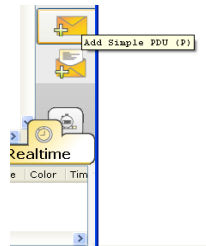


Рис. 6.18. Привласнення *ICMP*-пакета ПК

Результатом правильної роботи запиту посилки мережевих запитів (*ICMP-пакетів*) від одного ПК до іншого є поява в правому нижньому вікні повідомлення (рис. 6.19).

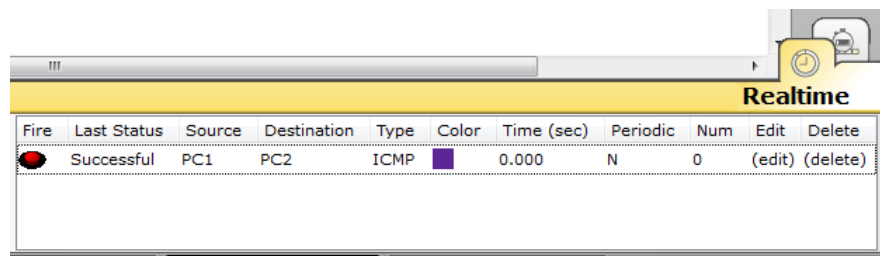


Рис. 6.19. Результат запиту *ICMP*-пакетів

5. Перейти в режим *Simulation* (рис. 6.20) і за допомогою кнопки *Even List* викликати вікно відображення подій у мережі *Simulation Panel*.

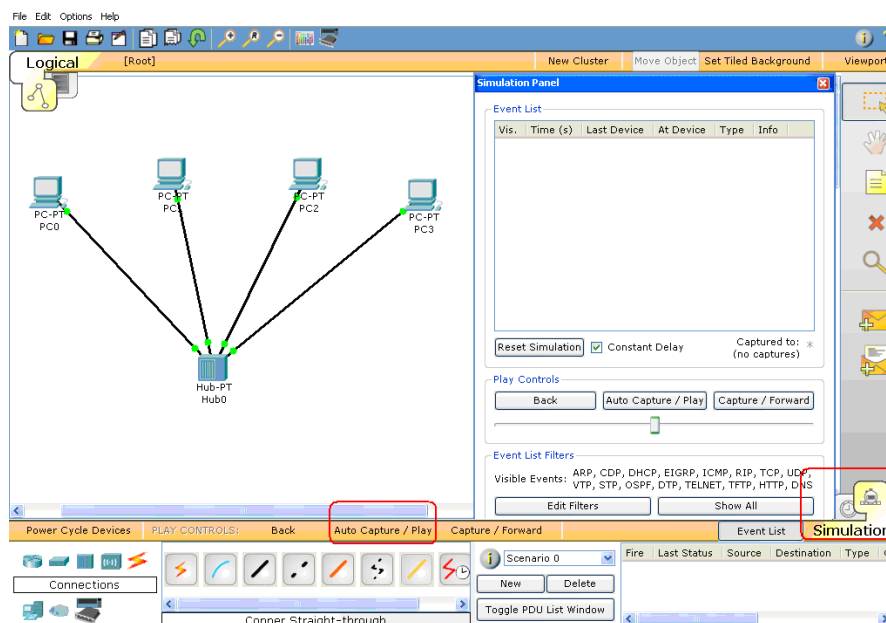


Рис. 6.20. Режим симуляції

6. Використовуючи кнопку *Auto Capture/Play* запустити симуляцію роботи

ICMP-пакетів. Простежити просування пакетів по мережі і зберегти цей скріншот.

7. Простежити за порядком і шляхом дотримання пакетів у вікні **Simulation Panel** (рис. 6.21). Відмітити періодичність посилення пакетів і їх поширення в мережі. Зберегти цей скріншот.

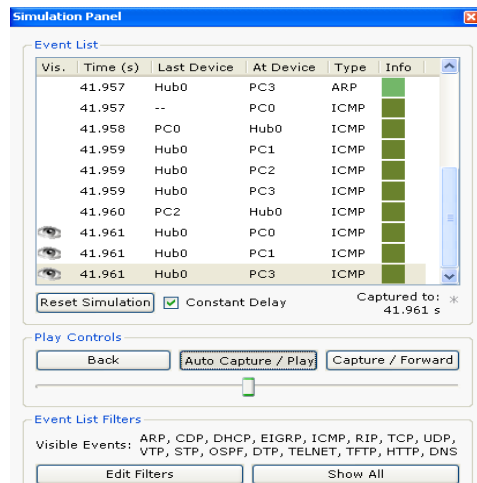


Рис. 6.21. Вид панелі *Simulation Panel*

8. Проглянути інформацію про пакети з вікна **Simulation Panel** і їх відповідність OSI моделі шляхом подвійного клацання по пакету у вікні (рис. 6.22). Ознайомитися з вмістом пакета і проаналізувати його призначення (рис. 6.23). Проаналізувати процес встановлення зв'язку між двома ПК. Результати зберегти у вигляді скріншоту.

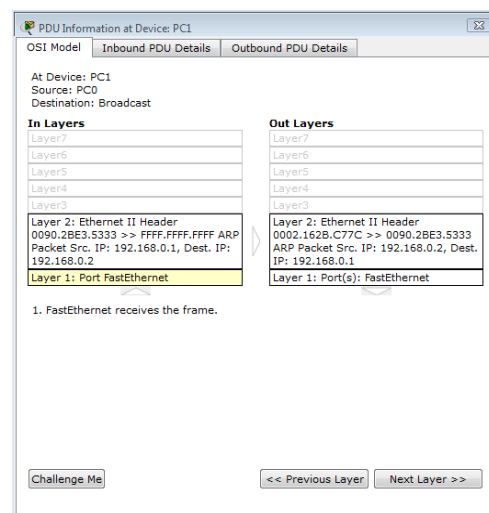


Рис. 6.22. Відповідність пакета моделі OSI пакету протоколу ARP

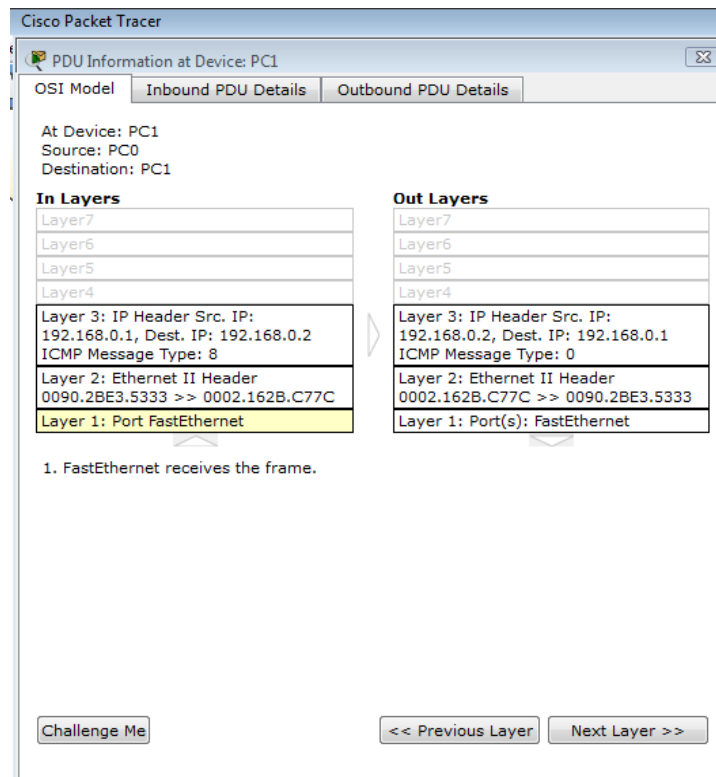


Рис. 6.23. Відповідність пакету моделі OSI пакету протоколу ICMP

Частина 2. Дослідження статичної маршрутизації

1. Зібрати проект (рис. 6.24), який містить: **3 ПК типу PC-PT**, **3 маршрутизатори (Router-PT)**.

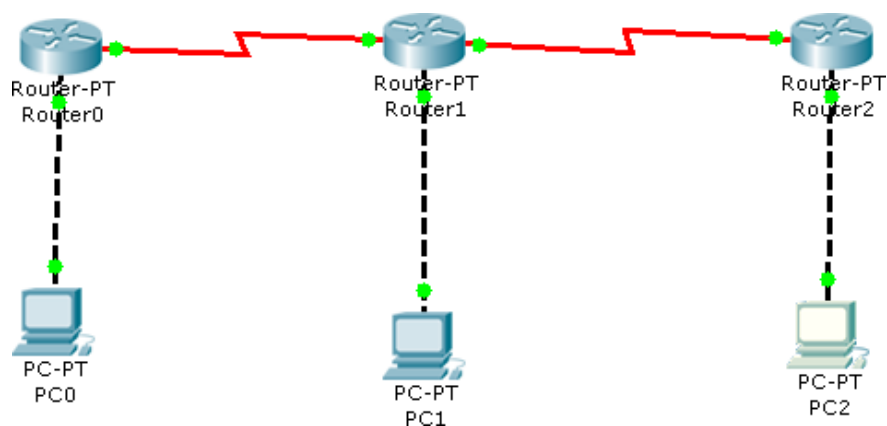


Рис. 6.24. Досліджувана топологія мережі 1

Кожен комп'ютер має бути сполучений з маршрутизатором за допомогою

кросового кабелю (*Copper Cross-over*), використовуючи порти *FastEthernet*.

Маршрутизатори з'єднати в топологію "шина" за допомогою спеціальних низькошвидкісних *Serial* портів і кабелю *Serial DCE Copper*. Кожному ПК присвоїти унікальну *IP-адресу*. Ці адреси наведені в табл. 6.2.

Таблиця 6.2

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

2. Маршрутизатор є активним мережевим пристроєм, тобто в цьому пристрої є функції перетворення мережевих адрес, що використовує таблицю маршрутизації. За допомогою маршрутизатора можна об'єднувати різні підмережі, що мають різні IP-адреси, наприклад, як у випадку на рис. 167. На відміну від комутаторів портам маршрутизатора призначаються унікальні IP-адреси (інтерфейси).

Приклад побудови мережі з 3 ПК і 3 маршрутизаторів.

Є три підмережі (клас C), в яких знаходиться 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 цих підмережах. Для цього потрібно задати IP-адреси вхідним (*FastEthernet*) і вихідним (*Serial*) портам маршрутизатора. Ці адреси наведені в табл. 6.3.

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, відповідно до адрес підмереж, які він обслуговує, призначаються відповідні інтерфейси. Для перегляду інтерфейсів необхідно навести курсор на необхідний маршрутизатор (рис. 6.25).

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	192.168.3.11/24	<not set>	0004.9A1E.3CB4
FastEthernet1/0	Up	<not set>	<not set>	0001.9610.AE84
Serial2/0	Up	192.168.10.2/24	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0001.C7C8.C3A9
FastEthernet5/0	Down	<not set>	<not set>	000B.BEB0.538D
Hostname: Router				
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet				

Рис. 6.25. Значення адрес інтерфейсів маршрутизатора

IP-адреси для портів маршрутизатора вводяться у вкладці **Config/Interface**. Необхідно також простежити, щоб статус робочого порту був активний (рис. 6.26).

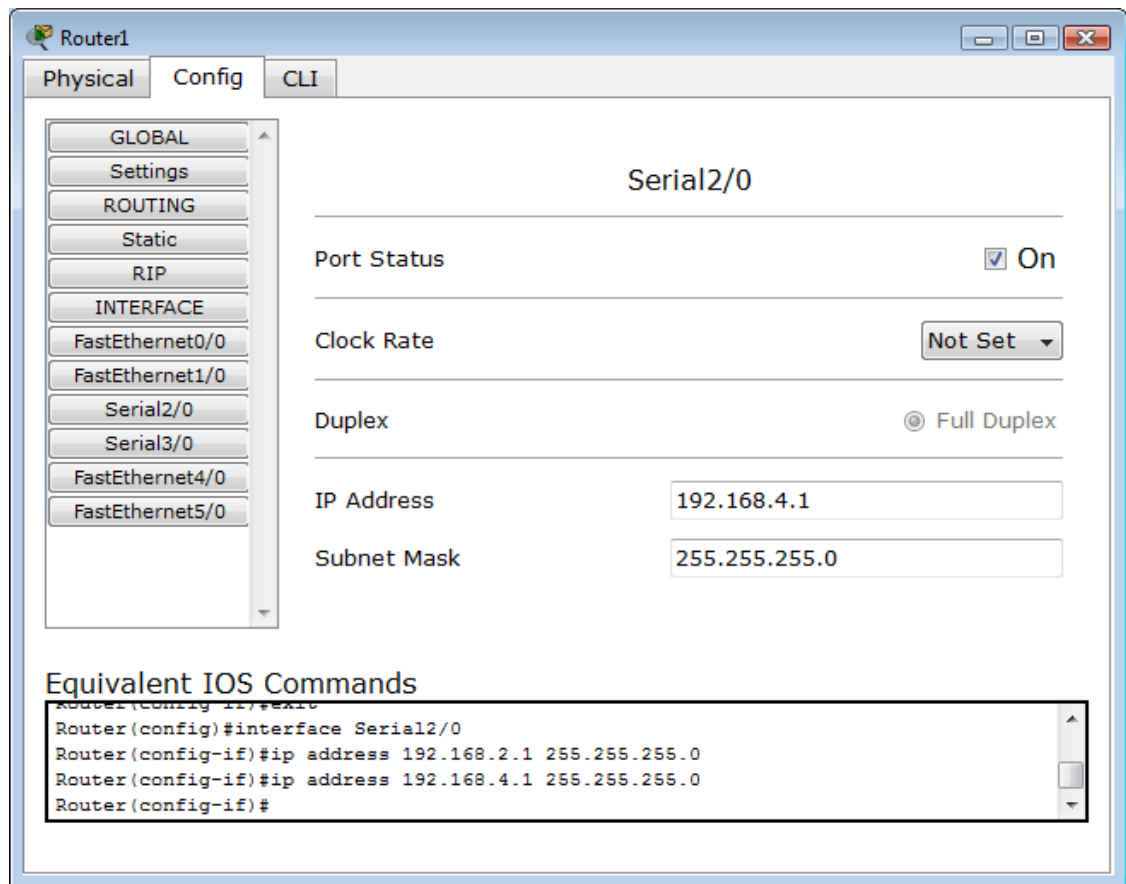


Рис. 6.26. Визначення параметрів одного з робочих портів маршрутизатора

3. Проставити для кожного ПК шлюз за замовчуванням. Це робиться у вкладці *Config/Global*. Для кожного ПК шлюзом за замовчуванням є та адреса порту маршрутизатора *FastEthernet*, з яким він сполучений. Ця дія сполучає локальну машину з активним мережевим пристроєм, в нашому випадку — з маршрутизатором.
4. Перевірити зв'язок між кожним ПК і маршрутизатором, використовуючи кроки, описані в пп. 5 — 9 частини 1.
5. Для кожного маршрутизатора призначити статичні маршрути, які зв'язуватимуть цей маршрутизатор з іншими підмережами. Для цього використовується вкладка конфігурації маршрутизатора *Config/Static*. Приклад призначення маршрутів для **Router 0** наведений на рис. 6.27.

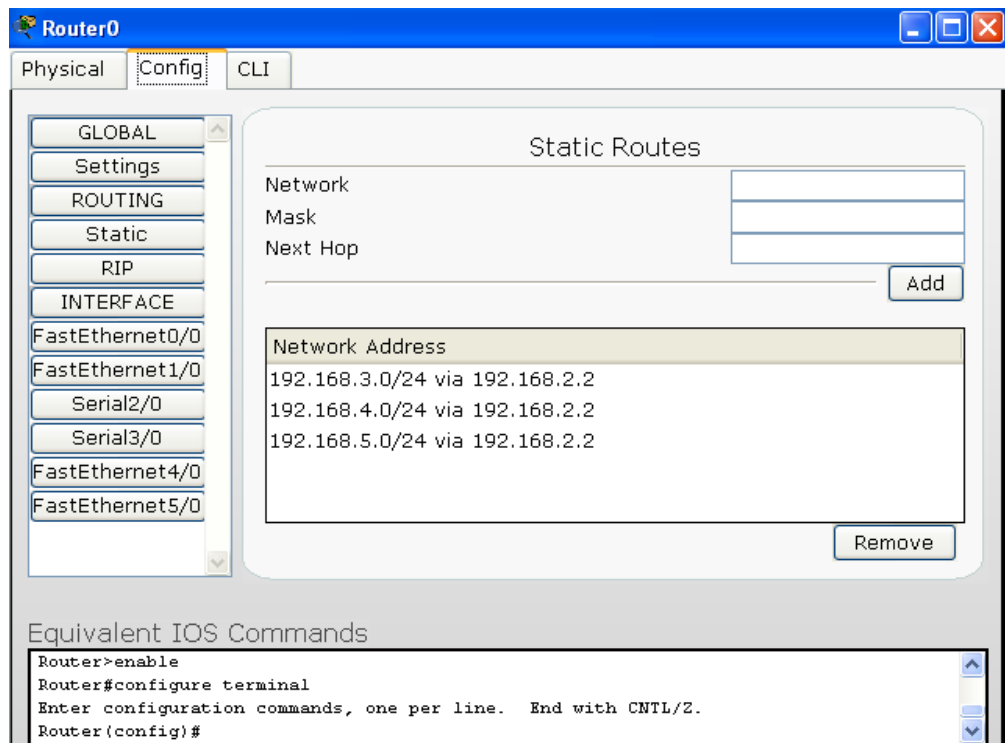


Рис. 6.27. Призначення статичних маршрутів

Потрібна підмережа задається у вкладці **Network**, маска підмережі в **Mask**, порт, через який робиться доступ до підмережі, прописується у вкладці **Next Hop**.

Наприклад, виходячи з рис. 6.24, у маршрутизаторі **Router 0** прописані три статичні маршрути – в підмережі 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 – підмережа **PC1**, 192.168.4.0 – підмережа між **Router 1** і **Router 2**, 192.168.5.0 – підмережа **PC2**. Аналогічним чином призначити статичні маршрути для інших маршрутизаторів. Використовуючи пп. 5 – 9 частини 1, перевірити працездатність зв'язку між **PC0-PC1**, **PC1-PC2**, **PC0-PC2**. Зберегти результати перевірки у вигляді скріншотів.

6. Створити новий проект (рис. 6.28). У цьому проекті на двох **Switch** створені підмережі, що складаються з трьох ПК. Маршрутизатори з'єднуються з комутаторами за допомогою витой пари (**Copper Straight – through**).

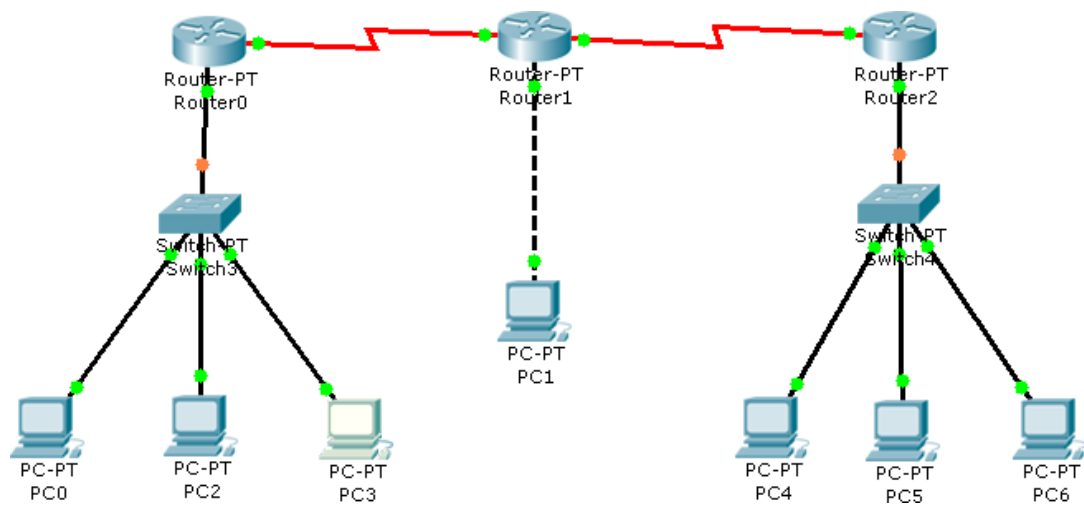


Рис. 6.28. Досліджувана топологія мережі 2

7. Кожному ПК присвоїти унікальну IP-адресу. Ці адреси наведені в табл. 6.4.

Таблиця 6.4

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 адрес: 255.255.255.0

Адреси портів маршрутизатора приведені в табл. 6.5.

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 адрес: 255.255.255.0

8. Визначити і проставити для кожного ПК шлюз за замовчуванням.
 9. Використовуючи пп. 5 – 9 частини 1 перевірити працездатність зв'язку між **PC0–PC4, PC2–PC5, PC3–PC0**. Виділити особливості встановлення зв'язку між крайовими вузлами. Зберегти результати перевірки у вигляді скріншоту.
 10. Виконати індивідуальне завдання відповідно до наступних варіантів (табл. 6.6). Під час виконання варіанта необхідно в кожному з підмереж включати не менше трьох РС.
- У процесі виконання завдань варіанта необхідно:
11. Вибрати базову мережу.
 12. Навести для кожної з масок підмереж діапазони адрес, що виділяються для РС. Звести отримані результати в таблицю.
 13. Розробити проект відповідно до п.п. 1 – 11, згідно з варіантом табл. 6.6.

Варіанти завдань

№ варіанта	Клас мережі	Маски	Кількість підмереж
1	B	20, 22, 23	11
2	C	24, 25, 29	10
3	B	17, 18, 19	9
4	C	24, 26, 28	11
5	B	16, 17, 20	10
6	C	25, 29, 31	9
7	B	20, 21, 23	11
8	C	26, 28, 31	10
9	B	18, 19, 21	9
10	C	26, 29, 30	11
11	B	16, 18, 20	10
12	C	24, 30, 31	9
13	B	16, 19, 22	11
14	C	27, 28, 29	10
15	B	17, 19, 21	9

6.3 Оброблення та аналізування результатів.

Оформлення звіту. При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

6.4 Контрольні питання

1. Що таке IP-адреса? Перелічіть її функції.
2. Що таке MAC-адреса? Перелічіть її функції.
3. У чому полягають функції ARP-пакета?

4. У чому полягають функції ICMP-пакета?
5. Перерахуйте види статичних маршрутів? Охарактеризуйте їх переваги, недоліки, сфери використання.

ПРАКТИЧНА РОБОТА №7

ДІАГНОСТИКА IP-ПРОТОКОЛУ

Мета та основні завдання роботи: навчитися перевіряти працездатність мережевого підключення.

Вивчити та стисло описати у протоколі практичної роботи:

— основні команди для перевірки працездатності мережевого підключення.

7.1 Теоретичні відомості

Існують різні утиліти, що дозволяють швидко продіагностувати IP-підключення. Однак більшість операцій легко може бути виконано з використанням команд самої операційної системи.

Користувачі *Windows XP* для діагностики мережного підключення можуть скористатися спеціальним майстром. Ця програма викликається з меню завдання Відомості про систему (Пуск> Всі програми> Стандартні>Службові> Відомості про систему> меню Сервіс> Діагностика мережі).

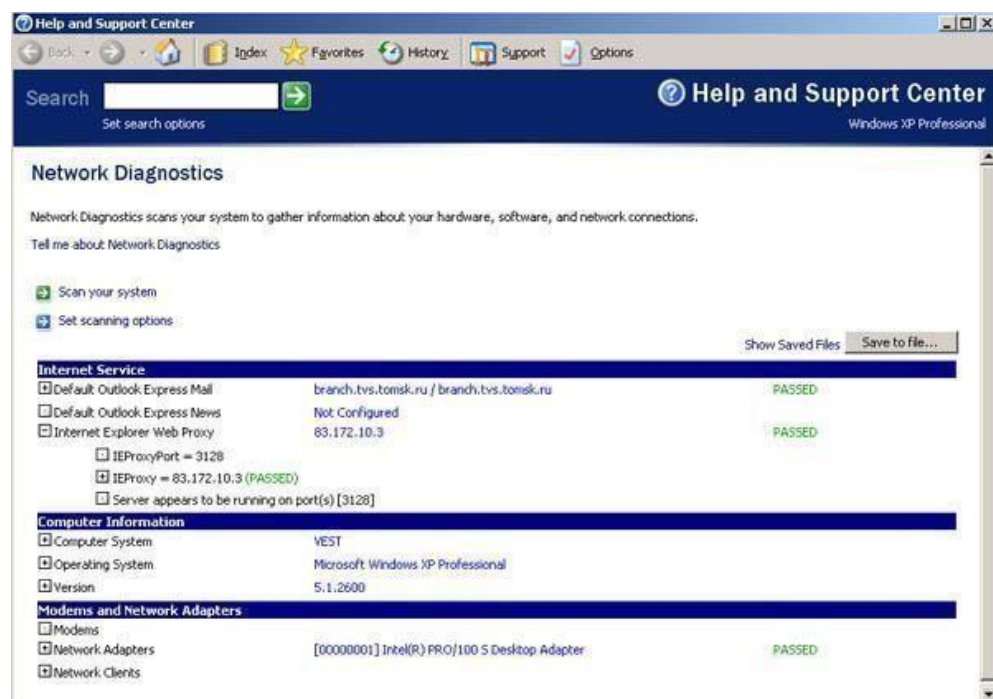


Рис.7.1. Вікно стану мережі

Команда *Ipconfig*

Для відображення параметрів IP-протоколу використовуються утиліти **ipconfig** (Windows NT / 2000 / XP). Ця утиліта виводить на екран основні параметри настройки протоколу TCP / IP: значення адреси, маски, шлюзу.

1. Для відображення параметрів IP-протоколу потрібно натиснути кнопку *Пуск*, обрати рядок меню *Виконати*, набрати символи *cmd* і натиснути клавішу Enter на клавіатурі.

2. У вікні потрібно набрати *ipconfig / all*. При нормальній роботі комп'ютера на екран повинен вивестися приблизно такий лістинг:

```
Windows IP Configuration
```

```
Host Name . . . . . : vest Primary Dns
Suffix . . . . . :
tvs.tomsk.ru Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : tvs.tomsk.ru
tomsk.ru
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : tvs.tomsk.ru
Description . . . . . : Intel(R) PRO/100 S Desktop
Adapter . . . . . :
Physical Address. . . . . : 00-02-B3-8D-44-53
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 83.172.10.54
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 83.172.10.254
DHCP Server . . . . . : 83.172.10.2
DNS Servers . . . . . : 192.168.0.1
                        83.172.10.2
Primary WINS Server . . . . . : 83.172.10.2
Secondary WINS Server . . . . . : 213.183.109.3
Lease Obtained. . . . . : 24 августа 2004 г. 9:40:41
Lease Expires . . . . . : 27 октября 2004 г. 9:40:41
```

Команда *Ping*

Дана команда призначена для перевірки доступності віддаленого вузла по мережі. Для цього використовується службовий протокол ICMP. З локальної машини на віддалений вузол надсилається запит з кодом "echo-request" і протягом деякого часу локальна машина чекає на відповідь "echo-reply". Якщо

така відповідь не отримана, то причин може бути кілька:

- 1) якщо отримано діагностичне повідомлення по протоколу ICMP, то необхідно проаналізувати це повідомлення (наприклад, потрібна фрагментація пакета);
- 2) якщо нічого не отримано, то віддалений вузол не відповідає на запит (не включений або на вузлі відповідь блокує брандмауер), або час проходження пакетів по лінії зв'язку більше ніж час очікування відповіді - в цьому випадку слід збільшити час очікування.

У найпростішому випадку в якості аргументу команді необхідно вказати ім'я вузла (DNS-ім'я або NetBIOS-ім'я) або IP-адреса вузла, наприклад: `ping 10.20.30.40`

Для перевірки доступності віддаленого вузла по мережі потрібно відкрити командний рядок і виконати команду `ping 127.0.0.1`

Адреса 127.0.0.1 - це особистий адреса будь-якого комп'ютера. Таким чином, ця команда перевіряє проходження сигналу "на самого себе". Вона може бути виконана без наявності будь-якого мережевого підключення. Ви повинні побачити приблизно такі рядки:

```
Pinging 127.0.0.1 with 32 bytes of data:
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 Reply from 127.0.0.1: bytes=32
time<1ms TTL=128 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 Reply from
127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 127.0.0.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times
in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

За замовчуванням команда посилає пакет 32 байта. Розмір пакета може бути збільшений до 65 кбайт. Так можна виявити помилки при пересиланні пакетів великих розмірів. За розміром тестового пакета відображається час відгуку віддаленої системи (в нашому випадку - менше 1 мілісекунди). Потім показується ще один параметр протоколу - значення TTL. TTL - "час життя"

пакета. На практиці це число маршрутизаторів, через які може пройти пакет. Кожен маршрутизатор зменшує значення TTL на одиницю. При досягненні нульового значення пакет знищується. Такий механізм запроваджено для виключення випадків зациклення пакетів.

Якщо буде показано повідомлення про недосяжність адресата, то це означає помилку установки протоколу IP. У цьому випадку доцільно видалити протокол з системи, перезавантажити комп'ютер і знову встановити підтримку протоколу TCP / IP.

Для перевірки видимості локального комп'ютера і найближчого комп'ютера мережі потрібно виконати команду `ping 192.168.0.19`.

На екрані повинні бути виведені приблизно такі рядки:

```
Pinging 212.73.124.100 with 32 bytes of data:
```

```
Reply from 192.168.0.19: bytes=32 time=5ms TTL=60 Reply from 192.168.0.19:
bytes=32 time=5ms TTL=60 Reply from 192.168.0.19: bytes=32 time=4ms TTL=60 Reply
from 192.168.0.19: bytes=32 time=4ms TTL=60
```

```
Ping statistics for 212.73.124.100:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times
in milli-seconds:
```

```
Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

Наявність відгуку свідчить про те, що канал зв'язку встановлений і працює.

Серед додаткових опцій команда **ping** приймає ключ **-f**, який забороняє фрагментацію IP-пакетів. Так як мережевий рівень абстрагується від використовуваної технології канального рівня, то необхідний механізм, за допомогою якого можна передавати блоки даних довільної довжини через різні транспортні мережі з їх власними технологіями канального рівня, які мають різні обмеження на розмір кадру (MTU). У разі якщо пакет даних плюс службові заголовки перевищує розмір кадру, то пакет розбивається на фрагменти, які вже можуть бути передані в кадрах канального рівня. На кінцевому вузлі фрагменти збираються в єдиний пакет даних.

Друга опція команди - це ключ **-l**, після якого через пробіл вказується цифра - розмір буфера, який буде надсилатися на віддалений вузол в пакеті

ICMP. Використовуючи спільно ключі **-l** і **-f** можна з'ясувати максимальний розмір блоку даних, поміщеного в IP-пакет, який ще інакше називається MSS (максимальний розмір сегмента). MSS буде дорівнює довжині блоку даних + довжина ICMP заголовка, який дорівнює 8 байт в разі команди `ping`. Розмір стандартного заголовка IP-пакета дорівнює 20 байт. Таким чином $MTU = \text{"розмір буфера команди ping"} + 8 + 20$.

Ще один ключ команди - це ключ **-a**, який дозволяє отримати ім'я DNS за адресою комп'ютера (як правило IP-адресою).

Наступний ключ команди - це ключ **-i**, який дозволяє задати TTL - «час життя» посилаються пакетів. Для вирішення проблем наявності петель в маршрутизації і, відповідно, нескінченної циркуляції IP-пакетів в мережі, кожен посилається пакет має поле TTL, яке містить деяке ціле число. Це число зменшується на одиницю при кожному проходженні пакета маршрутизаторів. У той момент, коли значення TTL стане рівним 0, такий пакет відкидається, а відправнику по протоколу ICMP надсилається повідомлення про те, що пакет відкинутий через нульовий TTL. За рекомендацією RFC 1700 початкове значення TTL має бути 64. Таким чином, це забезпечує проходження пакетом до 63 проміжних маршрутизаторів. Різні операційні системи можуть вибирати початкове значення TTL по-різному.

Команда Tracert

При роботі в мережі одні інформаційні сервери відгукуються швидше, інші повільніше, бувають випадки недосяжності бажаного хосту. Для з'ясування причин подібних ситуацій можна використовувати спеціальні утиліти.

Наприклад, команда **tracert**, яка зазвичай використовується для показу шляху проходження сигналу до бажаного хосту. Найчастіше це дозволяє з'ясувати причини поганої працездатності каналу. Точка, після якої час відгуку різко збільшено, свідчить про наявність "вузького місця", що не справляється з навантаженням.

Для показу шляху проходження сигналу до бажаного хосту в командному рядку потрібно ввести команду `tracert 192.168.0.19`

Відобразиться лістинг:

```
Tracing route to 192.168.0.19 over a maximum of 30 hops:
1             <1 ms      <1 ms      <1 ms    192.168.0.19
Trace complete.
```

Команда Route

Команда `Route` дозволяє переглядати маршрути проходження мережових пакетів при передачі інформації. Для виведення на екран таблиці маршрутів TCP / IP потрібно ввести в командному рядку **`route print`**.

Команда Net view

Виводить список доменів, комп'ютерів або загальних ресурсів на даному комп'ютері. Викликана без параметрів, команда **`net view`** виводить список комп'ютерів в поточному домені.

Команда Net send

Служить для відправки повідомлень іншому користувачу комп'ютера, що доступний в мережі.

Команда arp

Дана утиліта дозволяє отримати таблицю відповідності IP-адрес і MAC-адрес. У зв'язку з тим, що мережовий рівень вводить свою систему адрес, унікальних в межах всієї складової мережі, то необхідний механізм, за допомогою якого можна перетворювати IP-адреси в апаратні адреси канального рівня, що використовується у транспортній мережі.

У разі якщо IP-адреса призначення знаходиться в підмережі, підключеної безпосередньо до одного з мережових інтерфейсів комп'ютера (тобто не

використовуючи шлюз), то відправник може відправити пакет даних

«безпосередньо. Для цього відправник посилає в відповідний мережевий інтерфейс (згідно з таблицею маршрутизації) циркулярний запит по протоколу ARP, що містить наступні дані:

- MAC-адресу джерела
- IP-адреса джерела
- шукана IP-адреса

Той комп'ютер, який володіє потрібною IP-адресою, відповідає на запит. При цьому результат опитування, тобто MAC-адреса кінцевого комп'ютера, зберігається у таблиці ARP відправника протягом деякого часу, після якого запис видаляється. Кінцевий комп'ютер так само зберігає у своїй таблиці ARP відповідність IP-адреси і MAC-адресу відправника. Якщо ж віддалений вузол можна досягти через шлюз, то пакет передається йому, і він приймає рішення про метод доставки кінцевому вузлу. В цьому випадку ARP запит буде посланий для з'ясування апаратної адреси шлюзу.

Для отримання таблиці ARP, необхідно запустити команду **arp** з ключем - **a**, тобто **arp -a**.

Команда netstat

Якщо запустити команду **netstat** без параметрів, то можна отримати список активних TCP з'єднань між локальним і віддаленими комп'ютерами. У колонці "стан" відображається статус TCP-з'єднання.

За замовчуванням **netstat** виконує перетворення отриманих IP-адрес в символні імена DNS і номери портів в назву мережевих служб. Це уповільнює роботу **netstat**, тому якщо перетворення не вимагається, то можна вказати ключ -**n**.

Якщо вказати ключ **-a**, то в списку з'єднань будуть вказані також і порти, що прослуховуються комп'ютером TCP і UDP.

Команда telnet

Дана програма спочатку була призначена для реалізації сеансів віддаленого терміналу з комп'ютером по мережі по протоколу telnet. Як «побічний» ефект утиліти можна відзначити її здатність перевіряти порти протоколу TCP, що прослуховуються. Формат виконання команди наступний:
telnet хост порт

Хост - це віддалений комп'ютер, порт - це номер TCP-порту.

Таблиця 7.1

Значення номерів портів широко відомих мережевих служб

Порт	Служба	Протокол
25	Почтовий сервіс	SMTP
110	Почтовий сервіс	POP
143	Почтовий сервіс	IMAP
80	Веб-сервер	HTTP
443	Веб-сервер поверх SSL	HTTPS
21	Передача файлів	FTP

7.2 Порядок виконання

В ході виконання практичної роботи Ви познайомитеся з утилітами, що запускаються з командного рядка, що дозволяють детально продіагностувати працездатність підключення Вашого комп'ютера до мережі.

1. Виконайте команду **ipconfig** і запишіть інформацію про IP-адресу, маску мережі і шлюзі за замовчуванням для мережевого адаптера.
2. Виконайте команду **ipconfig / all** і запишіть інформацію про апаратне адресу мережевої карти, списку DNS-серверів мережевого підключення.
3. Отримайте таблицю маршрутизації локального комп'ютера за

допомогою команди **route print**.

4. Отримайте список комп'ютерів своєї робочої групи за допомогою команди **net view**.
5. Отримайте таблицю **arp** локального комп'ютера.
6. Отримайте список активних TCP-з'єднань локального комп'ютера.
7. Отримайте список активних TCP-з'єднань локального комп'ютера без перетворення IP-адрес в символні імена DNS.
8. Отримайте список портів, що прослуховує комп'ютер TCP і UDP з і безперетворення IP-адрес в символні імена DNS.

7.3 Оброблення та аналізування результатів. Оформлення звіту.

При оформленні звіту з практичної роботи до заздалегідь підготованого протоколу (див. завдання до самостійної роботи) додаються роздруковані аркуші з результатами виконаної роботи (скріншоти).

7.4 Контрольні питання

1. Для чого призначена команда **ipconfig**?
2. Для чого призначена команда **ping**?
3. Для чого призначена команда **route**?
4. Для чого призначена команда **tracert**?
5. Для чого призначена команда **arp**?
6. Для чого призначена команда **net send**?
7. Для чого призначена команда **net view**?
8. Для чого призначена команда **net send**?

ПРАКТИЧНА РОБОТА 8

КОНФІГУРУВАННЯ DHCP-СЕРВЕРА

Мета та основні завдання роботи: навчитися конфігурувати DHCP-сервер для автоматичного призначення IP-адрес робочих станцій (PC) комп'ютерної мережі в заданих діапазонах.

Вивчити та стисло описати у протоколі практичної роботи:

- роботу DHCP-сервера.

8.1 Теоретичні відомості

DHCP (англ. Dynamic Host Configuration Protocol - протокол динамічної настройки вузла) - мережевий протокол, що дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP. Даний протокол працює по моделі «клієнт-сервер».

Для автоматичної конфігурації комп'ютер-клієнт на етапі конфігурації мережевого пристрою звертається до так званого сервера DHCP, і отримує від нього потрібні параметри.

Адміністратор може задати діапазон адрес, що розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі і зменшує кількість помилок. Протокол DHCP використовується в більшості мереж TCP / IP.

DHCP є розширенням протоколу BOOTP, що використовувався раніше для забезпечення бездискових робочих станцій IP-адресами при їх завантаженні.

DHCP зберігає зворотну сумісність з BOOTP.

Протокол DHCP надає три способи розподілу IP-адрес:

Ручний розподіл. При цьому способі мережевий адміністратор зіставляє апаратного адресою (для Ethernet мереж це MAC-адресу) кожного клієнтського комп'ютера певний IP-адреса.

Фактично, даний спосіб розподілу адрес відрізняється від ручної настройки кожного комп'ютера лише тим, що відомості про адреси зберігаються централізовано (на сервері DHCP), і тому їх простіше змінювати при необхідності.

Автоматичний розподіл. При даному способі кожного комп'ютера на постійне використання виділяється довільний вільний IP-адреса з певного адміністратором діапазону.

Динамічний розподіл. Цей спосіб аналогічний автоматичному розподілу, за винятком того, що адреса видається комп'ютера не так на постійне користування, а на певний термін. Це називається орендою адреси. Після закінчення терміну оренди IP-адреса знову вважається вільним, і клієнт зобов'язаний запросити новий (він, втім, може виявитися тим же самим). Крім того, клієнт сам може відмовитися від отриманої адреси.

Приклад процесу отримання адреси.

Розглянемо приклад процесу отримання IP-адреси клієнтом від сервера DHCP. Припустимо, клієнт ще не має власного IP-адреси, але йому відомий його попередній адресу - 192.168.1.100. Процес складається з чотирьох етапів.

1. Виявлення DHCP

Спочатку клієнт виконує циркулярний запит по всій фізичної мережі з метою виявити доступні DHCP-сервери.

Він відправляє повідомлення типу DHCPDISCOVER, при цьому в якості IP-адреси джерела вказується 0.0.0.0 (так як комп'ютер ще не має власного IP-адреси), а в якості адреси призначення - ширококомовна адреса 255.255.255.255.

Клієнт заповнює кілька полів повідомлення початковими значеннями:

В поле xid поміщається унікальний ідентифікатор транзакції, який дозволяє відрізнити даний процес отримання IP-адреси від інших, протікають в той же час.

В поле chaddr поміщається апаратну адресу (MAC-адресу) клієнта.

В поле опцій вказується останній відомий клієнту IP-адреса. В даному прикладі це 192.168.1.100.

Це необов'язково і може бути проігноровано сервером.

Повідомлення DHCPDISCOVER може бути поширене за межі локальної фізичної мережі за допомогою спеціально налаштованих агентів ретрансляції DHCP, що перенаправляє надходять від клієнтів повідомлення DHCP серверів в інших підмережах.

Не завжди процес отримання IP адреси починається з DHCPDISCOVER.

У разі, якщо клієнт раніше вже отримував IP адреса і термін його оренди ще не пройшов - клієнт може пропустити стадію DHCPDISCOVER почавши з запиту DHCPREQUEST відправляється з ідентифікатором сервера, який видав адресу в минулий раз. У разі ж відсутності відповіді від DHCP сервера, яка видала настройки в минулий раз, клієнт відправляє DHCPDISCOVER. Тим самим, клієнт починає процес отримання з початку, звертаючись уже до всіх DHCP серверів у тій частині мережі.

2. Пропозиція DHCP

Отримавши повідомлення від клієнта, сервер визначає необхідну конфігурацію клієнта відповідно до зазначених мережевим адміністратором настройками.

В даному випадку DHCP-сервер згоден з запитаним клієнтом адресою 192.168.1.100. Сервер відправляє йому відповідь (DHCPOFFER), в якому пропонує конфігурацію. Пропонований клієнту IP-адреса вказується в поле yiaddr. Інші параметри (такі, як адреси маршрутизаторів і DNS-серверів) вказуються у вигляді опцій у відповідному полі.

Це повідомлення DHCP-сервер відправляє хосту, який послав DHCPDISCOVER, на його MAC, при певних обставинах повідомлення може поширюватися як ширококомовлення. Клієнт може отримати кілька різних пропозицій DHCP від ??різних серверів; з них він повинен вибрати те, яке його «влаштовує».

3. Запит DHCP

Вибравши одну з конфігурацій, запропонованих DHCP-серверами, клієнт відправляє запит DHCP (DHCPREQUEST). Він розсилається ширококомовно; при

цьому до опцій, зазначеним клієнтом в повідомленні DHCPDISCOVER, додається спеціальна опція - ідентифікатор сервера - вказує адресу DHCP-сервера, обраного клієнтом (в даному випадку - 192.168.1.1).

4. Підтвердження DHCP

Нарешті, сервер підтверджує запит і направляє це підтвердження (DHCPACK) клієнту. Після цього клієнт повинен налаштувати свій мережевий інтерфейс, використовуючи надані опції.

8.2 Порядок виконання роботи

Дослідження роботи DHCP-сервера здійснюється на віртуальній машині, встановленій на даній РС. Для установки серверів будемо використовувати *Microsoft Windows Server 2003*.

Необхідно провести налаштування VMWare Player. Встановити режим роботи мережевого адаптера "Host only", для віртуальної машини з Windows Server, вибрати та підключити у віртуальний CD/DVD привод файл "ru_win_srv_2003_r2_enterprise_with_sp2_vl_cd1_X13-46484.iso" який містить необхідні інсталяційні файли (рис. 8.1 – 8.3).

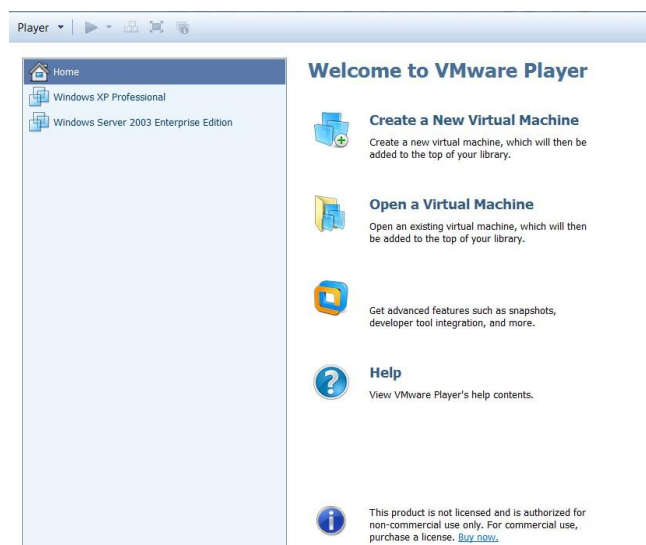


Рис. 8.1. Запуск VMware Player

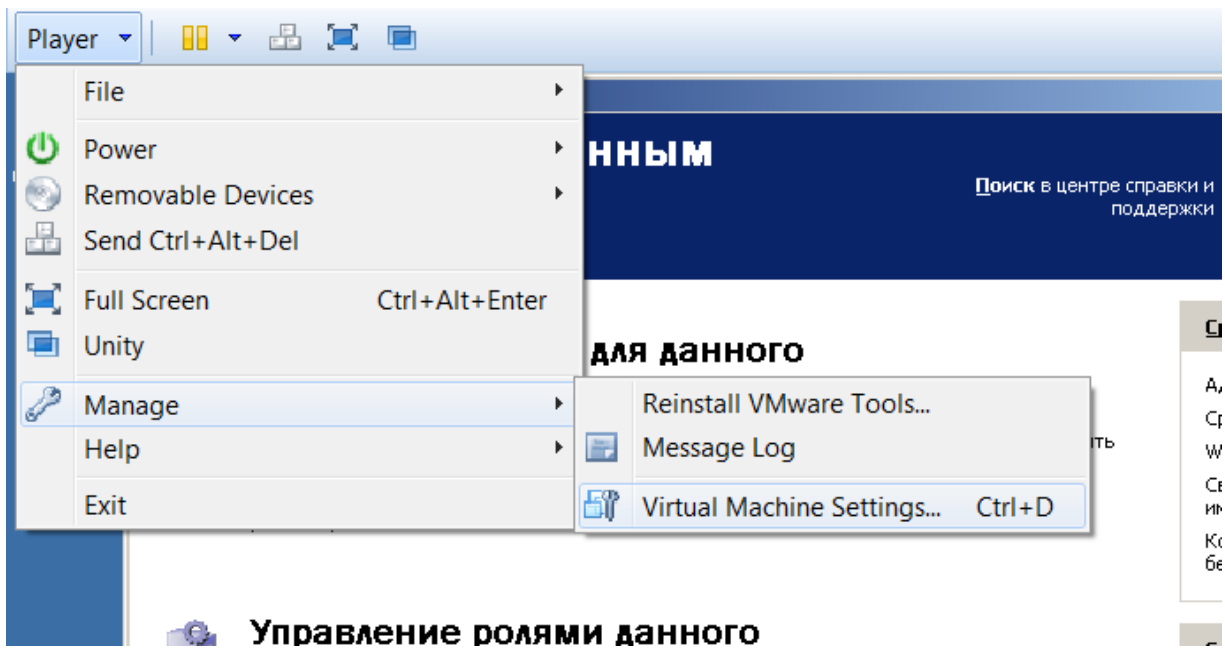


Рис. 8.2. Меню налаштувань

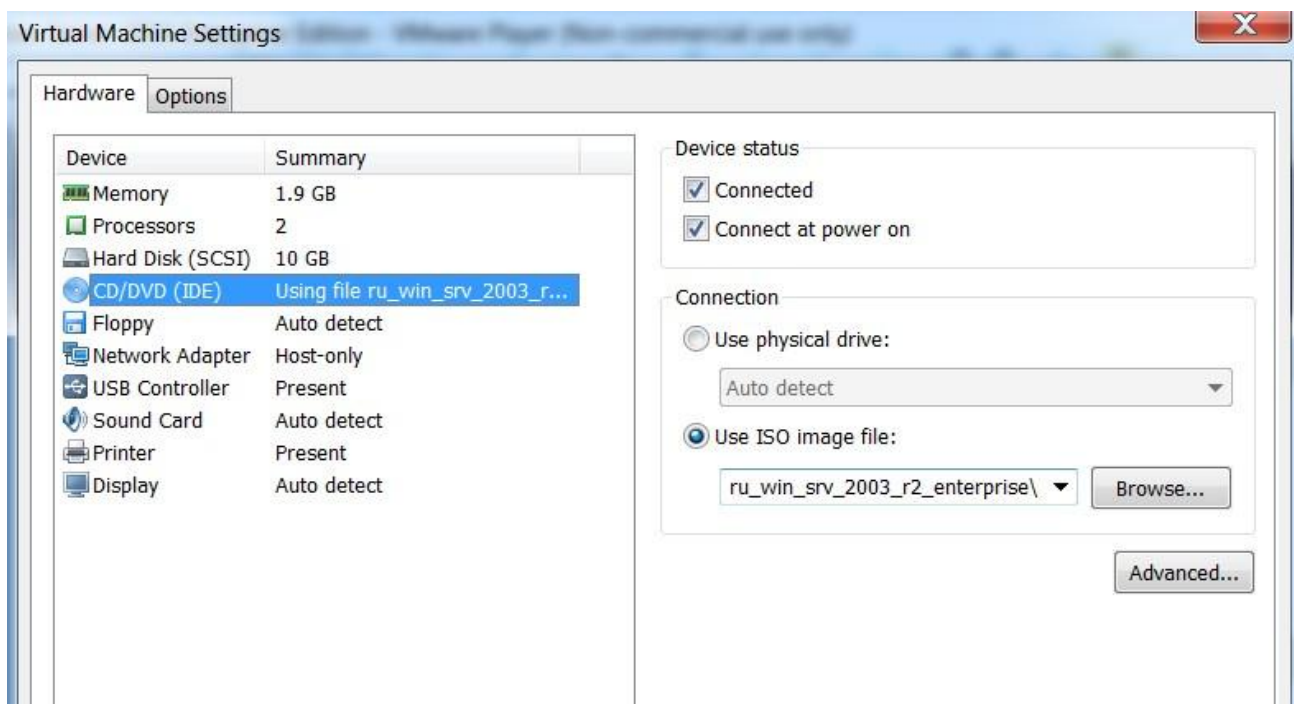


Рис.8.3. Перевірка налаштувань CD/DVD привода

Для конфігурування DHCP-сервера необхідно встановити IP-адресу Windows Server 2003.

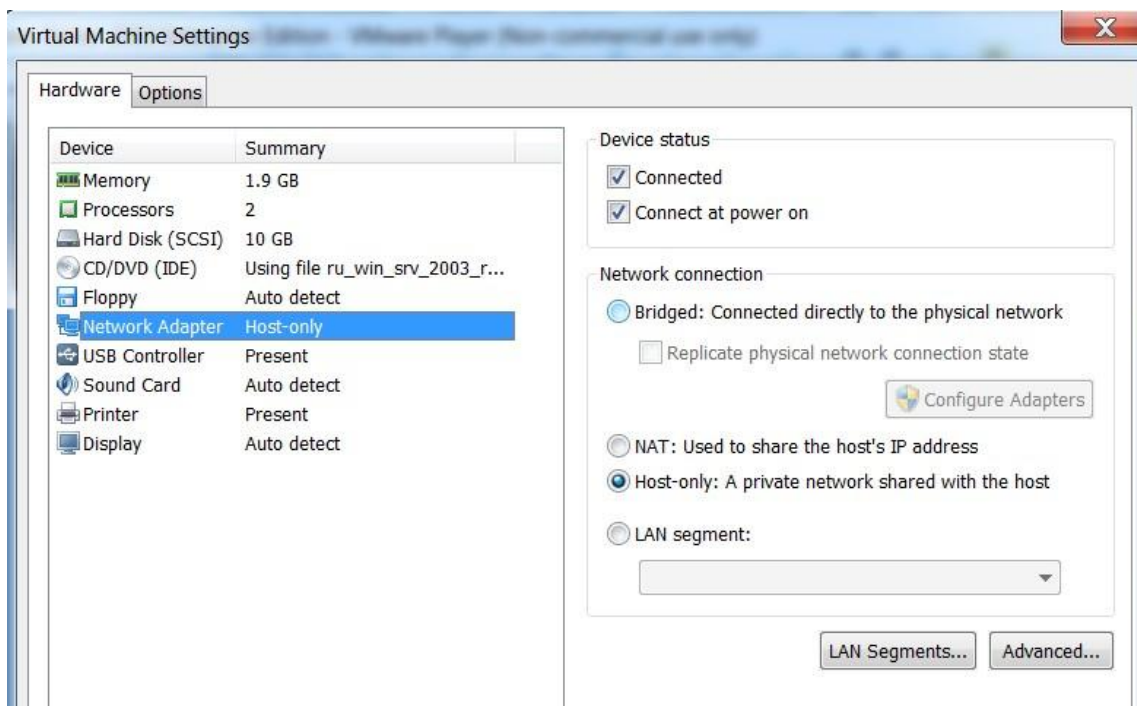


Рис. 8.4. Перевірка режиму роботи мережевого адаптера

IP-адреса комп'ютера буде мати вигляд 192.168.*.*, у якому 3-й байт буде визначатися сумою 100 + номер студента в журналі. Для його установки необхідно викликати властивості TCP/IP (рис. 8.5).

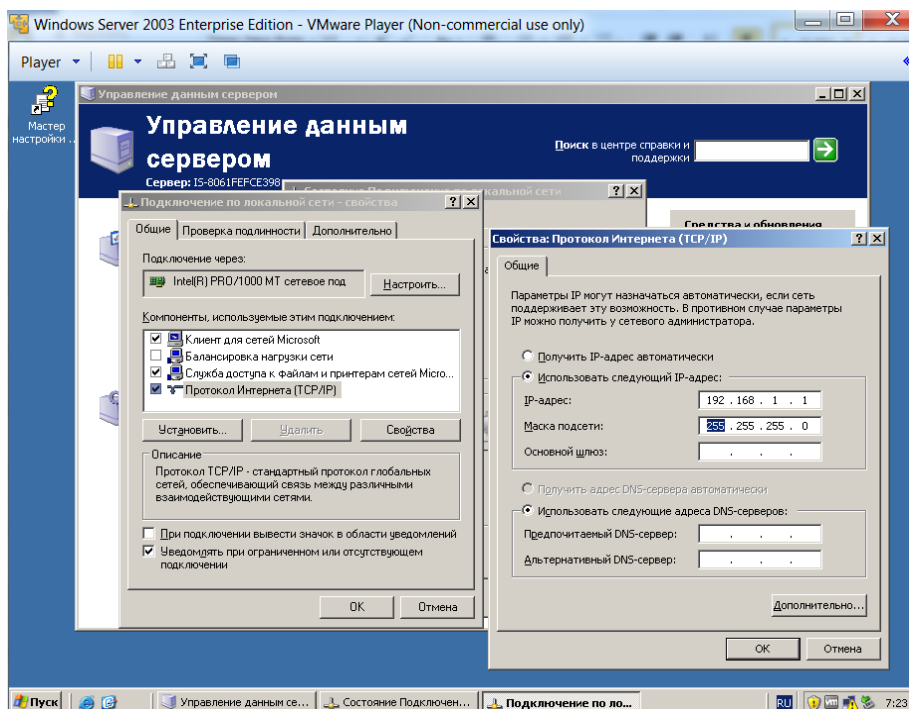


Рис. 8.5. Призначення IP-адреси сервера

Необхідно провести перевірку мережевих налаштувань (рис. 8.6).

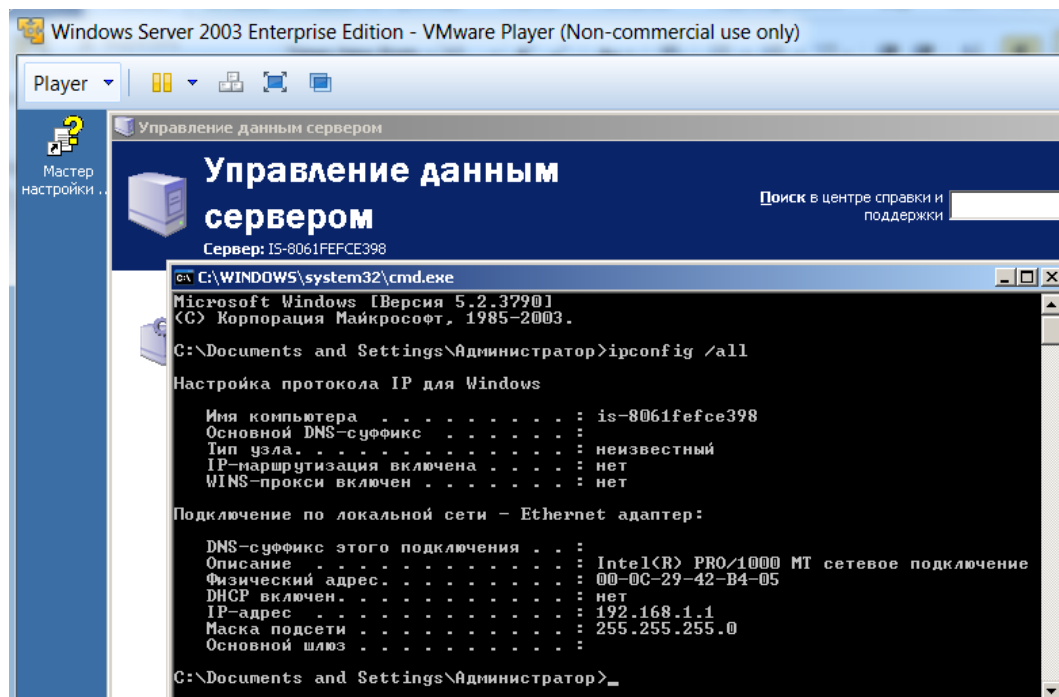


Рис. 8.6. Перевірка мережевих налаштувань командою "ipconfig /all"

Після цього вибрати в меню "Пуск" "Управление данным сервером" і запустити "Мастер настройки сервера". У вікні "Параметры настройки" необхідно обов'язково обрати "Особая конфигурация" (рис. 8.7).

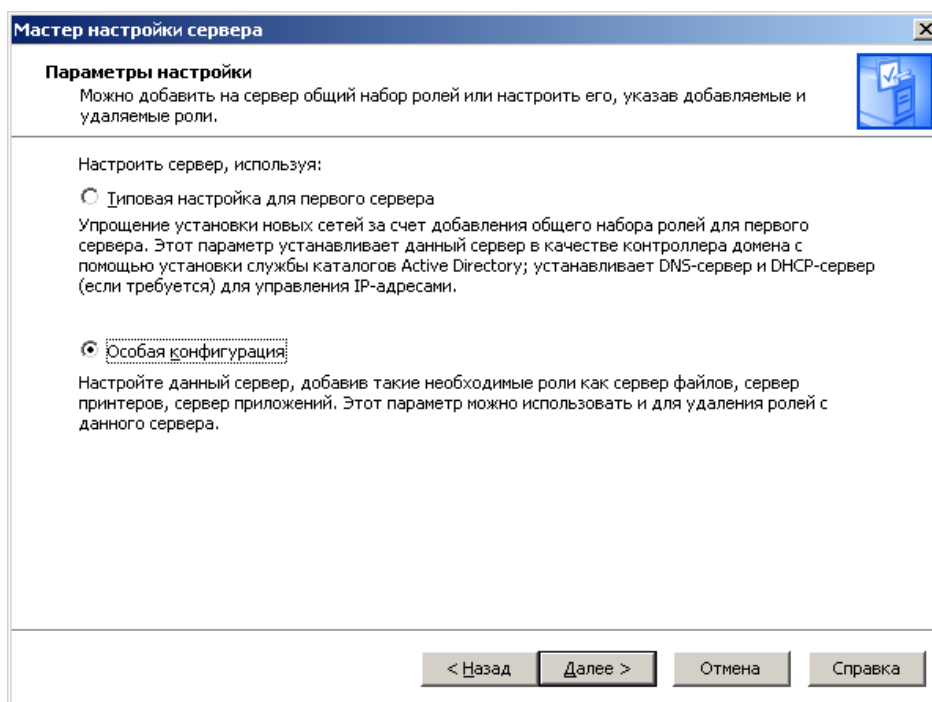


Рис. 8.7. Запуск майстра налаштувань Windows Server 2003

Для установки сервера DHCP обрати необхідну роль (рис. 8.8).

Якщо відповідну роль вже встановлено, її необхідно попередньо видалити.

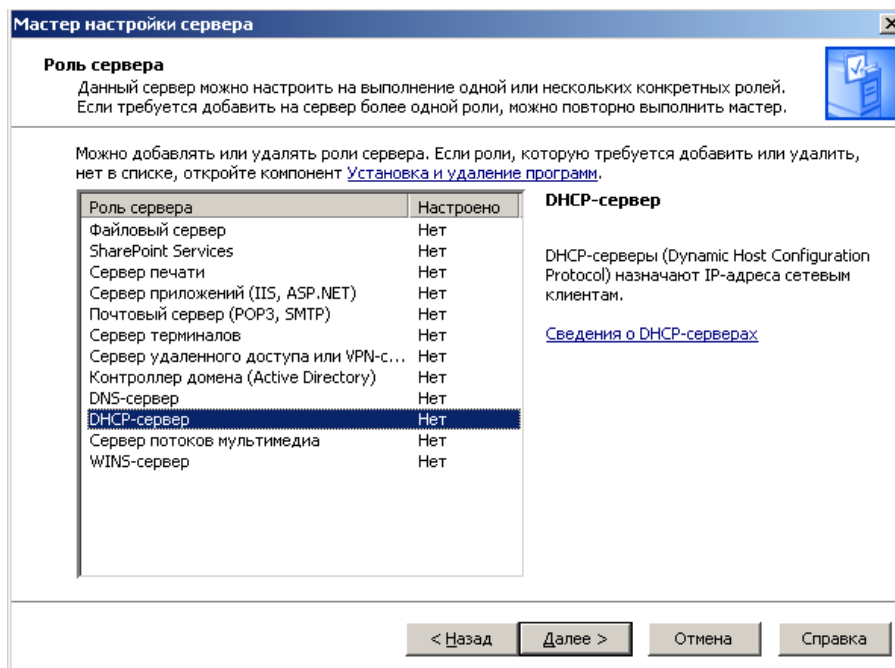


Рис.8.8. Вибір пункту установки DHCP

За допомогою майстра треба зробити необхідні налаштування (рис. 8.9-8.13). Ім'я області повинно містити прізвище студента. IP-адреса сервера і діапазон адрес, що виділяється, повинні бути в одній підмережі. Під час обрання діапазону IP-адрес зверніть увагу на адреси, які вже використовуються у підмережі.

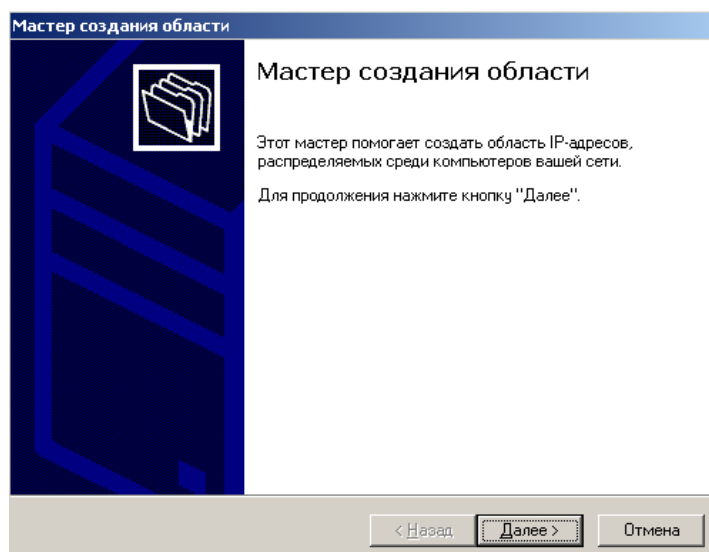


Рис. 8.9. Майстер створення області DHCP-сервера

Мастер создания области

Имя области

Необходимо обеспечить уникальное имя области. Кроме того, существует параметр, в котором можно задать описание области.

Введите имя и описание новой области. Эта информация поможет быстро идентифицировать, какую именно область следует использовать в сети.

Имя:

Описание:

< Назад Далее > Отмена

Рис. 8.10. Призначення ім'я області

Мастер создания области

Диапазон адресов

Определить диапазон адресов области можно задавая, диапазон последовательных IP-адресов.

Введите диапазон адресов, который описывает область.

Начальный IP-адрес:

Конечный IP-адрес:

Маска подсети определяет, сколько битов IP-адреса использовать для идентификации сети, а сколько битов использовать для идентификации узла внутри этой сети. Можно определить маску, задавая IP-адрес или ее длину.

Длина:

Маска подсети:

< Назад Далее > Отмена

Рис. 8.11. Призначення діапазону IP-адрес

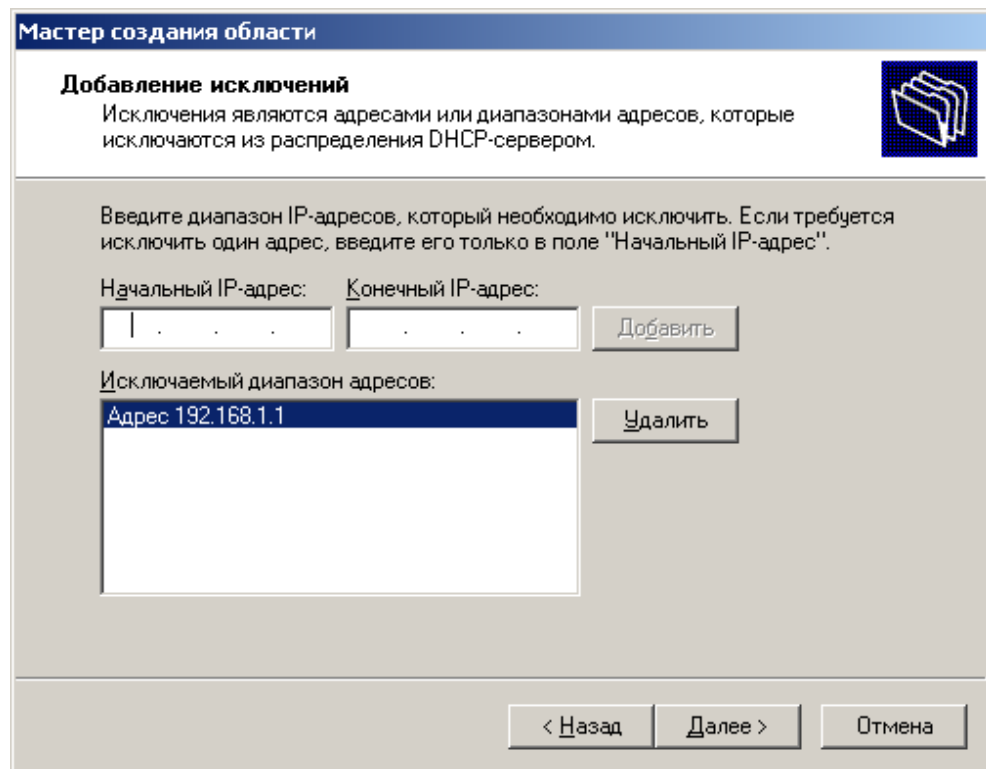


Рис. 8.12. Додавання виключень адрес

Перевірити правильність налаштувань DHCP-сервера (рис. 8.13).

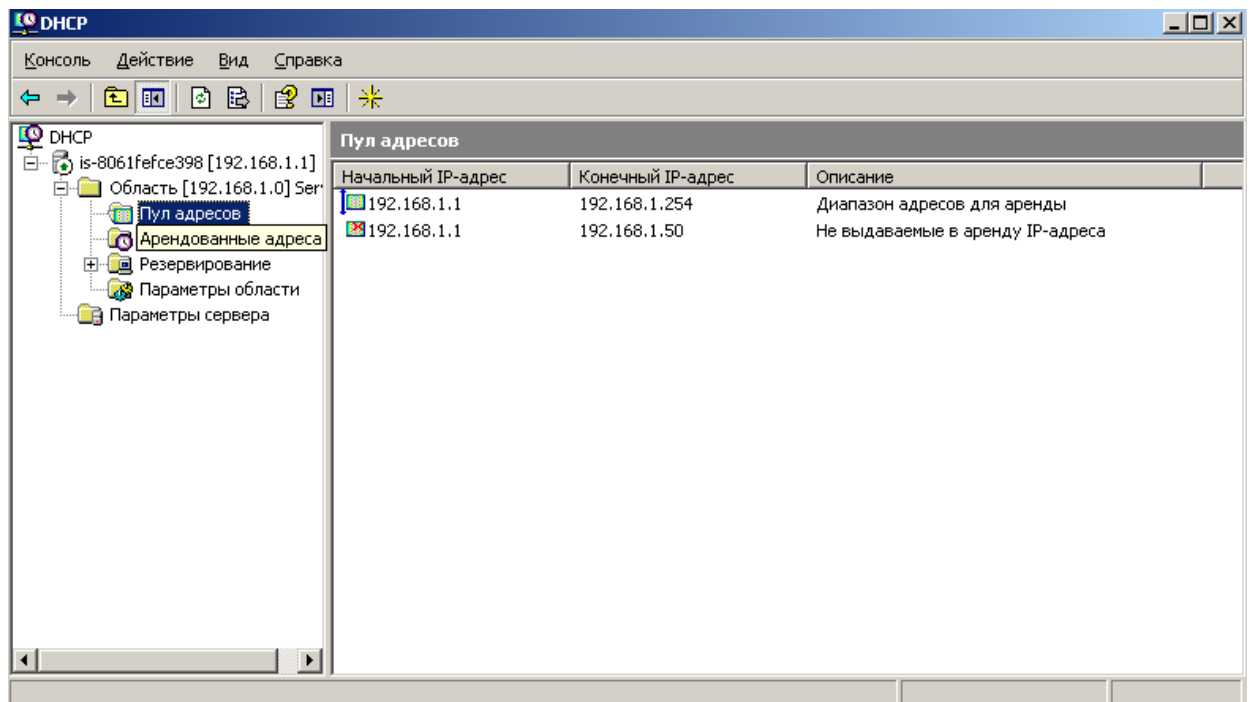


Рис. 8.13. Перевірка налаштувань DHCP-сервера

Далі необхідно налаштувати автоматичне отримання IP-адреси у *Windows XP* (рис. 8.14).

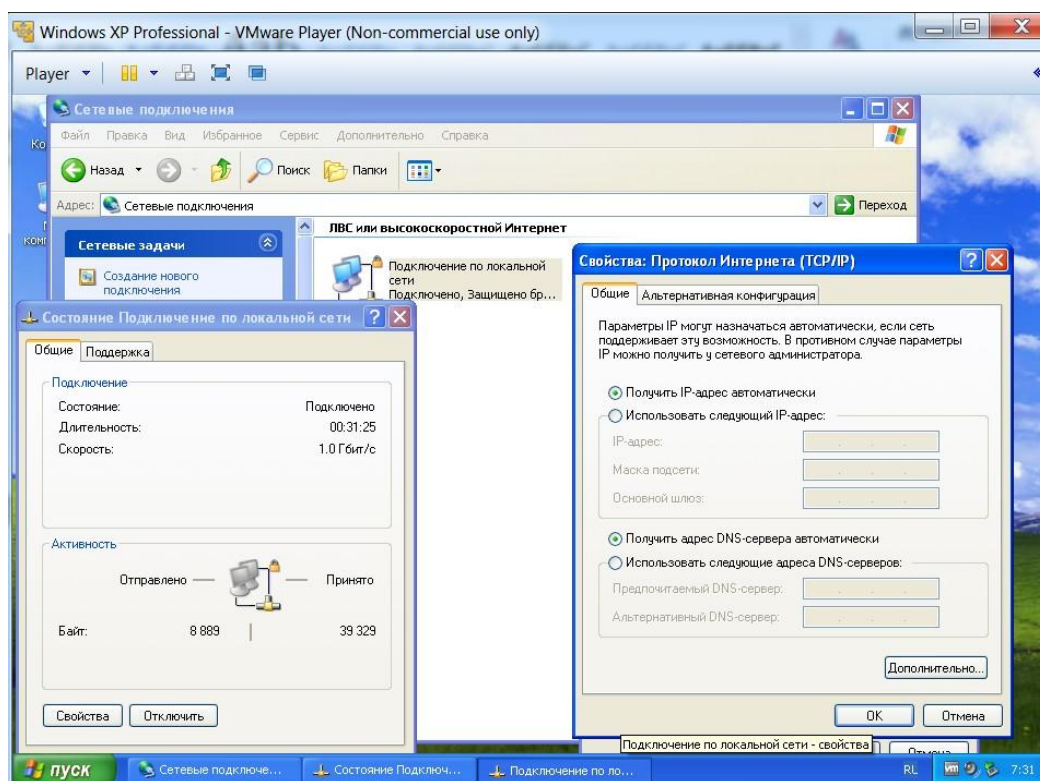


Рис. 8.14. Налаштування автоматичного отримання IP-адреси у *Windows XP*

Провести перевірку отриманих мережевих налаштувань (рис. 8.15).

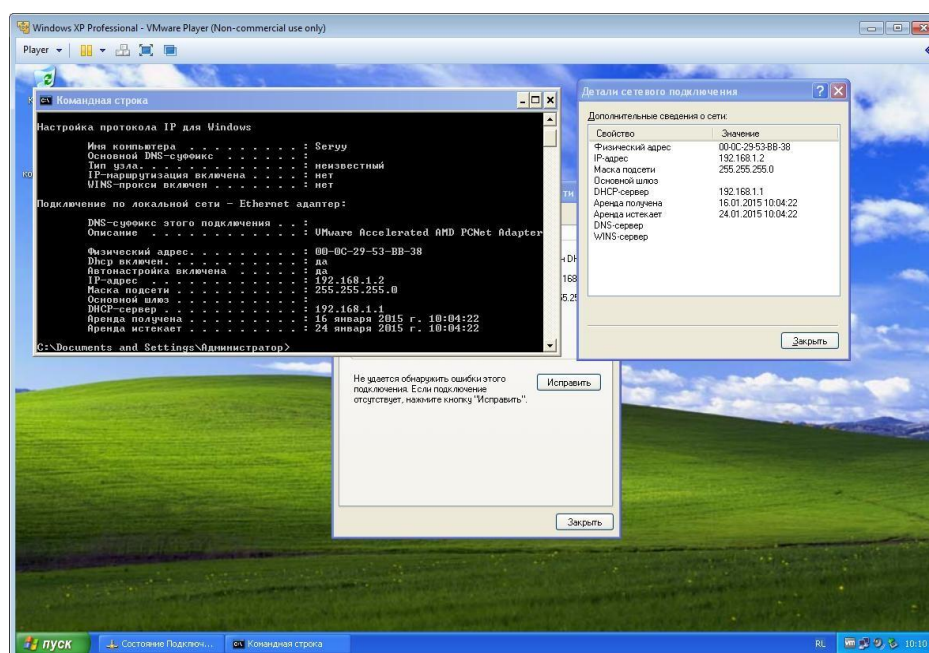


Рис. 8.15. Проверка полученной адреси від DHCP-сервера

За допомогою команд діагностики "ipconfig /all", "ping" слід провести перевірку роботи DHCP-сервера. Попередньо необхідно вимкнути бранд-мауер у Windows XP, який за замовчуванням блокує ICMP пакети (рис. 8.16).

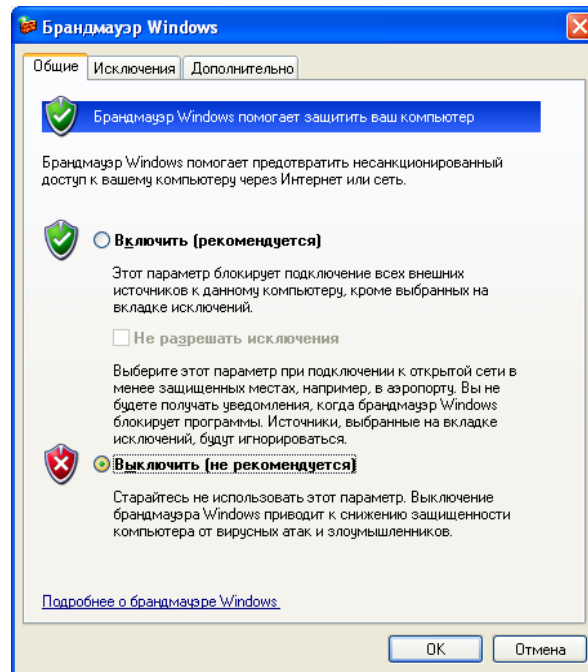


Рис. 8.16. Налаштування брандмауера

Команда "ipconfig /all" і "ping" повинна бути виконана на сервері і на робочій станції (рис. 8.17 і 8.18).

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Администратор>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : Серуу
Основной DNS-суффикс . . . . . : 
Тип узла . . . . . : неизвестный
IP-маршрутизация включена . . . . . : нет
WINS-прокси включен . . . . . : нет

Подключение по локальной сети - Ethernet адаптер:

DNS-суффикс этого подключения . . . : 
Описание . . . . . : VMware Accelerated AMD PCNet Adapter
Физический адрес . . . . . : 00-0C-29-03-0B-EC
DHCP-включен . . . . . : да
Автонастройка включена . . . . . : да
IP-адрес . . . . . : 192.168.1.51
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 
DHCP-сервер . . . . . : 192.168.1.1
Аренда получена . . . . . : 1 декабря 2013 г. 7:32:02
Аренда истекает . . . . . : 9 декабря 2013 г. 7:32:02

C:\Documents and Settings\Администратор>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байт:

Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь).
    Приблизительное время приема-передачи в мс:
        Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\Администратор>
```

Рис. 8.17. Перевірка роботи DHCP-сервера командами діагностування "ipconfig /all" та "ping" у BM з Windows XP

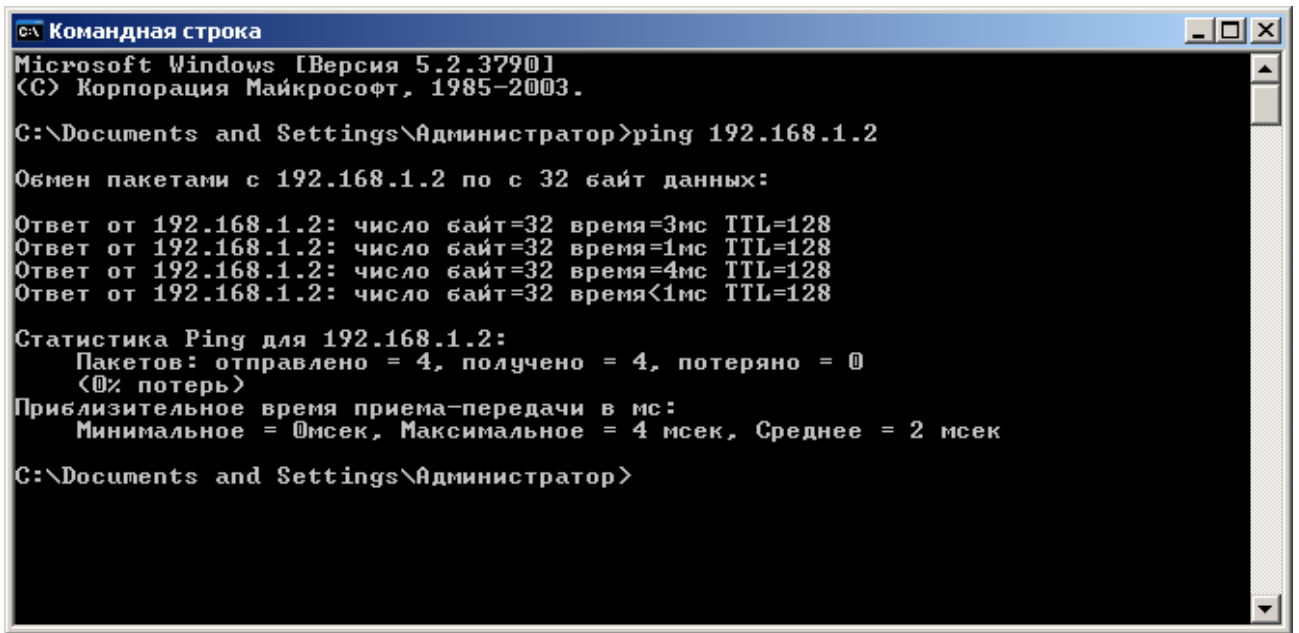


Рис. 8.18. Проверка работы DHCP-сервера командой "ping" из Windows Server

Проверить работу DHCP-сервера в консоли Windows Server 2003 (рис. 8.19).

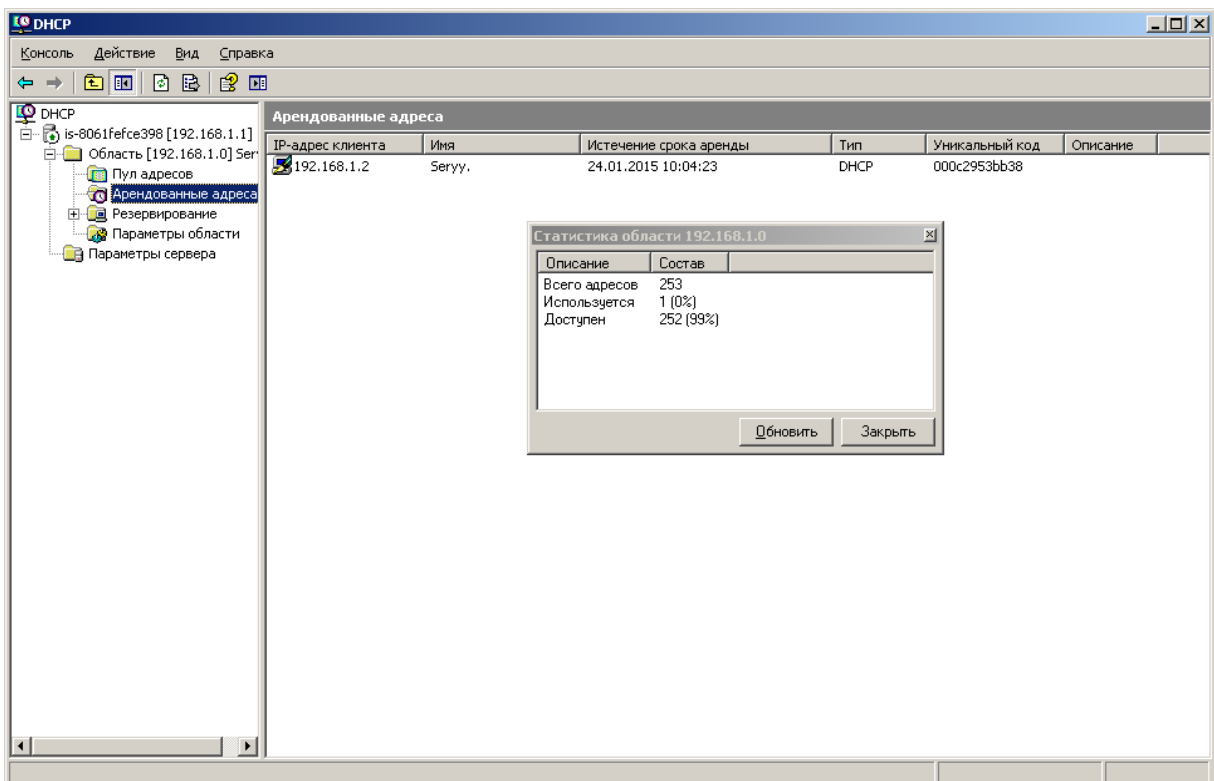


Рис. 8.19. Проверка работы DHCP-сервера в консоли Windows Server 2003

Резервування – це можливість видавати постійні IP-адреси клієнтам DHCP-сервера з пулу адрес.

8.3 Оброблення та аналізування результатів. Оформлення звіту.

1. Назва практичної роботи, тема, мета й зміст завдань практичної роботи (ЛР).
2. Вхідні дані до практичної роботи.
3. Отримані в результаті виконання ЛР скріншоти результатів виконання завдань практичної роботи.
4. Висновки з практичної роботи.

8.4 Контрольні питання

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

ПРАКТИЧНА РОБОТА 9

КОНФІГУРУВАННЯ DNS-СЕРВЕРА

Мета та основні завдання роботи: навчитися конфігурувати та перевіряти роботу DNS-сервера під час роботи комп'ютерної мережі.

Вивчити та стисло описати у протоколі практичної роботи:

- процедуру конфігурування й перевірки роботи DNS-сервера.

9.1 Теоретичні відомості

DNS-сервер (синонім - сервер імен) - це сервер, який містить базу даних публічних IP-адрес і пов'язаних з ними імен хостів. Як правило, DNS-сервер виконує роль перекладача, дозволяючи або переводячи імена хостів в IP-адреси.

В результаті виходить ряд чисел, які стають зрозумілим людині URL-адресою. DNS-сервери використовують спеціальне програмне забезпечення і взаємодіють один з одним за окремими протоколами. В процесі обробки запитів вони призначають правильний IP-адреса URL-адресою або правильний URL-адресу IP-адресою.

DNS є невід'ємною частиною Інтернету з 1985 року завдяки впровадженню «служби каталогів», що розповсюджується по всьому світу.

Абревіатура DNS розшифровується як «система доменних імен». Вона являє собою ієрархічний децентралізований каталог іменування комп'ютерів, служб чи інших ресурсів, які підключені до глобальної або окремої мережі.

Відвідування будь-якого сайту або сервера можливо через введення певного IP в браузері. Як правило, користувач не знає цей конкретний IP-адреса. Він знає тільки URL, наприклад, www.ukraine.com.ua.

Якщо користувач вводить цей URL-адресу в адресний рядок свого браузера, він відправляється на доменний сервер, який потім перенаправляє користувача на IP-адресу, прив'язаний до URL-адресою. Якщо перша служба не знаходить відповідного призначення, запит перенаправляється на наступний DNS-сервер.

Головний сервер імен, керований системою ICANN, є останнім варіантом призначення, якщо не було досягнуто збігів з попередніми серверами імен. Більшість приватних користувачів автоматично перенаправляються на DNS-сервер провайдера, коли робиться запит. Великі корпорації часто мають свої власні доменні сервера.

Служба DNS передає відповідальність за призначення доменних імен різних інтернет-ресурсів, вказавши релевантні сервери імен для кожного домена. Відповідальні особи також можуть делегувати вирішення для піддоменів призначеного їм простору імен інших серверів. Така схема роботи забезпечує постійне децентралізоване розподіл, а система була спеціально впроваджена, щоб уникнути централізованих баз даних.

Робота серверів також визначає елементи технологічної функціональності служби бази даних, яка лежить в її основі. Вона визначає себе як частину Internet Protocol Suite протоколу DNS, і надає детальну специфікацію структур даних і потоки обміну інформацією між серверами.

Принцип роботи DNS

Для розуміння принципу дії сервера може використовуватися аналогія з телефонним довідником.

DNS, що обробляє різні доменні імена, функціонує як надшвидка телефонна книга Інтернету. Вона безперервно проводить пошук і порівняння цифр, аналогічний пошуку імені в довіднику з використанням відомого телефонного номера (тут - IP-адреса).

Іноді можна говорити про так званому зворотному пошуку DNS (rDNS), який ведеться за URL-адресу. Однак, на відміну від телефонної книги, DNS-сервер можна швидко перенастроювати, так що якщо мережева служба змінює місце розташування, користувач може продовжувати використовувати той же ім'я хоста. Тобто, якби потрібна людина з телефонного довідника переїхав в інший будинок, але залишив собі той же номер телефону, ви б все одно подзвонили саме йому.

Головною і основною роллю DNS-сервера є його вплив на

децентралізовані інтернет-сервіси, такі як хмарні сервіси і мережі доставки контенту. Користувач отримує доступ до децентралізованої інтернет-служби через URL-адресу, наприклад, доменне ім'я URL-адреси вводиться в IP-адресу найближчого сервера.

Особливість DNS полягає в тому, що різні користувачі отримують різні сеанси для одного і того ж доменного імені одночасно. Цей процес описує головне призначення проксимальних серверів, а також є ключем до більш швидкого серфінгу в Інтернеті. Багато великих інтернет-сервіси також використовують цей варіант.

Якщо ви коли-небудь налаштовували веб-сайт, вам, ймовірно, також довелося створити запис DNS. Щоб ваш веб-контент був доступний «в режимі реального часу», ваш домен повинен вказувати на веб-сервер, для якого має бути створена відповідна запис.

Далі весь трафік даних направляється на ваш веб-сервер, щоб почати сеанс саме з вашим доменом. Однак, якщо є зміни в цьому наборі даних, можуть виникнути проблеми з продуктивністю.

Приклад: якщо ви зміните IP-адреса веб-сервера, існує ймовірність того, що частина потоку даних більше не зможе досягти вашого сервера. Це пов'язано з тим, що інформація з DNS дозволяють серверів імен кеширується поруч з вашими кінцевими користувачами. Це означає, що старі конфігурації записи даних можна переглядати через кілька хвилин і навіть годин після змін.

DNS-зона

Всіх пов'язані записи домену називаються зоною DNS. Це окрема частина простору імен домену, за яке зазвичай відповідає юридична особа – організація або компанія, які несуть відповідальність за підтримання регіональних зв'язків в веб-просторі. Зона DNS є адміністративною функцією, що дозволяє детально контролювати компоненти DNS, такі як авторитетні сервери імен.

Коли веб-браузеру або іншому мережевому пристрою необхідно знайти IP-адресу для імені хоста, наприклад «example.com», він виконує пошук DNS - по суті, перевірку зони DNS - і відправляється на сервер DNS, який керує зоною,

зазначеної в адресі для цього імені хоста. Цей сервер називається офіційним сервером імен для домену. Потім офіційний сервер імен дозволяє пошук DNS, надаючи IP-адреса або інші дані для запитаного імені хоста.

Основні сервера розділяють простір зони на кілька частин. Вони визначають домени верхнього рівня (такі, як «.org» або «.com»), домени другого рівня (наприклад, «ukraine.com.ua») і домени нижнього рівня, також звані піддоменами (наприклад, «support.ukraine.com.ua»). Кожен з цих рівнів може бути окремою зоною DNS.

Наприклад, кореневої домен «ukraine.com.ua» делегується корпорації Хостинг Україна. Вона приймає на себе відповідальність за настройку основного DNS-сервера, який містить правильні записи DNS для домену.

На кожному ієрархічному рівні системи DNS є сервер імен, що містить файл зони, в якому зберігаються захищені і правильні записи DNS для цієї зони.

Рекурсивні та нерекурсивні сервери

DNS сервера можуть забезпечувати рекурсивне і нерекурсивне (ітеративне) отримання імен. Основна відмінність тут проводиться за типом запитів. В обох випадках клієнт передає ім'я хосту і вказує тип запиту. У відповідь на дозвіл імені сервер дає тільки позитивний або негативний результат.

Клієнту найпростіше зробити рекурсивний запит до сервера імен. В цьому випадку адресується сервер відповідає за повне вирішення імені. Він послідовно запитує всі сервери, поки ім'я не буде повністю дозволено. Перевага цього типу запиту полягає в тому, що розпізнавач повинен тільки ініціювати один запит, прийняти відповідь і направити його в додаток.

При ітеративному отриманні пристрій повідомляє тільки адреси сервера, який повинен бути запитаний наступним. Потім розпізнавач повинен виконати додаткові запити до відповідного сервера імен, поки ім'я не буде повністю дозволено.

Іншими словами в ітеративному запиті DNS-сервер виконує дію, якщо він

не може дозволити рекурсивний запит DNS-клієнта через свій DNS-кеш і не є повноважним для доменів.

У цьому випадку він відправляє ітераційний запит на домашній сервер, який потім відправляє йому посилання на наступний можливий DNS-сервер. Потім локальний DNS-сервер відправляє ітераційний запит на DNS-сервер із заслання. Процес повторюється до тих пір, поки локальний DNS-сервер не знайде авторизаційний DNS-сервер для запиту. Потім він отримує відповідь (true / false), який потім пересилає клієнту DNS .

Унікальна адреса

Зараз з поняттям IP-адреси знаком кожен середній користувач Інтернету. Він необхідний в мережі постійно - але його обробка під час серфінгу завжди відбувається на задньому плані. Сам термін «IP-адреса» означає аббревіатуру інтернет-протоколу. Цей протокол забезпечує підтримку ідентифікаційного номера пристрою в мережі.

Більшість IP-адрес виглядають так:

165.202.64.111

Адреса також може виглядати так:

3fee: 1910,: 4546: 3: 200: f8ff: fe21: 67ef

IP-адреса - це унікальна адреса, яка мережеві IT-пристрої такі як ПК, планшети і смартфони, використовують для ідентифікації себе і для зв'язку з іншими пристроями. Для цього вони використовують особливу технологію типу Ethernet або Docsis, а на апаратному рівні - мережеві плати або флешки-роутери.

Кожному комп'ютеру в момент підключення до Інтернету, призначається IP-адресу. Це необхідно для того, щоб пристрій можна було чітко ідентифікувати, оскільки це єдиний спосіб, за яким можна верифікувати місце, звідки прийшли запити і куди пішли дані.

Приклад: якщо до веб-сайту звертаються з комп'ютера, браузер завжди також перенаправляє свій власний IP-адреса, щоб контрольований веб-сервер не тільки знав, на який веб-сайт він повинен перейти, але і куди вирушає

запитаний пакет даних.

Типи унікальних адрес

IP-адреса являє собою двійкове число на машинній мові, але його можна зберегти як текст для читачів.

32-розрядний тип (IPv4) записується у вигляді чотирьох десяткових чисел, розділених точками. Кожне число може бути від 0 до 255. Наприклад, 81.160.10.241 може бути дійсним IP.

Адреси типу IPv6-- це 128-бітові IP-адреси, які записані в шістнадцятковому форматі і розділені двокрапкою.

IP-адреса зазвичай призначається пристрою тільки на певний період часу. Тільки кілька мережевих пристроїв (наприклад, плати або роутери) повинні зберігати системний адресу (так званий фізичний MAC-адресу), оскільки всі інші пристрої використовують динамічний IP-адресу для зв'язку.

На сьогоднішній день існує дві версії інтернет-протоколу. IPv4 з 4 мільярдами адрес і IPv6 з такою кількістю адрес, що він може адресувати кожен піщинку на землі. IPV4 вичерпаний у багатьох відношеннях і привів до повільної міграції на IPv6. IPv6 сьогодні підтримується більшістю великих мереж і пристроїв.

Перетворення унікальну адресу

Незалежно від того, чи використовуються чотири або вісім блоків символів: рядки чисел важко запам'ятати. Тим більше, що ви повинні пам'ятати не тільки свою адресу, але і адреса улюблених сайтів, магазинів і т. Д. Оскільки це практично неможливо, були введені доменні імена і система доменних імен.

Це означає: наприклад, щоб викликати www.ukraine.com.ua, вам не потрібно вводити код з довгим номером, потрібно просто ввести літери «www.ukraine.com.ua» в рядку пошуку. Потім ваш комп'ютер переглядає центральну «телефонну книгу» - систему доменних імен (DNS), щоб дізнатися, який IP-адреса належить цьому доменному імені і встановлює з'єднання з відповідним веб-сервером.

Динамічне використання і захист

Принцип динамічного розподілу означає, що користувач може бути визначений безпосередньо з IP-адреси. Якщо ви хочете бути абсолютно впевненим у конфіденційності і не надати кому-небудь дані про вас випадково, вам слід пам'ятати наступні поради:

- регулярно переривайте інтернет-з'єднання, щоб перепризначити IP-адреса;
- оскільки IP-адреса міститься в кожному електронному листі: не відправляйте електронні листи на сумнівні адреси (наприклад, це стосується деяких веб-сайтів, які залучають безкоштовними завантаженнями);
- ретельно продумайте, які сервіси ви використовуєте для входу в систему, використовуючи своє ім'я користувача та пароль - тоді IP-адреса може бути призначений відвідувачеві;
- використовуйте спеціальне ПЗ для анонімізації, наприклад, розширення Tor для браузера Firefox: це допоможе вам приховати геолокацію і поведінку при серфінгу.

На закінчення можна відзначити, що принципи використання DNS-серверів і унікальних IP-адрес стали основоположними для нинішньої цифрової епохи. Тільки завдяки їм, Інтернет перетворився в справжнє середовище проживання сучасної людини.

Якщо DNS і IP типу IPv6 коли-небудь і втратять актуальності або втратять актуальність, це станеться точно не найближчі десятиліття.

9.2 Порядок виконання роботи

Конфігурування й перевірка роботи DNS-сервера.

Відкрити вікно для конфігурування ролей. Обрати роль "DNS-сервер"(рис. 9.1).

Якщо відповідну роль вже встановлено, її необхідно попередньо видалити.

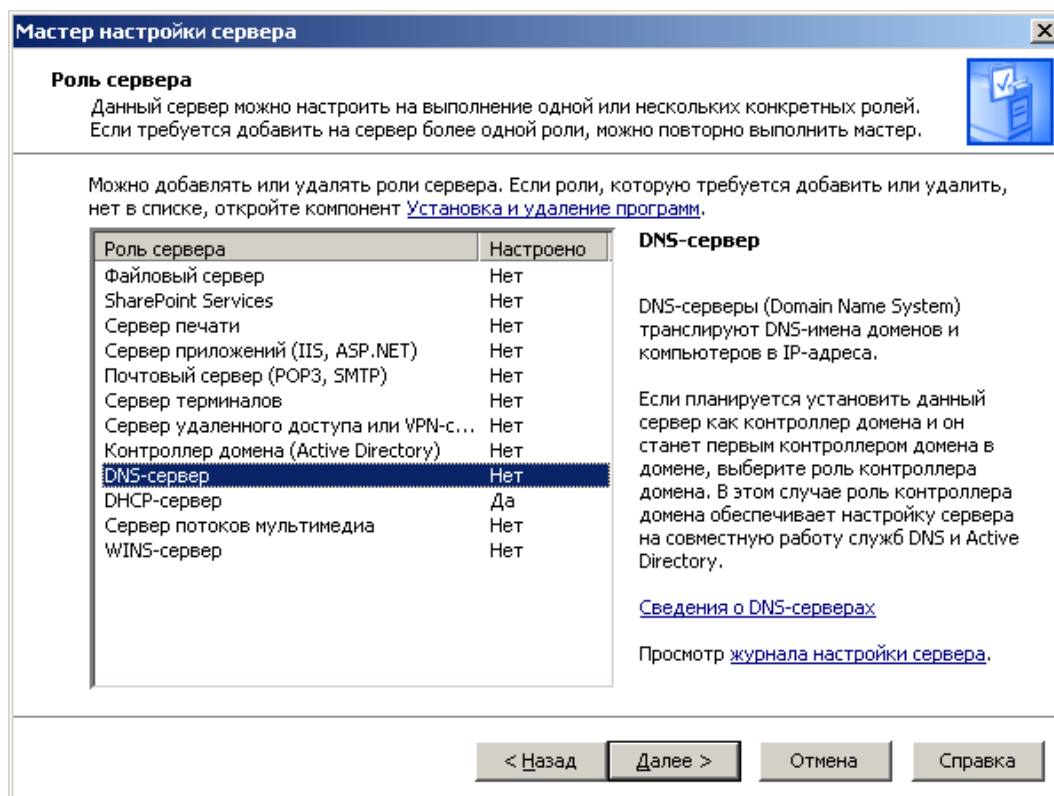


Рис. 9.1. Ролі сервера

За допомогою майстра налаштувань створити зону прямого перегляду (рис. 9.2 — 9.5).

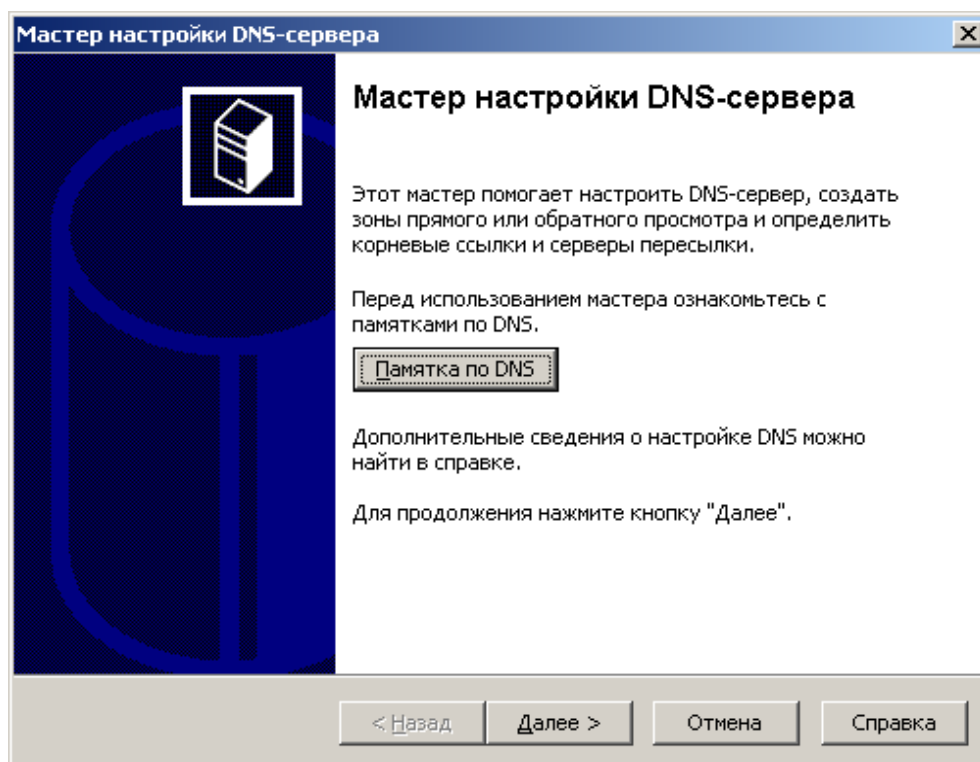


Рис. 9.2. Майстер налаштування DNS-сервера

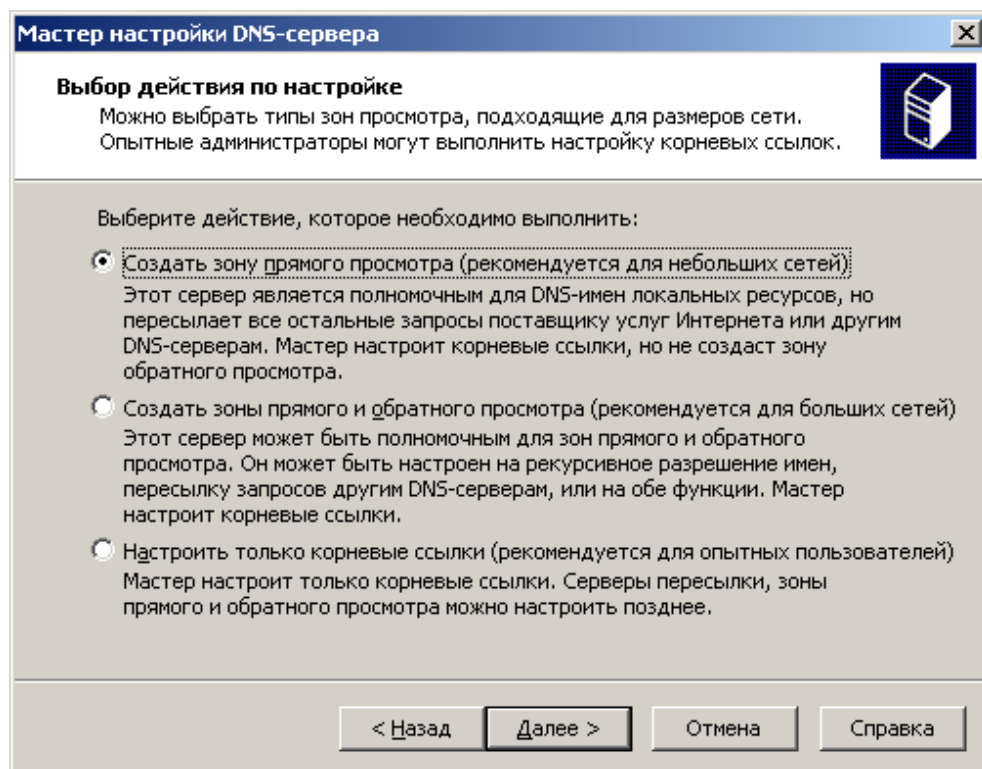


Рис. 9.3. Вибір типу зон

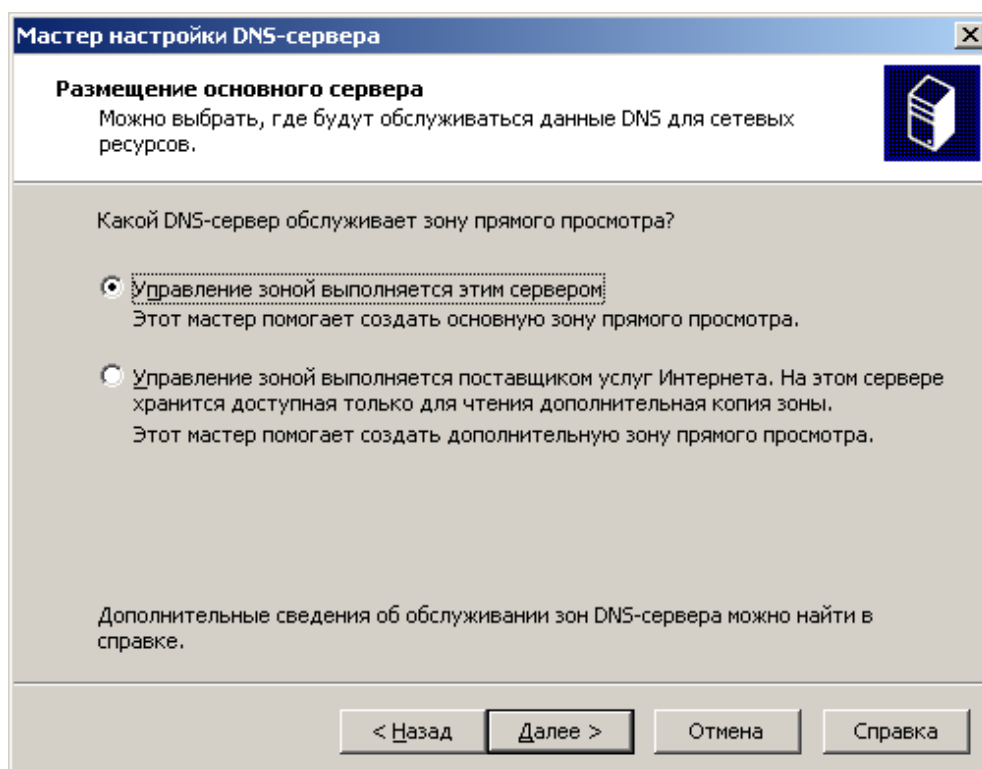
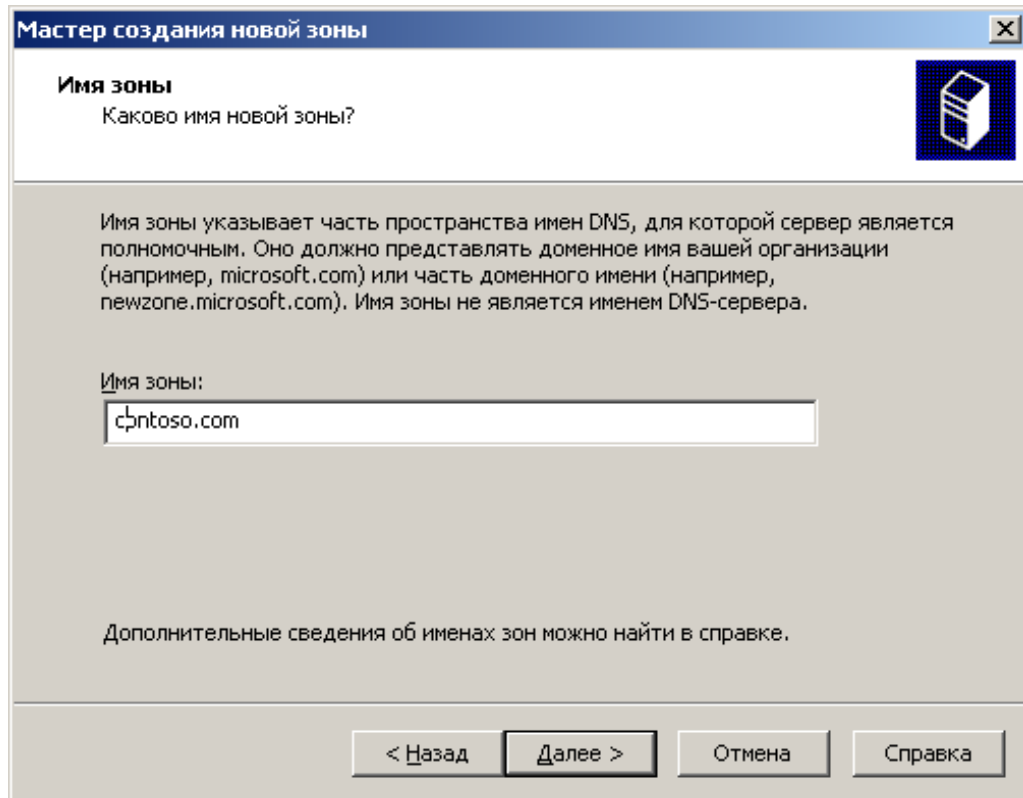


Рис. 9.4. Вибір управління зоною

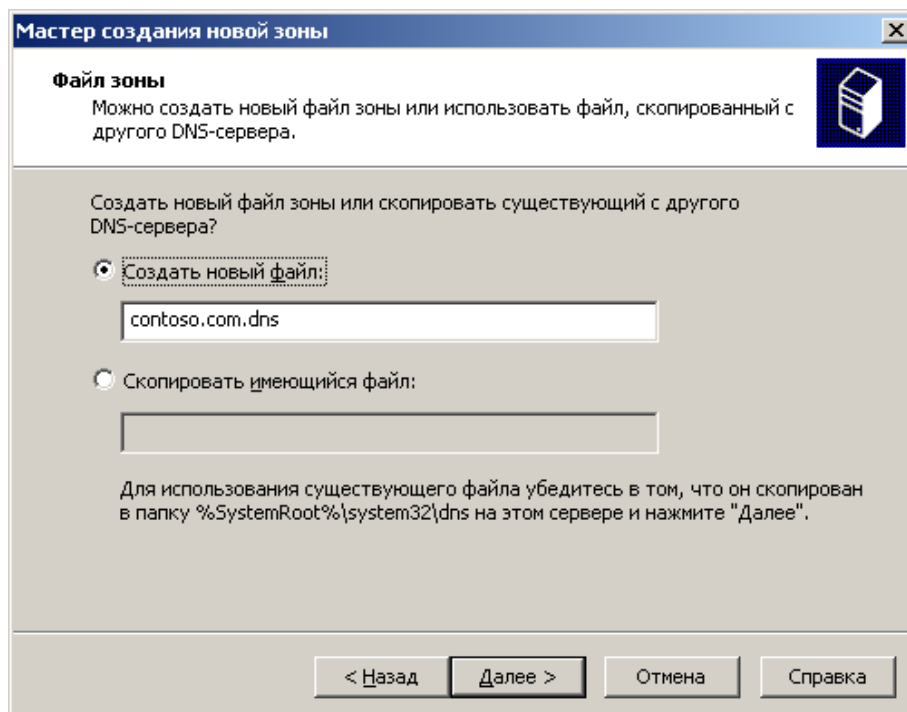
Призначити ім'я зони. Ім'я зони повинне містити прізвище студента (рис. 9.5).



The screenshot shows a Windows XP-style dialog box titled "Мастер создания новой зоны" (Master of creating a new zone). The "Имя зоны" (Zone Name) step is active, asking "Каково имя новой зоны?" (What is the name of the new zone?). A text box contains "cpntoso.com". Below the text box, there is explanatory text in Russian: "Имя зоны указывает часть пространства имен DNS, для которой сервер является полномочным. Оно должно представлять доменное имя вашей организации (например, microsoft.com) или часть доменного имени (например, newzone.microsoft.com). Имя зоны не является именем DNS-сервера." (The zone name indicates the part of the DNS namespace for which the server is authoritative. It should represent the domain name of your organization (for example, microsoft.com) or a part of the domain name (for example, newzone.microsoft.com). The zone name is not a DNS server name.). At the bottom, there are four buttons: "< Назад" (Back), "Далее >" (Next), "Отмена" (Cancel), and "Справка" (Help).

Рис. 9.5. Ім'я зони

Виконати подальші налаштування у майстрі (рис. 9.6).



The screenshot shows the same dialog box, but at the "Файл зоны" (Zone File) step. It asks "Можно создать новый файл зоны или использовать файл, скопированный с другого DNS-сервера." (Can you create a new zone file or use a file copied from another DNS server?). There are two radio button options: "Создать новый файл:" (Create new file:) which is selected, and "Скопировать имеющийся файл:" (Copy existing file:). The "Создать новый файл:" option has a text box containing "contoso.com.dns". Below the "Скопировать имеющийся файл:" option is an empty text box. At the bottom, there is explanatory text in Russian: "Для использования существующего файла убедитесь в том, что он скопирован в папку %SystemRoot%\system32\dns на этом сервере и нажмите 'Далее'." (To use an existing file, make sure it is copied to the %SystemRoot%\system32\dns folder on this server and click 'Next'). The same four buttons are at the bottom: "< Назад", "Далее >", "Отмена", and "Справка".

Рис. 9.6. Задавання імені файлу зони

Необхідно заборонити динамічне оновлення та пересилання запитів у зв'язку з тим, що в мережі не існує інших DNS-серверів (рис. 9.7 і 9.8).

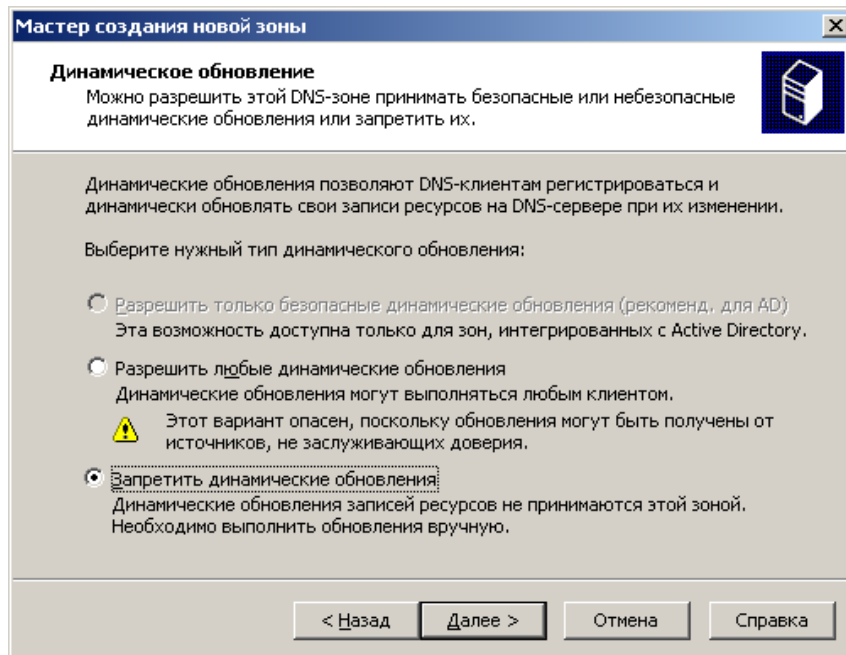


Рис. 9.7. Динамічне оновлення

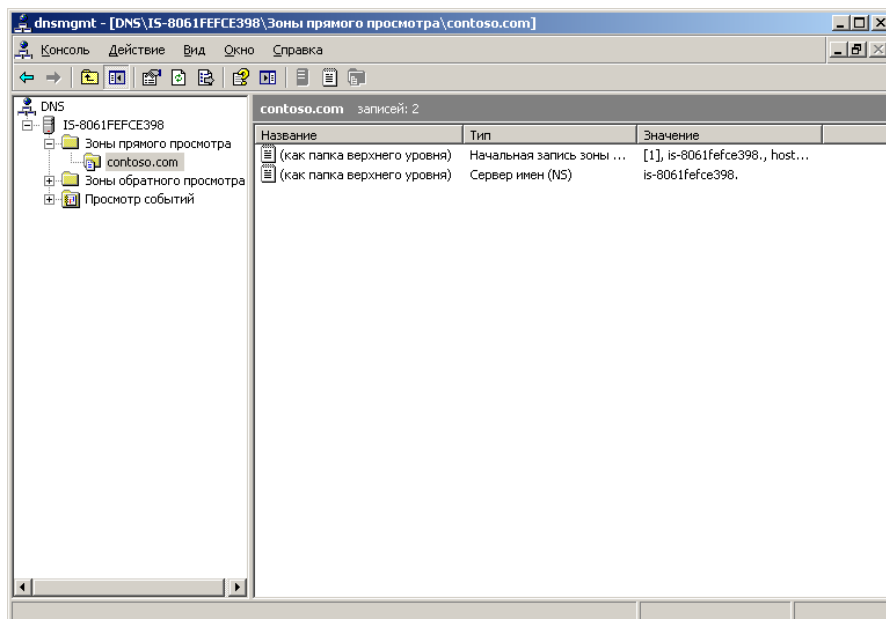


Рис. 9.8. Ролі сервера

Завершити роботу майстра (рис. 9.9).

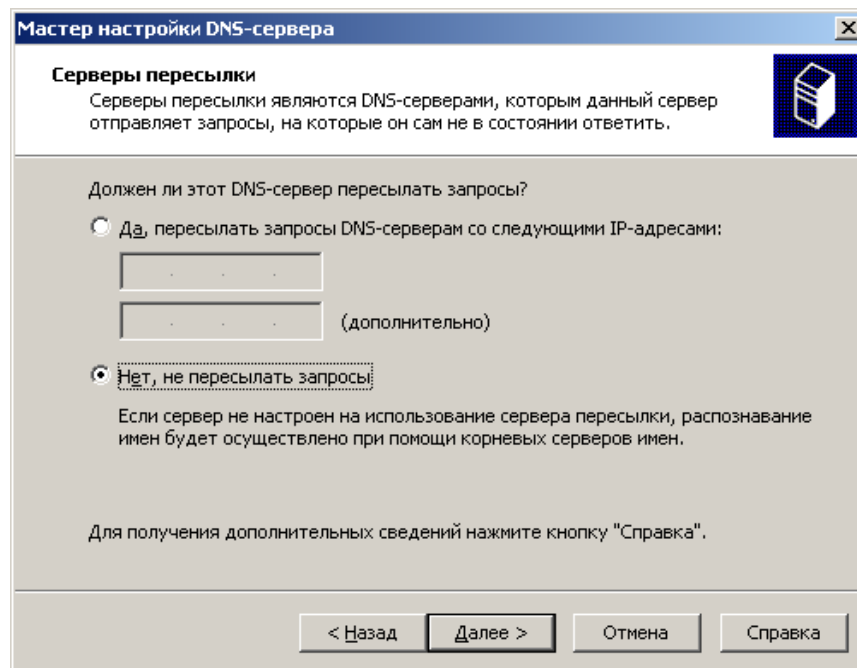


Рис. 9.9. Завершения работы мастера

Відкрити консоль управління DNS-сервером (рис. 9.10).

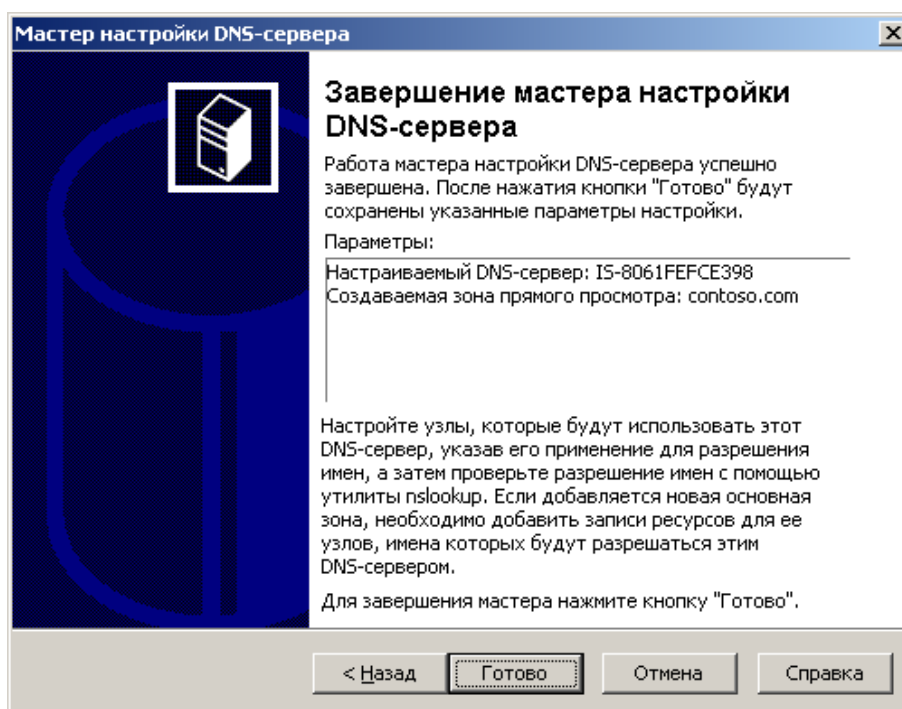


Рис. 9.10. Консоль управления DNS-сервером

Додати записи для кореневого вузла, який знаходиться на *Windows Server* і вузла робочої станції (рис. 9.11 — 9.13).

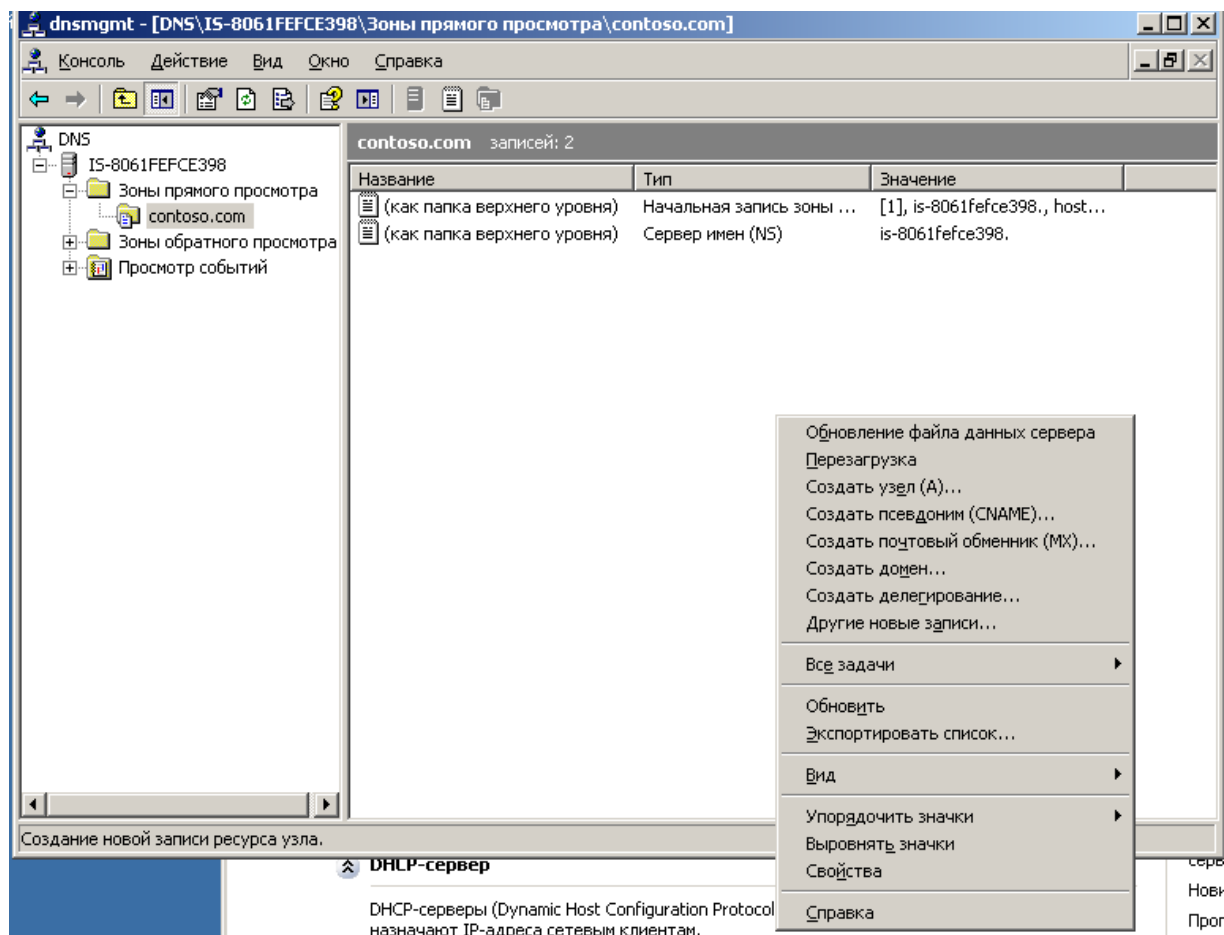


Рис. 9.11. Консоль управления DNS-сервером

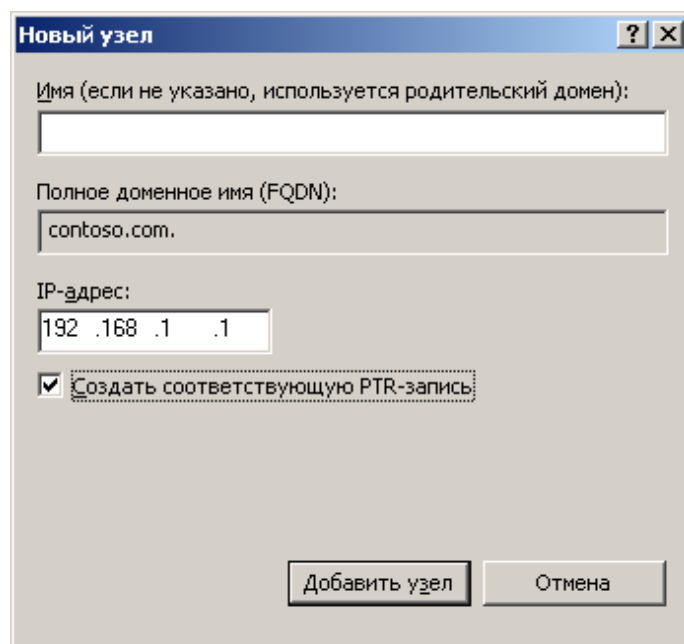


Рис. 9.12. Добавления узла

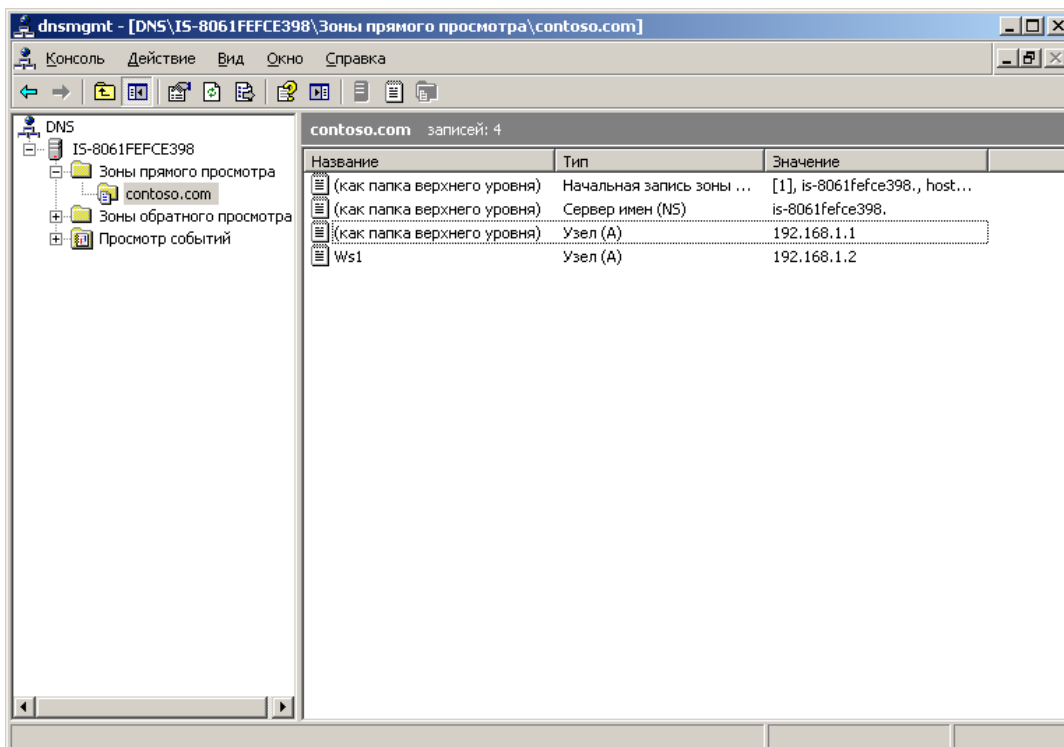


Рис. 9.13. Наластроена зона прямого перегляду

Створити зону зворотного перегляду (рис. 9.14 і 9.15).

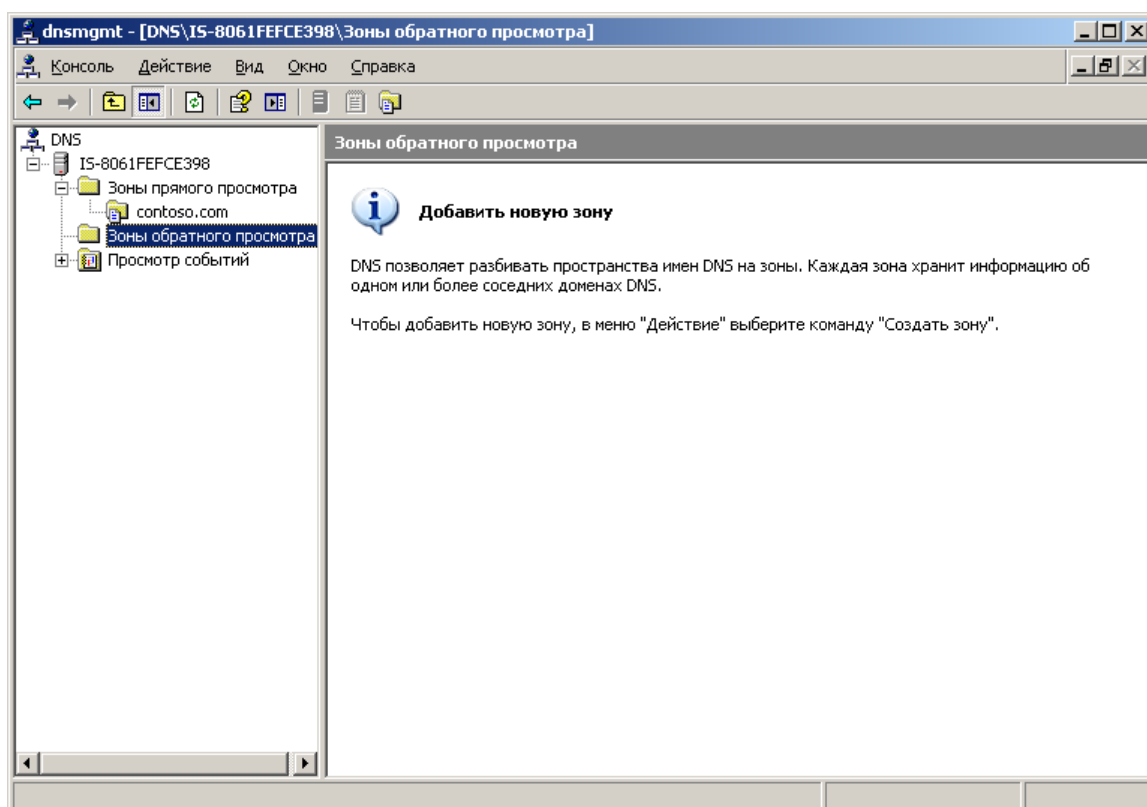


Рис. 9.14. Консоль DNS-сервера

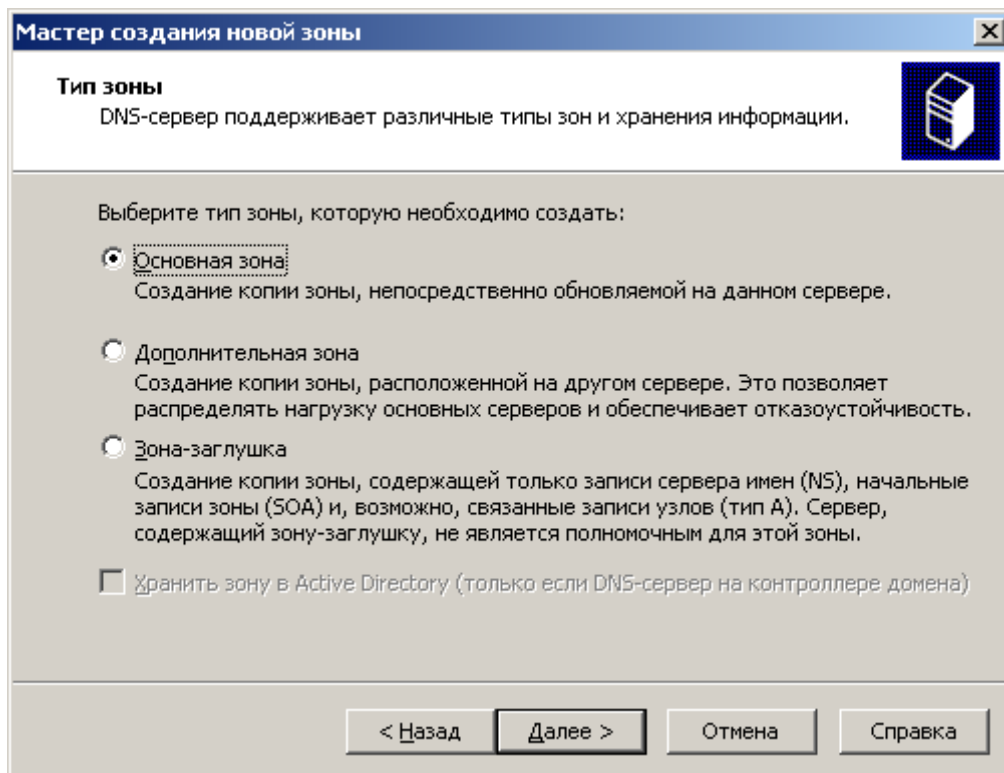


Рис. 9.15. Обрання типу зони

Далі ввести перші три байти мережі для підмережі DNS-сервера(рис. 9.16).

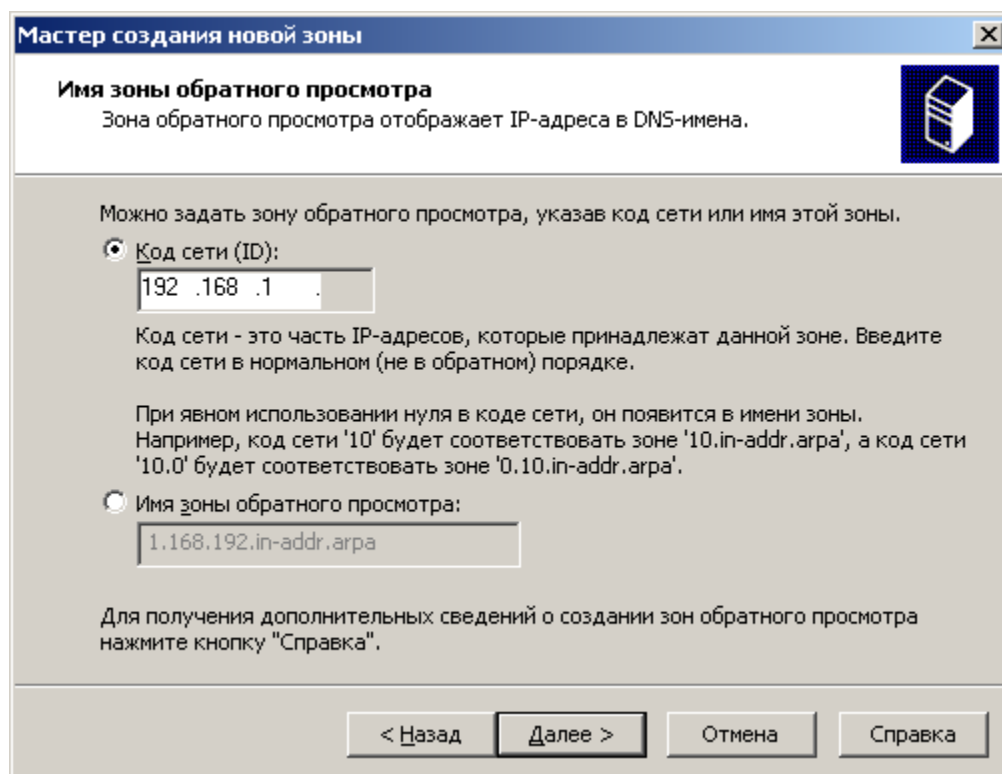


Рис. 9.16. Налаштування коду мережі

Створити файл зони, заборонити динамічне оновлення (рис. 9.17, 9.18).

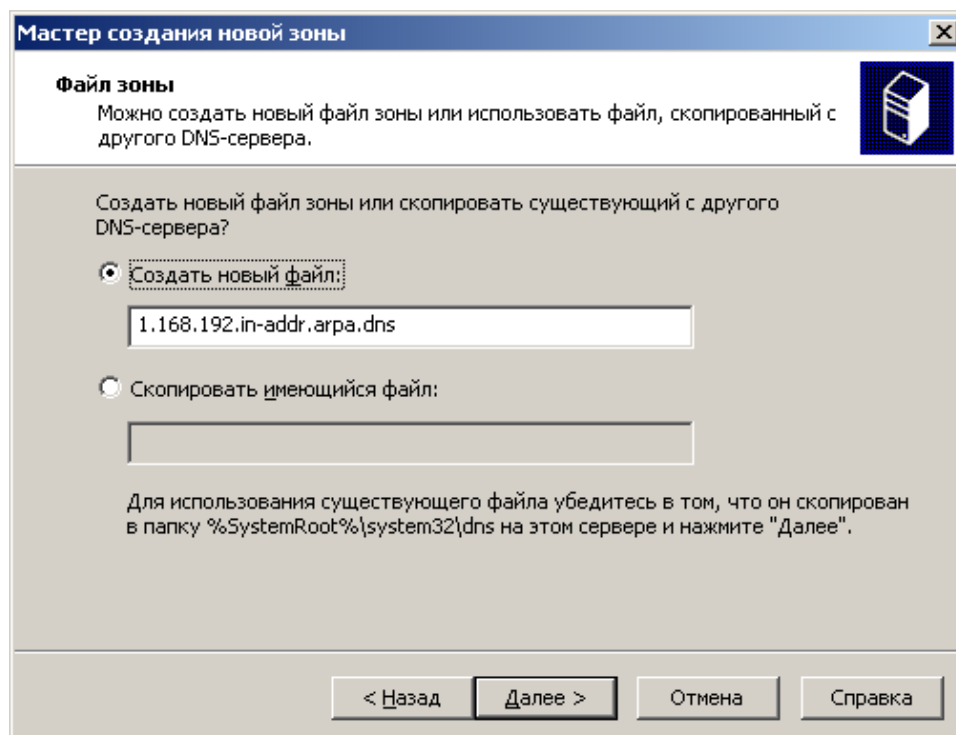


Рис. 9.17. Задавання імені файлу зони

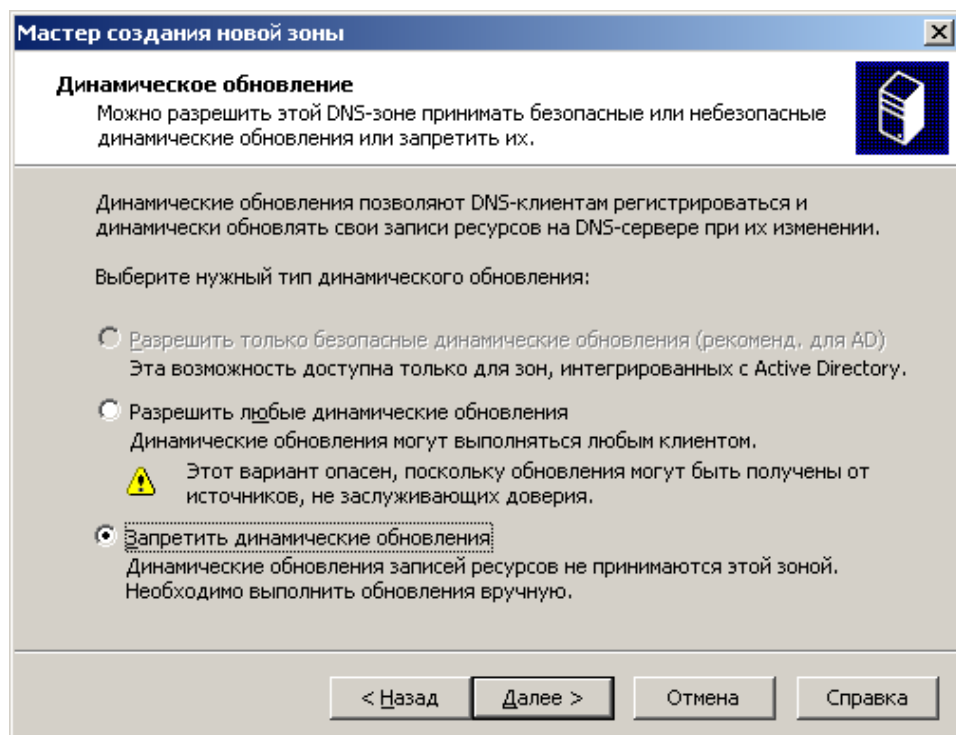


Рис. 9.18. Динамічне оновлення

Додати записи для кореневого вузла, який знаходиться на *WindowsServer* і вузла робочої станції (рис. 9.19 —9.23).

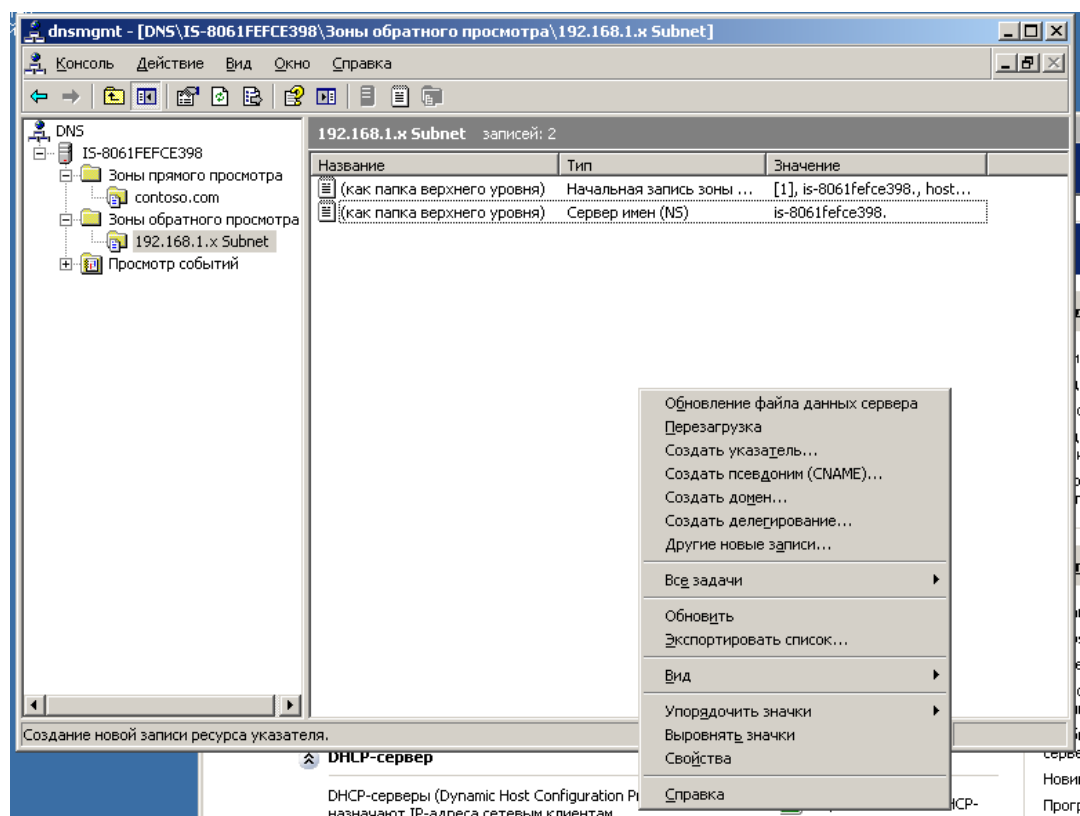


Рис. 9.19. Консоль управління DNS-сервером

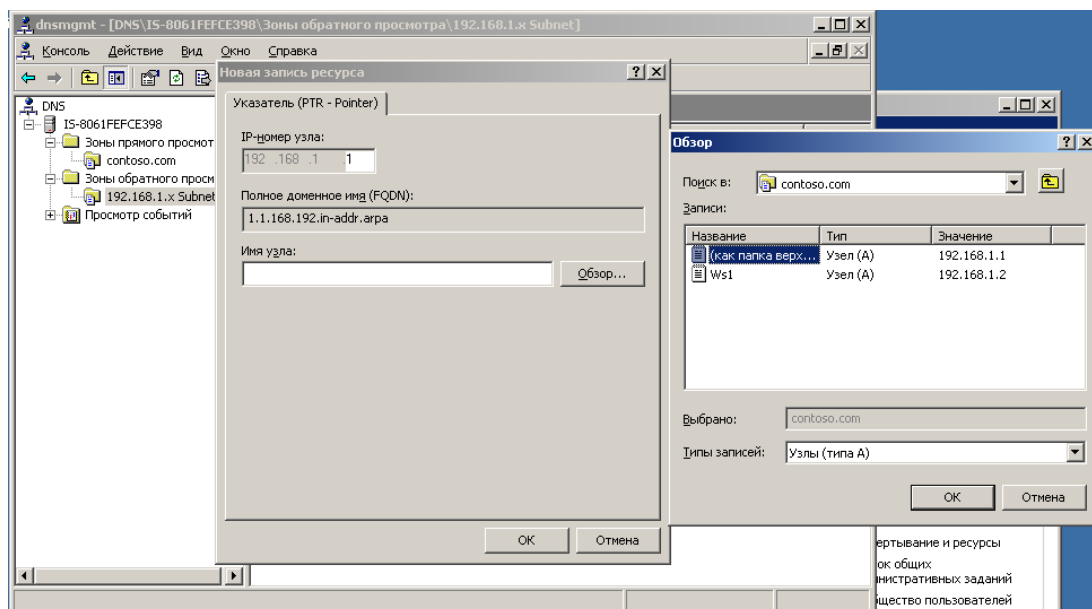


Рис. 9.20. Додавання вузла

Новая запись ресурса

Указатель (PTR - Pointer)

IP-номер узла:
192 .168 .1 .1

Полное доменное имя (FQDN):
1.1.168.192.in-addr.arpa

Имя узла:
contoso.com

Обзор...

OK Отмена

Рис. 9.21. Додавання вузла

Новая запись ресурса

Указатель (PTR - Pointer)

IP-номер узла:
192 .168 .1 .2

Полное доменное имя (FQDN):
2.1.168.192.in-addr.arpa

Имя узла:
Ws1.contoso.com

Обзор...

OK Отмена

Рис. 9.22. Створення нових записів

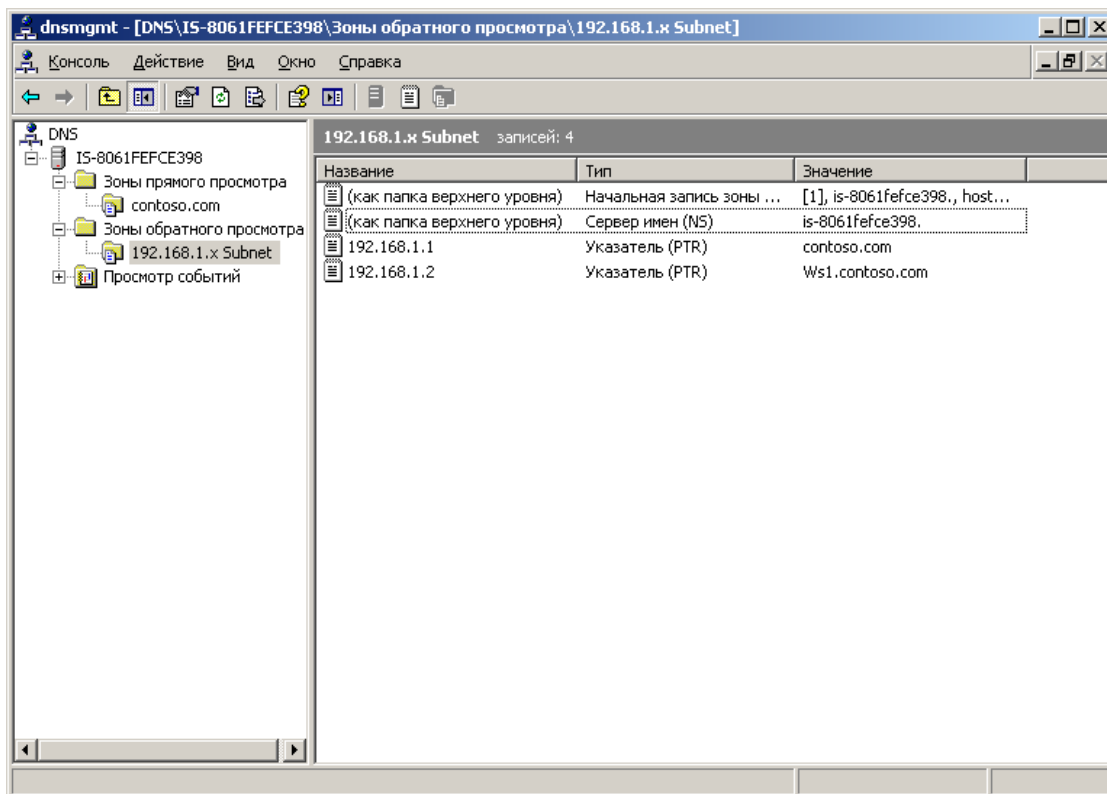


Рис. 9.23. Налаштована зона зворотного перегляду

Перед перевіркою роботи DNS-сервера необхідно виконати додаткові налаштування DHCP-сервера таким чином, щоб він видавав клієнтському комп'ютеру (*Windows XP*) крім IP-адреси і маски підмережі ще й адресу сервера, на якому встановлено роль DNS-сервера (рис. 9.24).

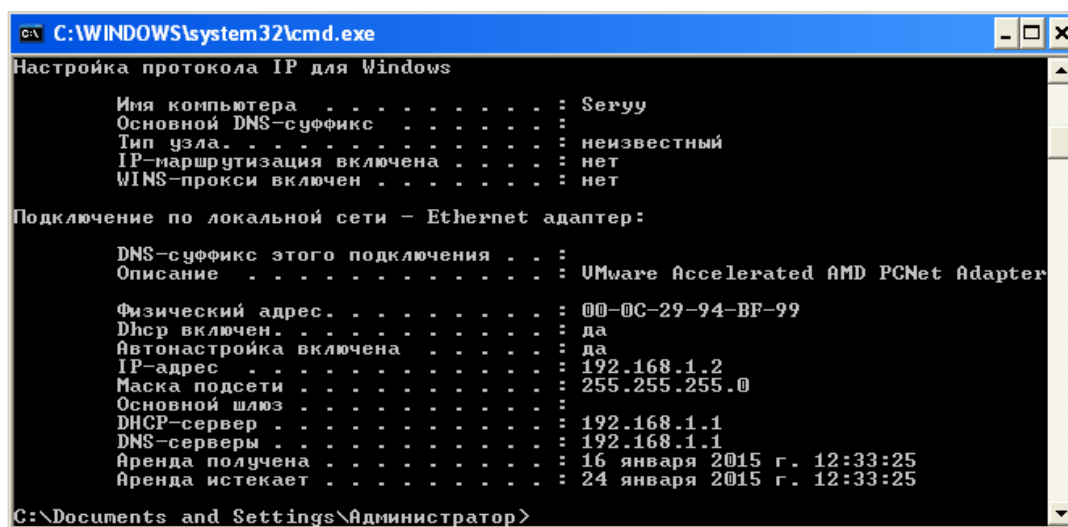


Рис. 9.24. Результаты выполнения nslookup у *Windows Server*

Перевірку роботи DNS-сервера здійснити в двох режимах: для першого використовувати команди для перевірки у *Windows Server*, для другого використовувати команди для перевірки у *Windows XP*. Для перевірки роботи DNS-сервера використати дві команди: *ping* і *nslookup*.

У командному рядку ввести *nslookup*. У програмі послідовно ввести IP-адреси і доменні імена *Windows Server* та *Windows XP* (рис. 9.25 і 9.26).

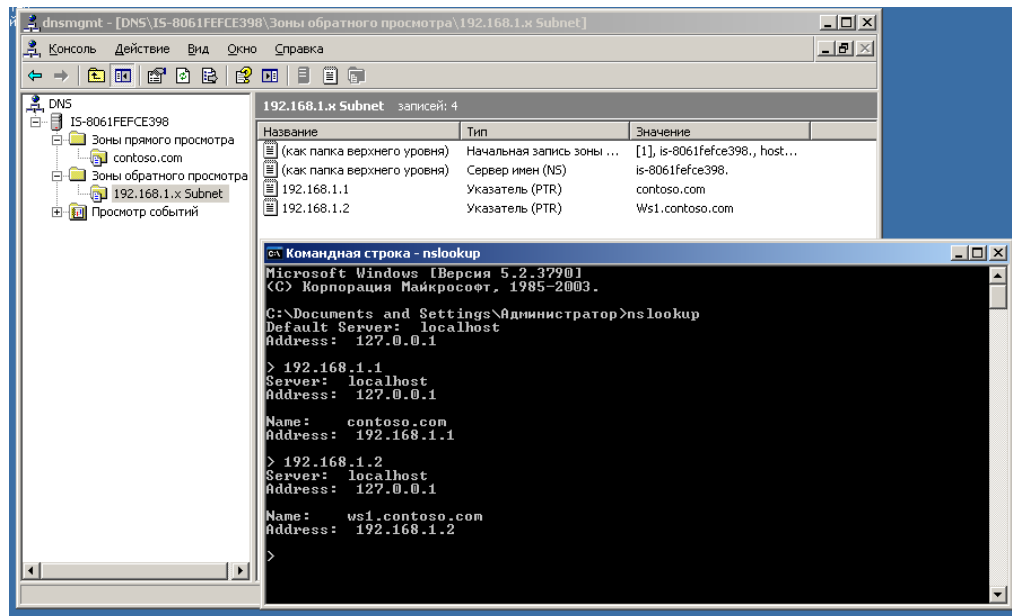


Рис. 9.25. Результати виконання *nslookup* у *Windows Server*

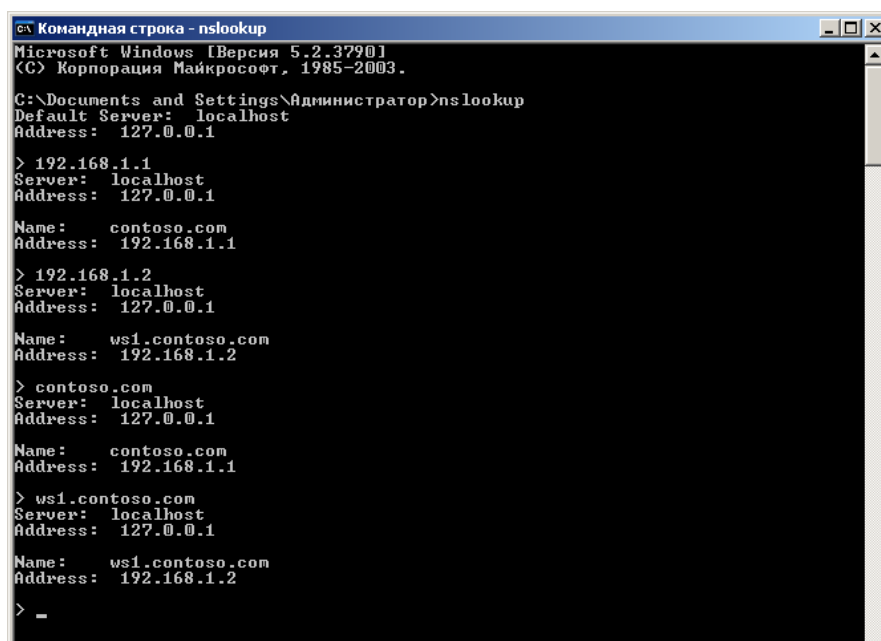
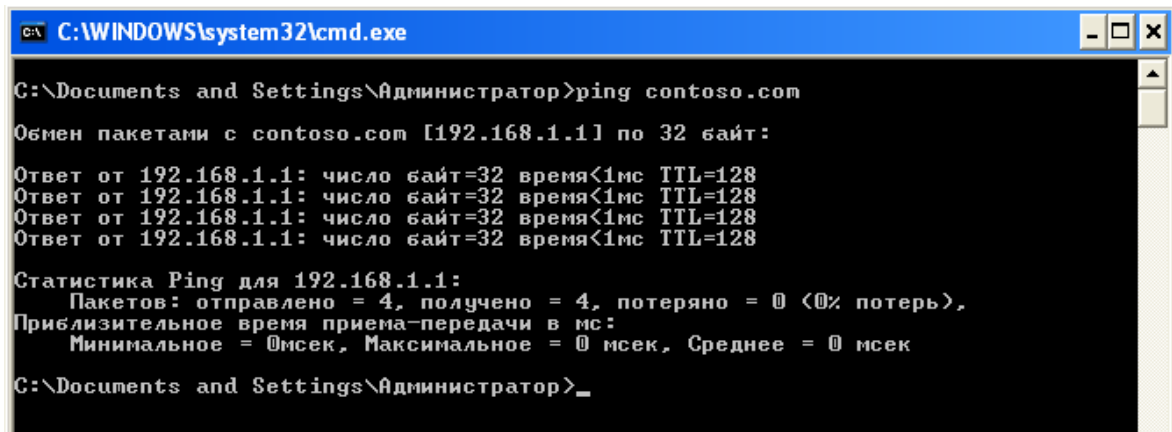


Рис. 9.26. Результат перевірки у *Windows Server*

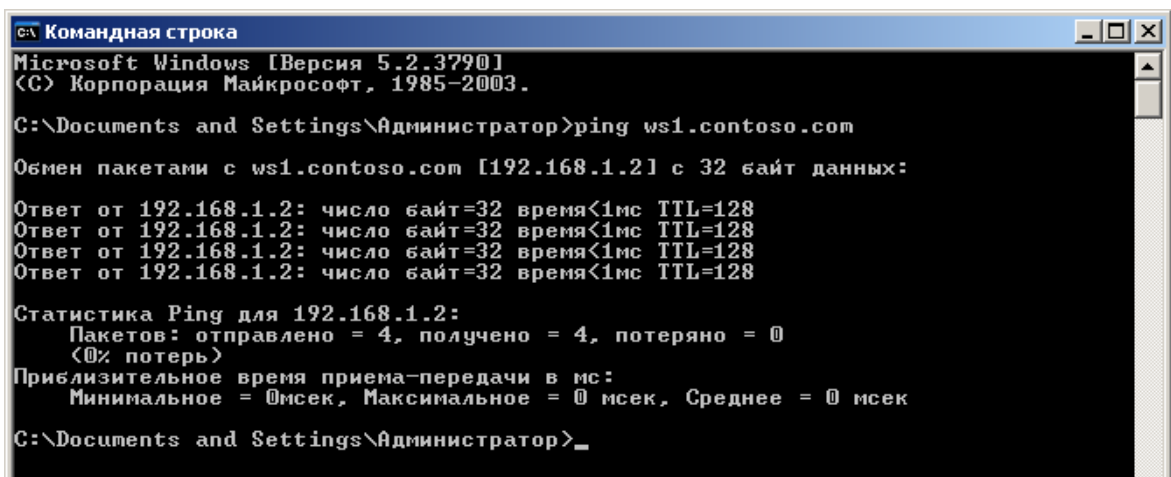
Провести перевірку роботи мережі з використання DNS імен за допомогою команди ping. Необхідно на *Windows Server* задати ім'я робочої станції, а у *Windows XP* ім'я сервера (рис. 9.27 і 9.28).



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Администратор>ping contoso.com
Обмен пакетами с contoso.com [192.168.1.1] по 32 байт:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
C:\Documents and Settings\Администратор>
```

Рис. 9.27. Результат перевірки у *Windows XP*



```
Командная строка
Microsoft Windows [Версия 5.2.3790.1
(C) Корпорация Майкрософт, 1985-2003.
C:\Documents and Settings\Администратор>ping ws1.contoso.com
Обмен пакетами с ws1.contoso.com [192.168.1.2] с 32 байт данных:
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.1.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
C:\Documents and Settings\Администратор>
```

Рис.9.28. Результат перевірки у *Windows Server*

9.3 Оброблення та аналізування результатів. Оформлення звіту.

1. Назва практичної роботи, тема, мета й зміст завдань лабораторної роботи (ЛР).
2. Вихідні дані до практичної роботи.
3. Отримані в результаті виконання ЛР скріншоти результатів виконання

завдань практичної роботи.

4. Висновки з практичної роботи.

9.4 Контрольні питання

1. Яке призначення DNS-сервера?
2. Що є прямою зоною DNS-сервера?
3. Що є зворотною зоною DNS-сервера?
4. Яким чином визначається батьківська адреса під час створення нової прямої зони в DNS-сервері?
5. Яким чином визначається дочірня адреса під час створення нової прямої зони в DNS-сервері?
6. Яким чином та де використовується на практиці DNS-сервер?

Список рекомендованої літератури

1. Комп'ютерні мережі : навч. посіб. для техн. спец. ВНЗ. Кн.2 / А. Г. Микитишин [та ін.] ; М-во освіти і науки, молоді та спорту України. – Львів : Магнолія 2006, 2014. – 328 с.
2. Комп'ютерні мережі: навчальний посібник / Ю. І. Лосев, К. М. Руккас, С. І. Шматков / За редакцією Ю. І. Лосева. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 248 с.
3. Комп'ютерні мережі : підручник / Є.В. Буров. – Львів : Магнолія 2006, 2010. – 262 с. - (Вища освіта в Україні).
4. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж : навчальний посібник / С.В. Мінухін, С.В. Кавун, С.В. Знахур; Міністерство освіти і науки України, Харківський національний економічний університет. – Харків : ХНЕУ, 2008. – 208 с.
5. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е издание / В.Г.Олифер, Н.А. Олифер – СПб.: Питер, 2010. – 944 с.: ил.
6. Промислові мережі та інтеграційні технології в автоматизованих системах / О.М. Пупена, І.В. Ельперін, Н.М. Луцька, А.П. Ладанюк; – К.: Вид-во «Ліра-К», 2011. – 552 с.
7. Комп'ютерні мережі. Навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. – Вінниця : ВНТУ, 2015. – 128 с.
8. Комп'ютерні мережі [Текст] : навчальний посібник для студентів вищих навчальних закладів / О. О. Гордєєв, Д. В. Гордєєва, М. В. Колдовський ; Державний вищий навчальний заклад “Українська академія банківської справи Національного банку України”. – Суми : ДВНЗ “УАБС НБУ”, 2011. – 250 с.
9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е издание – СПб.: Питер, 2010. – 944 с.: ил.
10. Кузин А.В. Компьютерные сети: учебное пособие. – 3-е изд. перераб. и доп. – М.: Форум: Инфра-М, 2011. – 192 с.: ил. – (Профессиональное образование).
11. Ноэл Майкл, Спенс Колин Microsoft SharePoint 2010. Полное руководство.:

Пер. с англ. – М.: ООО «И.Д.Вильямс», 2011. – 880 с.: ил.- Паралел. тит. англ.

12. Пупена О.М., Ельперін І.В., Луцька Н.М., Ладанюк А.П. Промислові мережі та інтеграційні технології в автоматизованих системах: Навчальний посібник.– К.: Вид-во "Ліра-К", 2011. – 552 с.