

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

# **КОМП’ЮТЕРНІ МЕРЕЖІ**

## **МЕТОДИЧНІ ВКАЗІВКИ**

до виконання лабораторних робіт  
з дисципліни “Комп’ютерні мережі”  
для студентів напряму підготовки 6.050101 “Комп’ютерні науки”

Затверджено  
на засіданні кафедри  
“Інформаційні системи та мережі”  
Протокол № \_\_\_\_ від \_\_\_\_\_ р.

Львів – 2015

**Комп'ютерні мережі** : методичні вказівки до виконання лабораторних робіт з дисципліни “Комп'ютерні мережі” для студентів напряму підготовки 6.050101 “Комп'ютерні науки” / уклад.: Ю. В. Ришковець, Є. В. Буров. – Львів, Видавництво “Львівська політехніка”, 2015. – 80 с.

**Укладачі:** Ришковець Ю.В., к.т.н., асист.,  
Буров Є.В., к.т.н., доц.

**Відповідальний за випуск:** Литвин В.В., д.т.н., проф.

**Рецензенти:** Голощук Р. О., к.т.н., доц.  
Григорович В. Г., к.фіз.-мат.н., доц.

## ЗМІСТ

Лабораторна робота № 1. Розрахунок комп'ютерних підмереж .....	4
Лабораторна робота № 2. Налаштування комп'ютерної мережі в ОС Microsoft Windows 7 .....	14
Лабораторна робота № 3. Дослідження роботи та налаштування протоколів стеку TCP/IP .....	23
Лабораторна робота № 4. Налаштування мережевих компонент ОС Linux Ubuntu .....	30
Лабораторна робота № 5. Робота у середовищі NetCracker Professional .....	36
Лабораторна робота № 6. Проектування однорівневої комп'ютерної мережі у середовищі NetCracker Professional.....	45
Лабораторна робота № 7. Багаторівневе проектування комп'ютерної мережі у середовищі NetCracker Professional.....	57
Лабораторна робота № 8. Проектування комп'ютерної мережі в Cisco Packet Tracer.....	59
Лабораторна робота № 9. Налаштування з'єднання з комутатором в Cisco Packet Tracer.....	70
Лабораторна робота № 10. Налаштування віртуальних мереж в Cisco Packet Tracer.....	75
Список використаних джерел.....	80

## Лабораторна робота № 1. Розрахунок комп'ютерних підмереж

**Мета роботи:** навчитися розподіляти простір IP-адрес, розробляти схеми IP-адресування в мережі з маскою підмережі змінної довжини.

### *Теоретичні відомості*

За адресацію пакетів у стеку ТСП/IP відповідає протокол IP, який належить до мережевого рівня. Він призначений для маршрутизації та надсилання пакетів у великій мережі, що об'єднує довільну кількість неоднорідних мереж з різною структурою зв'язків і різноманітними принципами передавання повідомлень між кінцевими вузлами.

**IP-адреса** (Internet Protocol address – IP-address) – це ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу ТСП/IP (наприклад, Інтернет).

Стандарти ТСП/IP описують дві версії протоколу IPv4 та IPv6, але найбільш поширеною є версія IPv4.

За стандартом протоколу IPv4 IP-адреса має довжину 32 біти, які поділені на чотири октети (по 8 бітів). IP-адреса може записуватись як у двійковому (binary) форматі, так і в десятковому форматі з крапковими розділювачами (dotted decimal notation). У десятковому форматі кожний октет записується у вигляді десяткового числа з діапазону від 0 до 255 і відокремлюється від іншого октета крапкою, наприклад, 192.168.5.31.

Кількість IP-адрес для хостів залежить від розмірів мережі, тому існує декілька класів мереж (табл. 1.1).

Таблиця 1.1.

Клас	Призначення	Найменша IP-адреса	Найбільша IP-адреса
A	Для декількох великих компаній	1.0.0.0	126.0.0.0
B	Для середніх організацій	128.0.0.0	191.255.0.0
C	Для порівняно невеликих організацій	192.0.0.0	223.255.255.0
D	Для багатоадресної групи (групова адресація)	224.0.0.0	239.255.255.255
E	Для досліджень	240.0.0.0	254.255.255.255

Для комерційного використання призначені лише класи А, В та С. IP-адреса 127.0.0.0 (клас А) зарезервована для кільцевої перевірки (контрольної петлі) і використовується для тестування ТСП/IP та для процесів внутрішньої комунікації в локальному вузлі; це не мережева адреса, тому трафік у мережу з неї не передається.

Адреси 224 і вище (класи D та E) зарезервовані для спеціальних протоколів і не можуть використовуватися як адреси хост-пристроїв. Адреси 0 і 255 використовуються як широкосповіщальні адреси, тому їх не варто призначати комп'ютерам.

Якщо певна мережа призначена для роботи в “автономному режимі”, тобто без зв'язку з Інтернет, то в стандартах Інтернет визначено декілька діапазонів адрес, рекомендованих для локального використання. Ці адреси не опрацьовуються маршрутизаторами глобальної мережі Інтернет за жодних умов. Адреси, зарезервовані для локальних цілей, вибрані з різних класів: для класу A – це мережа 10.0.0.0, для класу B – це діапазон мереж 172.16.0.0–172.31.0.0, а для класу C – це діапазон мереж 192.168.0.0–192.168.255.0.

IP-адреса складається з двох частин – адреси мережі та адреси хоста, розмір яких визначається на основі маски підмережі (рис. 1.1). У локальній мережі частина IP-адреси, що відповідає за адресу мережі, у всіх хостів повинна бути однаковою, а частина, що відображає адресу хоста, – для всіх хостів різна.

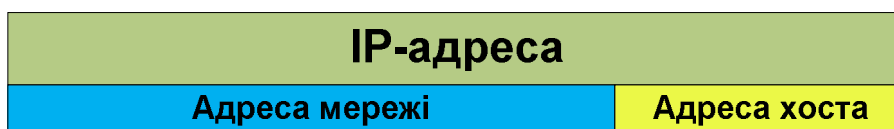


Рис. 1.1. Структура IP-адреси

**Маска підмережі** (network mask) визначає, яка частина IP-адреси використовується для ідентифікації мережі, а яка – для ідентифікації комп'ютера. Маска підмережі – це 32-розрядне значення, подане у вигляді послідовності чотирьох октетів (по 8 бітів), розділених крапками. Маска підмережі дає змогу отримувачу (адресату) пакета даних розділити (накласти маску) IP-адресу, за якою передається IP-пакет, на ідентифікатор мережі та ідентифікатор хост-пристрою.

У табл. 1.2 подані маски підмережі, які встановлюються за замовчуванням для стандартних мереж класів A, B і C.

Таблиця 1.2.

Клас	Маска підмережі	Кількість мереж	Кількість вузлів
A	255.0.0.0	$2^8 - 2 = 254$	$2^{24} - 2 = 16777214$
B	255.255.0.0	$2^{16} - 2 = 65534$	$2^{16} - 2 = 65534$
C	255.255.255.0	$2^{24} - 2 = 16777214$	$2^8 - 2 = 254$

IP-адреса завжди відображає одне з таких значень:

- адреса мережі;
- широкосповіщальна адреса;
- адреса інтерфейсу.

Інколи потрібно звернутися до всіх пристроїв мережі, тобто до самої мережі, а оскільки оперувати адресами всіх пристроїв мережі доволі складно, то використовується адреса мережі. У схемах IP-адресації будь-яка IP-адреса, що закінчується всіма двійковими нулями, резервується для адреси цієї мережі. Наприклад, для IP-адреси 192.168.5.35 з маскою 255.255.255.0, адреса мережі

буде дорівнювати 192.168.5.0, тому що 8 останніх бітів (останній октет) маски є нулями.

Процес, під час якого джерело надсилає дані всім пристроям у мережі, називається **ширококопівіщальним**.

*Ширококопівіщальна адреса (broadcast address)* використовується для трансляції пакетів повідомлень усім комп'ютерам, об'єднаним в мережу. Отже, якщо IP-адреса комп'ютера в мережі визначається останнім байтом (інакше кажучи, якщо маска дорівнює 255.255.255.0), то ширококопівіщальна адреса є результатом побітової операції **OR** маски 0.0.0.255 з IP-адресою комп'ютера. Наприклад, якщо IP-адреса комп'ютера є 128.253.154.32, а маска – 255.255.255.0, то ширококопівіщальна адреса буде дорівнювати 128.253.154.255.

Маски підмережі, що подані в табл. 2.1, не єдині маски, що можуть використовуватися для адресації в мережі. Іноді потрібно накласти маску тільки на деякі біти в октеті. Однак мережева адреса і маска підмережі повинні відповідати один одному для кожного хост-пристрою в локальній мережі.

В оригінальній схемі IP-адресації будь-якій фізичній мережі призначена унікальна мережева адреса; будь-який вузол у мережі використовує мережеву адресу як префікс до індивідуальної адреси вузла. Такий поділ зумовлений потребами процесу маршрутизації пакетів. Окремі територіальні мережі мають певну свободу в модифікації адрес і маршрутів, що дає змогу розширити кількість адрес.

Використання підмереж має низку переваг. В організаціях підмережі використовуються для об'єднання декількох фізичних сегментів в одну логічну мережу. Застосування підмережі дає змогу:

- спільно використовувати різні мережеві технології (наприклад, Ethernet, Token Ring);
- подолати обмеження, що існують, наприклад, на максимальну кількість вузлів в одному сегменті, а також спрощує адресацію між ними за рахунок скорочення кількості біт, що залишаються для визначення адреси хоста;
- зменшити навантаження на мережу, перенаправляючи мережевий трафік і зменшуючи кількість ширококопівіщальних пакетів.

Адреса підмережі визначається шляхом логічного множення (логічна операція **AND**) IP-адреси на маску:

$$\langle \text{Адреса підмережі} \rangle = \langle \text{IP-адреса} \ \& \ \text{маска} \rangle$$

Класова адресація не найефективніший метод використання обмеженої кількості IP-адрес, допустимих у 32-розрядній схемі адресації. Припустимо компанія бажає під'єднати до Інтернету 2000 комп'ютерів. Адреси класу C не підійдуть, тому що в цьому класі мережа може містити не більше 254 хостів. Наступний клас B дає змогу розмістити 65534 хостів, але це занадто багато. Тому якщо компанія розмістить свої 2000 хостів у мережі класу B, то інші 63534 IP-адрес не будуть використовуватись, тобто будуть втрачені. Для розв'язання цієї проблеми використовують метод безкласової адресації CIDR.

У методі безкласової адресації CIDR використовуються не класи IP-адрес, а суфікси, додані до кожної IP-адреси, які визначають кількість бітів, виділених для мережевої частини адреси. Мережі CIDR інколи називаються

мережами “слеш х”, тому що IP-адреса відокремлюється від суфікса символом слешу (/). Наприклад, типова адреса CIDR виглядає так: 192.168.1.0/24. Символи “/24” означають, що крайні ліві 24 біти IP-адреси використовуються для зберігання номера мережі, а інші вісім бітів – для номера хоста. У класовій схемі адресації розглянута мережа відповідає класу С.

**Приклад 1.1.** Нестандартні маски для створення підмереж класу С:

Кількість підмереж	Кількість хостів	Мережева маска
2	126	255.255.255.128 (11111111.11111111.11111111.10000000)
4	62	255.255.255.192 (11111111.11111111.11111111.11000000)
8	30	255.255.255.224 (11111111.11111111.11111111.11100000)
16	14	255.255.255.240 (11111111.11111111.11111111.11110000)
32	6	255.255.255.248 (11111111.11111111.11111111.11111000)
64	2	255.255.255.252 (11111111.11111111.11111111.11111100)

Для визначення максимальної кількості хостів у мережі використовується формула:  $N = 2^n - 2$ , де  $n$  – кількість двійкових розрядів, відведених під ідентифікатор хоста. Зменшення загальної кількості хостів у мережі на 2 пояснюється наявністю в полі адрес вузлів кожної з мереж адреси цієї мережі та її широкомовіщальної адреси.

У багатьох випадках, наприклад, з метою зниження трафіка, чи для організації робочих груп, з'являється необхідність розбиття на підмережі або сегменти. Здійснюється таке розбиття за допомогою масок підмереж. Це призводить до зниження кількості вузлів у мережі, а також спрощує адресацію між ними через скорочення кількості біт, що залишаються для визначення адреси хоста.

**Алгоритм визначення знаходження двох вузлів в одній підмережі** такий:

1. Переведіть адреси комп'ютерів і маску в двійковий вигляд.
2. Для отримання двійкового представлення номерів підмереж обох вузлів виконайте операцію побітового логічного множення AND над IP-адресою і маскою відповідного комп'ютера.
3. Двійковий результат переведіть у десятковий вигляд.
4. Порівняйте отримані результати для комп'ютерів і зробіть висновок. Якщо результати повністю співпадають, то вузли знаходяться в одній підмережі, а якщо ні – у різних.

**Приклад 1.2.** Визначити, чи розміщені вузли А і В в одній підмережі. IP-адреси комп'ютера А і комп'ютера В відповідно рівні: 26.219.123.6 та 26.218.102.31, маска підмережі 255.192.0.0.

Комп'ютер А:

**Десятковий вигляд:**

*IP-адреса:*

26.219.123.6

*Маска підмережі:*

255.192.0.0

**Двійковий вигляд:**

00011010.11011011.01111011.00000110

11111111.11000000.00000000.00000000

AND<sub>(2)</sub>

00011010.11000000.00000000.00000000

AND<sub>(10)</sub>

26

192

0

0

Комп'ютер В:

Десятковий вигляд:

IP-адреса:

26.218.102.31

Маска підмережі:

255.192.0.0

Двійковий вигляд:

00011010.11011010.01100110.00011111

11111111.11000000.00000000.00000000

AND<sub>(2)</sub>

00011010.11000000.00000000.00000000

AND<sub>(10)</sub>

26

192

0

0

Повне співпадіння номерів підмереж вузлів А та В, отриманих в результаті побітової операції AND (тобто 26.192.0.0), означає, що ці вузли знаходяться в одній підмережі. Отже, між ними можна встановити пряме з'єднання без застосування шлюзів.

**Алгоритм визначення маски підмережі за діапазоном IP-адрес такий:**

1. Переведіть початкову та кінцеву IP-адреси із заданого діапазону у двійковий вигляд і визначте співпадаючу частину бітів, починаючи зліва.
2. Заповніть співпадаючу частину бітів одиницями, а решту бітів – нулями.
3. Переведіть отриману адресу у десятиковий вигляд.

**Приклад 1.3.** Визначити маску підмережі, що відповідає діапазону IP-адрес 172.16.65.1 – 172.16.181.254.

- 1) Визначимо кількість незмінних біт в адресі, починаючи з початку:

початкова адреса:

172.16.65.1

10101100.00010000.00110110.00000001

кінцева адреса:

172.16.181.254

10101100.00010000.01000001.11111110

- 2) Визначимо маску:

маска підмережі:

11111111.11111111.10000000.00000000

- 3) Подамо отриману маску у десятиковій системі числення:

маска підмережі: 255.255.128.0

Отже, маска підмережі, що відповідає діапазону IP-адрес 172.16.65.1 – 172.16.181.254 дорівнює 255.255.128.0.

**Алгоритм визначення кількості вузлів і діапазонів їхніх IP-адрес у підмережі, якщо відомі номер та маска підмережі такий:**

1. Переведіть номер і маску підмережі у двійковий вигляд.
2. На основі маски визначте кількість біт, значення яких рівне нулю, і позначте їх літерою К; ці нульові біти використовуються для адресації вузлів; біти, що відповідають за номер підмережі, рівні одиниці.
3. Загальна кількість адрес мережі рівна  $2^K$ , але з цього числа слід виключити адресу мережі та широковещальну адресу, що складаються з усіх нулів та всіх одиниць відповідно. Отже, загальна кількість вузлів підмережі буде дорівнювати  $2^K - 2$ .



4. Щоб отримати початкову IP-адресу підмережі, потрібно біти IP-адреси (справа), що відповідають нульовим бітам у масці, заповнити нулями, а крайній правий біт встановити в одиницю. Отримана адреса буде першою з допустимих адрес певної підмережі.
5. Щоб отримати кінцеву IP-адресу підмережі, потрібно біти IP-адреси (справа), що відповідають нульовим бітам у масці, заповнити одиницями, а крайній правий біт встановити в нуль. Отримана адреса буде останньою з допустимих адрес певної підмережі.

**Приклад 1.4.** Визначити кількість і діапазон адрес вузлів у підмережі, якщо її номер дорівнює 26.219.128.0, а маска – 255.255.192.0.

- 1) Визначимо кількість співпадаючих біт в адресі та масці, починаючи справа:

*номер підмережі:* 26.219.128.0      00011010.11011011.10000000.00000000

*маска підмережі:* 255.255.192.0      11111111.11111111.11000000.00000000

$K = 14$ .

- 2) Визначимо кількість вузлів у підмережі:  $2^{14} - 2 = 16382$ .

- 3) Визначимо початкову адресу підмережі:

*початкова адреса:* 26.219.128.1      00011010.11011011.10000000.00000001

*маска підмережі:* 255.255.192.0      11111111.11111111.11000000.00000000

- 4) Визначимо кінцеву адресу підмережі:

*кінцева адреса:* 26.219.191.254      00011010.11011011.10111111.11111110

*маска підмережі:* 255.255.192.0      11111111.11111111.11000000.00000000

Отже, для підмережі 26.219.128.0 з маскою 255.255.192.0 кількість можливих адрес дорівнює 16382, а діапазон можливих адрес – 26.219.128.1 – 26.219.191.254.

**Алгоритм визначення кількості підмереж і діапазонів IP-адрес у підмережі, якщо відомі номер та маска підмережі** такий:

1. Визначаємо загальну кількість вузлів у мережі ( $2^K - 2$ ).
2. Для визначення кількості вузлів у підмережі загальну кількість вузлів у мережі потрібно поділити на задану (орієнтовну) кількість вузлів у проєктованій мережі. Далі потрібно знайти число, що кратне числу 2 і при цьому розміщене якнайближче до значення загальної кількості вузлів у мережі, але не більше останнього. Після цього подати його у вигляді  $2^N$ , де  $N$  – кількість бітів, які потрібно виділити під номер вузла, інші біти виділяються під маску.
3. Визначаємо нову маску підмережі.
4. Щоб визначити кількість підмереж, потрібно кількість вузлів у мережі поділити на кількість вузлів у підмережі.



### ***Варіанти завдань***

№ з/п	№ завдання			
	1	2	3	4
1	IP-адреса комп'ютера А: 94.235.16.59; IP-адреса комп'ютера В: 94.235.23.240; Маска підмережі: 255.255.240.0.	Номер підмережі: 192.168.1.0, маска підмережі: 255.255.255.0	119.38.0.1 – 119.38.255.254	192.210.10.0/24 Кількість вузлів ~ 70
2	IP-адреса комп'ютера А: 131.189.15.6; IP-адреса комп'ютера В: 131.173.216.56; Маска підмережі: 255.248.0.0.	Номер підмережі: 110.56.0.0, маска підмережі: 255.248.0.0	75.96.0.1 – 75.103.255.254	193.115.2.0/24 Кількість вузлів ~ 30
3	IP-адреса комп'ютера А: 215.125.159.36; IP-адреса комп'ютера В: 215.125.153.56; Маска підмережі: 255.255.224.0.	Номер підмережі: 88.217.0.0, маска підмережі: 255.255.128.0	48.192.0.1 – 48.255.255.254	194.78.120.0/24 Кількість вузлів ~ 100
4	IP-адреса комп'ютера А: 47.154.1.71; IP-адреса комп'ютера В: 47.154.13.240; Маска підмережі: 255.255.248.0.	Номер підмережі: 195.5.5.0, маска підмережі: 255.255.255.192	19.83.0.1 – 19.83.255.254	200.57.127.0/24 Кількість вузлів ~ 20
5	IP-адреса комп'ютера А: 145.19.10.16; IP-адреса комп'ютера В: 145.73.112.36; Маска підмережі: 255.252.0.0.	Номер підмережі: 53.109.0.0, маска підмережі: 255.224.0.0	16.46.0.1 – 16.53.255.254	197.20.55.0/24 Кількість вузлів ~ 250
6	IP-адреса комп'ютера А: 192.168.72.236; IP-адреса комп'ютера В:	Номер підмережі: 55.115.0.0, маска підмережі:	84.192.0.1 – 84.224.255.254	198.37.61.0/24 Кількість вузлів ~ 33

№ з/п	№ завдання			
	1	2	3	4
	192.168.253.14; Маска підмережі: 255.255.192.0.	255.255.255.0		
7	IP-адреса комп'ютера А: 14.74.19.171; IP-адреса комп'ютера В: 14.74.10.24; Маска підмережі: 255.255.224.0.	Номер підмережі: 199.99.11.0, маска підмережі: 255.255.255.224	39.94.0.1 – 39.94.255.254	199.42.111.0/24 Кількість вузлів ~ 80
8	IP-адреса комп'ютера А: 161.119.210.61; IP-адреса комп'ютера В: 161.178.12.136; Маска підмережі: 255.254.0.0.	Номер підмережі: 10.81.0.0, маска підмережі: 255.252.0.0	25.36.0.1 – 25.113.255.254	200.192.91.0/24 Кількість вузлів ~ 61
9	IP-адреса комп'ютера А: 198.225.19.145; IP-адреса комп'ютера В: 198.225.13.12; Маска підмережі: 255.255.240.0.	Номер підмережі: 71.127.0.0, маска підмережі: 255.255.192.0	54.192.0.1 – 54.240.255.254	201.168.72.0/24 Кількість вузлів ~ 25
10	IP-адреса комп'ютера А: 27.90.66.123; IP-адреса комп'ютера В: 27.90.88.211; Маска підмережі: 255.255.192.0.	Номер підмережі: 203.18.10.0, маска підмережі: 255.255.192.0	95.8.0.1 – 95.8.255.254	202.151.168.0/24 Кількість вузлів ~ 15
11	IP-адреса комп'ютера А: 172.16.92.5; IP-адреса комп'ютера В: 172.207.73.209; Маска підмережі: 255.240.0.0.	Номер підмережі: 61.93.0.0, маска підмережі: 255.254.0.0	65.16.0.1 – 65.96.255.254	203.134.83.0/24 Кількість вузлів ~ 94
12	IP-адреса комп'ютера А: 211.5.63.42;	Номер підмережі: 16.94.0.0,	61.192.0.1 – 61.248.255.254	204.127.98.0/24 Кількість вузлів ~ 42

№ з/п	№ завдання			
	1	2	3	4
	IP-адреса комп'ютера В: 211.5.98.73; Маска підмережі: 255.255.248.0.	маска підмережі: 255.255.224.0		
13	IP-адреса комп'ютера А: 11.12.93.68; IP-адреса комп'ютера В: 11.12.240.51; Маска підмережі: 255.255.252.0.	Номер підмережі: 220.145.74.0, маска підмережі: 255.255.224.0	122.156.0.1 – 122.156.255.254	205.73.16.0/24 Кількість вузлів ~ 47
14	IP-адреса комп'ютера А: 128.111.34.78; IP-адреса комп'ютера В: 128.222.86.132; Маска підмережі: 255.224.0.0.	Номер підмережі: 125.156.0.0, маска підмережі: 255.240.0.0	11.12.0.1 – 11.74.255.254	206.192.119.0/24 Кількість вузлів ~ 49
15	IP-адреса комп'ютера А: 223.255.36.57; IP-адреса комп'ютера В: 223.192.81.155; Маска підмережі: 255.255.252.0.	Номер підмережі: 37.59.0.0, маска підмережі: 255.255.248.0	12.192.0.1 – 12.252.255.254	207.54.189.0/24 Кількість вузлів ~ 97

### ***Контрольні запитання***

1. Поясніть поняття маски підмережі.
2. Що таке адреса мережі?
3. Навіщо використовується широкосповіщальна адреса?
4. Яке призначення адреси інтерфейсу?
5. Дайте визначення поняття “класова адресація”.
6. У чому полягає особливість методу безкласової адресації CIDR?
7. Для чого використовується розбиття на підмережі?

## **Лабораторна робота № 2.**

### **Налаштування комп'ютерної мережі в ОС Microsoft Windows 7**

**Мета роботи:** навчитися підключати комп'ютер до локальної мережі та одержати навички в налаштуванні мережевих компонентів комп'ютера.

#### ***Теоретичні відомості***

Для правильної роботи будь-якого пристрою в комп'ютері має бути встановлена програма-драйвер, яка є посередником між операційною системою та пристроєм. Під час встановлення драйвера операційна система виділяє для нового пристрою частину ресурсів комп'ютера та реєструє пристрій і його драйвер у спеціальному реєстрі.

Перед початком процесу встановлення мережевого клієнтського програмного забезпечення на комп'ютерах з операційною системою (ОС) Windows 7 необхідно встановити та налаштувати мережевий адаптер для кожного комп'ютера.

За допомогою програм-майстрів в ОС Windows 7 можна швидко налаштувати адаптер та комп'ютерні ресурси для нього, включаючи номер переривання IRQ, адресу пам'яті та порт введення/виведення (I/O).

Взаємодія комп'ютерних мереж ґрунтується на використанні спільного *протоколу* – набору правил обміну інформацією між комп'ютерами.

*Протокол керування передаванням/Протокол Інтернету* (Transmission Control Protocol/Internet Protocol – TCP/IP) – це протокол, що підтримується в мережі Інтернет. Він найчастіше використовується у локальних мережах, а в операційній системі Windows 7 протокол TCP/IP встановлюється автоматично.

Кожний клієнт мережі TCP/IP має власну IP-адресу. Без неї клієнтський комп'ютер не може передавати або отримувати інформацію.

Розрізняють протоколи TCP/IP v.4 та v.6. В TCP/IP v.4 IP-адреса складається з двох частин. Перша частина використовується для ідентифікації мережі, до якої підключено комп'ютер, а друга – для ідентифікації самого комп'ютера в мережі.

В одному комп'ютері можуть бути встановлені та працювати декілька мережевих адаптерів, кожен з яких одночасно може мати багато IP-адрес. Спосіб, що дає змогу закріплювати декілька IP-адрес за однією апаратною адресою, одержав назву **IP-аліасінг**. Варто зауважити, що одночасне призначення певної IP-адреси декільком мережевим інтерфейсам (одного чи різних пристроїв) призведе до виникнення помилок та колізій у комп'ютерній мережі.

Маска підмережі у протоколі TCP/IP v.4 містить чотири тетради, а в TCP/IP v.6 – вісім. Як правило, на основі протоколу TCP/IP v.4 маски мають вигляд 255.x.y.z, де x, y та z – цілі числа від 0 до 255; наприклад, 255.255.255.0.

**Адреса шлюза** (gateway address) – це адреса комп'ютера, який є “шлюзом” у зовнішній світ, тобто до комп'ютерів, які розташовані поза локальною мережею. При проектуванні мережі прийнято, щоб адреса

маршрутизатора виходила з IP-адреси комп'ютера заміною останніх груп цифр. Наприклад, якщо IP-адреса комп'ютера є 128.253.154.32, то адреса шлюза може бути 128.253.154.1. Але така рекомендація не є обов'язковою.

**Шлюз** (gateway) – це комп'ютер, що з'єднує дві різні мережі, забезпечуючи передачу пакетів повідомлень між цими мережами. З метою економії зовнішніх IP-адрес більшість мереж мають єдиний шлюз у “зовнішній світ”. Проте в деяких випадках локальна мережа з'єднується з кількома іншими мережами, кожна з яких має свій шлюз.

**Сервер імен** (Name server – NS) – сервер, який перетворює ім'я комп'ютера в IP-адресу, тобто встановлює відповідність доменного імені, що відображає адміністративну приналежність комп'ютера, і IP-адреси, що відображає місце комп'ютера в мережі Інтернет. Будь-яке звернення у мережі з використанням доменного імені вимагає перетворення його в IP-адресу. **Система доменних імен** (Domain Name System – DNS) дає змогу звертатися до певного ресурсу, використовуючи зрозумілу для людського сприйняття назву (наприклад, PC-01, а не 192.168.54.118). У робочих групах DNS не використовується.

У багатьох організаціях більшість робочих станцій налаштовується на використання **протоколу динамічної конфігурації хоста** (Dynamic Host Configuration Protocol – DHCP). Це дає змогу клієнтським комп'ютерам динамічно отримувати IP-адреси, тобто клієнт отримує IP-адресу тоді, коли його користувач починає працювати у мережі. Протокол DHCP також забезпечує автоматичне налаштування параметрів маски підмережі для клієнтського комп'ютера. Якщо протокол DHCP не використовується, то потрібно власноруч ввести статичну IP-адресу на кожному клієнтському комп'ютері.

Для роботи комп'ютера в мережі він повинен мати визначені такі параметри:

- ім'я комп'ютера, яке має бути унікальне в межах локальної мережі;
- робочу групу (домен), назва якої буде спільною для певної групи комп'ютерів;
- мережевий протокол (IP-адресу, маску підмережі, шлюз (за потреби) та DNS-сервери (за потреби)).

Розглянемо налаштування назви комп'ютера та робочої групи в ОС Microsoft Windows 7.

На піктограмі **Мій комп'ютер** викличте контекстне меню та виберіть команду **Властивості** або ж виконайте наступні дії: **Панель керування → Система і безпека → Система**. У вікні **Система** навпроти пункту **Ім'я комп'ютера, ім'я домену та параметри робочої групи** виберіть **Змінити параметри** (рис. 2.1).

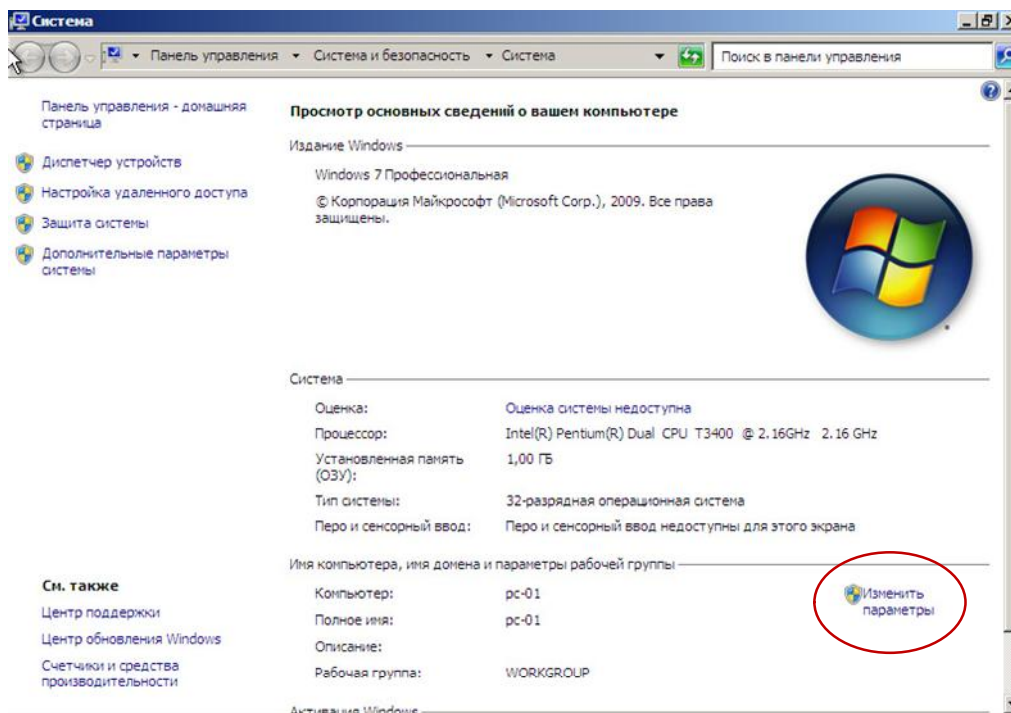


Рис. 2.1. Вікно властивостей системи

Відкриється вікно **Властивості системи** (рис. 2.2), в якому потрібно перейти на закладку **Ім'я комп'ютера**. Тут відображається ім'я комп'ютера та його робоча група або домен.

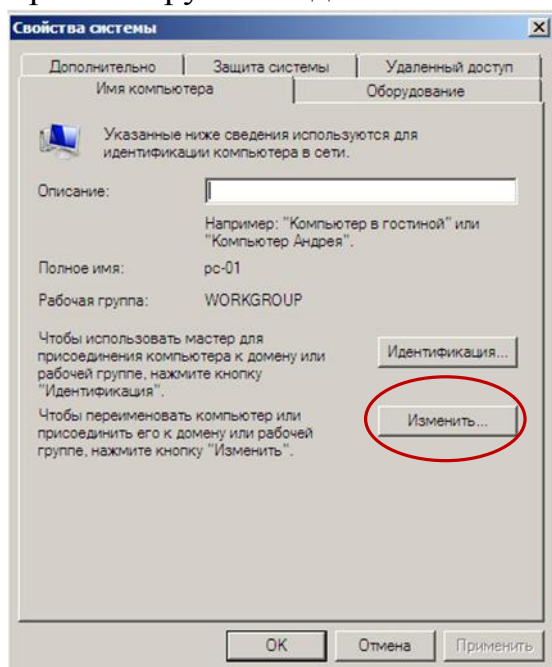


Рис. 2.2. Вікно властивостей системи: закладка імені комп'ютера

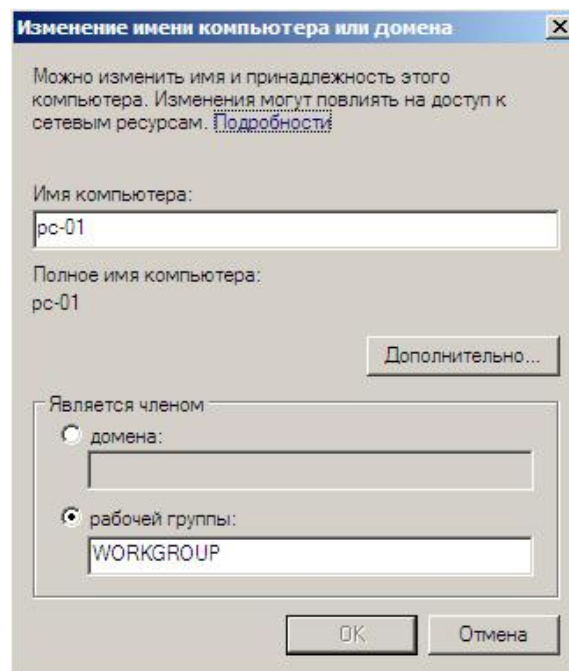


Рис. 2.3. Вікно зміни імені комп'ютера або домену

Щоб змінити один з цих параметрів або обидва, потрібно натиснути кнопку **Змінити** і у вікні **Зміна імені комп'ютера або домену** (рис. 2.3) ввести нові значення.



Після зміни назви комп'ютера система запропонує перезавантажити ОС, щоб нові параметри почали діяти.

Розглянемо налаштування мережевого протоколу в ОС Microsoft Windows 7.

На піктограмі робочого столу **Мережа** викличте контекстне меню та виберіть команду **Властивості** або ж виконайте наступні дії:

**Панель керування → Мережа та Інтернет → Цент керування мережами та спільним доступом** (рис. 2.4), у лівій частині цього вікна виберіть пункт **Зміна параметрів адаптера**. Відкриється вікно **Мережеві з'єднання** (рис. 2.5), в якому будуть відображені всі мережеві з'єднання даного комп'ютера.

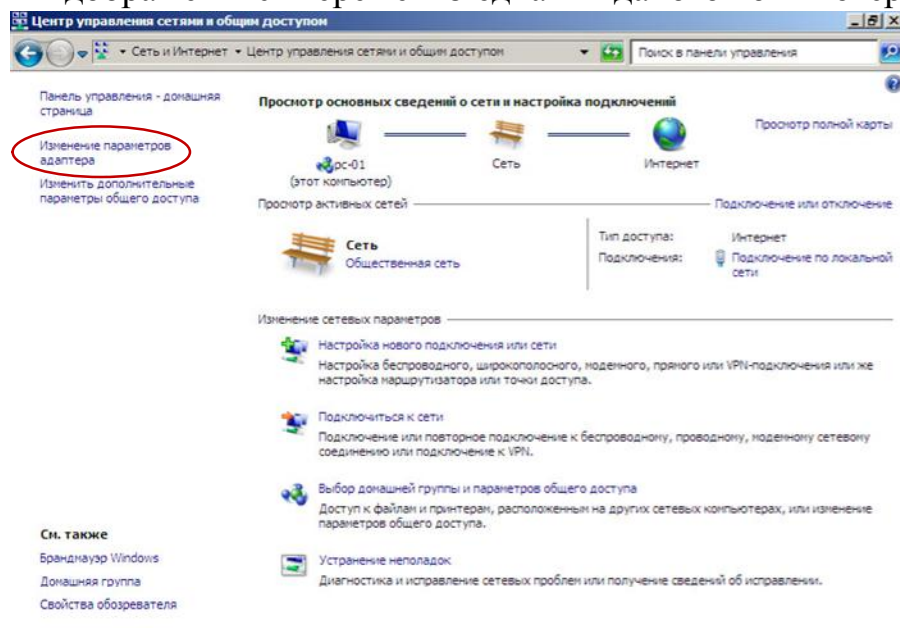


Рис. 2.4. Вікно центру керування мережами та спільним доступом

Для певного мережевого з'єднання викличте контекстне меню та виберіть команду **Властивості**.

У вікні властивостей цього з'єднання (рис. 2.6) зі списку компонентів вибираємо **“Internet Protocol Version 4 (TCP/IPv4)”** і натискаємо кнопку **Властивості**. Відкриється вікно властивостей протоколу TCP/IPv4 (рис. 2.7 а). Зверніть увагу на те, що за замовчуванням на закладці **Загальні** встановлені перемикачі **“Отримати IP-адресу автоматично”** та **“Отримати IP-адресу DNS-сервера автоматично”**, що дає змогу мережевому адаптеру автоматично отримувати мережеві налаштування.

Установіть перший перемикач у положення **“Використовувати таку IP-адресу”**, введіть IP-адресу та маску підмережі. За потреби вкажіть адресу основного шлюзу. Другий перемикач встановіть у положення **“Використовувати такі адреси DNS-серверів”** і введіть адреси двох DNS-серверів – основного та альтернативного (рис. 2.7 б). Натисніть кнопку **ОК** спочатку у вікні властивостей протоколу Інтернету, а потім – у вікні властивостей локального з'єднання.

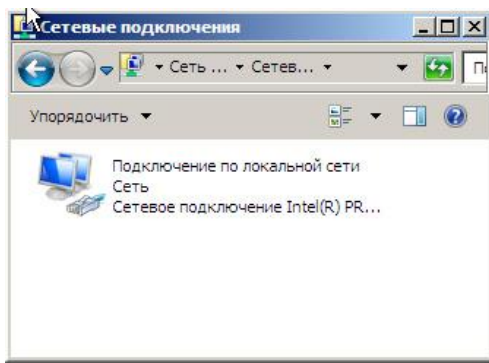


Рис. 2.5. Вікно мережевих з'єднань

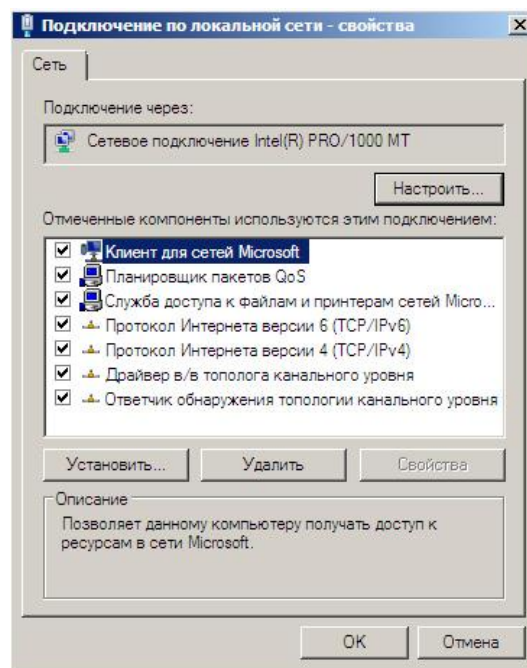
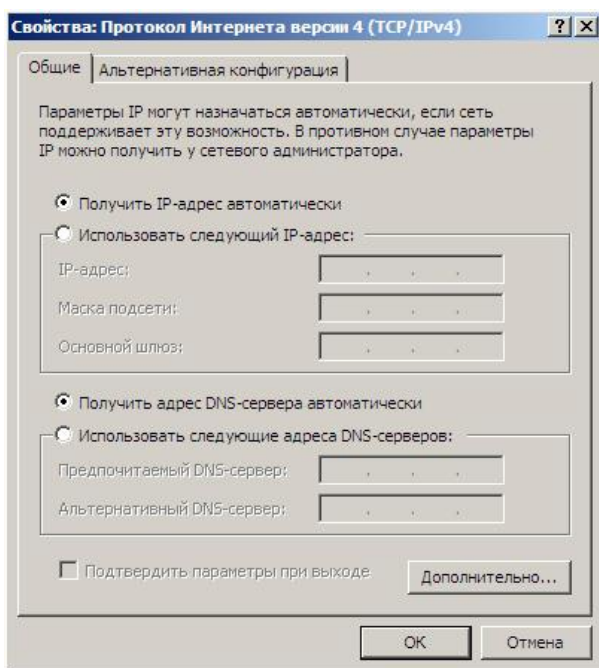
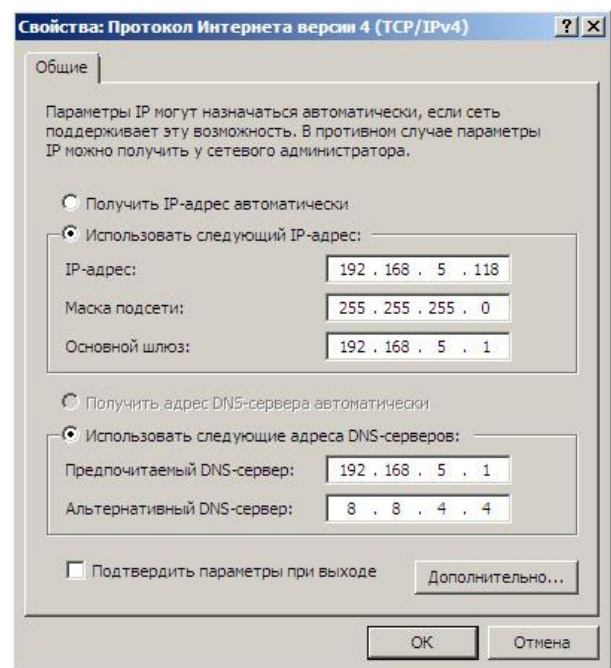


Рис. 2.6. Властивості мережевого з'єднання



а)



б)

Рис. 2.7. Властивості протокола TCP/IPv4:  
а) автоматичні налаштування; б) ручні налаштування

Інколи з'являється необхідність встановити новий або додатковий мережевий протокол, службу чи клієнта (мережевий компонент). Для цього у вікні властивостей з'єднання потрібно натиснути кнопку **Встановити** і вибрати відповідний тип мережевого компонента (рис. 2.8). Далі натиснути кнопку **Додати**, у новому вікні вибрати або встановити певний компонент і натиснути кнопку **ОК**. Після всіх цих дій мережевий компонент буде встановлений.

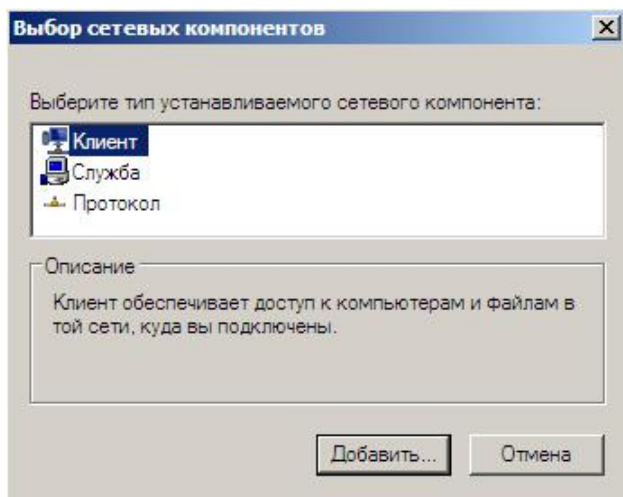


Рис. 2.8. Вибір типу мережевого компонента

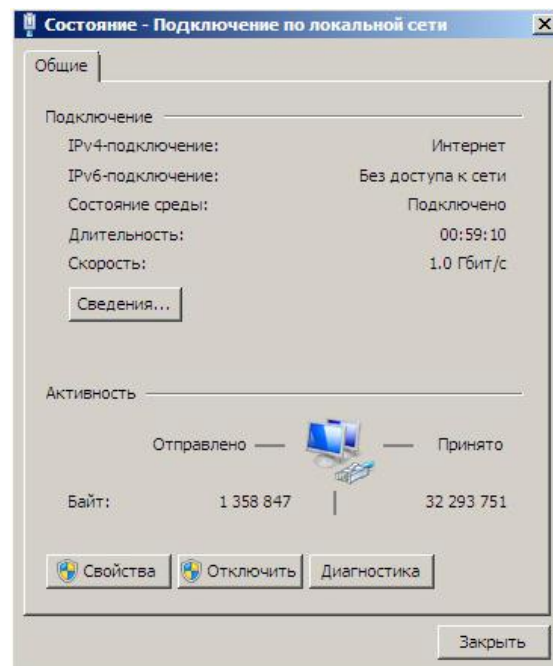


Рис. 2.9. Вікно стану мережевого з'єднання

Щоб тимчасово вимкнути певний мережевий компонент, потрібно вимкнути його прапорець у вікні властивостей з'єднання (рис. 2.6) і натиснути кнопку **ОК**, а для його увімкнення – увімкнути відповідний прапорець і натиснути кнопку **ОК**.

Щоб вилучити непотрібний мережевий компонент, потрібно його виділити у вікні властивостей з'єднання (рис. 2.6) і натиснути кнопку **Вилучити**, після чого натиснути кнопку **ОК**.

Під час усунення проблем з мережею слід перевірити стан з'єднання з мережею (рис. 2.9). Для цього потрібно виконати такі дії:

1. Відкрити вікно **Мережеві з'єднання** (рис. 2.4), в якому відображаються всі існуючі з'єднання з мережею.
2. На певному мережевому з'єднанні викликати контекстне меню і вибрати команду **Стан** або ж виконати такі дії: **Панель керування → Мережа та Інтернет → Цент керування мережами та спільним доступом** (рис. 4), у правій частині вікна у параметрі **Перегляд активних мереж** вибрати **З'єднання по локальній мережі**.

Для відлагодження TCP/IP-з'єднань використовуються утиліти командного рядка – програми, що запускаються з командного рядка і не мають графічного інтерфейсу користувача.

Для тестування TCP/IP-з'єднань використовують утиліти командного рядка **ipconfig** та **ping**.

Команда **ipconfig** відображає інформацію про кожне мережеве з'єднання комп'ютера (рис. 2.10).

Синтаксис команди **ipconfig**:

```
ipconfig [/all] [/renew [адаптер]] [/release [адаптер]]
         /flushdns    [/displaydns]  [/registerdns]  [/showclassid
адаптер] [/setclassid адаптер [код_класу]]
```

Таблиця 2.1.

## Основні параметри ipconfig

Параметр	Пояснення
/all	– виведення повної інформації TCP/IP про всі адаптери;
/renew [адаптер]	– оновлення конфігурації DHCP для всіх адаптерів;
/release [адаптер]	– звільнення поточної конфігурації DHCP та видалення конфігурації IP-адрес для всіх або для заданого адаптера;
/flushdns	– очищення вмісту кешу співставлення імен DNS-клієнта;
/displaydns	– відображення вмісту кешу співставлення імен DNS-клієнта;
/registerdns	– динамічна реєстрація, заданих вручну імен DNS та IP-адрес, налаштованих на комп'ютері.

Для виконання команди **ipconfig** потрібно виконати такі дії:

1. **Пуск** → **Виконати**, ввести команду **cmd** та натиснути кнопку **ОК**.
2. У вікні командного рядка ввести команду **ipconfig** і натиснути клавішу **Enter**.

```

C:\Windows\system32\CMD.exe
Microsoft Windows [Version 6.1.7600]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\lion>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::8940:4475:d276:49e2%11
    IPv4-адрес. . . . . : 192.168.5.118
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.5.1

Туннельный адаптер isatap.{0ECABC15-E2B2-4A29-8DC1-7E733DA6FD52}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

Туннельный адаптер Подключение по локальной сети*:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

C:\Users\lion>
  
```

Рис. 2.10. Результат виконання команди ipconfig

Використання команди **ipconfig** без параметрів дає змогу переглянути коротку інформацію про наявні мережеві інтерфейси. Використовуючи цю команду з параметрами (табл. 2.1), можна виконати такі задачі:

- розблокувати IP-адреси адаптера, щоб вона стала доступною для іншого комп'ютера або адаптера;

- відновити IP-адреси адаптера;
- змінити DNS-сервер, яким користується клієнт.

Команда **ping** надсилає ехо-пакети на вказаний вузол, визначаючи таким чином його доступність чи недоступність у мережі (рис. 2.11).

Синтаксис команди **ping**:

```
ping [-t] [-a] [-n число] [-l розмір] [-f] [-i TTL]
      [-v TOS] [-r число] [-s число] [[-j список_вузлів] | [-k
      список_вузлів]] [-w інтервал] список_розсилки
```

Параметри **ping** подані у табл. 2.2.

Таблиця 2.2.

Основні параметри ping

Параметр	Пояснення
-t	надсилання пакетів на вказаний вузол до команди переривання;
-a	визначення адрес за іменами вузлів;
-n <i>число</i>	кількість запитів, що відправляються;
-l <i>розмір</i>	розмір буфера відправки;
-f	установка прапора, що забороняє фрагментацію пакета;
-i <i>TTL</i>	задання часу життя пакета (поле "Time To Live");
-v <i>TOS</i>	задання типу служби (поле "Type Service");
-r <i>число</i>	запис маршрута для вказаної кількості переходів;
-s <i>число</i>	штамп часу для вказаної кількості переходів;
-j <i>список_вузлів</i>	вільний вибір маршрута за списком вузлів;
-k <i>список_вузлів</i>	жорсткий вибір маршрута за списком вузлів;
-w <i>інтервал</i>	інтервал очікування кожної відповіді в мілісекундах.

Для перегляду статистики і продовження виконання команди використовується комбінація клавіш <Ctrl>+<Break>, а для завершення – <Ctrl>+<C>.

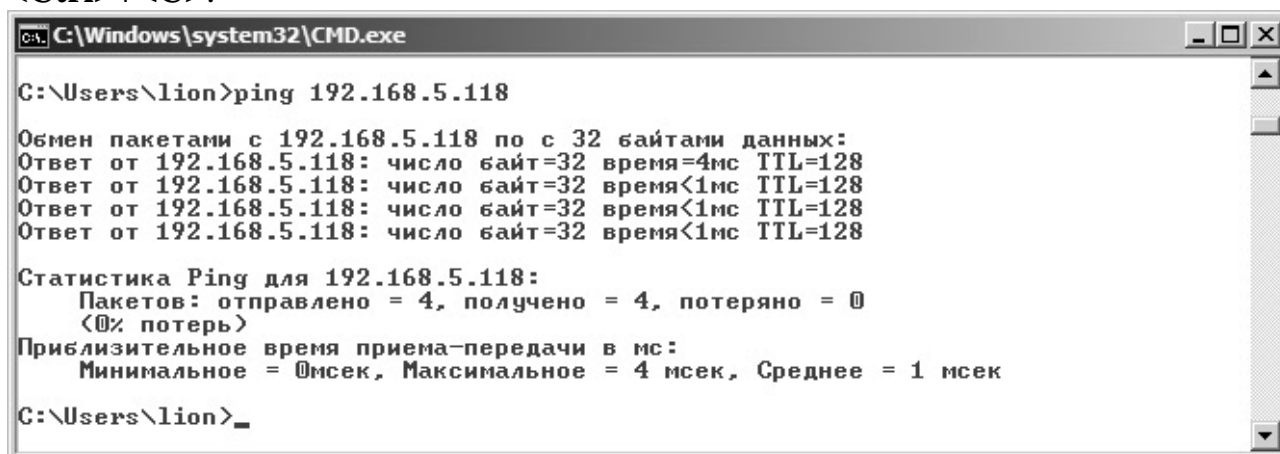


Рис. 2.11. Результат виконання команди Ping



### ***Хід роботи***

1. Перевірити фізичне з'єднання комп'ютера з локальною мережею.
2. Ввести ідентифікаційну інформацію: ім'я комп'ютера, назву робочої групи (як назву робочої групи використати назву своєї навчальної групи).
3. Установити протокол TCP/IPv4, вимкнувши інші протоколи обміну, та здійснити його налаштування: встановити IP-адресу 192.168.YYY.11, де **YYY** – порядковий номер студента у списку навчальної групи, та маску підмережі 255.255.255.0.
4. У командному рядку переглянути всі налаштування мережевого адаптера.
5. Налаштувати ще два комп'ютери, встановивши їм імена, однакову назву робочої групи, IP-адреси (192.168.YYY.ZZZ, де **YYY** – порядковий номер студента у списку навчальної групи, **ZZZ**=12,13 відповідно), та маску (255.255.255.0).
6. Використовуючи ехо-пакети, перевірити доступність різних вузлів мережі.

### ***Контрольні запитання***

1. Що таке “протокол”?
2. Що таке “IP-адреса” і з яких частин вона складається?
3. Для чого використовується “маска мережі”?
4. У чому полягає призначення служби DNS?
5. Для чого використовується протокол DHCP?
6. У яких випадках комп'ютер може належати робочій групі, а коли домену?
7. Як можна переглянути наявність мережевих адаптерів, їх статус та налаштування?
8. Який мережевий протокол використовується в ОС Windows 7 за замовчуванням?
9. Які команди використовуються для тестування TCP/IP-з'єднань?
10. Які типи мережевих компонентів можна встановлювати в ОС Windows 7?

## Лабораторна робота № 3.

### Дослідження роботи та налаштування протоколів стеку TCP/IP

**Мета роботи:** ознайомитися з файлами параметрів, налаштуваннями протоколу TCP/IP, утилітами командного рядка, навчитися використовувати та аналізувати результати їхнього виконання.

#### Теоретичні відомості

Набір протоколів TCP/IP застосовують у мережах на базі ОС UNIX, а також у популярній глобальній мережі Інтернет. Для налаштування протоколів використовують ряд текстових файлів конфігурації, а також утиліти командного рядка. Наприклад, ОС Windows XP всі текстові файли налаштувань можна знайти в у каталозі *Windows\System32\Drivers\etc*.

До файлів налаштувань належать такі файли:

1. Hosts.
2. Services.
3. Networks.
4. Protocol.

У файлі **Hosts** задається відповідність між IP-адресами та назвами комп'ютерів. Це текстовий файл, який містить рядки такого формату:

`<IP-адреса>      <назва комп'ютера>`

У файлі **Services** прописані відповідності між назвою програми, номером порту, та транспортним протоколом. Формат рядка для цього файла такий:

`<service name>   <port number>/<protocol>   [aliases...]   [#<comment>]`

де *service name* – назва застосування, *port number* – номер порту, *protocol* – назва транспортного протоколу (tcp або udp), *aliases* – синоніми до назви програми. Як правило, порти закріплені за програмами.

Файл **Networks** задає відображення між ім'ям мережі та мережевою частиною IP-адреси. Формат рядка цього файла такий:

`<network name>   <network number>   [aliases...]   [#<comment>]`

де *network name* – назва мережі, *network number* – IP-адреса мережі, *aliases* – синоніми до імені мережі.

У файлі **Protocol** задаються відповідності між назвою протоколу та його числовим ідентифікатором. Формат рядка цього файла такий:

`<protocol name>   <assigned number>   [aliases...]   [#<comment>]`

де *protocol name* – назва протоколу, *assigned number* – числовий ідентифікатор протоколу, *aliases* – синоніми до назви протоколу.

Крім файлів налаштувань, в операційних системах Microsoft Windows для налаштування додаткових параметрів використовують спеціальні утиліти командного рядка.

Утиліта командного рядка **Netsh** дає змогу локально або віддалено відображати, змінювати параметри мережі поточного комп'ютера, а також забезпечує засоби написання сценаріїв, за допомогою яких можна запускати групу команд у пакетному режимі на певному комп'ютері.

Команди **Netsh** для інтерфейсу IP використовуються для налаштування протоколу TCP/IP (IP-адрес, адрес основних шлюзів, серверів DNS та серверів WINS), а також для відображення конфігурації та статистики мережевих інтерфейсів.

Команда **netsh interface ip** має багато підкоманд, основні з яких такі:

- **set address** – налаштування IP-адреси та основного шлюза для вказаного інтерфейса;
- **add address** – додавання IP-адреси та основного шлюза для вказаного інтерфейса зі статичною адресою;
- **delete address** – видалення IP-адреси або основного шлюза для вказаного інтерфейса зі статичною адресою;
- **set dns** – налаштування адреси сервера DNS для вказаного інтерфейса;
- **add dns** – додавання сервера DNS у список серверів DNS для вказаного інтерфейса;
- **delete dns** – видалення одного сервера або всіх серверів DNS із списку для вказаного інтерфейса або всіх інтерфейсів.

Для прикладу розглянемо команду **set address**.

Синтаксис команди:

```
netsh interface ip set address [name =] ім'я_інтерфейса  
[source =] (dhcp | static [addr =] IP-адреса  
[mask =] маска_підмережі  
[gateway =] (none | основний_шлюз  
[[gwmetric =] метрика_шлюза]))
```

Параметри команди **set address**:

<pre>[name =] ім'я_інтерфейса</pre>	<p>– обов'язковий параметр. Вказує ім'я інтерфейса, для якого налаштовується IP-адреса та шлюз. Значення параметра <i>ім'я_інтерфейса</i> має збігатися з ім'ям інтерфейса, що відображається у вікні «Мережеві з'єднання». Якщо значення параметра <i>ім'я_інтерфейса</i> містить пропуски, його слід брати в лапки (наприклад "Локальне підключення");</p>
<pre>[source =] (dhcp   static [addr =] IP- адреса [mask =] маска_підмережі [gateway =] (none   основний_шлюз [[gwmetric =] метрика_шлюза]))</pre>	<p>– обов'язковий параметр. Вказує, чи IP-адреса задається автоматично за допомогою протокола ДНСР чи вона є статична. Якщо IP-адреса є статичною, то параметр <i>IP-адреса</i> позначає налаштування адреси, а параметр <i>маска_підмережі</i> позначає маску підмережі IP-адреси, що налаштовується. Крім того, для статичної адреси також можна вказати, чи використовувати поточний основний шлюз (якщо зазначений), або ж задати його для цієї адреси. Якщо шлюз необхідно задати, то значення параметра <i>основний_шлюз</i> вказує IP-адресу основного шлюза, що</p>



налаштовується, а значення параметра *метрика\_шлюза* задає метрику шлюза.

Наприклад, щоб налаштувати мережевий інтерфейс з ім'ям **З'єднання з локальною мережею**, статичною IP-адресою 10.0.5.99, маскою підмережі 255.255.255.0 та основним шлюзом 10.0.5.1, потрібно виконати таку команду:

```
netsh interface ip set address name="З'єднання з локальною мережею" source=static addr=10.0.5.99 mask=255.255.255.0 gateway=10.0.5.1 gwmetric
```

Команда **Arp** дає змогу переглядати та модифікувати таблиці трансляції IP-адрес у MAC-адреси, які використовує протокол ARP.

Синтаксис команди:

```
arp -a [inet_addr] [-N [if_addr]]
arp -d inet_addr [if_addr]
arp -s inet_addr ether_addr [if_addr]
```

Параметри команди **Arp**:

- a – виводить всю таблицю протоколу ARP. Якщо вказана IP-адреса *inet\_addr*, то виводиться інформація лише про неї;
- inet\_addr* – IP-адреса;
- N – виводить рядки таблиці лише для мережевого інтерфейса, визначеного за допомогою *if\_addr*;
- if\_addr* – IP-адреса одного з інтерфейсів комп'ютера;
- d – знищує рядок у таблиці, визначений за допомогою *inet\_addr*;
- s – додає рядок до таблиці, пов'язуючи IP-адресу *inet\_addr* з MAC-адресою *ether\_addr*. MAC-адреса подається як шість шістнадцяткових цифр розділених за допомогою тире;
- ether\_addr* – MAC-адреса.

Утиліта **Tracert** визначає шлях до хоста-адресата, виводячи адреси всіх проміжних маршрутизаторів шляхом надсилання ICMP-пакетів зі зростаючими значеннями TTL.

Синтаксис команди:

```
tracert [-d] [-h maximum_hops] [-j computer-list]
        [-w timeout] target_name
```

Параметри команди **Tracert**:

- d – не визначати назв хостів через DNS;
- h – максимальна кількість проміжних переходів;
- maximum\_hops*
- j *computer-list* – визначає список проміжних хостів (можливо, роз'єднаних маршрутизаторами);
- w *timeout* – задає час передавання у мілісекундах;

*target\_name* – адреса віддаленого хоста.

Команда **Netstat** відображає статистику передавань для різних протоколів та TCP з'єднань.

Синтаксис команди:

**netstat** [-a] [-e] [-n] [-s] [-p *protocol*] [-r] [*interval*]

Параметри команди **Netstat**:

- a – відображає всі наявні з'єднання та порти;
- e – відображає статистику Ethernet;
- n – виводить адреси та номери портів у числовому форматі;
- s – статистика передавань у розрізі окремих протоколів;
- p *protocol* – відображає статистику тільки для вказаного протокола;
- r – виводить вміст таблиці маршрутизації;
- interval* – відображає статистику циклічно, через вказану в *interval* кількість секунд. Зупинка – <CTRL>+<B>.

Команда **Hostname** відображає ім'я локального хоста. Синтаксис команди:

**hostname**

Команда **Route** призначена для роботи з таблицями маршрутизації. Синтаксис команди:

**route** [-f] [-p] [*command* [*destination*] [**mask** *subnetmask*]  
[**gateway**][**metric** *costmetric*]

Параметри команди **Route**:

- f – очищує таблиці. Якщо цей параметр використано в певній команді, то таблиці очищуються перед її виконанням;
- p – при використанні з командою *add* – занесений шлях зберігається після перезавантаження. При використанні з командою *print* – виводить всі постійні шляхи;
- command* – одна з наступних команд:
  - print* – вивести маршрут;
  - add* – додати маршрут;
  - delete* – знищити маршрут;
  - change* – змінити маршрут;
- destination* – ім'я хоста, на якому виконується команда;
- subnetmask* – визначає маску мережі. Якщо параметр *subnetmask* не заданий, то використовується маска 255.255.255.255;
- gateway* – визначає IP-адресу шлюза;
- costmetric* – визначає метрику (ціле число від 1 до 9999) для розрахунку маршрутів.

Команда **net use** використовується для приєднання мережевого ресурса з даними у вигляді логічного диску. Цією командою також можна від'єднувати мережеві ресурси від локального комп'ютера та здійснювати їхнє гнучке налаштування.

Синтаксис команди:

```
net use [{назва_пристрою | *}]  
[\\назва_комп'ютера\ресурс[\том]] [{пароль | *}]]  
[/user:[назва_домена\]]  
[/user:[назва_домена_з_крапкою\]ім'я_користувача]  
[/user:[ім'я_користувача@назва_домена_з_крапкою]  
[/savecred] [/smartcard] [{/delete | /persistent:{yes | no}}]
```

Основні параметри команди **net use**:

- |                                  |   |
|----------------------------------|---|
| <i>назва_пристрою</i>            | – визначає назву ресурса при під'єднанні або назву пристрою при від'єднанні. Існує два види назв пристроїв: назви для дискових пристроїв (диски з літерними позначеннями від D до Z) і для принтерів (від LPT1: до LPT3:). Введення зірочки (*) замість назви певного пристрою забезпечує йому присвоєння найближчої доступної назви; |
| <i>\\назва_комп'ютера\ресурс</i> | – визначає ім'я сервера та загального ресурса. Якщо цей параметр містить пропуски, то повне ім'я комп'ютера від подвійної зворотної риски до кінця має бути взято у прямі лапки (наприклад, "\\Computer Name\Share Name"). Довжина імені комп'ютера не може перевищувати 15 символів;   |
| <i>пароль</i>                    | – визначає пароль, необхідний для під'єднання до загального ресурса. Введення зірочки (*) забезпечує вивід запрошення на ввід пароля;   |
| <i>/user</i>                     | – визначає ім'я іншого користувача для під'єднання до загального ресурса;   |
| <i>назва_домена</i>              | – визначає назву іншого домена. Якщо цей параметр пропущено, то використовується назва домена, задана при вході у систему;  |
| <i>ім'я_користувача</i>          | – визначає ім'я користувача для під'єднання;  |
| <i>/persistent:{yes   no}</i>    | – якщо задано yes, то існуючі з'єднання відновлюються при наступному вході у систему, а якщо no – то не зберігаються.   |

Приклади використання команди **net use**:

1. Перегляд всіх приєднаних мережесих ресурсів:

```
net use
```

2. Приєднати у вигляді дискового пристрою з ім'ям *M*: мережесих ресурс, розташований у каталозі *Music* комп'ютера *Nemo*,:

```
net use m: \\nemo\music
```

3. Приєднати у вигляді дискового пристрою з ім'ям *D*: для користувача *Student* домену *lp* мережесих ресурс, розташований у каталозі *Data* комп'ютера *Nemo*:

```
net use d: \\nemo\data /user:lp\Student
```

або записати так:

```
net use d: \\nemo\data /user:Student@lp
```

4. Від'єднати мережесих ресурс, приєднаний з ім'ям *M*::

```
net use m: /delete
```

### *Хід роботи*

1. Ознайомитись із вмістом файлів Hosts, Services, Networks, Protocol і визначити, які порти використовуються службами FTP, FTP-data, SMTP, POP, telnet, HTTP, HTTPS.
2. Перевірити наявність з'єднання з комп'ютерами.
3. Установити та змінити налаштування мережесих інтерфейсу з командного рядка:
  - 3.1. Встановити статичну IP-адресу 192.168.YYY.XXX та маску підмережі 255.255.255.0, де **YYY** – порядковий номер студента у списку навчальної групи, **XXX** – номер навчальної групи.
  - 3.2. Установити DNS-сервер 5.5.NNN.YYY, де **NNN=YYY\*2**, **YYY** – порядковий номер студента у списку навчальної групи.
  - 3.3. Додати додаткову IP-адресу 192.168.NNN.KKK, де **NNN=YYY\*2**, **KKK = YYY\*2**, **YYY** – порядковий номер студента у списку навчальної групи.
  - 3.4. Видалити IP-адресу, встановлену у п.3.1.
  - 3.5. Додати додатковий DNS-сервер 192.168.NNN.1, де **NNN=YYY\*2**, **YYY** – порядковий номер студента у списку навчальної групи.
  - 3.6. Додати основний шлюз 192.168.NNN.1, де **NNN=YYY\*2**, **YYY** – порядковий номер студента у списку навчальної групи.
  - 3.7. Видалити DNS-сервер, встановлений у п.3.2.
4. Ознайомитись із вмістом таблиці arp локального комп'ютера.
5. Визначити всі проміжні маршрутизатори на шляху до певного хоста (наприклад, веб-сайту).
6. Переглянути статистику використання Інтернет-протоколів на локальному комп'ютері.
7. Переглянути вміст маршрутних таблиць локального хоста.
8. З командної стрічки переглянути всі приєднані існуючі мережесих ресурси.

9. За допомогою команди **net use** приєднати будь-який зовнішній мережевий ресурс у вигляді дискового пристрою з першою доступною назвою. При цьому вказати, що дане з'єднання не буде відновлене при наступному вході у систему.
10. Приєднати інший зовнішній мережевий ресурс у вигляді дискового пристрою з назвою V:, вказавши, що дане з'єднання буде постійним.
11. Від'єднати мережевий ресурс, створений у п. 10.

### ***Контрольні запитання***

1. Які файли конфігурації містять налаштування протоколів?
2. Яка інформація міститься у файлі Hosts?
3. Які порти використовують поштові протоколи?
4. Який файл служить для відображення ім'я мережі в мережеву частину IP-адреси?
5. Яка команда дає змогу локально або віддалено відображати, змінювати параметри мережі поточного комп'ютера?
6. Яка команда дає змогу переглянути та модифікувати таблиці трансляції IP-адрес у MAC-адреси?
7. Яке призначення утиліти Tracert?
8. За допомогою якої команди можна відобразити статистику передавань для різних протоколів та наявних TCP з'єднань?
9. Для чого потрібні таблиці маршрутизації?
10. Які ресурси комп'ютера можна зробити загальними?
11. Як зробити розподіленим ресурсом окремий логічний диск комп'ютера?
12. Як здійснити приєднання мережевого ресурсу у вигляді логічного диску?

## Лабораторна робота № 4.

### Налаштування мережевих компонент ОС Linux Ubuntu

**Мета роботи:** навчитися налаштовувати мережеві інтерфейси в ОС Linux за допомогою графічного та консольного режимів.

#### *Теоретичні відомості*

У системі Linux повністю реалізований протокол TCP/IP. Протокол TCP/IP виявився найуспішнішим засобом об'єднання комп'ютерів усього світу в єдину мережу. Маючи комп'ютер з системою Linux і адаптер Ethernet (мережевий адаптер або мережева плата), можна підключити комп'ютер до локальної мережі або (за наявності відповідного з'єднання) до мережі Інтернет, де обмін даними відбувається за протоколом TCP/IP.

У системі Linux можна використовувати протокол TCP/IP без будь-яких мережевих пристроїв, оскільки навіть на комп'ютері, що не має мережевих адаптерів (апаратних мережевих інтерфейсів), завжди є віртуальний інтерфейс – мережева “заглушка” або “петля” (loopback interface) на ім'я `lo`. Мережева заглушка дає змогу комп'ютеру вести діалог із самим собою, використовуючи мережеві протоколи. Це необхідно для деяких програм, у яких використовуються мережеві з'єднання.

Як правило, кожний мережевий інтерфейс має не менше однієї IP-адреси. Інтерфейсу `lo` за замовчуванням призначається IP-адреса `127.0.0.1` і вона є однаковою на всіх комп'ютерах.

Якщо використовується лише заглушка, то мережева адреса, широкосповіщальна адреса та адреса шлюзу відсутні.

Розглянемо налаштування мережевих параметрів в операційній системі Ubuntu.

Існує два способи налаштування мережевих параметрів:

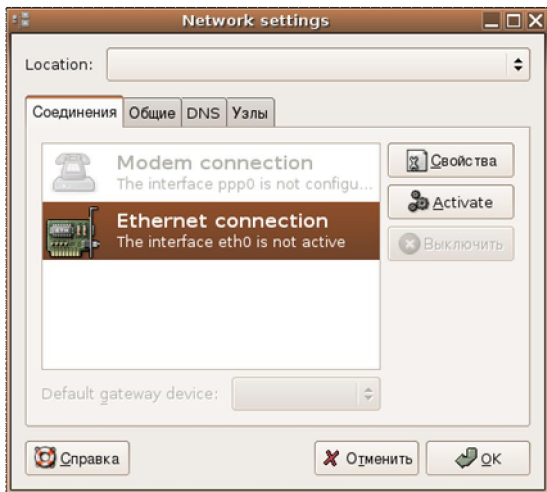
- 1) за допомогою графічного інтерфейсу ОС;
- 2) за допомогою консольного режиму.

Щоб налаштувати мережеві параметри за допомогою графічного інтерфейсу ОС Ubuntu, потрібно відкрити вікно мережевих налаштувань (рис. 4.1). Для цього слід виконати таку послідовність кроків: **Система → Адміністрування → Мережеві налаштування**.

У вікні мережевих налаштувань розташовано декілька закладок (З'єднання, Загальні, DNS, Вузли), кожна з яких має власні налаштування.

На закладці **З'єднання** відображається список існуючих з'єднань. Виділивши певне з'єднання, можна переглянути або задати його властивості, а також ввімкнути чи вимкнути його (рис. 4.2).

За замовчуванням мережеві параметри встановлюються автоматично, якщо в пункті **Конфігурація** задано **DHCP**. Для того, щоб мережеві параметри задати вручну, у пункті **Конфігурація** вказуємо **Static IP address** (статична IP-адреса), нижче задаємо IP-адресу, маску та шлюз відповідно. Після внесених змін натискаємо кнопку **ОК**, щоб зберегти зміни.



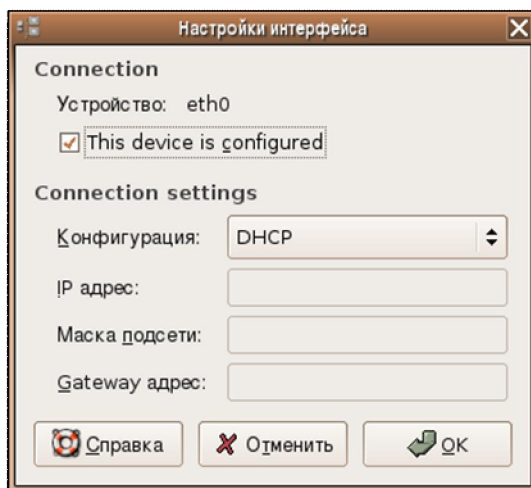
а)



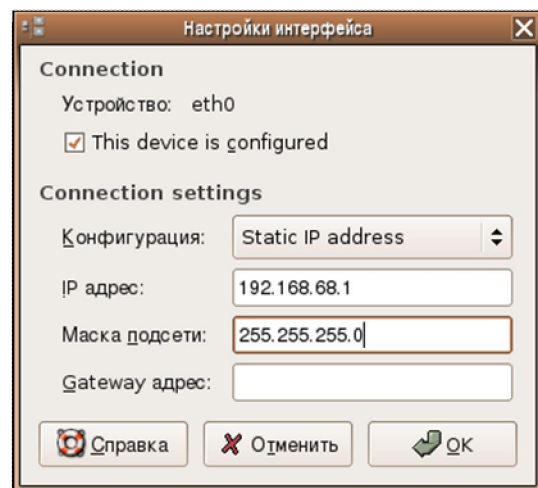
б)

Рис. 4.1. Закладка “З’єднання” вікна “Мережеві налаштування”:

а) мережеве з’єднання неактивне; б) мережеве з’єднання активне



а)



б)

Рис. 4.2. Властивості мережевого інтерфейсу eth0:

а) режим автоматичного налаштування; б) режим ручного налаштування

На закладці **Загальні** (рис. 4.3) вказується ім’я комп’ютера та назва домену (робочої групи).

На закладці **DNS** (рис. 4.4) задаються IP-адреси DNS-серверів.

Налаштування мережі комп’ютера за допомогою консолі зводиться до редагування декількох файлів. Як правило, цими файлами є `interfaces` та `resolv.conf`.

У файлі `/etc/network/interfaces` описуються назви мережевих інтерфейсів, IP-адреси, маски, шлюз. Також тут можна вказувати MAC-адреси мережевих адаптерів і інше.

Мережевий інтерфейс `lo` (IP-адреса `127.0.0.*`, як правило, `127.0.0.1`) переважно використовується для тестування мережевої підсистеми і завжди налаштовується автоматично.

Для налаштування інтерфейсу `lo` використовуються наступні рядки у файлі `/etc/network/interfaces`:

```
auto lo                                # мережева "петля"
iface lo inet loopback
```

Після налаштування `lo` налаштовується мережевий адаптер. Якщо мережевий адаптер один, то він буде називатися `eth0`, якщо два, тоді другий буде називатися `eth1` і т.д. Крім того, для одного мережевого інтерфейса можна встановлювати більше ніж одну IP-адресу.

Наприклад, налаштування мережевого адаптера `eth0` для автоматичного отримання мережевих налаштувань за допомогою служби DHCP задається так:

```
auto eth0
iface eth0 inet dhcp
```

Тут рядок `"auto eth0"` вказує операційній системі, що цей інтерфейс потрібно запускати автоматично з налаштуванням при завантаженні системи і при перевантаженні служби мережі.

Якщо потрібно задати мережеві налаштування вручну, то вносять зміни у файл `interfaces`, наприклад:

```
iface eth0 inet static
address адрес
netmask маска
gateway шлюз
```

Тут параметр `gateway` – необов'язковий. Якщо мережа немає виходу в Інтернет, то цей параметр можна не вказувати.

Також можна використовувати необов'язкові параметри `network` і `broadcast`, які визначають адресу підмережі та широкомовіщальну адресу мережі відповідно:

```
network 192.168.1.0                # адреса підмережі
broadcast 192.168.17.255           # широкомовіщальна адреса мережі
```

Іноколи виникає потреба призначити одному мережевому адаптеру декілька IP-адрес. У такому випадку, якщо ім'я першого віртуального інтерфейса є `eth0`, тоді ім'я другого інтерфейса буде `eth0:1`, а ім'я третього – `eth0:2` і т. д. Тут `eth0:1` означає, що це перший віртуальний інтерфейс, що працює через фізичний інтерфейс `eth0`.

Приклад:

```
auto eth0 eth0:1 eth0:2
iface eth0 inet static
address 192.168.0.201
network 192.168.0.0
netmask 255.255.255.0
broadcast 192.168.0.255
gateway 192.168.0.1

iface eth0:1 inet static
address 192.168.0.202
network 192.168.0.0
netmask 255.255.255.0
```



```
iface eth0:2 inet static
address 192.168.0.203
network 192.168.0.0
netmask 255.255.255.0
```

У файлі `/etc/resolv.conf` описуються адреси DNS-серверів. Якщо DNS-сервер один, наприклад, прописуємо його так:

```
nameserver 192.168.1.1
```

А якщо є два чи більше DNS-серверів, тоді кожний з них записується в новому рядку:

```
nameserver 192.168.1.1
nameserver 195.75.16.5
```

Якщо зміна параметрів мережі здійснювалася безпосередньо у файлах налаштувань мережі, тоді, щоб зміни почали діяти, потрібно перезавантажити мережеву службу такою командою:

```
/etc/init.d/networking restart
```

В ОС Ubuntu є низка програмних засобів для тестування мережі. Для того, щоб ними скористатися, необхідно виконати таку послідовність кроків: **Програми → Системні → Мережевих програм**. На екрані відобразиться вікно, зображене на рис. 4.5. До цих службових мережевих програм належать утиліти Ping, Netstat, Traceroute, Port Scan, Lookup, Finger та Whois.

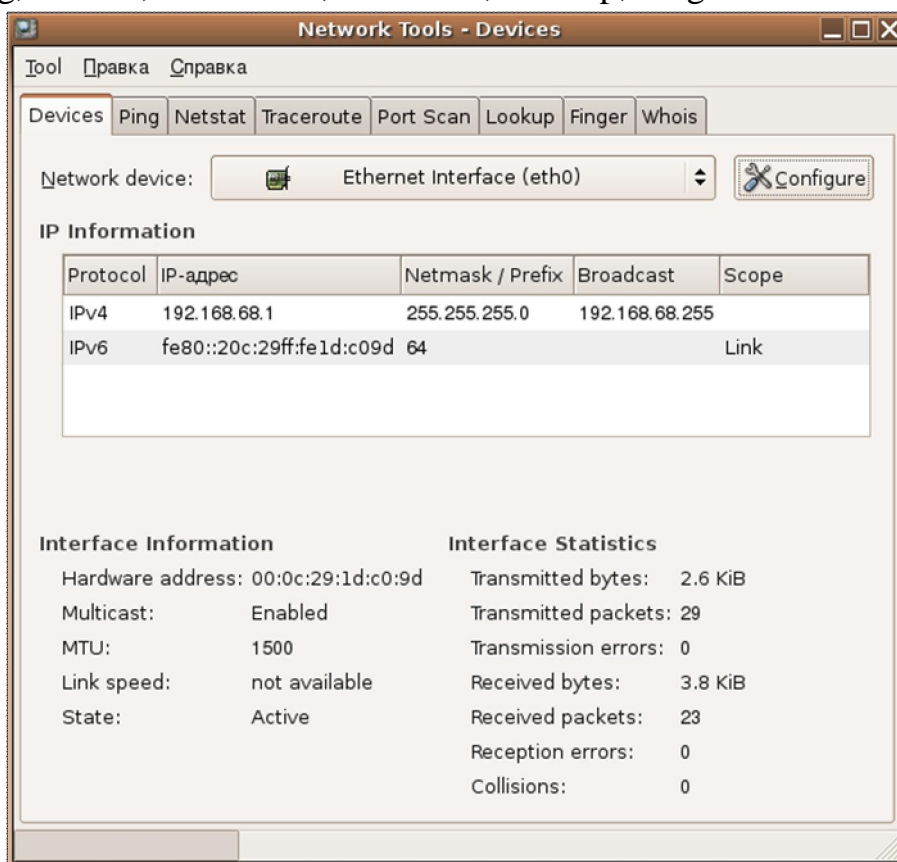


Рис. 4.5. Вікно “Мережеві програми”

### Використання консольного режиму

Для перегляду стану всіх мережевих інтерфейсів використаємо команду **ifconfig**. Головне призначення цієї команди полягає у прив'язці IP-адреси до мережевого адаптера (інтерфейса). Передусім, **ifconfig** допомагає зібрати інформацію про поточний стан мережевих інтерфейсів.

Наприклад, команда `ifconfig -a` дає змогу переглянути список усіх наявних мережевих інтерфейсів, а також перевірити їхню доступність у певний момент.

Слід пам'ятати, що мережеві налаштування має здійснювати користувач з правами адміністратора. А в ОС Ubuntu всі команди, що виконуються від імені адміністратора, повинні починатися зі слова **sudo**. Приклади використання команди **ifconfig** для налаштування мережевих інтерфейсів подані у табл. 4.1.

Таблиця 4.1.

Приклади використання команди **ifconfig**

Команда	Опис
<b>ifconfig</b> eth0 up	Увімкнення мережевого інтерфейса eth0
<b>ifconfig</b> eth0 down	Вимкнення мережевого інтерфейса eth0
<b>ifconfig</b> eth0 inet 192.168.140.1 або <b>ifconfig</b> eth0 192.168.140.1	Установлення інтерфейсу eth0 IP-адреси 192.168.140.1
<b>ifconfig</b> eth0:1 172.30.49.4	Додавання інтерфейсу eth0 віртуальної IP-адреси 172.30.49.4
<b>ifconfig</b> eth0 netmask 255.255.0.0	Установлення інтерфейсу eth0 маски мережі 255.255.0.0
<b>ifconfig</b> eth0 broadcast 192.168.140.255	Установлення інтерфейсу eth0 широковещальної адреси мережі 192.168.140.255
<b>ifconfig</b> eth0 hw ether 00:12:34:56:78:90	Установлення інтерфейсу eth0 MAC-адреси 00:12:34:56:78:90
<b>ifconfig</b> eth0 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255	Установлення інтерфейсу eth0 IP-адреси 192.168.2.2, маски мережі 255.255.255.0 та широковещальної адреси мережі 192.168.2.255

Щоб переконатися, що комп'ютер, який налаштовується, бачить мережу і має до неї доступ, можна використати команду **ping**. Вона надсилає запит на віддалений хост і, отримавши відповідь, чи не дочекавшись її, відображає статистику обміну пакетами між хостами: час проходження шляху в обидва кінці, відсоток втрат та інше.

### Хід роботи

1. У командному рядку переглянути список усіх наявних мережевих інтерфейсів першого комп'ютера.

2. Увімкнути мережевий адаптер першого комп'ютера і налаштувати статичний режим налаштування мережевих параметрів.
3. У командному рядку переглянути список наявних мережевих інтерфейсів першого комп'ютера. Зафіксувати зміни.
4. Налаштувати комп'ютерну мережу між двома комп'ютерами, встановивши їм IP-адреси згідно такого формату: 192.168.YYY.ZZZ, де **YYY** – порядковий номер студента у списку навчальної групи, **ZZZ**=1,2 відповідно, та маску 255.255.255.0.
5. Використовуючи ехо-пакети, перевірити доступність у мережі цих комп'ютерів.
6. Використовуючи файли мережевих налаштувань для першого комп'ютера, задати адресу шлюза (192.168.YYY.100) та адресу DNS-сервера (192.168.YYY.101), крім того, додати одну віртуальну адресу (192.168.RRR.200, де **RRR** = **YYY+50**). Застосувати зміну налаштувань.
7. У командному рядку переглянути параметри мережевого адаптера першого комп'ютера. Зафіксувати зміни.
8. У командному рядку для третього комп'ютера встановити IP-адресу (192.168.YYY.3, де **YYY** – порядковий номер студента у списку навчальної групи), маску (255.255.255.0), адресу шлюза (192.168.YYY.100) та адресу DNS-сервера (192.168.YYY.101), крім того, додати одну віртуальну адресу (192.168.RRR.200, де **RRR** = **YYY+60**). Застосувати зміну налаштувань.
9. З'ясувати призначення мережевих програм в ОС Ubuntu та скористатися ними.

### ***Контрольні запитання***

1. Які способи налаштування мережевих параметрів існують у Linux?
2. Чи можна використовувати протокол TCP/IP без жодних мережевих пристроїв?
3. В яких файлах містяться мережеві налаштування?
4. Яка IP-адреса віртуального інтерфейсу lo0 за замовчуванням?
5. Якою командою автоматично запускається певний мережевий інтерфейс?
6. Скільки IP-адрес може мати один мережевий інтерфейс?
7. Для чого необхідна мережева маска?
8. У яких випадках можна використовувати широковещальну адресу?
9. Яке призначення шлюза?
10. Який протокол використовується для автоматичного отримання мережевих налаштувань?
11. Що таке DNS і як він працює?
12. Яка інформація описується у файлі /etc/network/interfaces?
13. Які програмні засоби для тестування мережі наявні в ОС Ubuntu?
14. Яке призначення утиліти Netstat?
15. Яке призначення утиліти Traceroute?
16. Яке призначення утиліти Lookup?
17. Яке призначення утиліти Finger?
18. Яке призначення утиліти Whois?

## **Лабораторна робота № 5.**

### **Робота у середовищі NetCracker Professional**

**Мета роботи:** ознайомитися з графічним інтерфейсом користувача, вивчити засоби й способи доступу до інструментів та режимів, анімаційні та презентаційні можливості пакету NetCracker Professional.

#### ***Теоретичні відомості***

Постійне зростання кількості комп'ютерних мереж, ускладнення їхньої інфраструктури та збільшення обсягів переданих даних створюють серйозні проблеми забезпечення ефективного управління мережевими ресурсами як при адмініструванні та розвитку наявної мережевої інфраструктури, так і при проектуванні нових мереж і розробці мережевих додатків.

Одним з найпопулярніших на сьогоднішній день програмних продуктів, призначених для моделювання комп'ютерних мереж усіх типів, а також моделювання процесів у створених мережах, є пакет NetCracker Professional, фірми NetCracker Technology. З його допомогою можуть бути розв'язані такі завдання, як визначення продуктивності мережі при заданні топології і робочого навантаження, аналіз залежності пропускної здатності при зміні робочого навантаження на мережу, аналіз залежності пропускної здатності мережі при зміні її топології, підбір параметрів протоколів мережі для забезпечення максимальної пропускної здатності мережі при заданих топології і робочого навантаження, визначення оптимальної топології і співвідношення пропускна здатність – вартість проектованої мережі.

Як і всі сучасні програми такого типу, пакет оснащений засобами графічного проектування, що дають змогу будувати схеми мережі за допомогою спеціальної бібліотеки елементів мережевої інфраструктури, яка надає користувачеві широкий вибір конкретних моделей обчислювальних та телекомунікаційних пристроїв різних фірм-виробників. Також є змога створювати моделі пристроїв, що задовольняють вимогам користувача, регулювати рівень параметризації елементів бібліотеки, робити моделі реальних об'єктів.

Середовище моделювання використовується для збору даних про функціонування моделі, що, при необхідності, відображається на екрані або діаграмі завантаженості, або в процентному співвідношенні. Є також змога анімації процесу моделювання мережі. Можна призупиняти або припиняти роботу моделі, прокручувати назад анімаційну картинку і запускати її повторно.

Підсистема аналізу результатів моделювання обробляє дані, зібрані при прогонці моделі, обчислює характеристики продуктивності і подає результати у зручній для користувача формі.

Для запуску програми NetCracker Professional потрібно виконати такі дії

**Пуск → Всі програми → NetCracker Professional 4.1 → NetCracker Professional.**

Крім головного меню (рис. 5.1) і панелей інструментів, головне вікно NetCracker Professional містить *браузер, робочу область і панель зображення*. На початку роботи робоча область містить порожній сайт Net1. Панель зображень відображає пристрої та додатки для вибраної в браузері категорії.

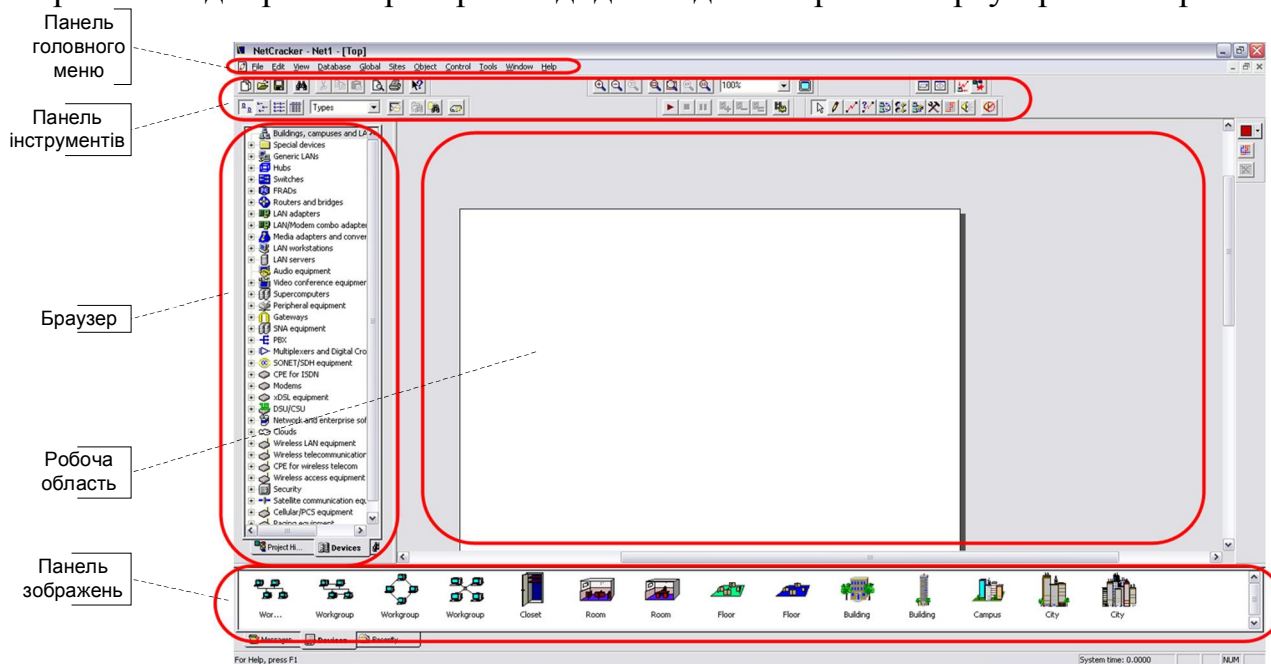


Рис. 5.1. Головне вікно NetCracker Professional

Відкриття файлу проекту NetCracker Professional (.NET) виконується за допомогою команди **Open** (Відкрити) меню **File** (Файл). Ця команда викликає діалогове вікно відкриття файла (рис. 5.2).

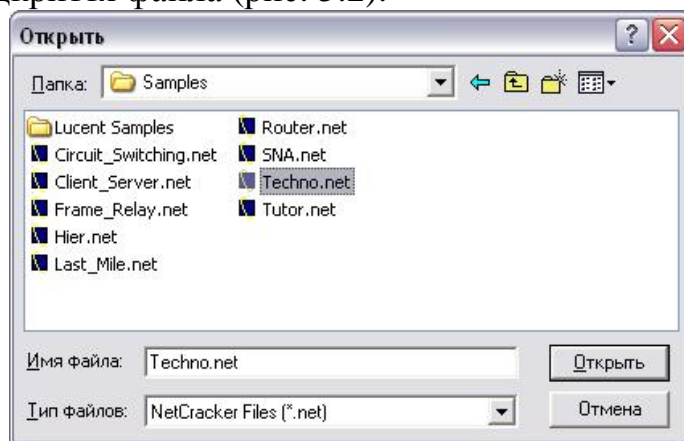


Рис. 5.2. Діалогове вікно відкриття файла

З каталогу **Samples** вибираємо файл **Techno.net**. В області робочого простору програми відкриється вміст проекту “Techno” (рис. 5.3).

Для збільшення ділянки перегляду використовується кнопка  (Zoom).

Перегляд пристроїв здійснюється у браузері на вкладці **Devices** (Пристрої). Щоб вибрати певний пристрій, виділіть його в браузері, тоді в панелі “Зображення” відобразяться усі пристрої з цієї категорії. Смуга прокрутки панелі “Зображення” дає змогу переглядати зображення усіх пристроїв цієї категорії.

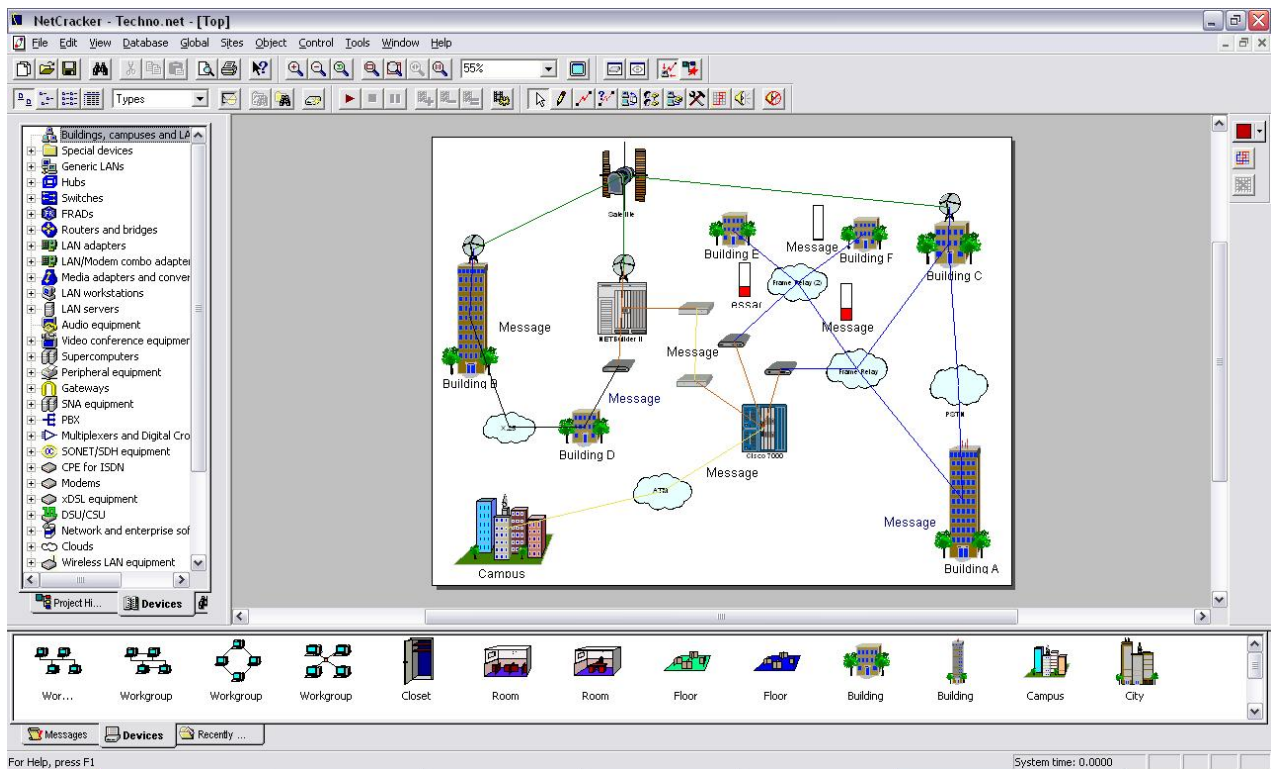


Рис. 5.3. Вікно проекту “Techno”

Пристрої в панелі браузера можуть відображатися за:

- типом (Types);
- виробниками (Vendors);
- користувачем (User).

В області панелі “Зображення” є такі закладки:

- повідомлення (Messages);
- пристрої (Devices);
- нещодавно використані (Recently used).

При виборі закладки “Нещодавно використані” в панелі “Зображення” відображаються зображення пристроїв, що пов'язані з проектом, відображеним у Робочому просторі.

Щоб отримати інформацію про пристрій, розташований у робочій області, необхідно двічі натиснути на ньому лівою кнопкою миші. Відкриється вікно діалогу конфігурації, у лівій частині якого буде відображатись даний пристрій, у правій – конфігураційна панель, а внизу – кнопки **Device Setup** (Налаштування пристрою), **Plug-in Setup** (Налаштування додаткових пристроїв), **Close** (Закрити вікно) та **Help** (Допомога).

Наприклад, двічі клацніть на маршрутизаторі Cisco 7000, розташованому в центрі вікна (рис. 5.4).

Щоб вибрати HSSI Interface Processor (Процесор зв'язку високошвидкісного послідовного інтерфейсу), на панелі вибору натисніть на другий зі списку змінних блоків – CX-HIP. Зверніть увагу, що при виборі змінного блоку, зображення пристрою змінюється, щоб відобразити, де цей блок розташований у пристрої.

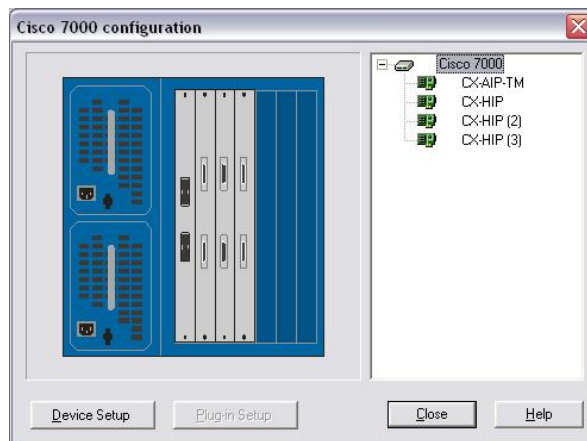


Рис. 5.4. Вікно діалогу конфігурації для маршрутизатора Cisco 7000

Для перегляду інформації про змінний блок використовують один з таких методів:

- на панелі вибору виберіть змінний блок ATM Interface Processor CX-HIP (процесор зв'язку асинхронної системи передачі), викличте контекстне меню і виберіть команду Properties;
- на панелі вибору виберіть змінний блок ATM Interface Processor CX-HIP і натисніть кнопку Plug-in Setup;
- на зображенні пристрою, виберіть змінний блок ATM Interface Processor CX-HIP і натисніть кнопку Plug-in Setup.

Діалогове вікно властивостей змінного блоку CX-HIP подано на рис. 5.5.

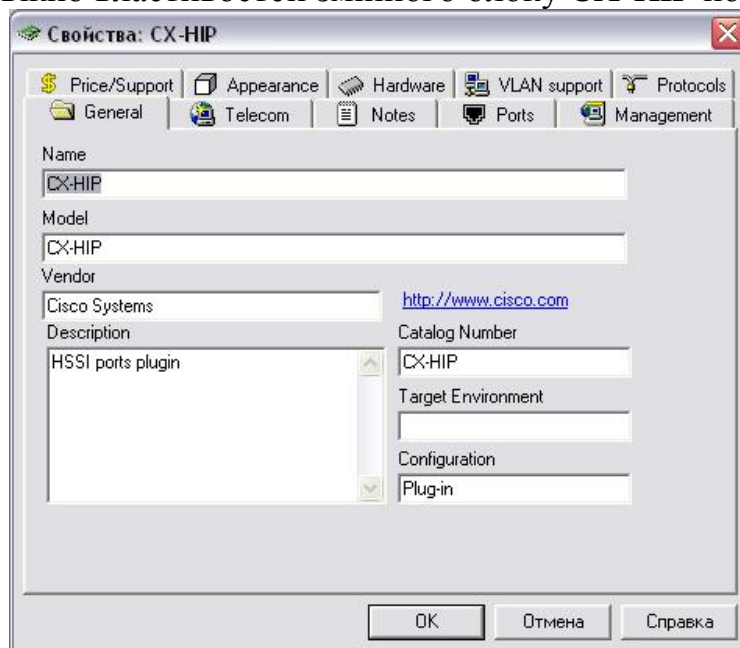


Рис. 5.5. Вікно діалогу властивостей блоку CX-HIP

У діалоговому вікні властивостей пристрою можна переглянути протоколи та порти цього пристрою на закладках **Protocols** (Протоколи) та **Ports** (Порти) відповідно.

Щоб переглянути або змінити конфігурацію пристрою у діалоговому вікні конфігурації, використовується кнопка **Device Setup**.



Для установлення змінного блоку в пристрій потрібно, в панелі браузера вибрати певний пристрій, у панелі “Зображення” перейти на закладку **Devices** (Пристрої), вибрати певну плату і, утримуючи ліву кнопку миші, перетягнути змінний блок у вікно діалогу конфігурації на вільний роз’єм у зображенні пристрою у діалоговому вікні.

Іншим методом вставки змінних блоків є вибір змінного блоку з панелі “Зображення” і вставка його прямо в зображення пристрою в робочому просторі. Використання цього методу не вимагає, щоб діалог конфігурації був відкритим.

Для отримання загальної інформації наведіть курсор на об’єкт у вікні сайту, щоб побачити підказку. Додаткову інформацію можна почути завдяки звуковим підказкам. Щоб почути звукову підказку, відкрийте контекстне меню пристрою і виберіть один з відповідних пунктів:

- Say Notes (озвучити зауваження);
- Say Description (озвучити опис);
- Say Current Statistics (озвучити статистику пристрою).

Щоб побачити, які види зв'язків використовуються для підключення пристроїв у проєкті, в меню **View** виберіть пункт **Media Colors**. Тут вказуються кольори, якими на схемі проєкту відображаються типи з'єднань:


- коаксіальний кабель;
- скручена пара;
- оптоволоконний кабель;
- багатопровідні лінії;
- радіоканал.

Є змога отримати інформацію про всю мережу, використовуючи проєктні звіти. Для виведення звіту в меню **Tools** (Інструменти), виберіть пункт **Reports** (Звіти).

Щоб отримати звіт про мости і маршрутизатори, виберіть **Routers/Bridges** (Маршрутизатори/Мости), потім натисніть кнопку **Next** (Далі) у майстрі звіту і кнопку **Finish** (Готово). Звіт відкриється у робочій області, а над звітом відобразиться інструментальна панель **Report**, за допомогою якої можна переглянути сторінки звіту (якщо він багатосторінковий), роздрукувати його або експортувати у файл.

Щоб переглянути список вартості обладнання та матеріалів, а також звіт про підсумкову вартість, виконайте такі дії: **Tools** → **Reports** → **Bill of Materials** (Інструменти → Звіти → Рахунок матеріалів). У майстрі звіту натисніть кнопку **Next** і кнопку **Finish**.

Для закриття звіту, скористайтеся кнопкою **Close** відповідного звіту.

Запуск анімації проєкту здійснюється кнопкою **Start**  панелі інструментів **Control** (Керування), або командою **Start** меню **Control**. У робочому просторі почнуть рухатися пакети (рис. 5.6).



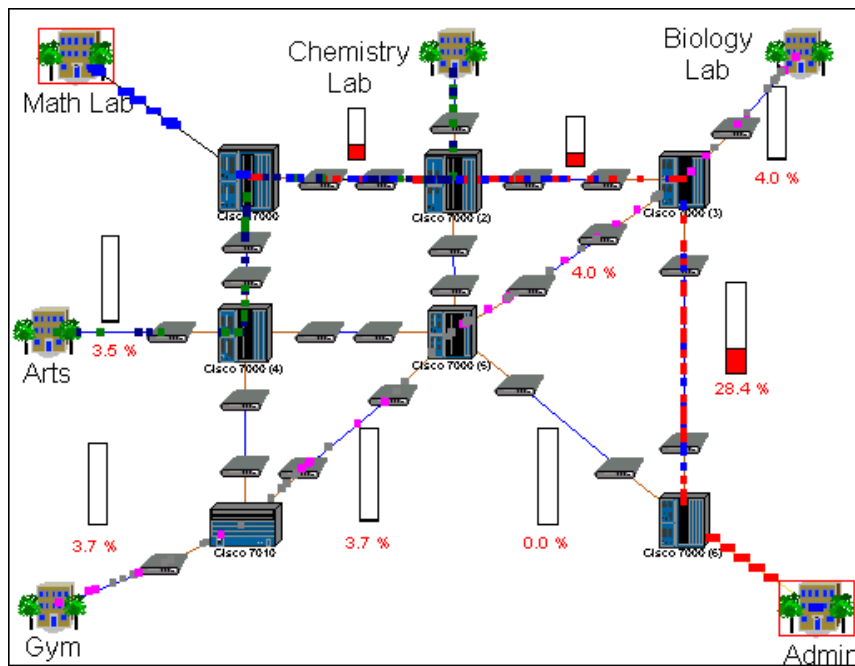






Рис. 5.6. Вікно проекту з анімацією

Зупинка та призупинення/відновлення анімації проекту здійснюється відповідно кнопками **Stop** (Зупинити)  та **Pause/Resume** (Призупинити/Відновити)  панелі інструментів Керування, або відповідними командами меню Керування.

Виклик вікна налаштувань параметрів анімації (рис. 5.7) виконується за допомогою кнопки **Animation Setup** (Налаштування анімації) .

Щоб відкрити один з нижчих рівнів проекту, двічі натисніть на відповідній будові. А щоб повернутися на верхній рівень цього проекту, закрийте відповідне вікно, використовуючи кнопку вікна **Close**.

Для розриву зв'язку на інструментальній панелі **Modes** клацніть на кнопці **Break/Restore** (Розірвати/Відновити)  (курсор набуде вигляду молотка) і в Робочій області натисніть на зв'язку між двома пристроями. На перерваному зв'язку відобразиться червоний спалах  і трафік через цю лінію припиниться. Повторне натискання курсором мишки на перерваному зв'язку при активованій кнопці **Break/Restore** (курсор набуде вигляду гайкового ключа) відновлює процес передавання пакетів, а мітка з червоним спалахом зникає.

Перевірка протоколу маршрутизації виконується за допомогою меню **Global** (Глобальний). У цьому меню виберіть пункт **Model Settings** (Налаштування моделі) і перейдіть на закладку **Protocols** (рис. 5.8).

Вибираючи різні мережеві протоколи, у правій колонці можна побачити заданий за замовчуванням протокол маршрутизації для цього мережевого протоколу. Наприклад, обраний протокол маршрутизації для TCP/IP – RIP (протокол обміну даними для маршрутизації). Зміна маршруту пакетів TCP/IP впливає з технічних вимог цього протоколу.

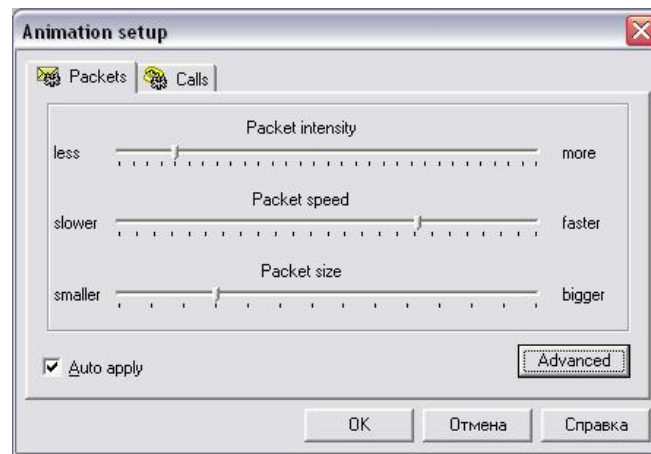


Рис. 5.7. Діалог налаштувань анімації



Рис. 5.8. Закладка Protocols у вікні налаштувань моделі

Щоб отримати інформацію про пакет, розмістіть курсор над будь-яким із пакетів і над ним відобразиться підказка. Коли курсор розташований над пакетом, викличте контекстне меню і виберіть команду **Say Info** (Озвучити інформацію), яка дасть змогу прослухати інформацію про нього.

Обравши пункт **Properties** (Властивості), можна переглянути властивості пакету (рис. 5.9).

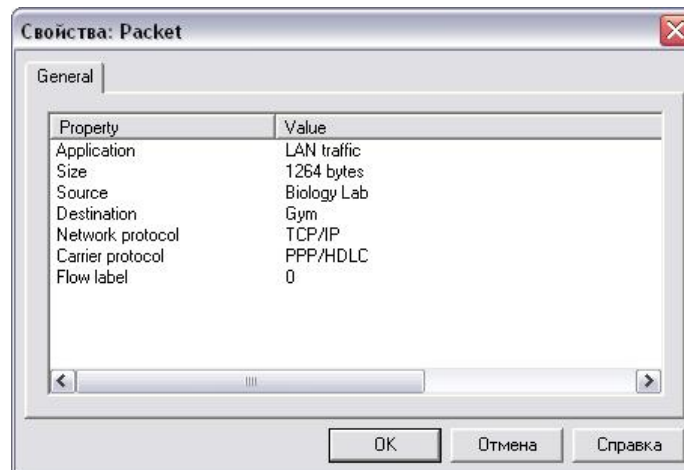


Рис. 5.9. Вікно властивостей пакета

У властивостях пакету відображається інформація про програму, її розмір, джерело, адресат, мережевий протокол та ін.

Розміщення карти на задньому фоні зображення мережі:

- 1) правою кнопкою миші натискаємо на задньому фоні робочої області, і таким способом викликаємо контекстне меню, у якому вибираємо команду **Site Setup** (Налаштування сайту) (рис. 5.10);
- 2) вибираємо закладку **Background** (Задній фон), а потім **Map** (Карта);
- 3) використовуючи кнопку **Browse** (Перегляд), вибираємо потрібний файл карти і натискаємо **OK**.

В NetCracker Professional існує механізм, що дає змогу аналізувати статистичні параметри роботи вузлів (активного устаткування), ліній зв'язку спроектованої мережі, а також заданого трафіка. Статистика розраховується з використанням NetCracker Professional simulation engine.

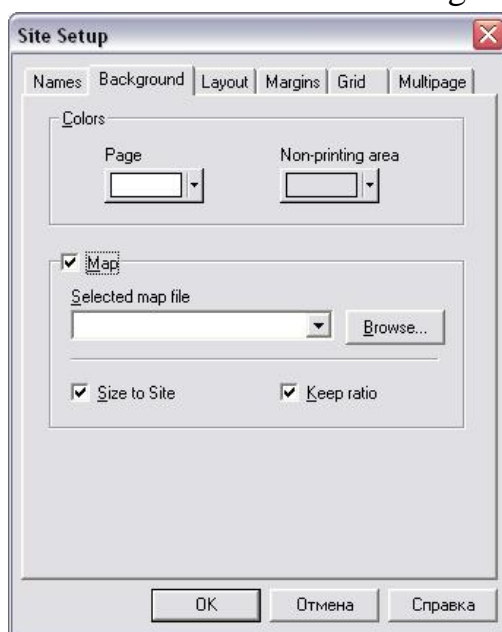


Рис. 5.10. Вікно Site Setup

### *Хід роботи*

1. Запустити програму NetCracker Professional і відкрити файл Techno.net.
2. Розгорнути список Routers and bridges у браузері пристроїв.
3. Розмістити в робочій області маршрутизатор, виготовлений Cisco Systems.
4. Розгорнути у браузері мережеві адаптери виробника D-Link для мережі Ethernet і виділити зображення пристрою Fast EtherLink 10/100 PCI. Вибрати детальний перегляд пристроїв у панелі зображень.
5. Установити режим відображення пристроїв у браузері за типом пристрою.
6. Переглянути пристрої, використані в проєкті.
7. Переглянути інформацію про маршрутизатор, розміщений в робочому полі.
8. Переглянути інформацію про наявні порти у певному змінному блоці маршрутизатора.
9. Додати новий змінний блок до маршрутизатора.
10. Включити звукову підказку з інформацією про опис пристрою.
11. Переглянути всі можливі звіти.

12. Закрити проект *Techno.net* без збереження змін і відкрити файл *Router.net*.
13. Запустити анімацію проекту, встановивши власні параметри інтенсивності руху пакетів, їхньої швидкості руху та розміру.
14. Відкрити один з нижчих рівнів проекту і переглянути пристрої будь-якої робочої станції.
15. Перервати зв'язок між вузлами мережі і переконатися, що між ними немає трафіка.
16. Перевірити протокол маршрутизації.
17. Відновити розірваний зв'язок і призупинити анімацію.
18. Отримати звукову інформацію про пакет та переглянути його властивості.
19. Закрити проект *Router.net* без збереження змін.

### **Контрольні запитання**

1. У чому полягає призначення програмного продукту NetCracker Professional?
2. Які можливості надає користувачеві NetCracker Professional?
3. Що належить до інструментальних засобів NetCracker Professional?
4. Якими інструментальними засобами забезпечується змога керування розмірами полотна проекту?
5. Які функціональні кнопки містить панель керування розмірами полотна проекту?
6. Де розташовано інструментальну панель бази даних і які функціональні кнопки вона містить?
7. Як можна переглянути зображення пристроїв, розміщені у базі даних?
8. За якими параметрами можна сортувати пристрої у браузері?
9. Як одержати інформацію про пристрій, відображений у робочій області проекту?
10. Як змінити налаштування пристрою?
11. Як одержати інформацію про властивості змінного блока пристрою?
12. Як визначити тип лінії, котра з'єднує пристрої у проекті?
13. Як задати параметри лінії зв'язку?
14. Як підготувати звіт про проект?
15. Як підготувати звіт про пристрій?
16. Де розташовано панель керування анімацією і які функціональні кнопки вона містить?
17. Для чого призначено механізм анімації?
18. Як змінити параметри анімації?
19. Де розташовано панель керування режимами роботи миші і які функціональні кнопки вона містить?
20. Як можна зруйнувати (відновити) зв'язки між пристроями проекту?
21. Як одержати інформацію про параметри пакета, що передається лінією?
22. Як можна змінювати конфігурацію ліній зв'язку в спроектованій мережі?
23. Як здійснити перейменування об'єктів проекту?

## Лабораторна робота № 6.

### Проектування однорівневої комп'ютерної мережі у середовищі NetCracker Professional

**Мета роботи:** ознайомитися з поширеними мережевими конфігураціями, отримати практичні навички роботи з NetCracker Professional при створенні моделі мережі, налаштуванні трафіку та отриманні результатів моделювання.

#### *Теоретичні відомості*

Запустіть NetCracker Professional і створіть новий проект меню **File** → **New**. Переконайтеся, що в списку **Hierarchy** обраний пункт **Types**.

Додавання комутатора в робочу область:

- у вікні браузера пристроїв знайти і розгорнути пункт **Switches** (Комутатори), далі пункт **Workgroup** (Робоча група), потім **Ethernet** і виділити потрібного виробника. У панелі зображень відобразяться комутатори відповідного виробника. Після цього потрібно виділити певний комутатор і перетягнути його в робочу область проекту.

Додавання робочих станцій в робочу область:

- 1) у браузері пристроїв вибираємо пункт **LAN workstations** (Робочі станції КМ), далі **Workstations** (Робочі станції) і потім потрібного виробника. У панелі зображень відобразяться робочі станції;
- 2) виділяємо мишкою певний комп'ютер і перетягуємо його в робочу область.


Додавання сервера в робочу область:


- 1) у браузері пристроїв вибираємо пункт **LAN servers** (Сервери КМ), далі **Generic Devices** (Загальні пристрої) або потрібного виробника. У панелі зображень відобразяться доступні сервери;
- 2) виділяємо мишкою певний сервер і перетягуємо його в робочу область.

Встановлення мережевого адаптера в робочу станцію чи сервер:

- у браузері пристроїв потрібно знайти пункт **LAN adapters** (Мережеві адаптери), потім **Ethernet** і вибрати потрібного виробника. У панелі зображень вибрати певний мережевий адаптер і перетягнути його на робочу станцію (коли під курсором миші з'явиться піктограма «+» (плюс), потрібно відпустити кнопку миші).

Під'єднання робочої станції чи сервера до комутатора/концентратора:

- 1) на панелі інструментів **Modes** (Режими) вибираємо інструмент **Link devices** (Зв'язок пристроїв) ;
- 2) виділяємо мишкою зображення робочої станції, а потім комутатора. На екрані відобразиться діалогове вікно налаштування з'єднання Link Assistant;
- 3) вибираємо відповідні порти пристроїв (рис. 6.1), якими буде здійснюватись з'єднання, натискаємо кнопку **Link** (Зв'язок) і закриваємо вікно кнопкою **Close**.

Для швидкого з'єднання робочої станції з комутатором, вибираємо інструмент **Link devices** , натискаємо на клавіатурі кнопку **Shift** і, не

відпускаючи її, за допомогою миші спочатку виділяємо комутатор, а потім робочу станцію.

Аналогічно здійснюється з'єднання будь-яких інших сумісних пристроїв.

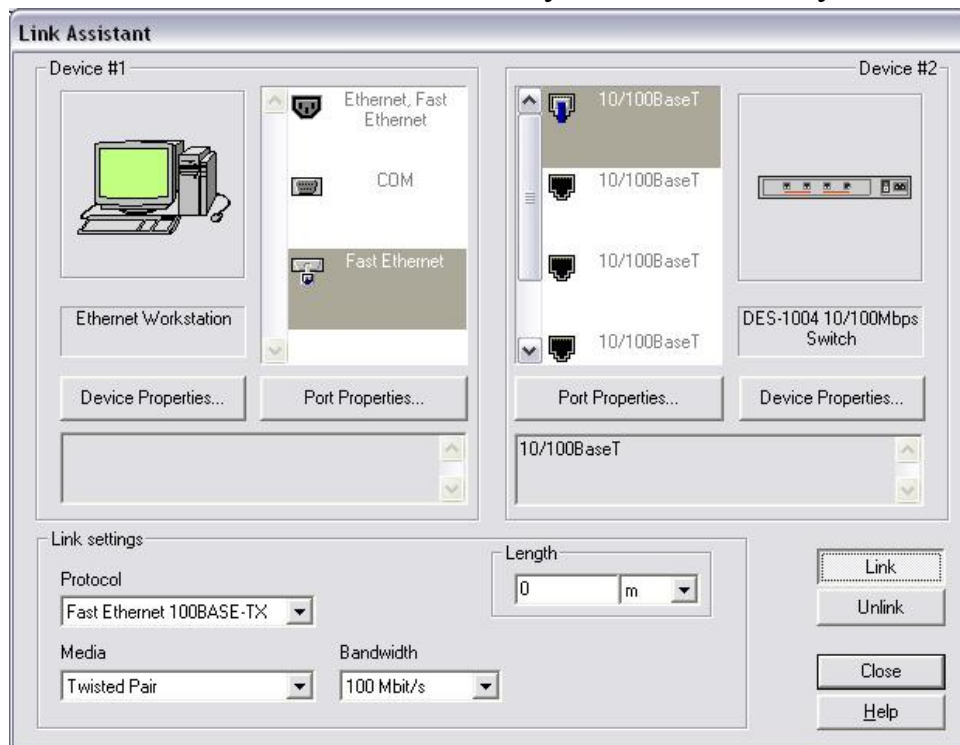


Рис. 6.1. Діалогове вікно налаштування з'єднання Link Assistant

У вікні Link Assistant для налаштованого з'єднання можна вказати протокол (поле Protocol), середовище передавання даних (поле Media), швидкість передавання даних (поле Bandwidth) та довжину кабеля (поле Length). Кнопки **Device Properties** та **Port Properties** дають змогу переглянути властивості пристрою та його порту відповідно. Також тут можна детальніше налаштувати телекомунікаційні та мережеві параметри. Кнопка **Unlink** використовується для роз'єднання пристроїв.

### **Трафік**

Повноцінне моделювання роботи комп'ютерної мережі реалізується шляхом налаштування певного виду трафіка між її вузлами. При цьому розрізняють серверний трафік та клієнтський трафік.

Серверний трафік задається серверу, на якому встановлено певне серверне програмне забезпечення (ПЗ). Серверне ПЗ знаходиться у пункті **"Network and Enterprise software"** браузера пристроїв. Щоб встановити таке ПЗ на сервер потрібно певне ПЗ методом Drag-and-Drop перетягнути на зображення сервера в робочій області.

В NetCracker Professional є змога встановлювати таке серверне програмне забезпечення:

- **FileServer** (файловий сервер) – серверне програмне забезпечення управління доступом до файлів та іншим дисковим ресурсів мережі. Встановлюється, як правило, на виділеному потужному комп'ютері, який, крім управління

доступом до файлів та іншим дисковим ресурсів КМ, забезпечує безпеку і синхронізацію. Безпека розуміється в тому сенсі, що доступ до окремих файлів можуть отримати тільки авторизовані користувачі, що володіють відповідними правами. Синхронізація полягає в блокуванні доступу до файлів і записів, і призначена для захисту даних від пошкодження при одночасній спробі їх зміни кількома користувачами;

- **SQL Server** (SQL-сервер) – серверна спеціалізована програма для роботи з базами даних, що підтримує мову структурованих запитів. Для своєї роботи не вимагає виділеного комп'ютера;
- **Smalloffice database server** (сервер баз даних малого офісу) – програмне забезпечення, за допомогою якого можна організувати доступ декількох вузлів мережі до записів бази даних. Не вимагає виділеного комп'ютера. Використовується в КМ, що підтримують архітектуру “клієнт-сервер”;
- **FTP Server** (FTP-сервер) – сервер, що надає ресурси баз даних віддаленим вузлам КМ, взаємодіє з ним в режимі “термінал-хост”. Для роботи використовує протокол передачі файлів (FTP, FileTransferProtocol), реалізований додатком для роботи в Internet. Він дає змогу передавати файли між різнотипними вузлами, оскільки використовує загальну файлову структуру, незалежну від операційних систем;
- **E-mail Server** (сервер електронної пошти) – програма, яка управляє доставкою електронної пошти та іншої інформації. Для роботи поштового сервера виділений комп'ютер не потрібно;
- **HTTPServer** (HTTP-сервер) – сервер, що надає ресурси web-сайтів. Взаємодіє з HTTP-клієнтом по протоколу передачі гіпертексту (HTTP, HyperTextTransferProtocol). Використовується в мережах Intranet, Extranet, що підтримують архітектуру “клієнт-сервер”.

У середовищі NetCrackerProfessional існують такі профілі трафіка:

- **CAM/CAD** – графічні файли;
- **Database** – дані розподілених ресурсів;
- **E-mail** – електронна пошта;
- **FTP client** – передача файлів;
- **Small office environment** – дані документообігу малого офісу;
- **HTTP client** – дані web-сторінок;
- **LAN peer-to-peer traffic** – передача даних в тимчасовий режим (точка-точка);
- **InterLAN traffic** – зовнішній трафік;
- **Small InterLAN traffic** – зовнішній трафік малого офісу;
- **File Server's client** – трафік клієнта файлового сервера;
- **Small office database server's client** – трафік клієнта сервера для бази даних малого офісу;
- **SQL server's client** – трафік клієнта SQL-сервера;
- **Small office peer-to-peer** – передача даних малого офісу в тимчасовий режим;
- **Voice over IP peer-to-peer** – передача голосового трафіка IP-пакетами;



- **E-mail (SMTP)** – трафік програми електронної пошти стека TCP/IP.

При виборі трафіка типу клієнт-сервер, спочатку потрібно задати трафік для сервера, а потім для всіх клієнтів.

Наприклад, для налаштування трафіка між клієнтом і файловим сервером потрібно виконати такі дії:

1. Встановити серверне програмне забезпечення: у браузері пристроїв (закладка **Devices**) знайти пункт **Network and Enterprise software** і методом Drag-and-Drop перетягнути зображення **File server** на відповідний сервер.
2. Налаштувати серверний трафік: для відповідного сервера викликати контекстне меню, в якому обрати пункт **Configuration**, далі виділити серверне ПЗ (рис. 6.2) і натиснути кнопку **Plug-in Setup** або викликати для нього контекстне меню, в якому вибрати пункт **Properties**. У вікні **Свойства: File server** потрібно обрати закладку **Traffic**, у списку **Application Layer Protocol** позначити додаткові протоколи обміну даними (рис. 6.3) і натиснути кнопку **OK**.

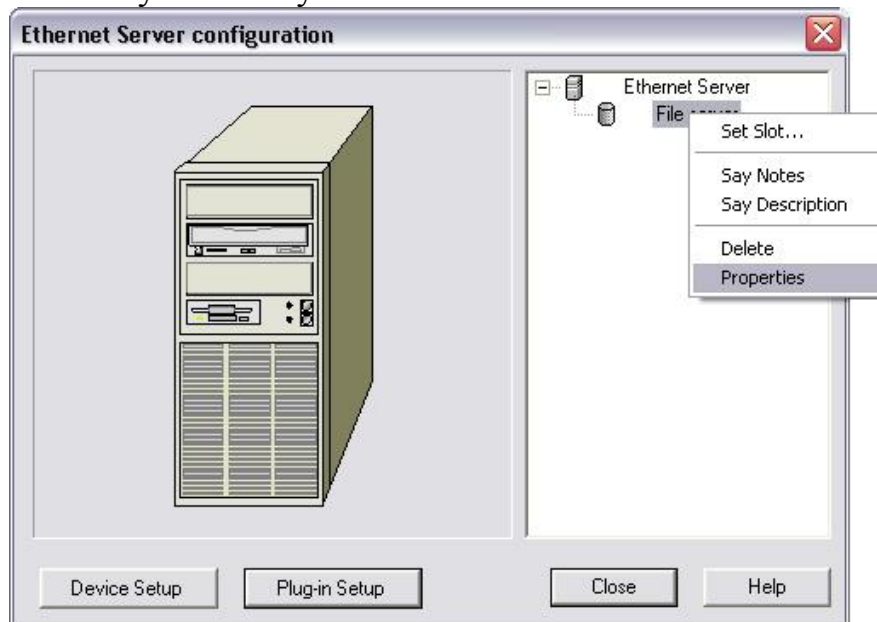



Рис. 6.2. Діалогове вікно налаштувань сервера

3. Налаштування клієнт-серверного трафіка: в панелі інструментів **Modes** вибираємо інструмент **Set Traffic** (Встановити трафік) , виділяємо мишкою спочатку комп'ютер клієнта, а потім сервер. На екрані відобразиться вікно **Profiles** (рис. 6.4), в якому у списку профілів вибираємо профіль **File Server's client** і натискаємо кнопку **Assign**.

Трафік у мережі потрібно задавати у двох напрямках.



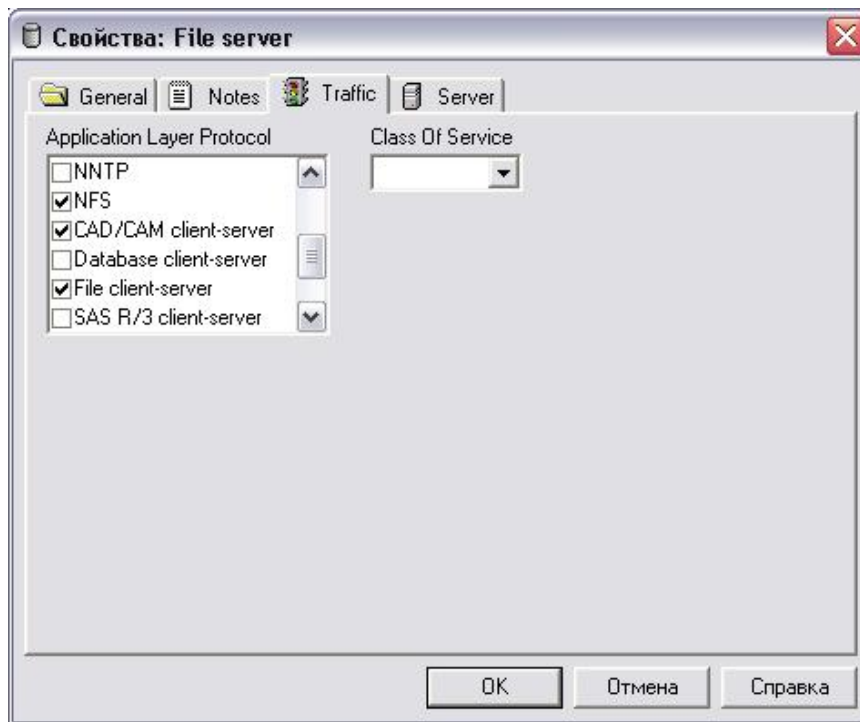


Рис. 6.3. Діалогове вікно властивостей файлового сервера

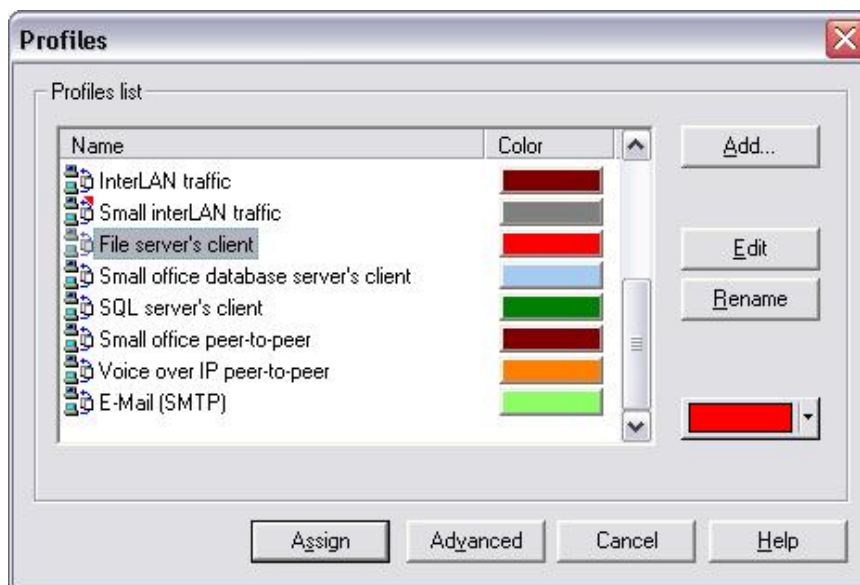



Рис. 6.4. Діалогове вікно профілів трафіка

Встановлення трафіка між двома комп'ютерами мережі:

1. У панелі інструментів **Modes** вибираємо інструмент **Set Traffic** .
2. Виділяємо мишкою спочатку перший об'єкт-джерело трафіка – PC1, а потім другий об'єкт-приймач – PC2. У вікні **Profiles** (рис. 6.4) вибираємо певний профіль трафіка і натискаємо кнопку **Assign**.
3. Виділяємо мишкою спочатку перший об'єкт-джерело трафіка – PC2, а потім другий об'єкт-приймач – PC1. У вікні **Profiles** (рис. 6.4) вибираємо певний профіль трафіка і натискаємо кнопку **Assign**.

Зауважимо, що напрям трафіка визначається від першого виділеного об'єкта до другого.

Огляд заданого трафіка здійснюється за допомогою пункта **Data Flow** (Потоки даних) головного меню **Global**, в якому є змога змінювати властивості трафіка, у тому числі додавати і видаляти мережевий трафік (рис. 6.5).

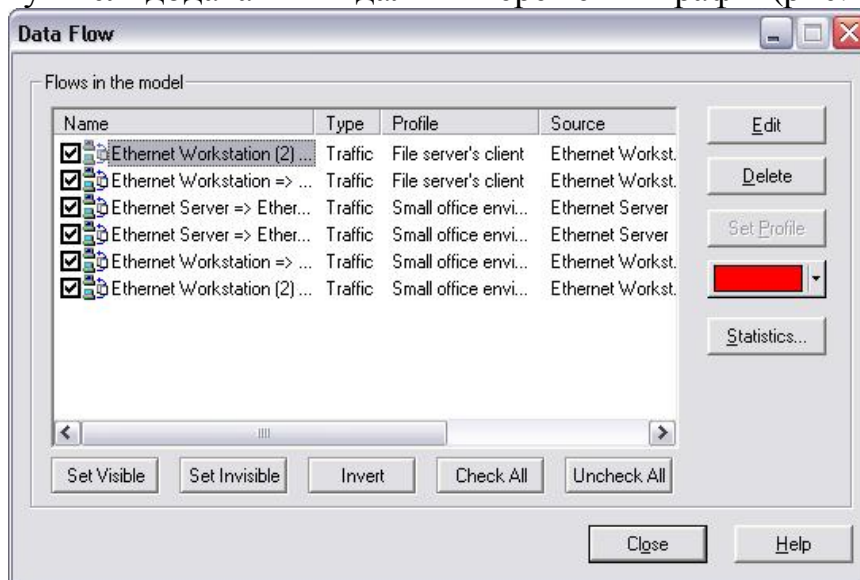


Рис. 6.5. Діалогове вікно заданих профілів трафіку

Щоб переглянути розподіл (вхідний і вихідний) трафіка для клієнтського комп'ютера або сервера, потрібно викликати на ньому контекстне меню і обрати пункт **Associated Data Flow** (Асоційовані потоки даних). На екрані відобразиться вікно, подане на рис. 6.6. У цьому вікні є дві закладки **Outgoing traffic** (Вихідний трафік) та **Incoming traffic** (Вхідний трафік).

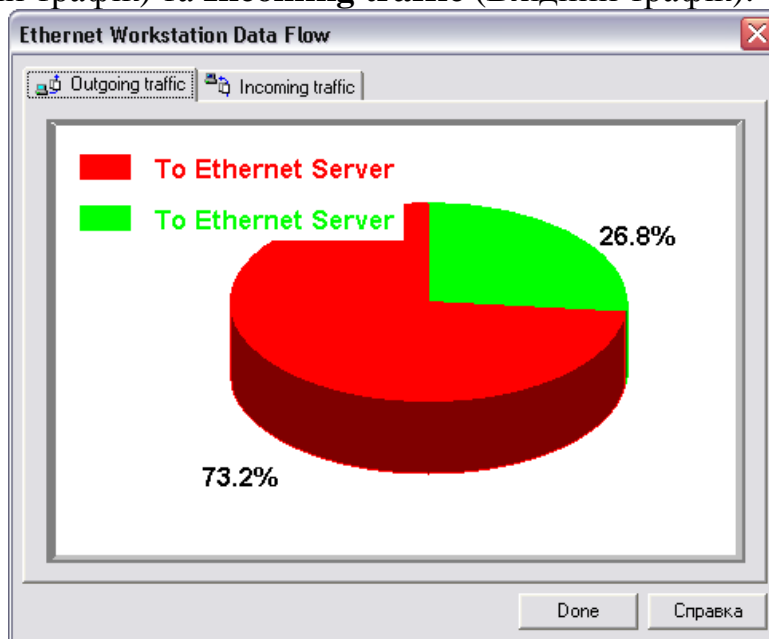


Рис. 6.6. Діалогове вікно потоків даних

При запуску анімації (кнопка **Start** ► на панелі інструментів **Control**) трафік відображається для всіх вузлів мережі, якщо він налаштований.

## Статистика

У NetCracker Professional пропонуються такі статистичні параметри ліній зв'язку:

- *average workload* – середнє навантаження характеризує кількість повідомлень (пакетів), переданих лінією зв'язку за певний період спостереження (хвилину, годину);
- *current workload* – поточне навантаження показує кількість повідомлень (пакетів), що проходять лінією в конкретний момент часу (щомиті);
- *current utilization* – поточне використання відображає частку пропускну здатності лінії, зайнятої поточним навантаженням;
- *average utilization* – середнє використання показує частку пропускну здатності лінії, задіяної під передавання навантаження за певного періоду спостереження;
- *current number of calls* – поточна кількість викликів.

Перелік статистичних параметрів вузла залежить від типу пристрою (PC, PBX, Hub, комутатор, телефон, відеотермінал тощо). У NetCracker Professional серед цих параметрів є такі (наведений список не є вичерпним):

- *current utilization* – поточне використання;
- *average utilization* – середнє використання;
- *average workload* – середнє навантаження;
- *current workload* – поточне навантаження;
- *average delay* – середня затримка;
- *packets for last second* – пакети, передані за останньої секунди;
- *packets dropped for last second* – пакети, загублені за останньої секунди;
- *calls received* – отримані виклики;
- *calls blocked* – блоковані виклики;
- *packets received* – отримані пакети;
- *transactions received* – завершені транзакції;
- *calls requested of* – кількість запитуваних викликів;
- *calls established of* – кількість завершених викликів.

Під використанням вузла розуміють частку його задіяної продуктивності.

Перелік статистичних параметрів трафіка визначається його профілем і в загальному випадку включає такі з них:

- *calls requested* – кількість запитуваних викликів;
- *calls established of* – кількість завершених викликів;
- *average call length* – середня тривалість виклику;
- *response time* – час відгуку;
- *travel time* – час передавання.

Для визначення статистичних параметрів певного вузла чи лінії зв'язку, для цього об'єкта необхідно викликати контекстне меню і вибрати пункт **Statistics** (Статистика). А визначення статистичних параметрів профільного трафіка здійснюється шляхом вибору в меню **Global** відповідного профіля трафіка, а у вікні **Data Flow** натисненням кнопки **Statistics**.

Для відображення статистичних параметрів може бути використано діаграми, цифрові показники та графіки.

**Status Bar** (Рядок стану) відображає інформацію, що належить до діяльності програми у певний момент. У правій частині рядку стану розташовано поле з написом **System Time** (Системний час) – це кількість секунд, протягом яких моделюється робота мережі. Переважно час моделювання не відповідає реальному часу.

*Встановлення індикатора використання трафіка між двома пристроями мережі:*

- 1) виділіть перший пристрій, викличте контекстне меню і виберіть пункт **Statistics**;
- 2) у вікні **Statistical Items** навпроти рядка **Current utilization** відмітьте комірки графічного та цифрового індикатора, графіка, звуку (рис. 6.7) і збережіть зміни.

*Налаштування цифрового індикатора:*

- 1) за допомогою мишки перемістіть його нижче лінії зв'язку;
- 2) у контекстному меню виберіть пункт **Properties**, установіть розмір шрифту 34, колір – червоний.

*Отримання звукового повідомлення про використання зв'язку:*

- 1) у панелі інструментів **Modes** виберіть кнопку **Say Information** (🔊) або в контекстному для певного зв'язку виберіть пункт **Say Current Statistics**;
- 2) виберіть зв'язок і в панелі інструментів **Modes** виберіть кнопку **Break/Restore** (🔧).

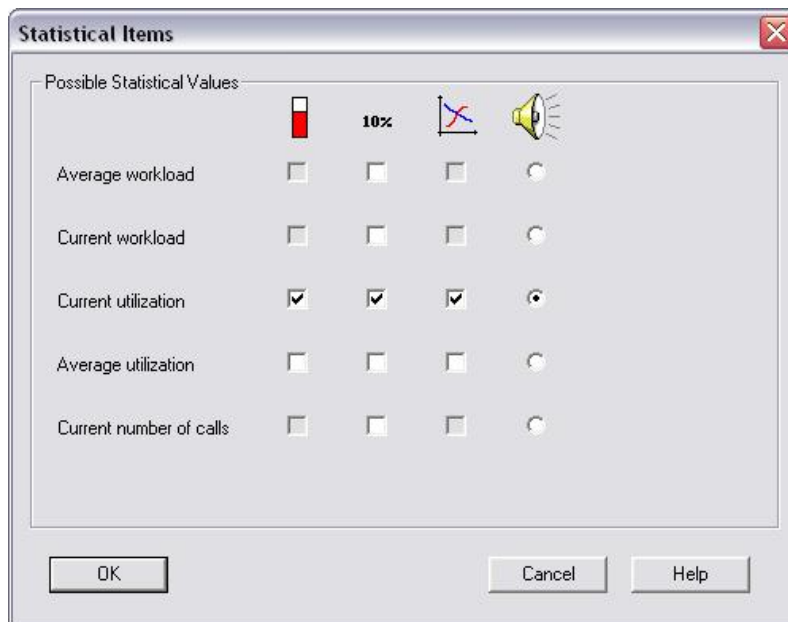


Рис. 6.7. Вікно діалогу Statistical Items

Звукове повідомлення також можна налаштувати для певного пристрою або конкретного пакету.

### *Хід роботи*

1. Ознайомитися із завданням та розробити проект мережі згідно топології та специфікацій. Проект назвати згідно такого формату: Lab06-Прізвище-Група-Рік, наприклад, Lab06-Bender-KN31-2015.

№ з/п	Завдання
1.	Робочі станції W1-W3 і сервер S1 з'єднані між собою за допомогою мережі FastEthernet, з використанням неекранованої скрученої пари категорії 5 і комутатора. Ethernet мережа, своєю чергою, за допомогою маршрутизатора і моста пов'язана з мережами 16 Мбіт/с Token Ring та FastEthernet відповідно. Робочі станції W4, W5 і сервер S2 з'єднані в мережу Token Ring. Станції W6-W8 і сервер S3 з'єднані за технологією FastEthernet.
2.	Сегмент 10BASE-T, що складається з 3-х робочих станцій W1-W3 на базі концентратора фірми D-Link, і сегмент на базі концентратора Fast Ethernet з робочих станцій W4, W5 з'єднані за допомогою комутатора за технологією 100BASE-TX, до якого підключені сервери S1 та S2 за тією ж технологією.
3.	Робочі станції W1-W5 і сервер S1 утворюють сегмент 10BASE-T. Інші п'ять комп'ютерів об'єднані в сегмент за технологією 10BASE-2, обидва сегмента з'єднані мостом. До сервера підключений принтер.
4.	У мережі є два концентратори (10BASE-2). До першого концентратора за допомогою коаксіального кабелю 10BASE-2 безпосередньо підключені робочі станції W1-W3, а станції W4 та W5 з'єднані з ним загальною шиною 10BASE-2. До сегмента Thin Ethernet підключені другий концентратор і сервер S1. До другого концентратора підключені робочі станції W6 та W7 і сервер S2.
5.	Робочі станції W1-W3 і сервер S1 на базі хаба утворюють сегмент 100BASE-TX. Хаб, своєю чергою, підключений до комутатора за технологією 10BASE-T. Комутатор підключений до маршрутизатора за цією ж технологією. Станції W4 та W5 і сервер S2 з'єднані за допомогою товстого коаксіального кабелю з комутатором. Маршрутизатор з'єднаний з сервером віддаленого доступу (Access server) через сегмент Thick Ethernet. До сервера доступу підключені 2 пристрої: DSU/CSU і телефонний модем, що забезпечують доступ до мереж ISDN і PSTN відповідно. До цього сервера мають доступ віддалені робочі станції W6 і W7 через мережі ISDN і PSTN відповідно. У робочу станцію W6 встановлено адаптер ISDN.
6.	Робочі станції W1-W6 і сервер S1 з'єднані між собою в мережу FDDI, використовуючи неекрановану скручену пару категорії 5. FDDI кільце, своєю чергою, за допомогою маршрутизаторів пов'язано з двома мережами Token Ring, у кожен з яких входить по одному серверу і по дві робочі станції.

7.	До мережі Frame Relay, з використанням скрученої пари 10BASE-T підключені 3 пристрої DSU/CSU: DSU1–DSU3. DSU1 та DSU2, своєю чергою, підключені до пристроїв FRAD (Frame relay access device) – F1 і F2. До пристрою F1 підключений концентратор Fast Ethernet. Робоча група, робоча станція W1 і сервер S1 підключені до цього концентратора скрученою парою 100BASE-TX. До F2 підключений сегмент Thick Ethernet з сервером S2, робочою станцією W2 і принтером.
8.	Робочі станції W1-W4, сервери S1 і S2, а також сервер віддаленого доступу (Access Server) утворюють сегмент мережі 100Base-T. До сервера віддаленого доступу підключено зовнішній модем, який має доступ до мережі PSTN. Сервер S3 і робочі станції W5-W8 утворюють сегмент Thick Ethernet, який з'єднаний з сегментом 100Base-T. Станції W5-W8 через сервер S3 мають доступ до серверів S1 і S2 та принтера на сервері S2.
9.	Робочі станції W1-W3 і сервер S1 з'єднані між собою в FDDI мережу, використовуючи неекрановану скручену пару категорії 5. FDDI кільце, в свою чергу, за допомогою маршрутизатора і моста, пов'язане з мережами 16 Мбіт/с Token Ring і 100 Мбіт/с Ethernet відповідно. Робочі станції W4 та W5 і сервер S2 з'єднані в мережу Token Ring. Станції W6-W8 і сервер S3 з'єднані за технологією Fast Ethernet.
10.	Робочі станції W1-W3 і сервер S1 з'єднані між собою за допомогою мережі 4 Мбіт/с Token Ring, з використанням комутатора Token Ring. Мережа Token Ring за допомогою моста пов'язана з мережею FastEthernet та сегментом Thin Ethernet. Робочі станції W4 та W5 і сервер S2 з'єднані в мережу FastEthernet. Станції W6-W8 і сервер S3 з'єднані за технологією Thin Ethernet.
11.	Сегмент 10BASE-T, що складається з робочих станцій W1-W3 на базі концентратора фірми D-Link, і сегмент на базі концентратора Fast Ethernet з робочих станцій W4-W8 з'єднані за допомогою комутатора за технологією 100BASE-TX, до якого підключені 3 сервери за технологією Fast Ethernet.
12.	У мережі є два концентратори (10BASE-5). Робочі станції W1 та W2 з'єднані з першим концентратором загальною шиною (10BASE-5), також до нього за допомогою коаксіального кабелю (10BASE-2) підключені робочі станції W3-W5. До сегмента Thin Ethernet підключені другий концентратор, робоча станція W6 та сервер S1. До другого концентратора підключені станції W7 та W8 і сервер S2.
13.	Робочі станції W1-W4, сервери S1 та S2, а також сервер віддаленого доступу (Access Server) утворюють сегмент мережі 100Base-T. До сервера віддаленого доступу підключено Wi-Fi точку, а також сегмент Thick Ethernet, який складається з сервера S2 та робочих станцій W5-W8.
14.	Робочі станції W1-W3 з'єднані з концентратором H1 за технологією 100BASE-TX. До другого концентратора H2 підключені ноутбук N1, сервер S1 та принтер. На сервері встановлені сервер баз даних та

	файловий сервер. Концентратори H1 та H2 з'єднані за технологією 100BASE-FX.
15.	Робочі станції W1-W2 з'єднані з комутатором SW1 за технологією 100BASE-T4, який у свою чергу з'єднаний з маршрутизатором R1, до якого ще підключений маршрутизатор R2 локальним кабелем за технологією ATM. Маршрутизатор R2 з'єднаний з комутатором SW2, до якого підключені робоча станція W3 та сервер S1. На сервер S1 встановлені поштовий сервер та веб-сервер.

1. Для розробленого індивідуального проекту мережі вивести статистику: для серверів поточне навантаження (current workload) та кількість отриманих пакетів, а для сегментів відсоток використання (average utilization). Запустити модель і визначити, чи є перевантаження обладнання або зв'язків:
  - 1.1. Запустити анімацію та моделювання.
  - 1.2. Переглянути інформацію, що стосується діяльності програми в певний момент.
  - 1.3. Зупинити анімацію та моделювання.
  - 1.4. Установити та налаштувати індикатори статистики на зв'язки між різними парами пристроїв, для яких налаштовано трафік, а також для деяких пристроїв мережі.
  - 1.5. Налаштувати отримання звукових повідомлень про використання зв'язку та пакетів.
  - 1.6. Вивести графіки використання зв'язку в режимі роботи та в режимі перерваного зв'язку.
2. Оформити звіт.

### ***Контрольні запитання***

1. Як підготувати робоче вікно нового проекту?
2. Що слід вчинити, щоб у вікні піктограм відбилися пристрої, котрі забезпечують вибір необхідного елемента планованої мережі?
3. Яким способом обраний пристрій переміщується до робочої області проекту?
4. Як збільшити розмір пристрою у робочій області?
5. Яким способом збільшується розмір шрифту напису під пристроєм у робочому вікні проекту?
6. Як установити мережевий адаптер у робочу станцію?
7. Як здійснити вибір сумісного устаткування? Що означає “сумісне устаткування”?
8. Як здійснюється з'єднання пристроїв у планованій мережі? Як установлюються параметри з'єднання (довжина лінії зв'язку, тип середовища передавання, ширина смуги, протокол зв'язку)?
9. У чому полягає функціональне призначення вікна Link Assistant?
10. Як швидко організувати з'єднання пристроїв мережі?
11. Що розуміється під профілем трафіка?
12. У чому полягає функціональне призначення вікна “Профілі трафіка”?

13. У чому полягає процедура призначення трафіка поміж активними пристроями мережі?
14. Як перевірити установку трафіка в мережі?
15. Як можна впливати на анімаційні параметри трафіка? Які параметри може бути змінено?
16. Як одержати довідку про профілі трафіка, встановленого в мережі?
17. Яку інформацію надає вікно профілів встановленого трафіка?
18. Як у вікні зображень відобразити пристрої, які використовуються у поточному проекті?
19. Як викликати вікно “Налаштування заднього фону” проекту? Які функції у ньому доступні?
20. Як розташувати карту на задньому плані проекту?
21. Як забезпечити нарощування блоків у стекових пристроях?
22. Як зберегти поточний проект?
23. Які можливості надає використання статистики при моделюванні роботи мережі?
24. Для яких елементів мережі можна встановити індикатори статистичних параметрів?
25. Які статистичні параметри можна проаналізувати для ліній зв'язку?
26. Які статистичні параметри можна проаналізувати для вузлів мережі?
27. Які статистичні параметри можна проаналізувати для трафіка?
28. Що розуміється під утилізуванням лінії зв'язку, вузла мережі?
29. Які індикатори можна встановити для відбиття значень статистичних параметрів елементів мережі?
30. Що слід зробити, щоб встановити індикатор для лінії зв'язку?
31. Що слід зробити, щоб встановити індикатор для вузла?
32. Що слід зробити, щоб встановити індикатор для трафіка конкретного профілю?
33. Як викликати вікно налаштування статистики?
34. У чому полягає процедура налаштування зображення індикатора?
35. Як скласти статистичний звіт?



## Лабораторна робота № 7.

### Багаторівневе проектування комп'ютерної мережі у середовищі NetCracker Professional

**Мета роботи:** навчитися створювати схеми багаторівневих мереж та клієнт-серверних архітектур, структурувати багаторівневі проекти.

#### *Теоретичні відомості*

Додавання об'єкта **Building** (Будинок) і створення багаторівневого з'єднання:

- 1) у робочій області розмістіть мережу, що, наприклад, містить декілька комп'ютерів та комутатор;
- 2) на закладці **Devices** браузера пристроїв виберіть пункт **Buildings, campuses and LAN Workgroups**. Перетягніть зображення одного з об'єктів **Building** у робочу область вікна;
- 3) налаштуйте зв'язок між комутатором та об'єктом **Building**;
- 4) відкрийте вікно **Building**: у контекстному меню для об'єкта **Building** виберіть **Expand** або ж виконайте **Objects** → **Expand** чи двічі клацніть на об'єкті **Building**. Якщо зв'язок між комутатором та об'єктом **Building** існує, то в лівому верхньому куті вікна **Building** відобразиться зменшене зображення комутатора .
- 5) у робочу область вікна **Building** додайте робочу групу (рис. 7.1) і комутатор, налаштуйте між ними зв'язок;

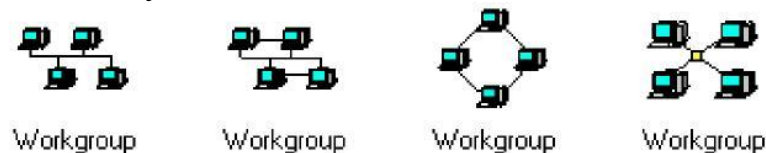


Рис. 7.1. Зображення робочих груп

- 6) налаштуйте зв'язок між комутатором та зменшеним зображенням комутатора, що відображається у лівому верхньому куті.

Налаштування робочої станції як сервера:

- 1) у браузері пристроїв виберіть **Network and enterprise software** → **Server software**. На панелі зображень будуть зображені доступні типи серверів;
- 2) перетягніть **E-mail server** на робочу станцію.



Відображення проекту сайту у вигляді ієрархічної структури:

- у меню **Views** виберіть пункт **Project Hierarchy**.


Перейменування вікна сайта:

- перейдіть у вікно **Building**, в панелі меню **Sites** виберіть пункт **Site Setup**, виберіть закладку **Names** і в поле **Site name** введіть **MacNally Building**.



Вставка приміток:

- 1) зробіть вікно **MacNally Building** поточним;
- 2) на панелі **Modes** виберіть режим **Draw** ;
- 3) на панелі інструментів **Drawing** виберіть кнопку **Line**  і намалюйте стрілку, спрямовану до правого верхнього кута;
- 4) змініть колір намальованої стрілки. Виділіть лінію, виконайте дії **Object** → **Styles** → **Draw Color** і виберіть певний колір або двічі натисніть на лінії і виберіть певний колір.

Підсвітка трафіка:

- запустіть анімацію. На панелі інструментів **Modes** виберіть кнопку **Trace** , у вікні **MacNally Building** виберіть одну робочу станцію, а потім виберіть іншу робочу станцію.

Підсвітка трафіка зі збереженням установлених підсвіток:

- 1) запустіть анімацію. Розмістіть два вікна так, щоб бачити як трафік з **MacNally Building** проходить у вікно **Top** і навпаки;
- 2) натисніть кнопку **Trace**  та кнопку  на панелі інструментів **Toggle Multi-Trace Mode** і одразу ж вкажіть колір зв'язку;
- 3) у вікні **MacNally Building** виберіть **Building** (2), а у вікні **Top** – робочу станцію.

### *Хід роботи*

1. Ознайомитися із теоретичними відомостями.
2. Створити новий проект комп'ютерної мережі. Проект назвати згідно такого формату: Lab07-Прізвище-Група-Рік, наприклад, Lab07-Bender-KN31-2015.
3. Відкрити проект комп'ютерної мережі, створений у попередній лабораторній роботі, виділити всі об'єкти, скопіювати їх та вставити у новостворений проект.
4. Додати міст і налаштувати зв'язок між ним та існуючою мережею.
5. Додати об'єкт Building і налаштувати зв'язок між ним та мостом.
6. Відкрити об'єкт Building, додати декілька робочих станцій і файловий сервер, які за допомогою комутатора об'єднати у мережу.
7. Додати міст, який з'єднати з даним комутатором.
8. Налаштувати зв'язок між об'єктом Building та мостом.
9. Задати мережевий трафік між різними рівнями проекту.
10. Оформити звіт.

### *Контрольні запитання*

1. Для чого потрібна багаторівнева мережа?
2. Між якими об'єктами можна створити багаторівневе з'єднання?
3. Які типи зв'язку можна використовувати для багаторівневого з'єднання?
4. Як налаштувати робочу станцію у вигляді сервера?
5. Які типи трафіка можна використати у багаторівневій мережі?
6. Як розрізняються різні типи трафіку?

## Лабораторна робота № 8.

### Проектування комп'ютерної мережі в Cisco Packet Tracer

**Мета роботи:** ознайомитися з графічним інтерфейсом Cisco Packet Tracer, навчитись моделювати комп'ютерну мережу, а також здійснювати її моніторинг.

#### *Теоретичні відомості*

Cisco Packet Tracer – програма фірми Cisco Systems, що дає змогу моделювати комп'ютерні мережі, розробляти працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару). Крім того є змога додавати та налаштовувати сервери DHCP, HTTP, TFTP, FTP, робочі станції, різні модулі до комп'ютерів та маршрутизаторів, пристрої WiFi, різні кабелі.

Cisco IOS – багатозадачна операційна система, що виконує функції мережевої організації, маршрутизації, комутації та передачі даних, використовується в маршрутизаторах і комутаторах. Ця ОС має інтерфейс командного рядка, який оперує набором команд, доступні команди визначені режимом і рівнем привілеїв користувача.

Packet Tracer доповнює фізичні пристрої, даючи змогу створювати віртуальні мережі з практично необмеженою кількістю пристроїв.

Для запуску програми Cisco Packet Tracer потрібно виконати такі дії:

**Пуск → Всі програми → Cisco Packet Tracer → Cisco Packet Tracer.**

Головне вікно програми Cisco Packet Tracer, подане на рис. 8.1, складається з таких частин:

- головне меню (1);
- верхня панель інструментів (2);
- перемикач між логічною та фізичною організацією (3);
- панель інструментів (4);
- перемикач між реальним режимом (Real-Time) та режимом симуляції (5);
- панель створення сценаріїв користувача (6);
- панель типів пристроїв (7);
- панель моделей пристроїв (8);
- робоча область (9).

Панель інструментів (4) містить піктограми інструментів для роботи з проектом та об'єктами проекту. Кожний з інструментів, активується при виборі відповідної піктограми. Розглянемо призначення кожного з інструментів цієї панелі у порядку зверху вниз:

- **Select** (вибрати) використовується для виділення одного або кількох об'єктів для подальшого переміщення, копіювання або видалення;
- **Move Layout** (перемістити) використовується для прокручування великих проектів;

- **Place Note** (додати підпис) додає підпис у будь-якій частині проекту. Зручно використовувати для коментарів або ж для розміщення основної інформації сценарію безпосередньо у проекті для подальшої роботи;
- **Delete** (видалити) видаляє об'єкт або групу об'єктів;
- **Inspect** (збільшити) використовується для збільшення об'єктів проекту. Залежно від типу пристрою можна переглядати вміст таблиці ARP, таблиці маршрутизації, таблиці NAT і т.д.;
- **Resize Shape** (змінити розмір) призначений для зміни розмірів об'єктів (чотирикутників і кіл);
- **Add Simple PDU** (додати простий пакет) і **Add Complex PDU** (додати складний пакет) призначені для моделювання надсилання з подальшим відстеженням довільного пакету даних усередині проекту.

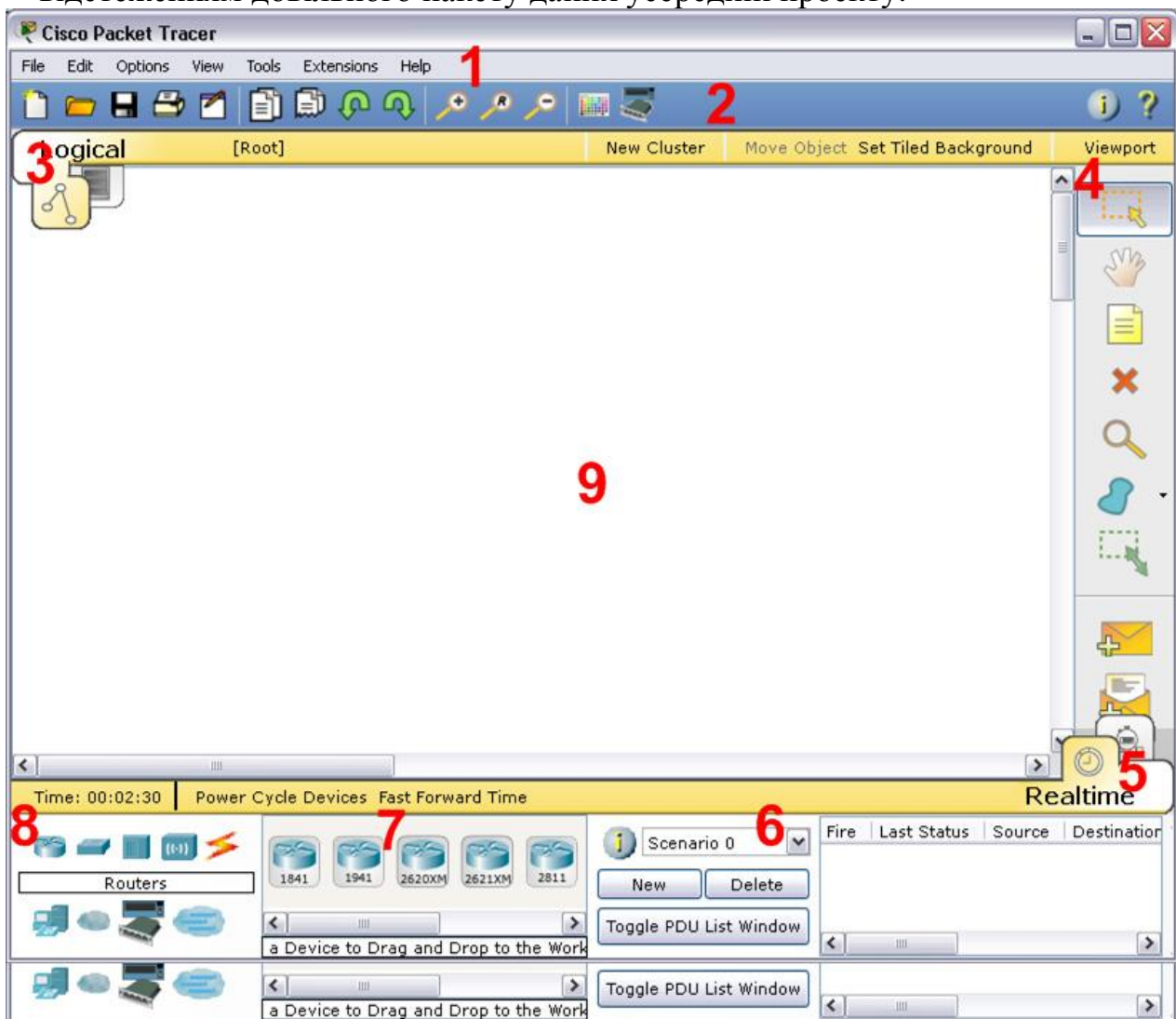


Рис. 8.1. Головне вікно Cisco Packet Tracer

Панель (8) дає змогу вибрати тип пристрою, а панель (7) безпосередньо сам пристрій.

У панелі (7) доступні такі типи пристроїв (рис. 8.2):

- комутатори другого і третього рівня (switches);
- маршрутизатори (routers);

- мережеві концентратори (hubs);
- кінцеві пристрої: робочі станції, ноутбуки, сервери, принтери (end devices);
- бездротові пристрої: точки доступу, бездротові маршрутизатори (wireless devices);
- глобальна мережа WAN;
- вибіркові пристрої;
- багатокористувацькі з'єднання.

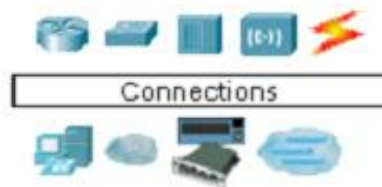


Рис. 8.2. Панель типів пристроїв

У робочій області (9) розташовують всі мережеві пристрої, здійснюється їхнє налаштування, моделюється робота мережі і переглядається її статистика.

### Додавання маршрутизатора у проект

Для того щоб додати маршрутизатор у проект мережі, потрібно послідовно виконати такі кроки (рис. 8.3):

- на панелі типів пристроїв вибрати піктограму **Routers** (1);
- на панелі кінцевих пристроїв вибрати певну модель маршрутизатора (2);
- додати вибраний маршрутизатор у проект, натиснувши лівою кнопкою миші у робочій області (3).

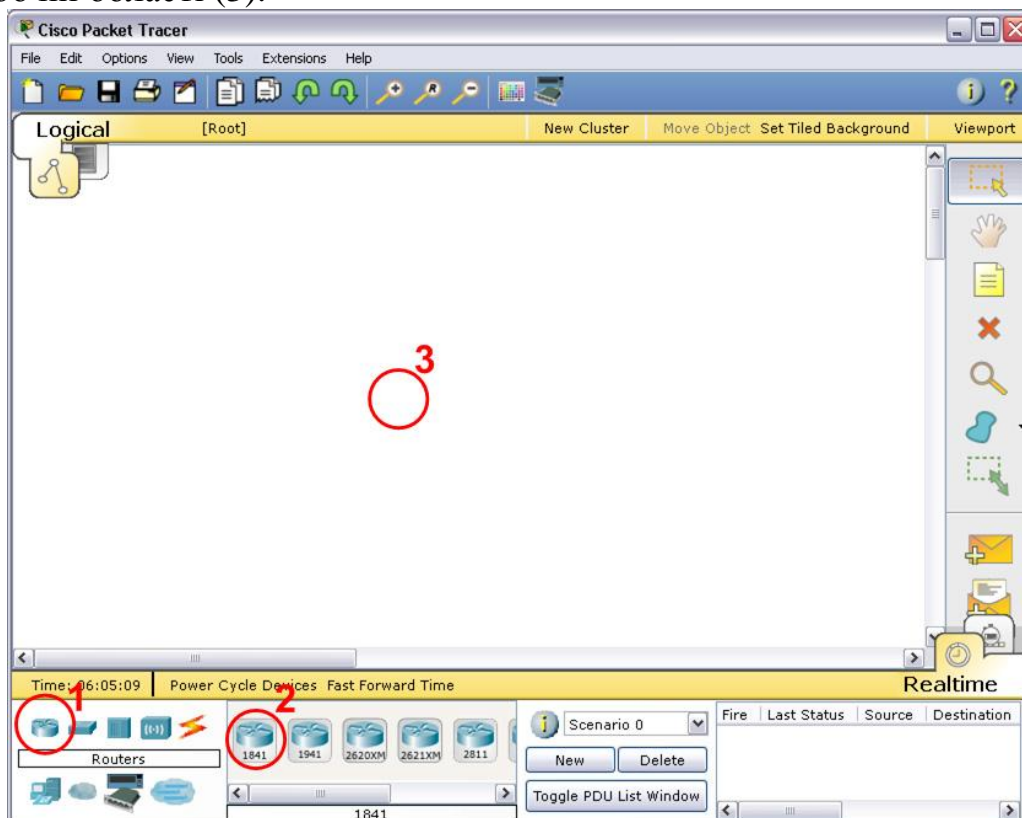


Рис. 8.3. Додавання маршрутизатора

Після того як пристрій додано у проект, можна відкрити вікно його налаштувань (рис. 8.4), у якому є змога доступу до апаратної конфігурації певного модуля, а також її зміни засобами IOS CLI або меню. Щоб відкрити вікно налаштувань пристрою, потрібно натиснути лівою кнопкою миші на його піктограмі в робочій області.

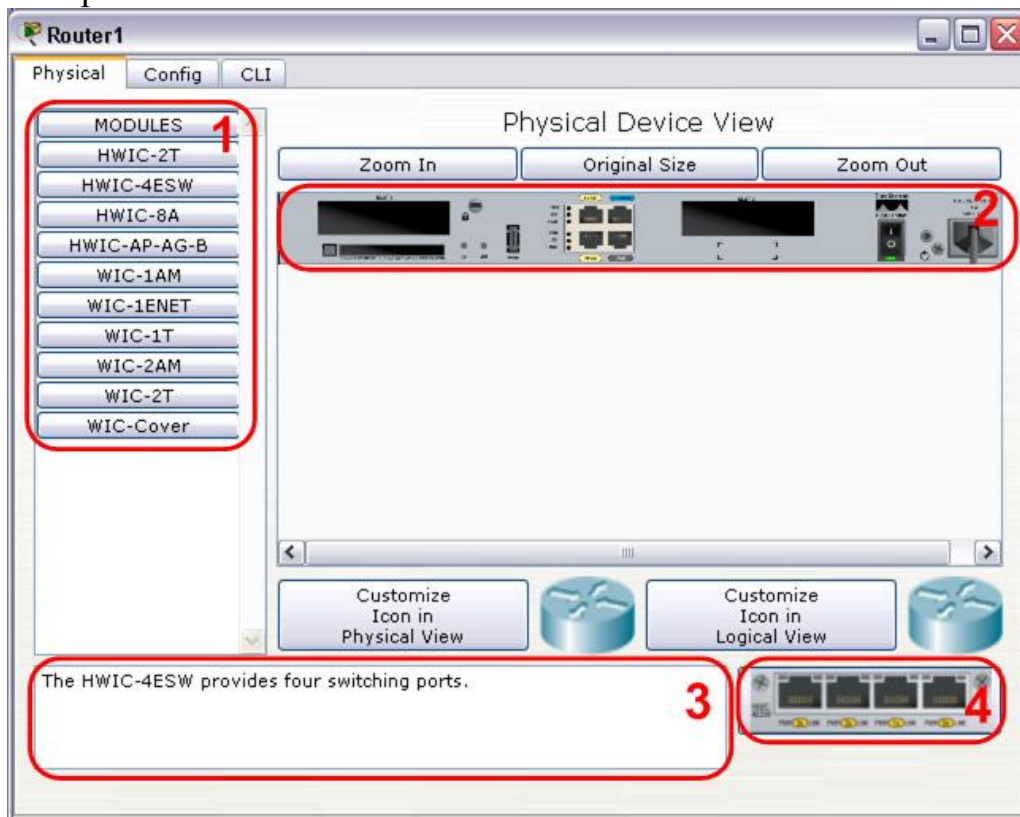


Рис. 8.4. Закладка апаратної конфігурації маршрутизатора

Закладка **Physical** (рис. 8.4) дає змогу керувати апаратною конфігурацією маршрутизатора і відображає такі елементи:

- 1) список доступних для установки модулів;
- 2) зовнішній вигляд обладнання;
- 3) опис обраного модуля;
- 4) зовнішній вигляд обраного модуля.

На закладці **Physical** є змога встановлювати певні модулі у вільні роз'єми (рис. 8.5). Крім того, вільні роз'єми можуть бути закриті фальш панелями (WIC-Cover).

Перед тим як додати або видалити певні модулі обов'язково потрібно вимкнути пристрій, натиснувши на кнопку живлення (1). Після встановлення чи видалення модуля потрібно ввімкнути кнопку живлення пристрою (1).

Для встановлення нового модуля у пристрій спочатку потрібно вибрати певний модуль (2) і після цього лівою кнопкою миші перетягнути його зображення у вільний роз'єм (3-4).

Видалення вже встановленого модуля з пристрою виконується шляхом перетягування зображення цього модуля (4) лівою кнопкою миші з пристрою у місце зовнішнього вигляду модуля (3).

Закладка **Config** містить налаштування маршрутизатора (рис. 8.6).



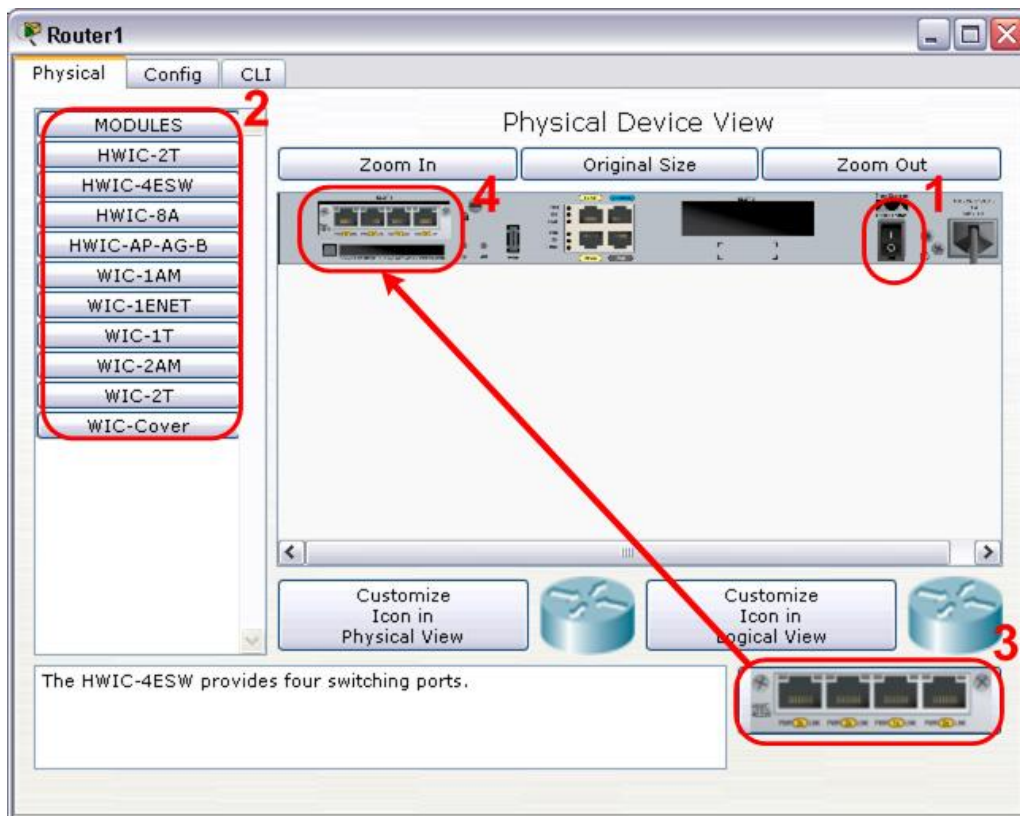


Рис. 8.5. Встановлення нового модуля

Закладка **CLI** надає доступ до консолі Console0 маршрутизатора (рис. 8.7). За замовчуванням пароль на доступ до консолі не встановлений.

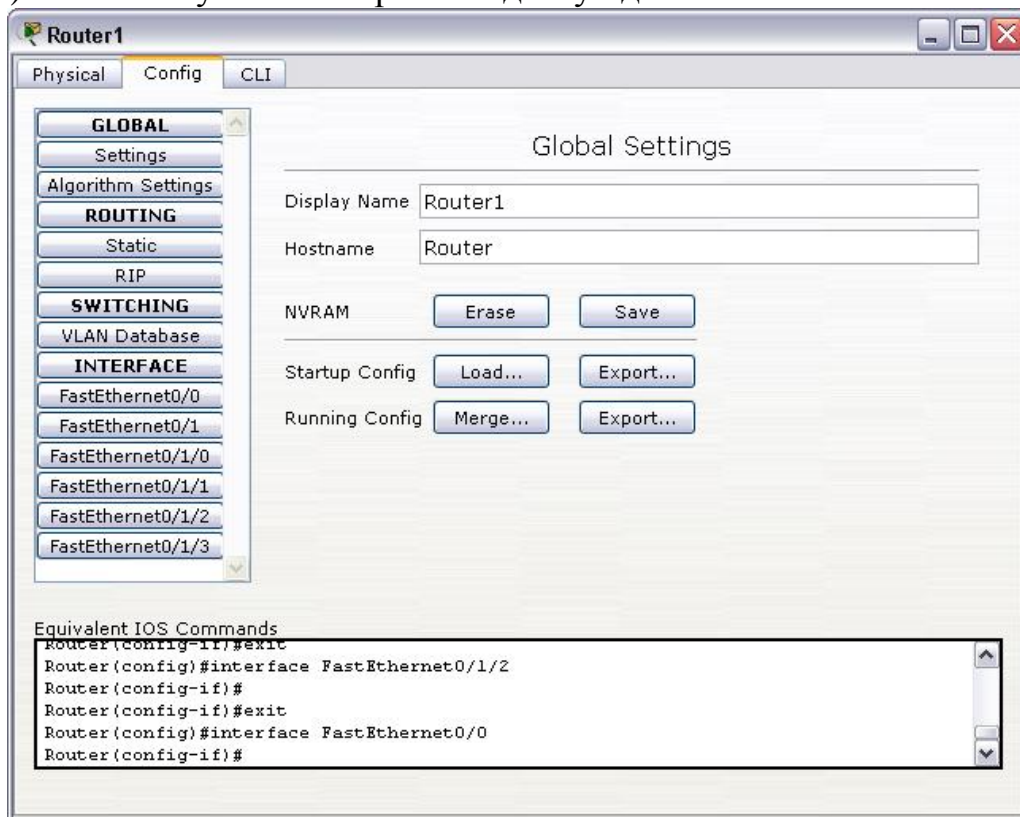


Рис. 8.6. Закладка налаштувань маршрутизатора

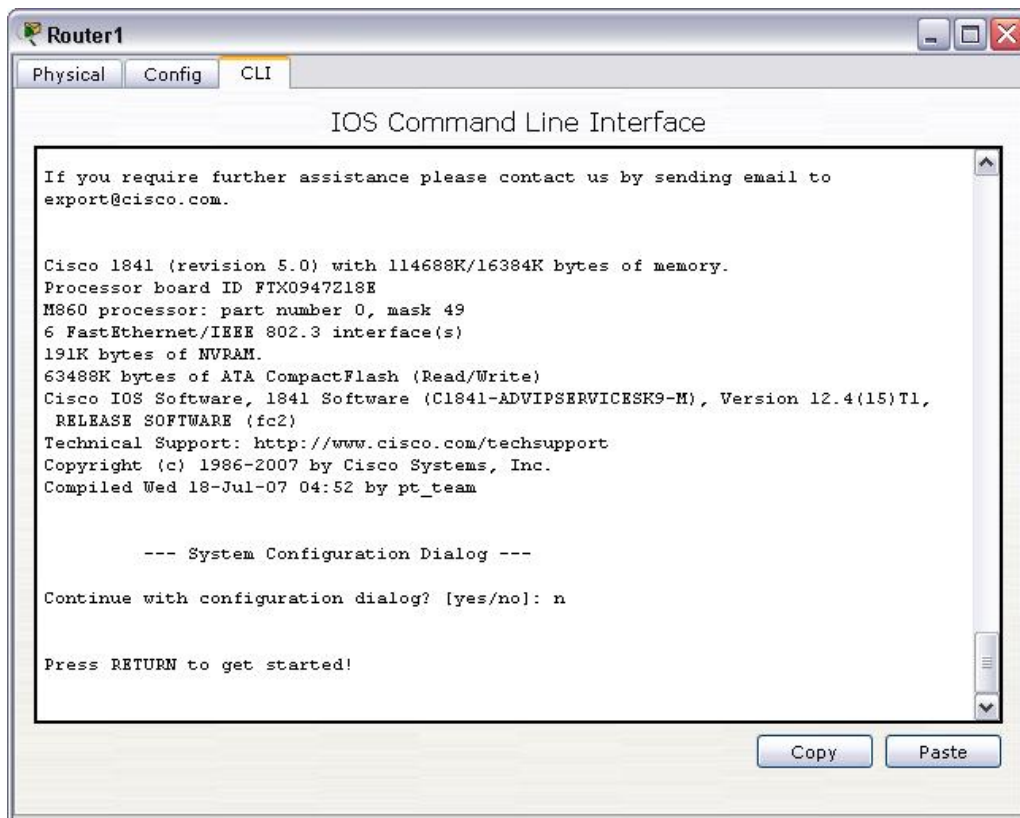


Рис. 8.7. Консоль маршрутизатора

### Додавання комутатора в проект

Процес додавання комутатора в проект мережі полягає спочатку у виборі на панелі типів пристроїв піктограми **Switches**, а після цього на панелі кінцевих пристроїв моделі комутатора. Додавання комутатора в робочу область відбувається натисканням лівої кнопки миші у робочій області.

У параметрах комутатора на закладці **Physical** відсутня можливість зміни апаратної конфігурації обладнання, оскільки комутатори доступні в Cisco Packet Tracer не є модульними. Виняток становить спеціальний тип пристроїв **Generic**, який практично не використовується.

Закладка комутатора **Config** містить його налаштування, а закладка **CLI** – доступ до консолі Console0. За замовчуванням пароль на доступ до консолі не встановлений.

### Додавання кінцевих вузлів мережі

Кінцеві вузли мережі додаються у проект мережі аналогічно до інших пристроїв за винятком того, що на панелі типів пристроїв потрібно вибрати піктограму **End devices**, а на панелі кінцевих пристроїв певний кінцевий пристрій (робочу станцію, ноутбук, сервер, принтер, планшет тощо).

Вміст вікна параметрів кінцевих пристроїв залежить від самого пристрою.

Параметри мережевих інтерфейсів для певного кінцевого пристрою встановлюються за допомогою меню **Settings** (рис. 8.8) та меню **FastEthernet** (рис. 8.9) на закладці **Config** відповідного кінцевого пристрою.

Крім того, на закладці **Config** певні пристрої мають додаткове меню **SERVICES** (сервіси), за допомогою якого налаштовується лише необхідна для



тестування базова функціональність, як-от служби HTTP, DHCP, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP.

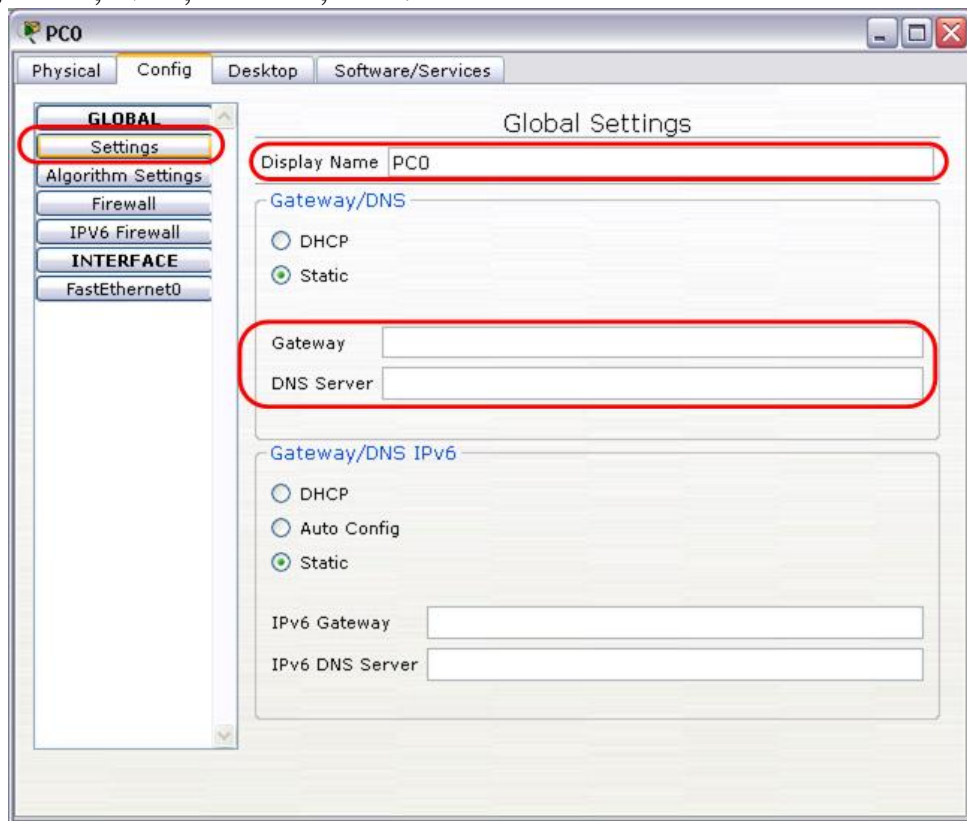


Рис. 8.8. Меню Settings закладки Config робочої станції

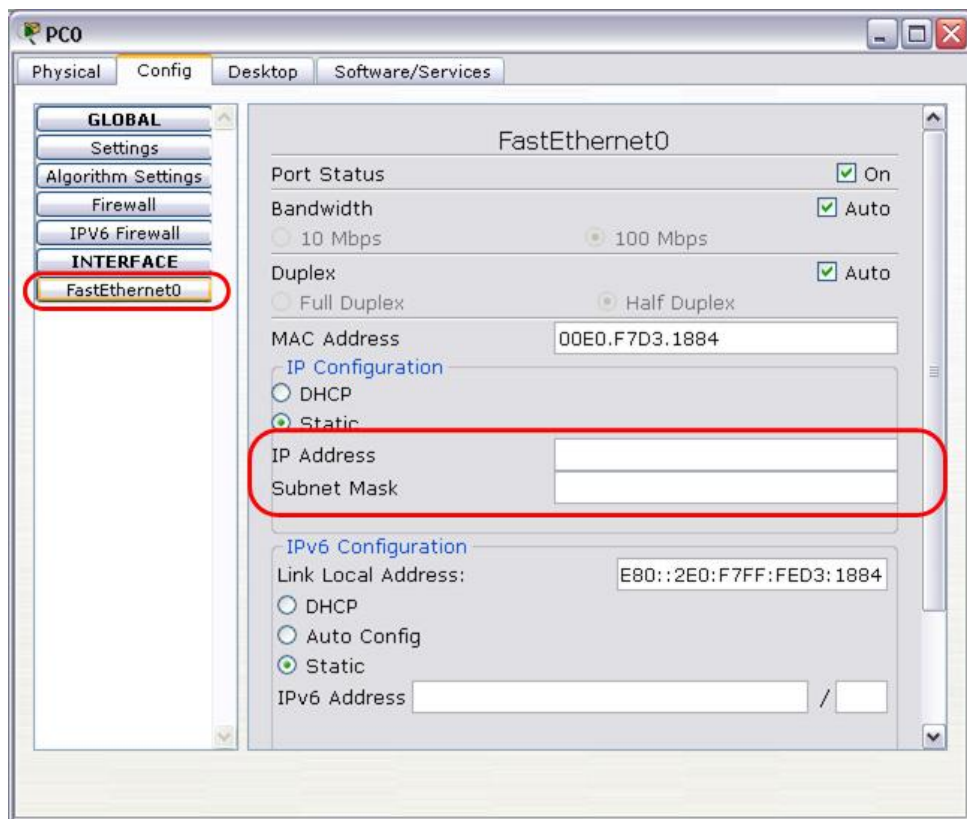


Рис. 8.9. Меню FastEthernet закладки Config робочої станції

Крім того, мережеві налаштування кінцевого пристрою задають у вікні його параметрів, використовуючи пункт **IP Configuration** на закладці **Desktop** (рис. 10). Вміст вікна **IP Configuration** подано на рис. 8.11.



Рис. 8.10. Пункт IP Configuration закладки Desktop робочої станції

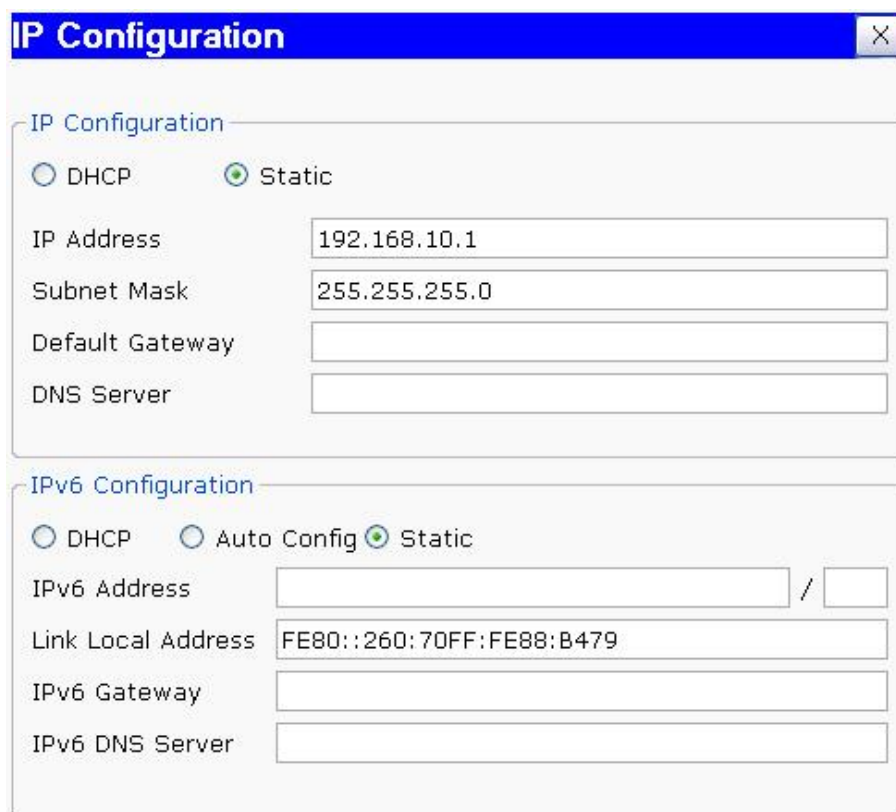


Рис. 8.11 Вікно IP Configuration закладки Desktop робочої станції

### З'єднання пристроїв

Після того, як всі необхідні для роботи пристрої додані у проект, їх потрібно з'єднати. Вибір кабеля з'єднання залежить як від пристроїв, так і від технології з'єднання.

Між пристроями в Cisco Packet Tracer підтримуються такі типи з'єднань

- automatically choose connection type (автоматичний тип);
- console (консоль);
- cooper Straight-Through (мідний кабель з прямим підключенням);
- cooper cross-over (мідний кабель з перехрещенням);
- fiber (волоконно-оптичний кабель);
- phone (телефонна лінія);

- coaxial (коаксіальний кабель);
- serial DCE/DTE (послідовні порти DCE/DTE).

Для з'єднання двох пристроїв, наприклад робочої станції та комутатора, потрібно виконати такі дії:

- 1) на панелі типів пристроїв виділити піктограму **End devices**, після цього на панелі кінцевих пристроїв вибрати, наприклад, робочу станцію **PC-PT** і лівою кнопкою миші вказати місце в робочій області, де потрібно його розмістити;
- 2) на панелі типів пристроїв виділити піктограму **Switches**, після цього на панелі кінцевих пристроїв вибрати, наприклад, комутатор **2960** і лівою кнопкою миші вказати місце в робочій області, де потрібно його розмістити (рис. 8.12 а);
- 3) на панелі типів пристроїв виділити піктограму **Connections**, тоді на панелі кінцевих пристроїв вибрати кабель **Cooper Straight-Through**;
- 4) вибрати **PC-PT** і вказати тип інтерфейса FastEthernet0 (рис. 8.12 б);
- 5) вибрати **2960 switch** і вказати тип інтерфейса FastEthernet0/1 (рис. 8.12 в);
- 6) зачекати поки індикатори обох пристроїв не стануть зеленими (рис. 8.12 г).

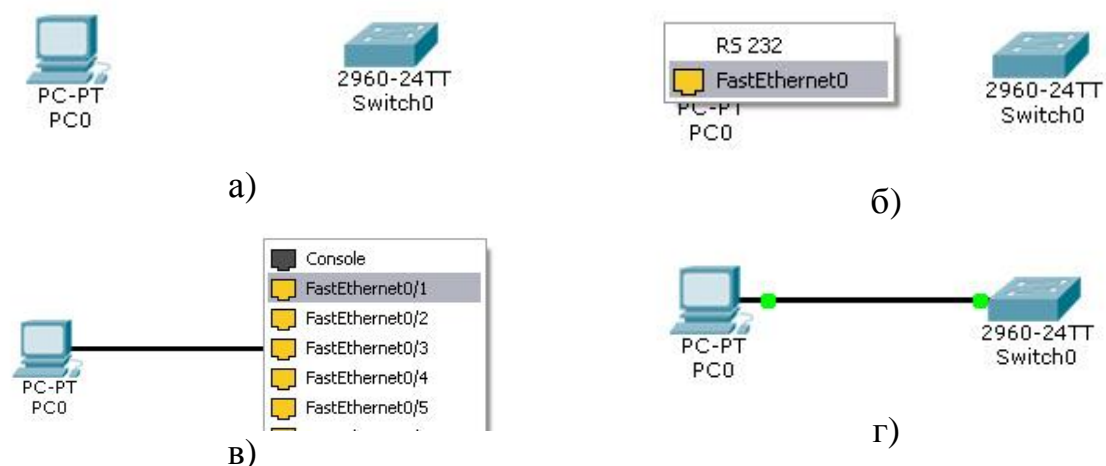




Рис. 8.12. Процес з'єднання робочої станції з комутатором

### Перевірка з'єднання в режимі реального часу

Перед перевіркою з'єднання двох вузлів мережі (джерела та приймача), наприклад двох робочих станцій, що з'єднані з комутатором, джерелу та приймачу потрібно встановити IP-адреси та маску з однієї підмережі. Після цього потрібно переконавшись, що в даний момент часу встановлений режим

**Realtime** (реального часу) ; якщо ні, то встановити його, вибравши відповідну піктограму у правому нижньому куті вікна Cisco Packet Tracer. На панелі інструментів, розміщеній у правій частині вікна, вибрати режим формування простих пакетів для перевірки роботи мережі за допомогою ехо-пакетів, скориставшись піктограмою **Add Simple PDU** . Далі потрібно послідовно вибрати джерело і приймач ring-запиту. Для цього слід навести курсор і натиснути лівою кнопкою миші спочатку на PC0 (джерело ping-

запиту), а потім перемістити курсор на PC1 (приймач ping-запиту) і натиснути лівою кнопкою миші на ньому.

Так як всі мережеві інтерфейси та з'єднання налаштовані правильно (про що свідчать зелені індикатори стану), то ping-запит повинен виконатись успішно. У вікні управління пакетами **User Created Packet Window** з'явиться відповідний запис. Запис **Successful** у полі **Last Status** свідчить про успішне виконання ping-запиту від PC0 до PC1 (рис.8.13).

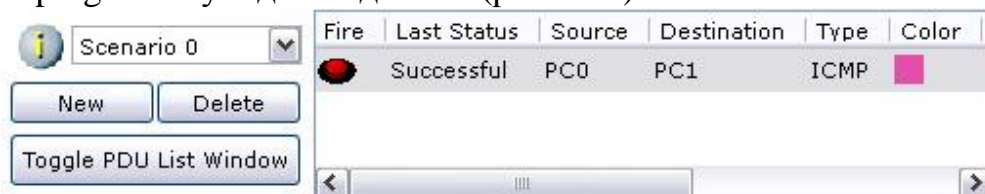


Рис. 8.13. Вікно управління пакетами User Created Packet Window

### Використання командної стрічки

Для переходу в режим командної стрічки потрібно відкрити вікно параметрів кінцевого пристрою, перейти на закладку **Desktop** і вибрати пункт **Command Prompt** (рис. 8.14).

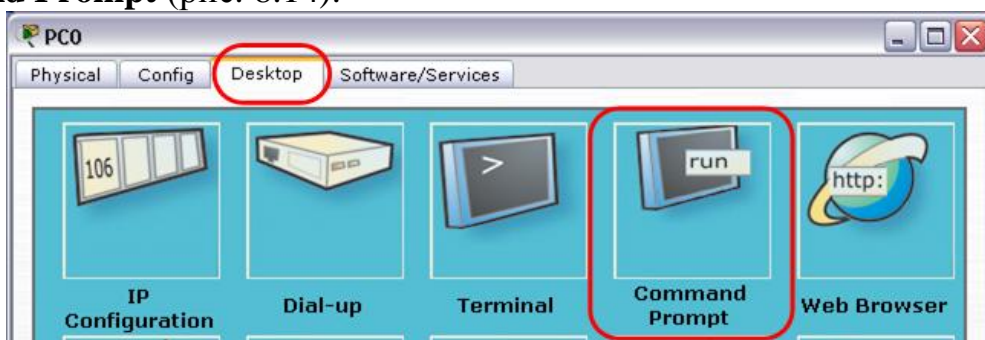


Рис. 8.14. Пункт Command Prompt закладки Desktop робочої станції

На екрані відкриється вікно **Command Prompt** подане на рис. 8.15. У цьому вікні є змога виконувати всі команди, пов'язані з налаштуванням та тестуванням мережі, як і в повноцінній командній стрічці операційної системи.

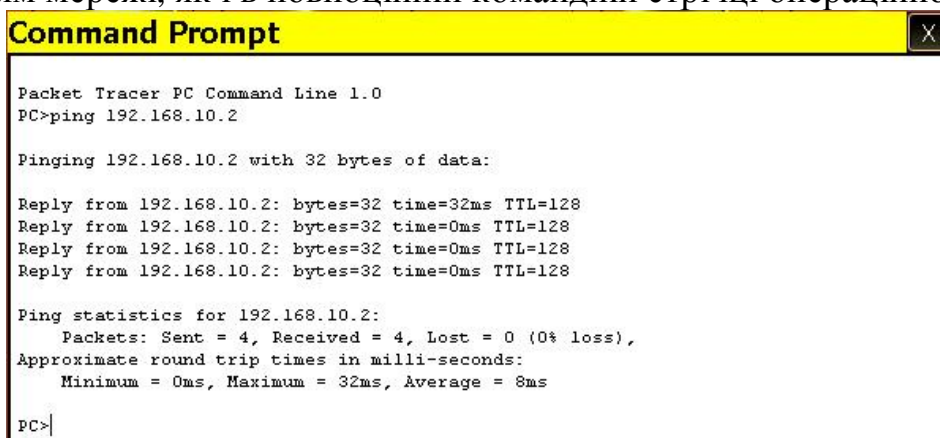


Рис. 8.15. Вікно Command Prompt закладки Desktop робочої станції

### ***Хід роботи***

1. Запустити програму і створити новий проект мережі. Проект назвати згідно такого формату: Lab08-Прізвище-Група-Рік, наприклад, Lab08-Bender-KN31-2015.
2. Додати у проект кінцеві пристрої – декілька робочих станцій, ноутбуків та сервер.
3. Змінити кінцевим пристроям, доданим у п.2, стандартні імена і налаштувати IP-адреси (192.168.YYY.ZZZ, де **YYY** – порядковий номер студента у списку навчальної групи, **ZZZ**=1,2,3,...) та маску (255.255.255.0).
4. Додати у проект комутатор і з'єднати всі пристрої за топологією “зірка”.
5. Використовуючи ехо-пакети, перевірити доступність різних вузлів мережі.
6. Зберегти проект мережі.

### ***Контрольні запитання***

1. Для чого призначена програма Cisco Packet Tracer?
2. З яких основних частин складається вікно Cisco Packet Tracer?
3. Як додати певний пристрій у проект?
4. Як переглянути конфігурацію певного пристрою?
5. Як встановити новий модуль у пристрій?
6. Як задати ім'я пристрою?
7. Як задати IP-адресу та маску пристрою?
8. Які типи зв'язків між пристроями використовуються в Cisco Packet Tracer?
9. Як видалити декілька пристроїв з проекту?
10. Як виконати перевірку з'єднання двох пристроїв в режимі реального часу?

## **Лабораторна робота № 9.**

### **Налаштування з'єднання з комутатором в Cisco Packet Tracer**

**Мета роботи:** ознайомитись з призначенням та роботою комутатора, виконати його налаштування у консольному режимі.

#### ***Теоретичні відомості***

Сьогодні неможливо уявити офіс навіть невеликої компанії, який не має локальної мережі та доступу в Інтернет. Такі пристрої, як комутатори та маршрутизатори широко використовуються не тільки в офісах та операторських мережах, а й домашніми користувачами.

**Мережевий комутатор** (network switch) – це пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

Комутатор працює на канальному рівні моделі OSI, і тому в загальному випадку може тільки з'єднувати вузли однієї мережі за їхніми MAC-адресами.

Комутатор зберігає у пам'яті таблицю MAC-адрес вузлів з прив'язкою до певних портів комутатора. Одразу після включення комутатора ця таблиця є порожньою, а комутатор працює у режимі навчання. У цьому режимі дані, що надходять на будь-який порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри й, визначивши MAC-адресу хоста-відправника, записує її у таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, записаний у таблиці. Якщо MAC-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси (порти). Згодом комутатор побудує повну таблицю для всіх своїх портів, і як результат трафік локалізується.

Існує дві категорії комутаторів: некеровані та керовані.

**Некеровані комутатори** (Unmanaged Switches) використовуються для розгортання мереж невеликих робочих груп або домашніх мереж (SOHO, Small-Office-Home-Office). Також їх можна використовувати на рівні доступу мереж малих підприємств. Ці комутатори прості у встановленні та підтримують, в залежності від моделі, такі функції, як Green Ethernet, діагностика кабелю, керування потоком (IEEE 802.3x), автоматичне визначення полярності кабелю (MDI/MDIX), можливість передачі Jumbo-фреймів та пріоритезацію трафіку.

Некеровані комутатори не підтримують функції керування та оновлення програмного забезпечення.

**Керовані комутатори** (Managed Switches) у порівнянні з некерованими є складними пристроями, які підтримують розширений набір функцій 2 та 3 рівнів моделі OSI. Ці пристрої надають великий вибір інтерфейсів, мають високошвидкісну внутрішню магістраль, змогу встановлення додаткових модулів та з'єднання у фізичний стек. Керувати комутаторами можна за допомогою WEB-інтерфейсу або з командного рядка (CLI), використовуючи протоколи SNMP, Telnet/SSH тощо.



## Підключення до комутатора через консоль

У робочій області Cisco Packet Tracer розмістити комп'ютер і комутатор (серія 2960). Використовуючи консольний кабель, з'єднати комп'ютер через порт RS-232 та комутатор через порт Консоль (рис. 9.1).



Рис. 9.1. Проект мережі

Далі потрібно зайти в налаштування комп'ютера, перейти на закладку **Desktop** і вибрати пункт **Terminal**. На екрані монітора відобразиться вікно **Terminal Configuration** (рис. 9.2), в якому вказуються параметри порта термінального з'єднання. Значення цих параметрів потрібно залишити без змін і натиснути кнопку **ОК**. Після цього відкриється вікно **Terminal** (рис. 9.3), призначене для налаштування комутатора.

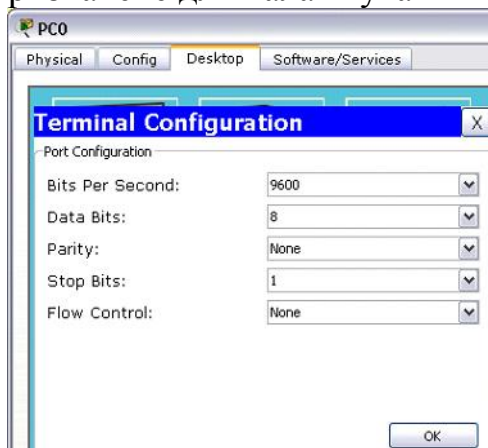


Рис. 9.2. Вікно Terminal Configuration

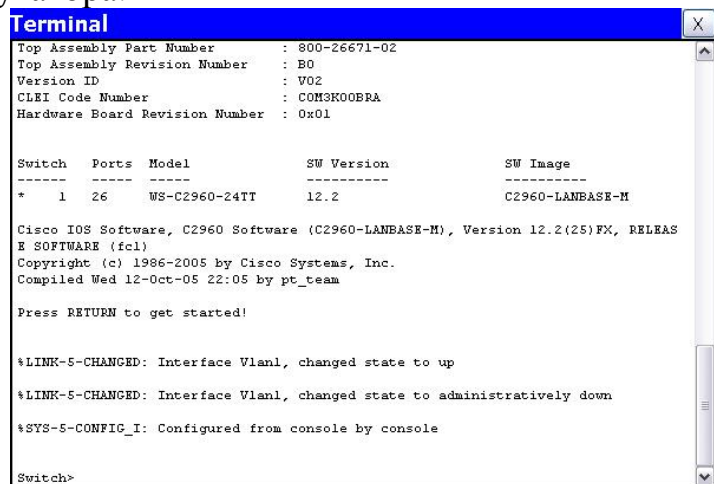


Рис. 9.3. Вікно Terminal

Для перегляду доступних команд у командному рядку потрібно виконати команду `Switch>?` (знак запитання). Для переходу у привілейований режим потрібно виконати команду `Switch>enable`

Про перебування у привілейованому режимі свідчить символ # (решітка), записаний після слова `switch` (`Switch#`), а символ > (`Switch>`) – про використання режиму користувача. Поділ на режими використовується для забезпечення безпеки.

Повернення з привілейованого режиму у користувацький виконується за допомогою команди `Switch#disable` або `Switch#exit`. Для виходу одразу з усіх режимів можна виконати команду `end`

Для перегляду налаштувань комутатора потрібно виконати команду `Switch#show running-config` або `Switch#show run`

Перед тим, як почати налаштування комутатора, потрібно перейти у режим глобальних налаштувань, виконавши команду `Switch#configure terminal` або `Switch#conf t`

Для перегляду всіх параметрів певної команди потрібно записати так:

`<команда> ?`

Наприклад, для перегляду параметрів команди `show` потрібно виконати:

`Switch#show ?`

### **Встановлення паролю на привілейований режим**

Для забезпечення безпеки потрібно задати пароль доступу у привілейований режим. Команда, яка дає змогу встановити цей пароль має такий формат:

`Switch(config)#enable password <пароль>`

Якщо пароль доступу у привілейований режим встановлено, то його потрібно захистити (зашифрувати), оскільки він зберігається у відкритому вигляді. Для цього спочатку потрібно виконати команду `Switch(config)#service password-encryption`, а потім команду `Switch(config)#enable secret <пароль>`

Перевага між паролями, встановленими за допомогою цих команд, надається останньому. Тобто для входу у привілейований режим потрібно вводити пароль, заданий за допомогою такої команди:

`Switch(config)#enable secret`

### **Створення користувача**

Для створення користувача у локальній базі даних використовується команда, яка має такий формат:

`Switch(config)#username <користувач> privilege <рівень> password <пароль>`  
де `<користувач>` – ім'я нового користувача, `<рівень>` – рівень привілеїв користувача, що належить діапазону `[0;15]`; тобто користувач з 15 рівнем привілеїв має найбільші права; `<пароль>` – пароль користувача.

### **Встановлення авторизації на з'єднання через консоль**

Для налаштування авторизації через консоль у режимі налаштування термінальних ліній (`Switch(config-line)#`) потрібно виконати команду `line console <номер>`, де `<номер>` – номер консолі, переважно 0; наявні номери консолей можна переглянути за допомогою команди

`Switch(config-line)#line console ?`

Встановлення режиму авторизації з локальної бази даних виконується такою командою:

`Switch(config-line)#login local`

де `local` – локальна база даних.

### **Встановлення IP-адреси комутатора**

З привілейованого режиму перегляд наявних фізичних (FastEthernet, GigabitEthernet) та логічних (Vlan) інтерфейсів комутатора виконується командою `Switch#show run`. За замовчуванням всі порти комутатора включені у `Vlan1`.

З режиму глобальних налаштувань потрібно перейти у режим налаштування інтерфейсів за допомогою такої команди:



```
Switch(config-if)#interface Vlan1.
```

Встановлення IP-адреси комутатору виконується такою командою:

```
Switch(config-if)#ip address <IP-адреса> <маска>
```

де <IP-адреса> – це IP-адреса, яка задається комутатору, наприклад, 192.168.0.1, а <маска> – маска підмережі, наприклад, 255.255.255.0.

Для того, щоб переконатися чи інтерфейс комутатора включений, виконаємо команду `Switch(config-if)#no shutdown`. Після цього на екрані має з'явитися повідомлення приблизно такого вмісту «Interface Vlan1, changed state to up», яке свідчить про успішне підняття інтерфейсу.

### **Встановлення типу віддаленого з'єднання та увімкнення авторизації**

Для налаштування віртуального терміналу потрібно зайти у режим налаштування термінальних ліній, використавши команду `Switch(config-line)#line vty 0 4`, де `vtu` – віртуальний термінал, 0 – номер початкової лінії, 4 – номер кінцевої лінії.

Після цього потрібно визначити транспортний протокол для лінії, наприклад, `telnet`. Для цього виконуємо таку команду:

```
Switch(config-line)#transport input telnet
```

Для встановлення режиму авторизації з локальної бази даних виконаємо команду `Switch(config-line)#login local`

Виходимо з режиму налаштувань командою `end` і зберігаємо налаштування командою `Switch#write memory` або `Switch#wr mem`

### **Перевірка налаштувань комутатора**

Щоб перевірити IP-адресу комутатора, потрібно з'єднати комп'ютер із комутатором скрученою парою, встановити комп'ютеру IP-адресу з того ж діапазону IP-адрес, що й IP-адреса комутатора, і за допомогою `ping`-запитів перевірити встановлене з'єднання.

Для перевірки віддаленого з'єднання за протоколом `telnet`, потрібно для віддаленого комп'ютера відкрити вікно командної стрічки і ввести таку команду:

```
telnet <IP-адреса комутатора>
```

Після чого має з'явитися запит імені та паролю користувача. Ввівши правильні дані, стає доступним відповідний режим налаштування комутатора.

### ***Хід роботи***

1. Запустити програму Cisco Packet Tracer і створити новий проект мережі. Проект назвати згідно такого формату: Lab09-Прізвище-Група-Рік, наприклад, Lab09-Bender-KN31-2015.
2. Додати у проект 4 робочі станції та комутатор, з'єднати комп'ютери з комутатором скрученою парою.
3. Для комп'ютерів налаштувати IP-адреси (192.168.YYY.ZZZ, де **YYY** – порядковий номер студента у списку навчальної групи, **ZZZ**=1,2,3,...) та маску (255.255.255.0).

4. Один із комп'ютерів з'єднати з комутатором ще й консольним кабелем. Підключитись до комутатора через консоль.
5. Встановити власний пароль на привілейований режим.
6. Створити власного користувача.
7. Встановити авторизацію на з'єднання через консоль.
8. Встановити IP-адресу комутатора (IP-адреса комутатора має бути з того ж діапазону IP-адрес, що й комп'ютери).
9. Встановити віддалене з'єднання по telnet та увімкнути віддалену авторизацію.
10. Перевірити доступність комутатора для будь-якого вузла мережі (за допомогою ping-запиту).
11. Перевірити з'єднання з комутатором на основі протоколу telnet.
12. Зберегти проект мережі.

### ***Контрольні запитання***

1. Яке призначення мережевого комутатора?
2. В якому вигляді комутатори зберігають записи про MAC-адреси та порти?
3. Які основні відмінності між керованими та некерованими комутаторами?
4. Які є способи доступу до налаштувань комутатора?
5. Які є режими налаштування комутатора?

## Лабораторна робота № 10.

### Налаштування віртуальних мереж в Cisco Packet Tracer

**Мета роботи:** ознайомитись з призначенням віртуальних мереж комутатора, навчитися налаштовувати інтерфейси VLAN комутатора.

#### *Теоретичні відомості*

**VLAN** (Virtual Local Area Network) – це логічно об'єднана група хостів, що характеризується загальним набором певних вимог, і яка взаємодіє таким чином, що хости бачать один одного незалежно від їхнього фізичного місцезнаходження так, немов би вони були підключені до окремого широкоповіщального домену. Іншими словами Vlan дає змогу з'єднати комп'ютери в одну мережу на канальному рівні навіть, якщо вони фізично з'єднані з різними комутаторами.

До основних переваг Vlan належать структурування мережі, забезпечення безпеки, об'єднання вузлів на канальному рівні моделі OSI та зменшення широкоповіщального трафіку.

За замовчуванням всі порти комутатора належать Vlan1, тобто одному широкоповіщальному домену. **Широкоповіщальний домен** – це сегмент, усередині якого передаються широкоповіщальні кадри. **Широкоповіщальні кадри** – це кадри, що передаються у всю мережу даного сегмента, тобто у кожний порт комутатора. Ці кадри необхідні для роботи багатьох протоколів, зокрема, DHCP.

Створення декількох Vlan в комутаторі означає розбиття комутатора на декілька широкоповіщальних доменів. Крім того, Vlan дає змогу ізолювати трафік певної групи вузлів від решти мережі, тобто трафік одного Vlan закритий від іншого Vlan.

Налаштовувати Vlan можна лише у керованих комутаторах, з'єднавшись з ними через консоль чи віддалено (telnet, SSH), або ж через Веб-інтерфейс.

У кожній віртуальній мережі є свій ідентифікатор Vlan ID або VID, який використовується у стандарті 802.1Q. Стандартний для мережевих пристроїв діапазон значень Vlan ID – від 0 до 4095. При цьому, переважно, значення VID 0 і 4095 використовувати не можна, так як вони зарезервовані для інших завдань. Для обладнання Cisco розрізняють дві групи Vlan – normal-range (звичайний) і extended-range (розширений). У стандартний діапазон входять Vlan – від 1 до 1005, а в розширений – від 1006 до 4094. При цьому треба враховувати, що VID 1002–1005 зарезервовані для Token Ring і FDDI Vlan.

Для сполучення кінцевих пристроїв з комутатором та одного комутатора з іншим використовуються різні види портів. У комутаторів є два види портів: Access Port – для підключення кінцевих пристроїв та Trunc Port – для з'єднання між комутаторами.

#### **Налаштування VLAN в одному комутаторі**

Створюємо в Cisco Packet Tracer новий проект мережі. У робочу область переносимо 4 комп'ютери і комутатор (серія 2960). З'єднуємо кожний комп'ютер з комутатором, використовуючи скручену пару.

Перші два комп'ютери з'єднаємо у Vlan2, а інші два – у Vlan3 (рис. 10.1), оскільки за замовчуванням всі порти комутатора належать Vlan1.

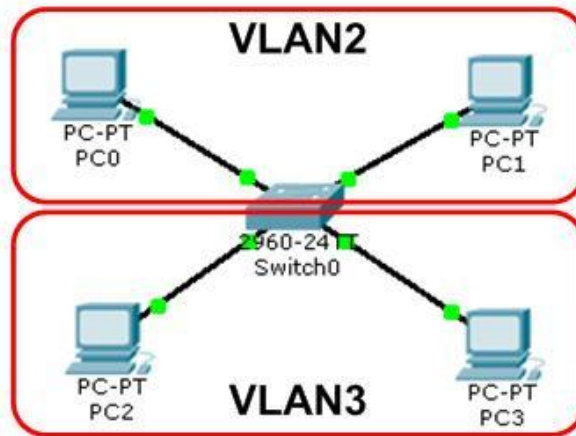


Рис. 10.1. Проект мережі з одним комутатором

Відкриваємо налаштування комутатора і переходимо на закладку **CLI**. Заходимо спочатку у привілейований режим: `Switch>enable`, а потім у режим глобальних налаштувань: `Switch#conf t`

Перед тим, як розмістити комп'ютери в нових віртуальних сегментах, ці сегменти потрібно створити. Формат команди створення нового Vlan такий:

```
Switch(config)#vlan <номер>
```

де <номер> – номер нового Vlan, наприклад, 2.

Після цього відбудеться перехід у режим налаштування Vlan, який має вигляд `Switch(config-vlan)#`, в якому потрібно визначити назву цього Vlan.

Назва Vlan задається командою `Switch(config-vlan)#name <назва>`

де <назва> – назва нового Vlan, наприклад, staff.

Виходимо з режиму налаштування Vlan `Switch(config-vlan)#exit`

Щоб визначити номер порту комутатора, до якого підключений певний комп'ютер, наводимо курсор мишки на з'єднання цього комп'ютера з комутатором, тоді біля комутатора відобразиться підказка про використаний у цьому з'єднанні номер порту.

Визначаємо таким чином порти комутатора, до яких підключені перші два комп'ютери, наприклад, вони підключені до 1 та 2 портів.

Налаштування певного інтерфейсу комутатора виконується командою:

```
Switch(config)#interface fastEthernet <порт>
```

де <порт> – номер порту комутатора, наприклад 0/1 та 0/2.

Визначимо цей порт як Access-порт:

```
Switch(config-if)#switchport mode access
```

і визначаємо його у цей же Vlan:

```
Switch(config-if)#switchport access vlan <номер>
```

де <номер> – номер Vlan, наприклад, 2.

Виходимо з режиму налаштування інтерфейсу `Switch(config-if)#exit`

Аналогічні дії виконуємо з другим комп'ютером для введення його у Vlan2.

Щоб переглянути всі налаштування Vlan, у привілейованому режимі виконуємо команду Switch#show vlan. На екрані відобразиться інформація про наявні віртуальні сегменти та порти, що їм належать.

Виконаємо аналогічні дії щодо розміщення інших двох комп'ютерів у Vlan3, яку назвемо asp.

Для перегляду основних відомостей про віртуальні сегменти у привілейованому режимі скористаємось командою Switch#show vlan brief, результат якої подано на рис. 10.2.

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
2 staff	active	Fa0/1, Fa0/2
3 asp	active	Fa0/3, Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Рис. 10.2. Різні VLAN в одному комутаторі

Для перевірки роботи Vlan усім комп'ютерам мережі потрібно встановити IP-адреси з одного діапазону, наприклад, 192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4. Тоді за допомогою ping-запитів перевірити з'єднання між комп'ютерами спільної та різних Vlan. Якщо налаштування Vlan правильне, то комп'ютери одного Vlan будуть бачити один одного, але не будуть бачити комп'ютери іншого Vlan.

### Налаштування VLAN у двох комутаторах

Щоб спростити завдання, відкриваємо проект мережі з одним комутатором і зберігаємо цей проект з новою назвою. Виділяємо 4 комп'ютери та комутатор, копіюємо та вставляємо копію у проект. Таким чином в робочій області є 8 комп'ютерів і 2 комутатори (серія 2960). З'єднуємо комутатори перехресною скрученою парою через порти GigabitEthernet (рис. 10.3).

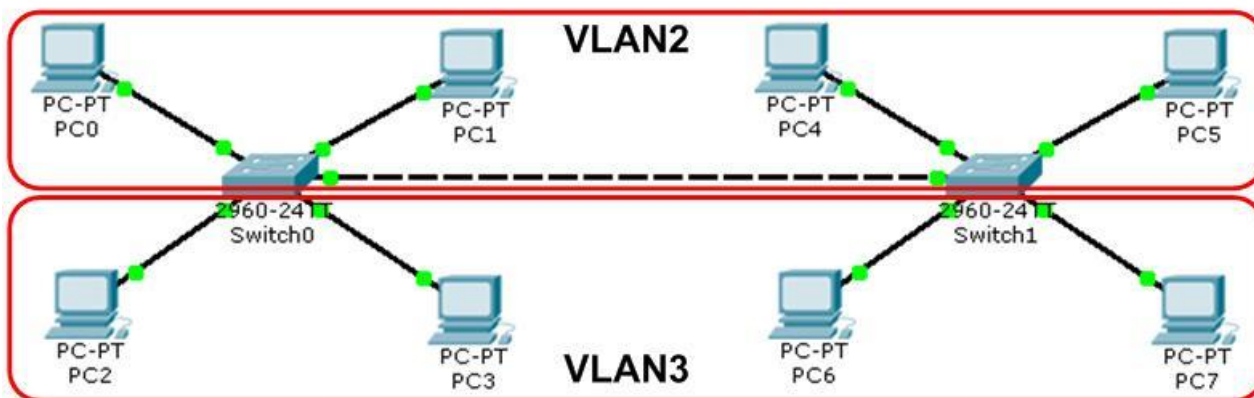


Рис. 10.3. Проект мережі з двома комутаторами

Оскільки перші 4 комп'ютери і комутатор вже налаштовані, то їхня копія буде мати ті ж налаштування. Єдине, що треба змінити, то це IP-адреси нових комп'ютерів, але так, щоб вони належали даному діапазону IP-адрес.

Переглянемо налаштування другого комутатора за допомогою команди `Switch#show run`

На екрані відобразиться інформація про налаштування портів, тобто який порт якому Vlan належить і в якому режимі використовується.

Отже, комп'ютери PC0, PC1, PC4 та PC5 з'єднані у vlan2, а комп'ютери PC2, PC3, PC6 та PC7 – у vlan3 (рис. 10.3).

Після цього потрібно налаштувати порти, що з'єднують комутатори.

Відкриваємо налаштування першого комутатора і переходимо на закладку **CLI**. Заходимо у режим налаштування коммутатора і виконуємо команду:

```
Switch(config)#interface gigabitEthernet <порт>
```

де <порт> – номер порту комутатора, наприклад 1/1. Оскільки комутатори з'єднані через порти GigabitEthernet, тому ці порти й налаштовуються.

Вказуємо режим використання цього порту:

```
Switch(config-if)#switchport mode trunk
```

І вказуємо які Vlan потрібно передавати через фізичне з'єднання певного комутатора

```
Switch(config-if)#switchport trunk allowed vlan <номери Vlan,  
записані через кому>
```

де <номери Vlan, записані через кому> – номер Vlan комутатора, наприклад 2, 3.

Зберігаємо налаштування комутатора командою `Switch#wr mem`

Аналогічні дії виконуємо для відповідного порта другого комутатора.

За допомогою ping-запитів перевірити з'єднання між комп'ютерами спільної та різних Vlan. Якщо налаштування Vlan правильне, то комп'ютери одного Vlan будуть бачити один одного, але не будуть бачити комп'ютери іншого Vlan.

### ***Хід роботи***

1. Запустити програму Cisco Packet Tracer і створити новий проект мережі. Проект назвати згідно такого формату: Lab10-Прізвище-Група-Рік, наприклад, Lab10-Bender-KN31-2015.
2. Додати у проект 4 робочі станції (PC0, PC1, PC2, PC3) та комутатор, комп'ютери з комутатором з'єднати скрученою парою.
3. Для комп'ютерів налаштувати IP-адреси (192.168.YYY.ZZZ, де **YYY** – порядковий номер студента у списку навчальної групи, **ZZZ**=1,2,3,...) та маску (255.255.255.0).
4. Створити Vlan2, Vlan3 та Vlan4.
5. У Vlan2 включити комп'ютери PC0 та PC2, у Vlan3 – комп'ютер PC1, а у Vlan4 – комп'ютер PC3.
6. За допомогою ping-запиту перевірити коректність налаштувань всіх Vlan.
7. Виділити всі комп'ютери та комутатор, скопіювати і вставити копії в робочу область проекту.

8. Для копій комп'ютерів змінити імена на PC4, PC5, PC6, PC7 відповідно, а також змінити їхні IP-адреси (продовжити IP-адресацію).
9. Комутатори з'єднати перехресною скрученою парою через порти GigabitEthernet.
10. Налаштувати комутатори для передавання всіх Vlan через відповідні фізичні з'єднання.
11. За допомогою ping-запиту перевірити коректність налаштувань всіх Vlan.
12. Зберегти проект мережі.

### ***Контрольні запитання***

1. Що таке VLAN?
2. На якому рівні OSI працює VLAN?
3. Які комутатори дають змогу налаштовувати VLAN?
4. Скільки VLAN можна створити на одному комутаторі?
5. Які групи Vlan розрізняють на обладнанні Cisco?
6. Які види портів має керований комутатор?
7. Які з ідентифікаторів Vlan ID зарезервовані для Token Ring та FDDI Vlan?

## Список використаних джерел

1. Ришковець Ю. В. Комп'ютерні мережі : лабораторний практикум [для студентів напряму підготовки 6.050101 “Комп'ютерні науки”] / Ю. В. Ришковець. – Дрогобич : Редакційно-видавничий відділ Дрогобицького державного педагогічного університету імені Івана Франка, 2012. – 88 с.
2. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповнене вид. – Л. : Бак, 2003. – 584 с.
3. Гук М. Аппаратные средства локальных сетей. Энциклопедия. – СПб. : Питер, 2002. – 576 с.
4. Оглтри Т. Модернизация и ремонт сетей. 2-е изд.: пер. с англ. – М. : Издательский дом “Вильямс”, 2001. – 928 с.
5. Cisco Systems и др. Руководство по технологиям объединенных сетей, 3-е изд. : пер. с англ. – М. : Издательский дом “Вильямс”, 2002. – 1040 с.
6. Камер Д. Компьютерные сети и Internet. Разработка приложений для Internet. – М.–СПб.–К. : Вильямс, 2002. – 640 с.
7. Столлингс В. Беспроводные линии связи и сети : пер. с англ. – М.–СПб.–К. : Издательский дом “Вильямс”, 2003. – 640 с.
8. Валецька Т.М. Комп'ютерні мережі. Апаратні засоби. – К. : Центр навчальної літератури, 2004. – 208 с.
9. Дебра Литтлджон Шиндер. Основы компьютерных сетей. – М.–СПб.–К. : Вильямс, 2002. – 656 с.
10. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. 2-е издание. – М.–СПб.–К. : Вильямс, 2001. – 368 с.
11. Хелеби С, Мак-Ферсон Д. Принципы маршрутизации в Internet. – М.–СПб.–К. : Вильямс, 2001. – 448 с.
12. Вито А. Основы организации сетей Cisco. Том 1. Том 2. – М.–СПб.–К. : Вильямс, 2002. – 464 с.
13. Microsoft TCP/IP: Учебный курс. 2-е издание. – М. : Русская редакция, 1999. – 344 с.
14. Палмер М., Синклер Р. Проектирование и внедрение компьютерных сетей. Учебный курс. – СПб. : БХВ-Петербург, 2004. – 756 с.



НАВЧАЛЬНЕ ВИДАННЯ

**КОМП'ЮТЕРНІ МЕРЕЖІ**

**МЕТОДИЧНІ ВКАЗІВКИ**

до виконання лабораторних робіт  
з дисципліни “Комп’ютерні мережі”  
для студентів напряму підготовки 6.050101 “Комп’ютерні науки”

*Укладачі:* Ришковець Юрій Володимирович  
Буров Євген Вікторович

*Редактор:*

*Комп’ютерне верстання:*