

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

**МЕТОДИЧНІ ВКАЗІВКИ**

до лабораторних робіт з навчальної дисципліни  
*“Комп’ютерні мережі”*

для студентів III року навчання денної та заочної форми навчання  
спеціальності 122 «Комп’ютерні науки»

**ЗАТВЕРДЖЕНО**

на засіданні групи забезпечення спеціальності  
протокол № \_\_\_\_ від «\_\_» \_\_\_\_\_ 2022 р.

Голова групи \_\_\_\_\_ Кузніченко С.Д.

**ЗАТВЕРДЖЕНО**

на засіданні кафедри інформаційних технологій  
протокол № \_\_\_\_ від «\_\_» \_\_\_\_\_ 2022 р.

Завідувач кафедри \_\_\_\_\_ Казакова Н.Ф.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

**МЕТОДИЧНІ ВКАЗІВКИ**

до лабораторних робіт з навчальної дисципліни  
*“Комп’ютерні мережі”*

для студентів III року навчання денної та заочної форми навчання  
спеціальності 122 «Комп’ютерні науки»

**ЗАТВЕРДЖЕНО**

на засіданні групи забезпечення спеціальності  
протокол № \_\_\_\_ від «\_\_» \_\_\_\_\_ 2022 р.

Одеса – 2022

Методичні вказівки до виконання лабораторних робіт студентів з дисципліни “Комп’ютерні мережі” для студентів III року навчання денної та заочної форми навчання за спеціальністю 122 «Комп’ютерні науки», рівень вищої освіти бакалавр /Кузніченко С.Д., к.г.н., доц., Клепатська В.В., асистент – Одеса, ОДЕКУ, 2022. – 122 с.

## ЗМІСТ

ВСТУП.....	5
ЛАБОРАТОРНА РОБОТА № 1 Логічна організація комп'ютерних мереж. Робота з мережними утилітами.....	7
ЛАБОРАТОРНА РОБОТА № 2 Устаткування локальних мереж. Знайомство з програмним емулятором Cisco Packet Tracer.....	30
ЛАБОРАТОРНА РОБОТА №3 Налаштування VLAN на комутаторах фірми Cisco .....	64
ЛАБОРАТОРНА РОБОТА № 4 Конфігурування маршрутизаторів Cisco .....	85
ЛАБОРАТОРНА РОБОТА № 5 З'єднання з мережевими пристроями Cisco. Статична маршрутизація.....	100

## ВСТУП

Методичні вказівки призначені для студентів III року навчання денної та заочної форми навчання. Мета виконання лабораторних робіт – закріплення теоретичного лекційного матеріалу та придбання практичних навичок у використанні мережного емулятора Cisco Packet Tracer 5.3.2 на базі устаткування компанії Cisco System, стандартних мережних утиліт ОС Windows, та розрахунків пропускної здатності і конфігурації локальних мереж. Для досягнення поставленої мети розглянуті основні принципи, методи та можливості технологій комп'ютерних мереж, до яких в першу чергу відносяться: топології мереж, методи фізичної та логічної структуризації за допомогою мережного комунікаційного обладнання, особливості адресації вузлів у мережі, багаторівнева система передачі даних, протоколи комп'ютерних мереж та ін. Методичні вказівки містять приклади конфігурування віртуальних машин мережевого устаткування (маршрутизаторів) компанії Cisco та приклади розрахунку конфігурації локальної мережі Ethernet, які можуть служити базою при виконанні аналогічних завдань лабораторних робіт.

Дисципліна «Комп'ютерні мережі» є однією з основних дисциплін формуючих спеціальність 122 «Комп'ютерні науки», яка розглядає моделі та методи побудови сучасних локальних і глобальних мереж.

Внаслідок вивчення дисципліни студент повинен:

**вміти:** розробляти специфікації комп'ютерного обладнання, засобів зв'язку та обслуговування; тестувати й налагоджувати апаратно-програмні засоби і комплекси систем автоматизації та управління; проводити розрахунки пропускної здатності і конфігурації локальних мереж.

За перший практичний модуль встановлена максимальна оцінка 32 бали. Перший практичний модуль складається з трьох лабораторних робіт, за якими встановлені максимальні оцінки:

- 1 лабораторна робота – 17 балів;

- 2 лабораторна робота – 7 балів;
- 3 лабораторна робота – 8 балів.

За другий практичний модуль встановлена максимальна оцінка 18 балів. Другий практичний модуль складається з двох лабораторних робіт, за якими встановлені максимальні оцінки:

- 4 лабораторна робота – 8 балів;
- 5 лабораторна робота – 10 балів.

Контроль по кожній лабораторній роботі проводиться в формі:

- *усного опитування* при підготовці до кожної лабораторної роботи з метою допуску до її виконання (кількість запитань – до 4, максимальна кількість балів – 4),
- *захисту результатів* лабораторної роботи наведених у звіті до лабораторної роботи (кількість запитань залежить від ходу виконання студентом роботи і якості звіту, максимальна кількість балів: 1 лабораторна робота – 13 балів,  
2 лабораторна робота – 3 бали,  
3 лабораторна робота – 4 бали,  
4 лабораторна робота – 4 бали,  
5 лабораторна робота – 6 балів).

Детальніше критерії оцінювання наведені в силлабусі навчальної дисципліни «Комп'ютерні мережі».

## ЛАБОРАТОРНА РОБОТА № 1

### *Логічна організація комп'ютерних мереж.*

### *Робота з мережними утилітами.*

#### 1. Мета роботи

**Метою лабораторної роботи** є ознайомлення студентів з прийомами роботи із сервісними мережними утилітами для отримання даних про організацію мережі, її ресурси та для управління окремими ресурсами, а також ознайомлення з типами IP-адрес та правилами розрахунку VLSM (маски підмережі змінної довжини).

#### 2. Теоритичні відомості до лабораторної роботи

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Архітектура складеної мережі”, „Адресація в IP-мережах” і „Багаторівнева структура стека TCP/IP. Протокол IP.” Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

##### 2.1 Типи адрес стека TCP/IP

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

- локальні, або апаратні, адреси, які використовуються для адресації вузлів у межах підмережі;
- мережні, або IP-адреси, які використовуються для однозначної ідентифікації вузлів у межах всієї складеної мережі;
- доменні імена, або DNS-імена - символні ідентифікатори вузлів, до яких часто звертаються користувачі.

### 2.1.1 Адресація в протоколі IP. Визначення маски під мережі

IP-адреси використовуються для глобального з'єднання всіх вузлів і мереж в середині Інтернет. Кожному ПК підключеному до мережі необхідно присвоїти IP-адресу. Можливий також варіант під'єднання певної кількості ПК до мережі Інтернет без власного IP-адреса. Суть цих методів полягає у використанні проксі служб та трансляції мережних адрес.

**Класи IP-адрес.** Адресація (IPv4) припускає використання 32-бітного коду. IP-адресу прийнято записувати у вигляді чотирьох октетів (4 байт), у десятковій системі числення, наприклад:

IP-адреса **192.168.4. 25** – це код **11000000 10101000 00000100 00011001**.

Кожне із значень, розділених точками – це 8-ми бітове число, яке може приймати значення від 0 до 255.

Будь-яка IP-адреса складається із двох частин: адреси мережі (*net*) та адреси хоста (*host*). Тут можна провести деяку аналогію з міжміськими телефонними номерами, у яких перші числа вказують на місто, де розміщується абонент, а інших – безпосередньо на самого абонента.

Для виділення з IP-адреси адреси мережі та адреси хоста (вузла) використовується мережева маска (*net mask*) – бітовий шаблон, в якому бітам, що використовуються для адреси мережі, присвоюються значення 1, а бітам адреси хоста – значення 0. Здійснюється це з використанням побітової логічної операції «І» (табл.2.1).

Таблиця 2.1 – Застосування маски

Біт маски	Біт адреси	Біт результату
0	0	0
0	1	0
1	0	0
1	1	1



Наприклад, маска мережі **255.255. 255.0** (**11111111 11111111 11111111 00000000**) визначає, що поле адреси мережі містить 24 біта, а поле адреси хоста – 8 біт. Для наведеного вище прикладу адреси це означає: **192.168.4** – мережна частина (адресу мережі прийнято записувати **192.168.4. 0**), а **25** – адреса хоста в цій мережі.

$$192.168.4.25_{10} = 11000000\ 10101000\ 00000100\ 00011001_2$$

$$\underline{255.255.255.0_{10} = 11111111\ 11111111\ 11111111\ 00000000_2}$$

$$192.168.4.0_{10} = 11000000\ 10101000\ 00000100\ 00000000_2$$

IP-адреса може належати до одного із класів. В залежності від класу адреса може містити різну кількість біт під адресу мережі та різну кількість біт під адресу для хоста. Перший байт (октет) вказує на приналежність IP - адреси до певного класу. Існує 5 класів IP-адрес (рис.2.1).

У таблиці 2.2 наведені діапазони номерів мереж, що відповідають кожному класу мереж. Адреси класу D використовуються для багатоадресної передачі даних. Перший октет в них може містити значення від 224 до 239. В групових адресах поняття адреси мережі відсутнє. Призначення даних адрес полягає у обміні даними з декількома вузлами при використанні однієї адреси одержувача пакетів. Для того, щоби такий обмін міг відбутися, потрібно об'єднати ці вузли у групу та присвоїти їй групову IP-адресу.

Клас А	0	Номер мережі		Номер вузла		
Клас В	1	0	Номер мережі		Номер вузла	
Клас С	1	1	0	Номер мережі		Номер вузла
Клас D	1	1	1	0	Адреса групи multicast	
Клас Е	1	1	1	1	0	Зарезервований

Рисунок 2.1 – Структура різних класів IP-адрес

Таблиця 2.2 – Характеристики адрес різного класу

Клас	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів у мережі	Маска
A	1.0.0.0	126.255.255.255	$2^{24}-2$	255.0. 0.0
B	128.0.0.0	191.255.255.255	$2^{16}-2$	255. 255.0.0
C	192.0.0.0	223.255.255.255	$2^8-2$	255. 255.255.0
D	224.0.0.0	239.255.255.255	групова адресація	
E	240.0.0.0	247.255.255.255	зарезервовано	

**Особливі IP-адреси.** У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес (див. табл.2.3):

- якщо IP-адреса складається тільки із двійкових нулів, то вона позначає адресу того вузла, що згенерував цей пакет. Це спеціальна адреса що вказує на станцію, яка завантажується і яка не знає власного IP адреса. Дана адреса не може бути вказана в пакеті інформації в полі адреси отримувача;

- якщо в полі номера мережі стоять 0, то за замовчуванням вважається, що цей вузол належить тій же самій мережі, що й вузол, який відправив пакет;

- якщо всі двійкові розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, які перебувають у тій же мережі, що й джерело цього пакета. Таке розсилання називається обмеженим широкомовним повідомленням (*limited broadcast*);

- якщо в полі адреси хоста стоять всі 1, то пакет, що має таку адресу розсилається всім вузлам мережі із заданим номером. Таке розсилання називається широкомовним повідомленням (*broadcast*). Приклад визначення широкомовної адреси для IP-адреси 192.168.4.25 з маскою 255.255.255.0

$$192.168.4.25_{10} = 11000000\ 10101000\ 00000100\ 00011001_2$$

$$! \underline{255.255.255.0}_{10} = \underline{00000000\ 00000000\ 00000000\ 11111111}_2$$

$$192.168.4.0_{10} = 11000000 10101000 00000100 1111111_2$$

– адреса 127.0.0.1 зарезервована для організації зворотного зв'язку при тестуванні роботи програмного забезпечення вузла без реального відправлення пакета по мережі. Ця адреса має назву *loopback*.

Форма групової IP-адреси – *multicast* – означає, що даний пакет повинен бути доставлений одразу декільком вузлам, які складають групу з номером, зазначеним у полі адреси. Вузли самі ідентифікують себе, тобто визначають, до якій із груп вони ставляться. Той самий вузол може входити в кілька груп. Такі повідомлення на відміну від ширококомовних називаються мультимовним.

Приватні діапазони адрес – використовуються в закритих мережах різного розміру. Використання даних адрес в мережі Інтернет – заборонено.

Таблиця 2.3 – Службові IP-адреси

Адреси	Призначення
0.0.0.0	Обмежена адреса відправника
255.255.255.255	Обмежена ширококомовна адреса
X.X.X.255	Мережева (чи підмережева) ширококомовна адреса
127.X.X.X, де $0 \leq X \leq 255$	Зарезервовано для програмного інтерфейсу loopback (lo)
10.0.0.0/8 172.16.0.0./12 192.168.0.0/16	Діапазони приватних (білих) IP адрес

З ростом мережі Інтернет необхідність у додаткових IP-адресах зростає. Вже зараз тієї кількості IP-адрес, яка закладена в IP версії 4 не вистачає. Тому був розроблений протоколу IP версії 6.

Даний протокол має довжину не 32, а 128 бітів. Записується він у вигляді восьми шістнадцятирозрядних шістнадцяткових чисел, які розділені між собою двокрапками. Приклад:

1. 2100:0:0:0:4D:31AC:12:45
2. 0:0:0:0:0:0:0:1
3. AA0C:0:0:0:36:0:0:1

4. CDCE:0:0:0:FA:0:0:0

5. 3FA:2:17:1EF2:AD:CB:200:11

IP-адреса версії 6 складається з двох частин: адреси мережі, адреси хоста.

**Використання підмереж (*subnetting*).** Як вже згадувалося вище маска мережі визначає ту частину IP-адреси, яка відноситься до адреси мережі. Маску мережі можна змінювати, змінюючи таким чином, число октетів IP-адреси які відносяться до адреси мережі. На рис. 2.1 зображено мережу з адресою 10.0.0.0 та маскою 255.0.0.0. Дана мережа складається з певної кількості вузлів, кожен з яких фізично належить мережі 10.0.0.0 та формально об'єднаний з певними ПК (кожне об'єднання характеризується видом діяльності робочих станцій, які входять в групу). Мережа складається формально з трьох груп (відділ продажу, маркетингу та технічна група). Обмін даними здійснюється інтенсивно в межах групи і практично не здійснюється між групами. Тим не менше, всі ці групи підключені до єдиної мережі. Ріст числа вузлів такої мережі приводить до погіршення характеристик самої мережі (збільшується кількість колізій). Крім цього, інколи виникають проблеми безпеки при передачі даних в межах групи, оскільки всі ПК підключені до спільної шини.

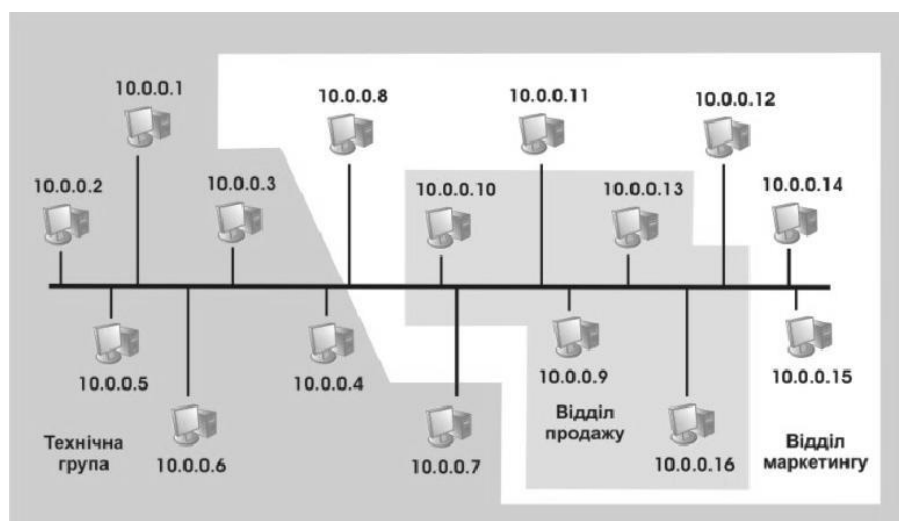


Рисунок 2.1 – Мережа, яку необхідно розділити на підмережі для

## покращення її характеристик

Для вирішення вище описаних проблем необхідно розбити мережу на окремі підмережі. Всі підмережі, що утворяться об'єднати маршрутизатором. Маршрутизатор необхідний для того щоби забезпечити обмін інформацією між підмережами. Також необхідно буде змінити маску підмереж. На рис. 2.1 зображено мережу, всі вузли якої використовують IP-адреси мережі 10.0.0.0 з маскою 255.0.0.0. Для розбиття мережі на декілька частин необхідно змінити маску. Таким чином ми отримуємо 2 октети для ідентифікації підмережі. Перший з октетів змінювати не можна. Другий октет буде ідентифікувати власне підмережу. Маска для кожної з підмереж буде мати вигляд 255.255.0.0. Відділ маркетингу матиме адресу 10.3.0.0, відділ продажу – 10.2.0.0, технічна група – 10.1.0.0 (рис.2.2).

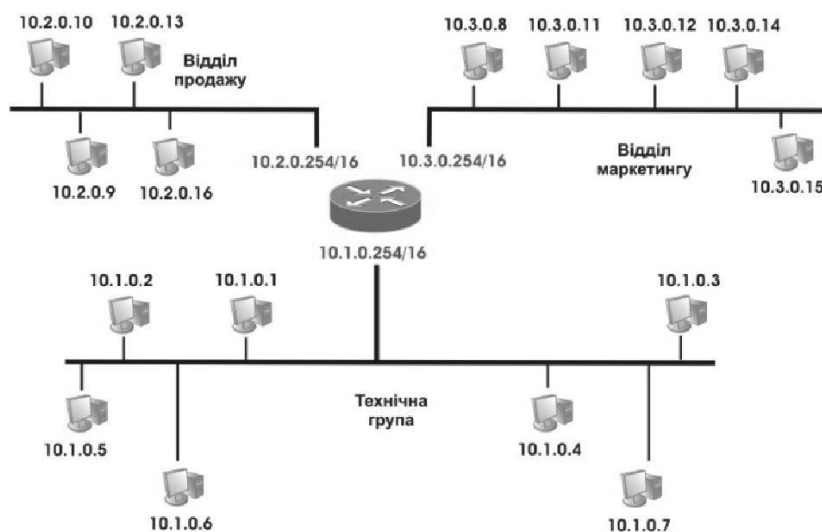


Рисунок 2.2 – Розбиття мережі на підмережі

Вище описаний приклад поділу мережі на окремі підмережі справедливий для адрес мереж класів А та В. Якщо необхідно поділити мережу класу С на підмережі, використовують маску підмережі змінної довжини (VLSM).

Розглянемо приклад поділу мережі на підмережі за допомогою розрахунку маски змінної довжини. Для виділення підмереж у мережі

адміністраторові необхідно визначити кількість сегментів і кількість вузлів у кожному сегменті з урахуванням потреб мережі. Наприклад, якщо необхідно розбити мережу 192.168.8. 0 (блок містить 256 адрес) на 6 підмереж з максимальною кількістю вузлів 30 у кожній підмережі, те по-перше, потрібно визначити кількість біт у полі адреси підмережі (3 біти тому що  $2^3=8$ ) і в полі адреси вузла (5 біт тому що  $2^5=32$ ). Максимальна кількість вузлів у підмережі дорівнює 30-ти, а не 32, тому що коди, що містять всі одиниці і всі нулі, не можуть бути адресою вузла. Визначивши поля адреси підмережі і вузла, запишемо маску підмережі:

11111111 11111111 11111111 11100000 – 255.255. 255. 224.

Таблиця 2.4 – Адреси підмереж, отримані в результаті застосування маски підмережі

Адреса мережі	Широкомовний адрес	Адреси хостів
<b>192. 168.8.0</b>	192. 168.8.31	від 192.168.8.1 до 192.168.8.30
<b>192. 168.8.32</b>	192. 168.8.63	від 192.168.8.33 до 192.168.8.62
<b>192. 168.8.64</b>	192. 168.8.95	від 192.168.8.65 до 192.168.8.94
<b>192. 168.8.96</b>	192. 168.8.127	від 192.168.8.97 до 192.168.8.126
<b>192. 168.8. 128</b>	192. 168.8. 159	від 192.168.8.129 до 192.168.8.158
<b>192. 168.8. 160</b>	192. 168.8. 191	від 192.168.8.161 до 192.168.8.190
<b>192. 168.8. 192</b>	192. 168.8. 223	від 192.168.8.193 до 192.168.8.222
<b>192. 168.8. 224</b>	192. 168.8. 255	від 192.168.8.225 до 192.168.8.254

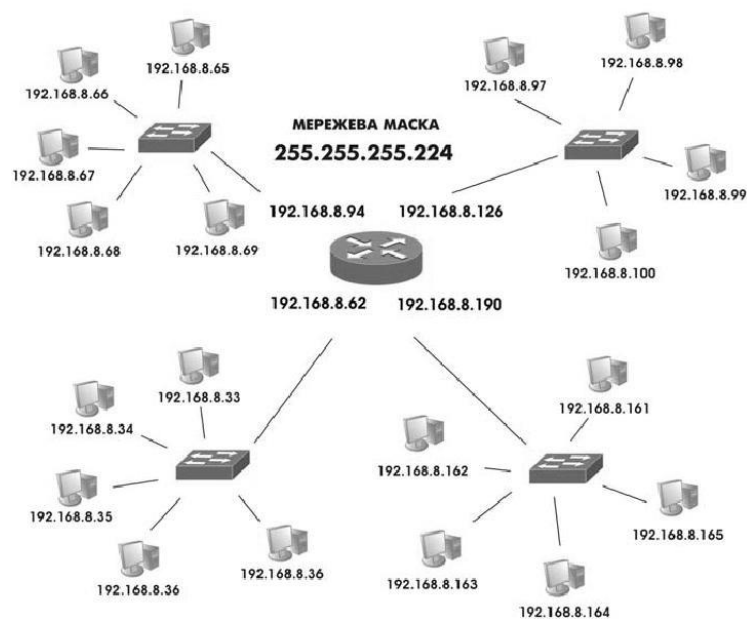


Рисунок 2.3 – Схема мережі 192.168.8.0/24

**Призначення IP-адрес.** IP-адреса призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів, при цьому номер мережі може бути обраний адміністратором довільно, або призначений організацією ICANN. Для отримання власної IP-адреси, необхідно звернутися до Інтернет-провайдера, або на сайт організації ICANN <http://www.icann.org>.

У великих мережах підтримується автоматичний розподіл адрес на основі протоколу *Dynamic Host Configuration Protocol (DHCP)*. Протокол DHCP працює відповідно до моделі клієнт-сервер. Комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на одержання IP-адреси. DHCP-сервер відгукується і посилає повідомлення відповідь, що містить IP-адресу з діапазону вільних для розподілу адрес. Передбачається, що DHCP-клієнт і DHCP-сервер перебувають в одній IP-мережі.

### 2.1.2 Протоколи перетворення адрес

**Фізична адреса.** Фізична, або апаратна адреса вузла, визначається технологією, за допомогою якої побудована мережа, до якої входить даний вузол. Для вузлів, що входять у локальні мережі - це MAC-адреса мережевого адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками устаткування і є унікальними адресами, тому що управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байтів: старші 3 байти - ідентифікатор фірми виробника, а молодші 3 байти призначаються унікальним чином самим виробником.

1 біт	1 біт	22 біта	24 біта
I/G	U/L		

## Рисунок 2.4 - Структура MAC-адреси

Крайній лівий біт числа називається ознакою *індивідуальної* або *групової* адреси (I/G). Якщо біт дорівнює 0, то інші біти визначають індивідуальну адресу; значення 1 вказує на те, що інші біти визначають групову адресу. Якщо другий біт (U/L) дорівнює 0, то адреса підмережі є *універсальною*, тобто призначеною комітетом IEEE, у противному випадку адреса є *локальною*.

**Протокол ARP.** Щоб відправити дейтаграму з одного комп'ютера на інший у локальній або глобальній мережі, відправник повинен знати фізичну адресу одержувача. Повинен існувати механізм перетворення IP-адрес, які задаються додатками, у фізичні адреси устаткування, що з'єднують комп'ютери з мережею. Для рішення цієї проблеми був розроблений протокол перетворення адрес **ARP (Address Resolution Protocol)**. ARP веде таблицю відповідності між IP-адресами і фізичними адресами, яка називається *таблицею ARP*. Крім того, ARP підтримує кеш записів - *кеш ARP*.

Алгоритм роботи протоколу ARP:

1. Звичайно пошук починається з кеша ARP, і тільки у випадку невдачі дані шукаються в таблиці ARP. Записи кеша ARP, які були динамічно згенеровані, стають недійсними при закінченні інтервалу тайм-ауту, тоді як на статичні записи тайм-аут не повинен поширюватися. Знищення статичних записів у результаті тайм-ауту є ознакою псування даних у кеші ARP.

2. Якщо в записах таблиці необхідна IP-адреса не знайдена, то вихідний IP-пакет запам'ятовується в буфері, а протокол ARP формує запит (ARP запит), вкладає його в кадр протоколу канального рівня і розсилає ширококомовно.

3. Всі інтерфейси підмережі одержують ARP-запити і порівнюють зазначену там адресу з власною. При збігу вузол чи маршрутизатор формує ARP -відповідь, указуючи в ньому свої IP і MAC адреси та відправляє його по IP-адресі вузла відправника ARP-запиту.



Структура ARP-запита наведена на рис. 2.5. Поле «Тип протоколу» дозволяє використовувати протокол ARP не тільки для протоколу IP, але й для інших мережевих протоколів. У полі коду операції для ARP-запитів вказується значення 1, якщо це запит, і 2, якщо це відповідь.

Тип мережі (16 біт)	
Тип протоколу (16 біт)	
Довжина апаратної адреси	Довжина мережевої адреси
Код операції (16 біт)	
Апаратна адреса відправника	
IP-адреса відправника	
Апаратна адреса одержувача	
IP-адреса одержувача	

Рисунок 2.5 – Структура запитів і відповідей ARP

4. Якщо в мережі немає машини із шуканою IP-адресою, то ARP-відповіді не буде. Протокол IP знищує IP-пакети, спрямовані по цій адресі.

5. Якщо відповідність знайдена, то вона записується в ARP-таблицю відповідного інтерфейсу. Новий запис в ARP-таблиці з'являється автоматично, через декілька мілісекунд після того, як модуль ARP проаналізував ARP-відповідь. Крім динамічних записів, побудованих на підставі даних ширококомовних розсилянь, ARP-таблиці можуть містити статичні записи, які створюються вручну за допомогою утиліти `arp` і не мають строку старіння по тайм-ауту.

Нижче наведений синтаксис команди `arp`.

```
ARP -s inet_addr eth_addr [if_addr]
```

```
ARP -d inet_addr [if_addr]
```

```
ARP -a [inet_addr] [-N if_addr]
```

`-a`                      Відображає поточні ARP-записи, опитуючи поточні дані протоколу. Якщо задано `inet_addr`, то будуть

відображені IP і фізична адреса тільки для заданого комп'ютера. Якщо більше одного мережевого інтерфейсу використовують ARP, то будуть відображатися записи для кожної таблиці.

-g                   Теж саме, що й ключ -a.

inet\_addr           Визначає IP-адресу.

-N if\_addr           Визначає ARP-записи для заданого в if\_addr мережевого інтерфейсу.

-d                   Видаляє вузол, що задає inet\_addr. inet\_addr може містити символ шаблону \* для видалення всіх вузлів.

-s                   Додає вузол і зв'язує internet адресу inet\_addr з фізичною адресою eth\_addr. Фізична адреса задається 6 байтами (в шістнадцятиричному вигляді), розділеним дефісом. Цей зв'язок є постійним.

eth\_addr            Визначає фізичну адресу.

if\_addr             Якщо параметр заданий, він визначає інтернет-адресу інтерфейсу, чия таблиця перетворення адрес повинна змінитися. Якщо не заданий, - буде використано перший доступний інтерфейс.

Приклад:

Додати статичний запис

```
> arp -s 157.55.85.212 00-aa-00-62-c6-09
```

Використання із ключем -a дозволяє побачити поточний стан кеша ARP

```
> arp -a
```

**Доменні імена.** Доменне, або символічне ім'я, наприклад, SERV1.IBM.COM – адреса, що призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домена. Така адреса, названа також DNS-ім'ям, використовується на прикладному рівні, наприклад, у протоколах FTP або telnet. Ієрархія доменних імен аналогічна ієрархії імен файлів, однак запис доменного імені починається із наймолодшої складової, а закінчується найстаршою. Наприклад, в імені `partnering.microsoft.com` складова `partnering` є ім'ям одного з комп'ютерів у домені `microsoft.com`. Сукупність імен, у яких кілька старших складових частин збігаються, утворюють домен (domain) імен. Наприклад, імена

www.chip.kiev.ua, www.itc.kiev.ua і www.infocity.kiev.ua входять у домен kiev.ua.

**Файл HOSTS і служба DNS.** Відповідність між доменними іменами і IP-адресами може встановлюватися як засобами локального хосту, так і засобами централізованої служби. У першому випадку, вручну підтримується файл HOSTS, що містить інформацію про те, яка IP-адреса зв'язується з тим або іншим символічним ім'ям. Коли вузлу необхідно знайти інший вузол у мережі, він звертається до локального файлу HOSTS. Синтаксис записів HOSTS можна подивитися у файлі hosts.sam .

У другому випадку використовується спеціальна служба - система доменних імен (Domain Name System, DNS), яка заснована на розподіленій базі відображень «доменне ім'я - IP-адреса». Служба DNS використовує протокол типу «клієнт-сервер». У ньому визначені DNS-сервери і DNS-клієнти, які звертаються до серверів із запитом про дозвіл доменних імен в IP-адресу. Для кожного домена імен створюється свій DNS-сервер. Кожний DNS-сервер крім таблиці відображень імен містить посилання на DNS-сервери своїх піддоменів. Ці посилання зв'язують окремі DNS-сервери в єдину службу DNS.

Мережене програмне забезпечення комп'ютера настроєне таким чином, щоб воно переглядало локальний файл HOSTS перед тим, як звертатися до сервера DNS, тому що вибірка інформації з файлу відбувається набагато швидше, ніж пошук засобами DNS.

**Дозвіл імен в NetBIOS.** Для спілкування в мережах з вузлами, керованими ОС Windows, вживаються імена комп'ютерів, які визначаються по системі NetBIOS. Варто пам'ятати, що це не теж саме, що DNS імена хостів в IP-мережах.

Ім'я NetBIOS привласнюється комп'ютеру при установці операційної системи, але може бути змінено пізніше. Воно повинне бути унікальним у межах мережі. Щоб визначити ім'я комп'ютера потрібно викликати діалогове вікно «Мережа», клацнувши правою кнопкою миші на значку «Мережеве

оточення» і вибравши в контекстному меню команду «Властивість» і вкладку «Ідентифікація». Ім'я хоста настраюється у властивостях протоколу TCP/IP. За замовчуванням ім'я хоста збігається з ім'ям комп'ютера в NetBIOS, тому що це полегшує процес діагностики.

В операційних системах Microsoft використовуються наступні способи перетворення імен NetBIOS в IP-адреси:

- **Кеш імен.** Щоб переглянути вміст кеша імен, введіть команду NBTSTAT–с у режимі командного рядка мережевої операційної системи Microsoft, що використовує TCP/IP.

- **Сервер WINS** - підтримує базу даних з інформацією про зв'язки імен комп'ютерів з IP-адресами. Щоб перетворити ім'я комп'ютера в IP-адресу, клієнт звертається до сервера WINS із запитом.

- **Широкомовне розсилання** – клієнти мережі Microsoft можуть розіслати запит у локальному сегменті мережі, щоб довідатися, чи належить дозволене ім'я цьому сегменту.

- **Файл LMHOSTS** – статичний файл, що містить список IP-адрес із відповідними їм іменами комп'ютерів. Синтаксис записів можна подивитися у файлі lmhosts.sam (sample).

Черговість, у якій клієнтська система намагається дозволити ім'я NetBIOS, залежить від типу вузла NetBIOS. Існують чотири типи вузлів NetBIOS:

1. **В-вузол** - широкомовні вузли (Broadcast). Дозвіл імен NetBIOS здійснюється тільки за допомогою розсилання запитів у локальному сегменті. Розширені В-вузли шукають інформацію у файлі LMHOSTS, якщо ім'я не було знайдено в локальному сегменті.

2. **Р-вузол** - дозвіл імен здійснюється крапковим (Point-to-point) звертанням до сервера WINS, широкомовне розсилання в локальному сегменті не використовується.

3. **М-вузол** - змішані (Mixed) системи спочатку розсилають запит у локальному сегменті, а потім звертаються за дозволом імені до сервера WINS.

4. **Н-вузол** - гібридні (Hybrid) системи спочатку звертаються за дозволом імені до сервера WINS. Якщо одержати відповідь не вдається, Н-вузол розсилає запит у локальному сегменті.

Всі клієнти NetBIOS спочатку перевіряють зміст кеша імен. За замовчуванням використовуються типи вузлів В и Н. Розширені В-вузли використовуються за замовчуванням для всіх комп'ютерів, на яких не задана адреса сервера WINS. При наявності адреси сервера WINS за замовчуванням використовується Н-вузол.

## 2.2 Службові файли TCP/IP

Крім файлів HOSTS і LMHOSTS в операційній системі Windows 2000 використовуються ще три файли - NETWORKS, PROTOCOL і SERVICES.

**Файл NETWORKS.** Файл NETWORKS використовується для ідентифікації мереж, що входять в об'єднану мережу (тобто мережа, що складається з декількох мереж, звичайно зв'язаних через маршрутизатори). У файлі зберігається інформація про відповідність між іменами мереж (ідентифікаторами, що представляють дану мережу) і номерами мереж (мережевими частинами IP-адрес цих мереж). Символьне ім'я мережі не може містити пробілів, символів табуляції й знаків # і повинне бути унікальним в межах файлу NETWORKS. Імена мереж, зазначених у файлі NETWORKS, використовуються в конфігураційних утилітах і командах - наприклад, ім'я мережі може вказуватися замість мережевої адреси. Файл NETWORKS звичайно редагується мережевими адміністраторами, щоб замість мережевих адрес, що важко запам'ятовуються, у командах і утилітах використовувалися більш зручні символічні імена.

**Файл PROTOCOL.** Файл PROTOCOL призначений для ідентифікації імен протоколів і відповідних їм номерів. Номер протоколу в сімействі

протоколів Інтернету збігається зі значенням ідентифікатора протоколу в заголовку IP.

Файл PROTOCOL доповнює модуль TCP/IP і містить визначення основних протоколів; не змінюйте його вміст без крайньої потреби.

**Файл SERVICES.** У файлі SERVICES визначаються назви служб і використовувані ними транспортні протоколи й номери портів.

Служби являють собою програми, що працюють на прикладному рівні моделі TCP/IP, - Telnet, FTP, SMTP, SNMP і т.д. Кожна служба працює на базі певного транспортного протоколу (TCP і UDP). Інформація про те, який транспортний протокол використовується тією або іншою службою, зберігається в конфігураційному файлі SERVICES. Деякі служби доступні як через TCP, так і через UDP. У цьому випадку служба представлена у файлі двома записами: для TCP і для UDP.

Файл SERVICES доповнює модуль TCP/IP і містить визначення основних служб TCP/IP; не змінюйте його вміст без крайньої потреби.

### 2.3 Програми командного рядка TCP/IP

**Утиліта hostname.** Виводить ім'я локального комп'ютера (хоста). Вона доступна тільки після установки підтримки протоколу TCP/IP. Приклад виклику команди hostname :

```
C:\>hostname  
ws 327b103
```

**Утиліта ipconfig.** Виводить діагностичну інформацію про конфігурації мережі TCP/IP та дозволяє переглянути поточну конфігурацію IP-адрес комп'ютерів мережі. Синтаксис утиліти ipconfig:

```
ipconfig [/all | /renew [адаптер ] | /release [адаптер ]],
```

де all - виводить відомості про ім'я хоста, DNS (Domain Name Service), тип

вузла, IP-маршрутизації та ін. Без цього параметра команда `ipconfig` виводить

тільки IP-адреси, маску підмережі і основний шлюз;

`/renew [адаптер]` - оновлює параметри конфігурації DHCP. Ця можливість доступна тільки на комп'ютерах, де запущені служби клієнта DHCP. Для завдання адаптера використовується ім'я, виведене командою `ipconfig` без параметрів;

`/release [адаптер]` - очищає поточну конфігурацію DHCP. Ця можливість відключає TCP/IP на локальних комп'ютерах і доступна тільки на клієнтах DHCP. Для завдання адаптера використовується ім'я, виведене командою `ipconfig` без параметрів. Ця команда часто використовується перед переміщенням комп'ютера в іншу мережу. Після використання утиліти `ipconfig/release`, IP-адреса стає доступна для призначення іншому комп'ютеру.

Запущена без параметрів, команда `ipconfig` виводить повну конфігурацію TCP/IP, включаючи IP адреси й маску підмережі.

**Утиліта ping.** Утиліта `ping` (Packet Internet Groper) перевіряє з'єднання з віддаленим комп'ютером або комп'ютерами. Вхідними даними для утиліти `ping` є адреса вузла, маршрут до якого підлягає трасуванню. Адреса вузла задається у вигляді IP-адреси або доменної адреси в командному рядку при запуску утиліти. Запити утиліти `ping` передаються по протоколу ICMP (Internet Control Message Protocol). Одержавши такий запит, програмне забезпечення, що реалізує протокол IP в адресата, негайно посилає луну-відповідь. Луни-запити посилають задану кількість разів (ключ `-n`) або за замовчуванням доти, поки користувач не введе команду переривання (`Ctrl+C` або `Del`), після чого виводяться статистичні дані.

Формат команди:

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

Таблиця 2.5 - Параметри утиліти ping

Ключі	Функції
-t	Відправка пакетів на вказаний вузол до команди переривання. Перегляд статистики та продовження - Control-Break; Закінчення- Control-C.
-a	Визначення адресів по іменам вузлів.
-n	Число відправляємих запитів. За замовчуванням - 4
-l	Розмір буфера відправки. За замовчуванням – 32 байта, максимум – 65527
-f	Установлення прапору, який забороняє фрагментацію пакету.
-i TTL	Задання часу життя пакета(поле "Time To Live").
-v TOS	Задання типу служби(поле "Type Of Service").
-r	Запис маршруту для вказанного числа переходів.
s	Штамп часу для вказанного числа переходів.
-j перелік вузлів	Вільний вибір маршруту по переліку вузлів.
-k перелік вузлів	Жорсткий вибір маршруту по переліку вузлів.
-w інтервал	Інтервал очікування кожної відповіді в мілісекундах
перелік_розсилк и	Список комп'ютерів, яким спрямовуються запити

На практиці більшість опцій у форматі команди можна опустити, тоді в командному рядку може бути: ping ім'я вузла. Зверніть увагу на те, що максимальне значення TTL за замовчуванням приймається рівним 255 вузлів. Отже, щоб визначити кількість вузлів, через які пройшов пакет, треба від 255 відняти отримане значення TTL.

**Утиліта tracert.** Утиліта tracert використовується для визначення маршруту пакета, який прямує до вказаного вузла. Утиліта передає ряд дейтаграм і очікує відповіді на кожну з них. Перед відправленням першої дейтаграми, значення TTL для неї встановлюється в 1. Перший маршрутизатор, що виявиться на шляху проходження цієї дейтаграми, зменшить значення TTL на одиницю та, якщо це значення стане рівним 0, поверне помилку ICMP про закінчення TTL. Оскільки повідомлення ICMP



передається також у вигляді дейтаграми IP, то *tracert* може витягти IP-адресу джерела і вивести на екран адресу маршрутизатора. Для наступної дейтаграми значення TTL буде збільшено на одиницю й т.д., поки не буде отриманий запит від комп'ютера призначення.

Параметри команди наведені нижче:

*tracert* [-d] [-h макс\_число] [-j перелік\_вузлів] [-w інтервал] ім'я

Таблиця 2.6 - Параметри утиліти *tracert*

Ключі	Функції
-d	Без визначення адреси по іменам вузлів. Використовується для відключення визначення dns-імен по IP-адресах маршрутизаторів.
-h макс_число	Максимальне число переходів при пошуку вузла.
-j перелік_вузлів	Вільний вибір маршруту за переліком вузлів.
-w інтервал	Інтервал очікування кожної відповіді в мілісекундах.

### 3. Порядок проведення лабораторної роботи

При проведенні роботи студенти об'єднуються в бригади по дві особи. Для виконання роботи кожен повинен:

1. Відповісти на контрольні питання та пройти усне опитування за теоретичним матеріалом лабораторної роботи, який викладається в п.2;
2. Пройти інструктаж по правилам охорони праці;
3. Отримати варіант завдання у викладача;
4. Запустити комп'ютер, переглянути і занотувати усі функції та параметри програм *ping*, *tracert*, *ipconfig*.
5. Визначити ім'я локального комп'ютера. Вивести інформацію про конфігурації мережі TCP/IP за допомогою утиліти *ipconfig*. Проаналізувати отримані результати. Занотувати результати роботи програми та висновки щодо поточної конфігурації мережі;

6. За допомогою команди ping перевірити стан зв'язку з вузлами, зазначеними викладачем. Переглянути маршрути проходження пакетів до даних вузлів мережі за допомогою утиліти tracert;
7. Переглянути стан ARP-кеша за допомогою утиліти arp;
8. Переглянути вміст службових файлів TCP/IP;
9. Розрахувати кількість підмереж згідно варіанту завдання (табл.2.7) і побудувати логічну топологію мережі.
10. Проаналізувати отримані результати;
11. Підготувати і захистити звіт до лабораторної роботи.

#### **4. Варіанти індивідуальних завдань**

Таблиця 2.7 – Варіанти завдання до лабораторної роботи

Варіант	IP-адреса	Маска	Завдання
1	194.138.33.0	/24	Розбити мережу на 4 підмережі
2	192.168.45.0	/24	Розбити мережу на 4 підмережі
3	82.207.118.0	/24	Розбити мережу на 3 підмережі
4	113.45.25.0	/24	Розбити мережу на 2 підмережі
5	164.34.24.0	/24	Розбити мережу на 6 підмереж
6	155.150.100.0	/24	Розбити мережу на 3 підмережі
7	164.90.34.0	/24	Розбити мережу на 8 підмереж
8	197.230.100.0	/24	Розбити мережу на 10 підмереж
9	87.217.118.0	/24	Розбити мережу на 12 підмереж
10	182.207.120.0	/24	Розбити мережу на 10 підмереж
11	178.18.25.0	/24	Розбити мережу на 8 підмереж
12	112.54.12.0	/24	Розбити мережу на 6 підмереж

#### **5. Контрольні питання**

- 1) Які три типи адреси хоста в мережі TCP/IP ви знаєте?
- 2) Пояснити поняття loopback, broadcast, multicast.

- 3) Що відбудеться при відправленні пакета за адресою 127.0.0.1?
- 4) Яку частку всієї безлічі IP-адрес становлять адреси класу А? Класу В? Класу С?
- 5) Дайте визначення маски підмережі? У яких цілях вона використовується?
- 6) Яким способом може відбуватися дозвіл адрес? Приведіть приклади протоколів дозволу адрес.
- 7) Перелічіть стандартні службові файли TCP/IP. Для чого вони призначені?
- 8) Які функції виконують системні утиліти ping, tracer, ipconfig? Яке призначення має кожний параметр програм?
- 9) Для чого необхідна утиліта hostname?
- 10) Навіщо використовується параметр all в утиліті ipconfig?

## **6. Перелік літератури**

### **Основна література**

1. Кузніченко С.Д. «Комп'ютерні мережі» Конспект лекцій. – Одеса: ОДЕКУ, 2018.– 175 с.
2. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: «Магнолія 2006», 2012.– 262с.
3. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. – К.:Київ ун-т ім. Б.Грінченка, 2011. – 291 с.

### **Додаткова література**

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб.: Питер, 2010. 944 с.: ил.
2. Э. Таненбаум, Д. Уэзеролл Компьютерные сети. 5-е изд. – СПб.: Питер, 2012.– 542 с.
2. Колomoец Г.П. Организация компьютерных сетей: учебное пособие.

3. Кравец, О.Я. Практикум по вычислительным сетям и телекоммуникациям : учебное пособие / О. Я. Кравец. – Изд. 2-е, перераб. и доп. – Воронеж: Научная книга, 2006. – 156 с.

4. Новиков Ю.В. Основы локальных сетей: курс лекций : учеб. пособие: для студентов вузов, обучающихся по специальностям в обл. информ. технологий . М.: Интернет-ун-

5. Смирнова Е.В., Пролетарский А.В., И.В. Баскаков, Р.А. Федотов Построение коммутируемых компьютерных сетей: учебное пособие / Е.В. Смирнова и др. – М.: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. – 367 с.: ил.

## **7. Правила техніки безпеки та охорони праці**

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

## **8. Оформлення і захист звіту**

Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Титульна сторінка :
  - Найменування лабораторної роботи.
  - Відомості про виконавця, номер варіанту.
2. Мета роботи та завдання до лабораторної роботи.
3. Перелік функцій та параметрів утиліт ping, tracert, ipconfig з поясненнями, які виводяться довідковою підсистемою.
4. Результати (скріншоти) запуску всіх зазначених у завданні утиліт у мережі (повідомлення утиліт при їх роботі як з усіма окремими параметрами так і з усіма припустимими комбінаціями параметрів).

5. Вміст ARP-кэша і службових файлів TCP/IP.
6. Таблиця розрахунку кількості підмереж згідно варіанту завдання (табл.2.7).
7. Висновки за результатами роботи.
8. Контрольні питання та відповіді на них.

## ЛАБОРАТОРНА РОБОТА № 2

### *Устаткування локальних мереж.*

#### *Знайомство з програмним емулятором Cisco Packet Tracer*

### **1. Мета роботи**

**Метою лабораторної роботи** є здобути практичні навички роботи з мережною операційною системою комутаційного обладнання та маршрутизаторів Cisco IOS.

### **2. Теоретичні відомості до лабораторної роботи**

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Фізична і логічна структуризація мережі за допомогою різних типів комунікаційного обладнання” і „Принципи роботи комутаторів”. Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

#### **2.1 Компоненти устаткування Cisco**

Склад внутрішніх компонентів Cisco в певній мірі залежить від призначення устаткування, потужності блоку живлення, конструкції та складу модулів. Всі устаткування практично завжди мають деякі основні компоненти. Зокрема, будь-який маршрутизатор або комутатор можна розглядати як спеціалізований комп'ютер, в якому аналогічні компоненти можна використовувати для тієї ж мети. Устаткування Cisco можуть включати не тільки внутрішні компоненти, але і зовнішні, склад яких також залежить від моделі устаткування.

**Внутрішні компоненти.** До числа найбільш використовуваних компонентів відносяться модулі оперативної пам'яті (флеш-пам'ять, ПЗП), процесор, об'єднувальна плата и енергонезалежний ОЗП (рис.2.1).

*Оперативна пам'ять.* Моделі DRAM (Dynamic RAM – динамічний ОЗП) застосовуються в устаткуваннях Cisco з тією ж метою, що і в персональному комп'ютері: в якості оперативної пам'яті. Оперативна пам'ять в маршрутизаторах Cisco має наступні характеристики:

- енергозалежна;
  - пересписувана;
  - об'єм від 16 до 512 Мбайт;
- і функції:
- зберігає таблицю маршрутизації (routing table);
  - містить ARP кеш;
  - буферизує пакети;
  - під час роботи маршрутизатора містить файл робочої конфігурації (running-config file).

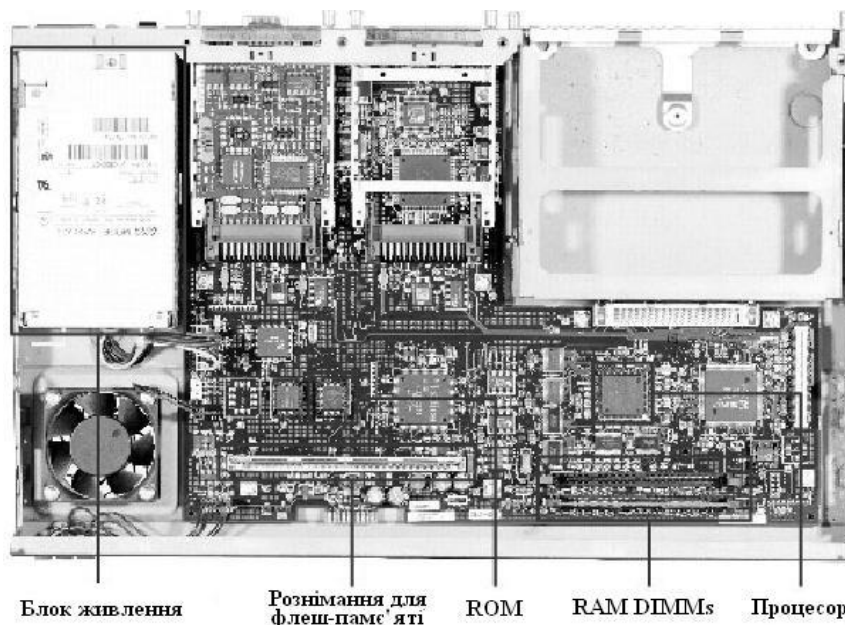


Рисунок 2.1 – Внутрішні компоненти Cisco Router 2600

На маршрутизаторах Cisco виконується високопродуктивна операційна система IOS (Cisco Internetworking Operating System), створена на базі ОС UNIX, яка фізично розміщена в енергонезалежній пам'яті маршрутизатора (FLASH).

*Флеш–пам'ять.* Флеш–пам'ять в маршрутизаторах Cisco використовується приблизно з тією ж метою, що і жорсткий диск на комп'ютері. Флеш–пам'ять має наступні характеристики:

- енергонезалежна;
- пересписувана;
- об'єм від 8 до 128 Мбайт;

і функції:

- зберігає образ або образи Cisco IOS;
- зберігає файли конфігурації.

*Постійний запам'ятовуючий пристрій.* Постійний запам'ятовуючий пристрій призначений тільки для читання. Для переходу на нову версію потрібно замінити мікросхему ПЗП, котрий має наступні характеристики:

- енергонезалежний;
- не пересписуваний;

і функції:

– зберігає спрощену (резервну) версію Cisco IOS, призначену для використання у тому випадку, якщо всі інші способи завантаження устаткування не вдаються;

– містить код функції ROM Monitor, який застосовується у тому випадку, якщо програмне забезпечення Cisco IOS, яке знаходиться на флеш-пам'яті, спотворено і не завантажується. А також він служить для діагностики та перенастроювання конфігурації на низькому рівні (наприклад, в тому випадку, якщо хтось змінив пароль, виключив тим самим доступ мережевого адміністратора до маршрутизатора).

*Енергонезалежний ОЗП.* Енергонезалежний ОЗП (NVRAM) має наступні характеристики:



- енергонезалежний;
- пересписуваний;
- об'єм від 32 до 256 Кбайт;

і функції:

- вказує шлях до образу Cisco IOS і файлу пускової конфігурації;
- зберігає файл пускової конфігурації (startup-config file).

*Процесор.* Процесор в устаткуваннях Cisco служать тієї ж меті, що і в ПК: він є «мозком» устаткування. В більшості устаткування Cisco програмне забезпечення виконує багато обчислень, і для цього використовується процесор. В комутаторах процесор – це не такий важливий елемент, як в маршрутизаторах, тому що загальна частина обчислень виконується комутатором за допомогою спеціалізованих апаратних компонентів, що називаються модулями ASIC.

*Об'єднувальна плата.* Об'єднувальну плату можна порівняти з магістраллю, по якій ідуть всі взаємодії всередині мереженого устаткування. Її продуктивність має велике значення в комутаторах і інших устаткуваннях з високою густиною розміщення інтерфейсів.

**Зовнішні компоненти.** До зовнішніх компонентів відноситься консольний інтерфейс, допоміжний (AUX) інтерфейс, інтерфейси Ethernet, послідовні інтерфейси і слоти PCMCIA (рис.2.2).

*Консольний інтерфейс.* Консольний інтерфейс використовується для введення до системи Cisco IOS первісної інформації про конфігурацію і є окремим розніманням (connector) RJ-45. Консольний інтерфейс – це низькошвидкісний асинхронний послідовний інтерфейс, який має особливе розташування виводів, і встановлює певні вимоги до типу кабелю, який повинен використовуватися для підключення станції керування (рис.2.3). Консольні кабелі зазвичай поставляються разом з маршрутизатором.

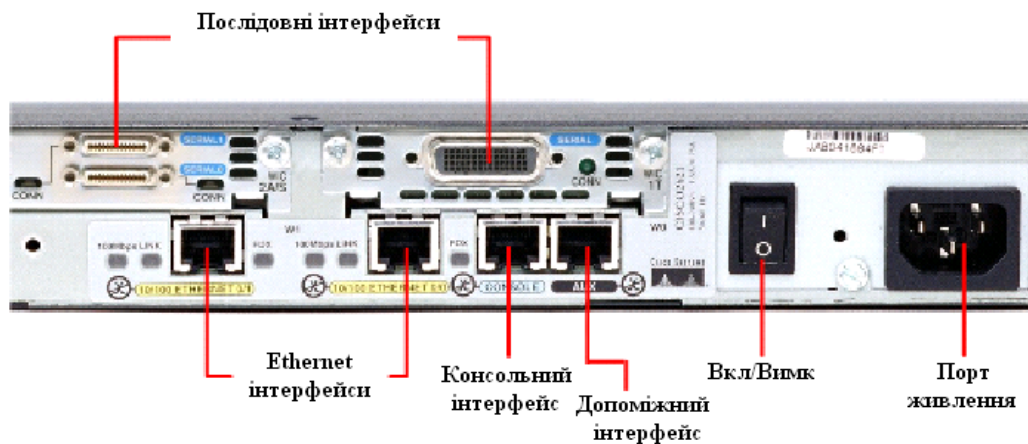


Рисунок 2.2 – Внутрішні компоненти Cisco Router 2600

*Допоміжний інтерфейс.* Допоміжний інтерфейс (AUX) - це ще один низькошвидкісний асинхронний послідовний інтерфейс, який звичайно використовується для підключення модему, що дозволяє здійснювати дистанційне адміністрування.

*Ethernet інтерфейси.* Ethernet інтерфейс – це інтерфейс, який дозволяє підключити дане мережне устаткування к Ethernet мережі.

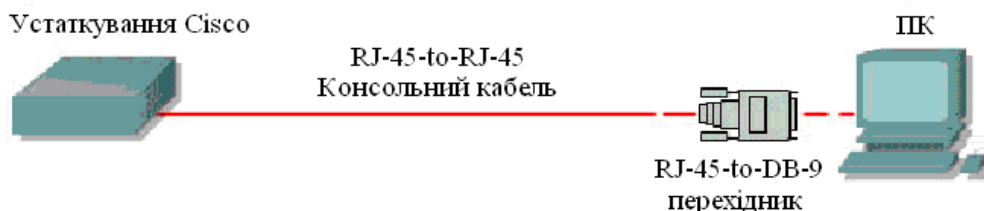


Рисунок 2.3 – Схема підключення до консольного інтерфейсу

*Послідовний інтерфейс.* Існує шість загальних специфікацій послідовного підключення: EIA/TIA-232, X.21, V.35, EIA/TIA-449, EIA-530 і HSSI. Послідовний інтерфейс призначений для підключення DCE<sup>1</sup> і DTE<sup>2</sup> устаткування.

1 DCE – Data Communications Equipment – Апаратура передачі даних. Як правило це модем (модуль даних або модулятор/демодулятор пакетів на боці мережі каналу зв'язку), призначений для забезпечення сумісності двійкових даних, що передаються послідовно від джерела або передавача, з каналом зв'язку.

2 DTE – Data Terminal Equipment – Термінальне устаткування. Апаратура користувача лінії зв'язку, яка виробляє дані для передачі лінією зв'язку и підключається безпосередньо к апаратурі передачі даних DCE. Це, наприклад, комп'ютери, комутатори і маршрутизатори.

## 2.2 Основні відомості про операційну систему Cisco IOS

На маршрутизаторах Cisco виконується високопродуктивна операційна система IOS (Cisco Internetworking Operating System), створена на базі ОС UNIX, яка фізично розміщена в енергонезалежній пам'яті маршрутизатора (FLASH).

Процес ініціалізації маршрутизатора виконується в наступній послідовності:

- POST (Power On Self Test) – тестування обладнання після включення живлення.
- Bootstrap IOS – програма завантаження основного IOS.
- Cisco IOS – основна операційна система маршрутизатора.
- Файл конфігурації із NVRAM. Виконуються команди, які зберігаються в цьому файлі.

Після автоперевірки включення живлення в процесі ініціалізації маршрутизатора відбуваються наступні події (рис.2.5):

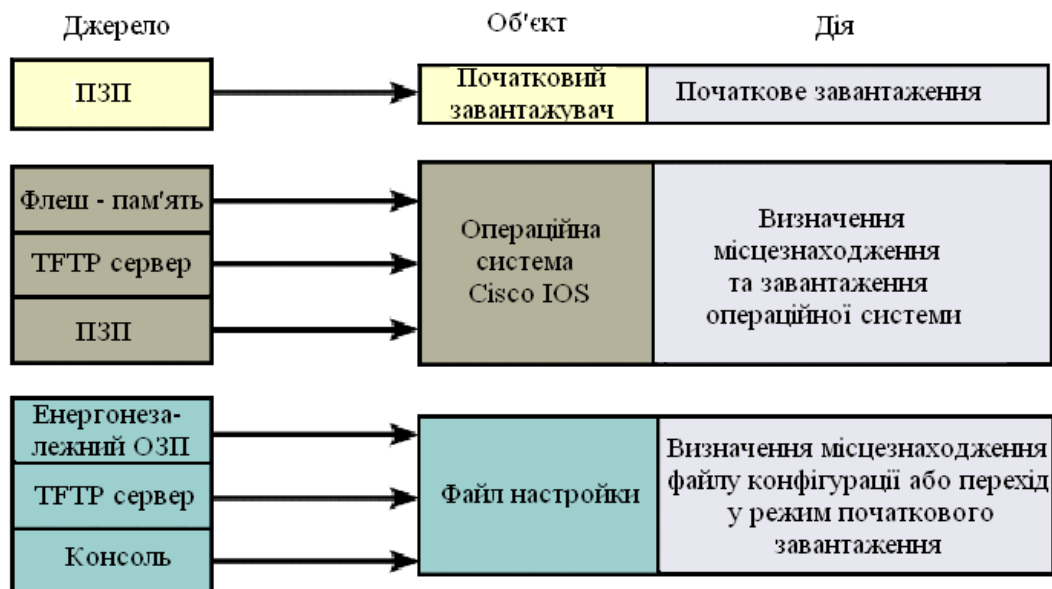


Рисунок 2.5 – Послідовність завантаження Cisco IOS

Підключення до маршрутизатора здійснюється програмою TELNET до IP-адреси будь-якого з його інтерфейсів або при посередництві будь-якої іншої термінальної програми через консольний порт маршрутизатора CON, або додатковий порт AUX. Останньому способу слід надати перевагу, оскільки в процесі конфігурування маршрутизатора можуть змінюватися параметри IP – інтерфейсів, що може призвести до втрати з'єднання через TELNET. Окрім того, з міркувань безпеки доступ до маршрутизатора через TELNET слід заборонити.

Аварійне відключення оператора від консолі не реєструється маршрутизатором і сеанс залишається в тому ж стані. При повторному підключенні оператор опиниться в тому ж самому контексті, з якого відбулося аварійне відключення (якщо не спрацював автоматичний вихід по таймеру неактивності). Навпаки, при втраті TELNET-з'єднання маршрутизатор закриває сеанс роботи оператора.

При першому завантаженні IOS намагається завантажити конфігурацію з глобальної мережі. При невдалому завершенні цієї процедури IOS пропонує здійснити початкове конфігурування маршрутизатора за допомогою програми SETUP. Програма SETUP пропонує встановити деякі основні глобальні параметри конфігурації маршрутизатора шляхом діалогу питання-відповідь. До початкового конфігурування маршрутизатора відносяться наступні дії:

- Завдання імені маршрутизатора (за замовчуванням пропонується “Router”).
- Завдання пароля enable secret.
- Завдання пароля enable password.
- Завдання пароля віртуального терміналу.
- Конфігурування протоколів SNMP, IP, протоколів маршрутизації RIP IGRP.
- Конфігурування інтерфейсів.

Кожен з наведених вище етапів, запропонованих програмою SETUP, може бути проігнорований, а необхідні конфігураційні параметри можуть встановлюватися без посередництва програми SETUP за допомогою відповідних команд Cisco IOS. Крім цього, запуск програми SETUP є можливим в довільний момент з привілейованого режиму.

**Правила роботи з командним рядком Cisco IOS.** Взаємодія з системою Cisco IOS відбувається при посередництві інтерфейсу командного рядка (Command Line Interface, CLI). В загальному випадку формат команди виглядає наступним чином:

### **Команда [параметри або опції]**

Параметри або опції, залежно від команди, можуть бути обов'язковим, необов'язковими або відсутніми взагалі. Для орієнтування в системі команд в Cisco IOS передбачена залежна від контексту система допомоги.

Допомога може знадобитися при необхідності отримання переліку команд, які розпочинаються попередньо введеною послідовністю символів. В цьому випадку пропонується завершити введену послідовність символом “?” (знак питання) – у відповідь Cisco IOS надасть перелік команд, які починаються шуканою послідовністю символів. Наступний приклад демонструє використання допомоги слова:

```
Router# co?  
configure connect copy
```

Допомога синтаксису дозволяє отримати перелік допустимих ключових слів та команд даного контексту або перелік допустимих параметрів команди. Для використання допомоги синтаксису пропонується одразу після ключового слова через пробіл ввести символ “?” (знак питання). В результаті буде видано перелік можливих команд чи параметрів команди.

У випадку введення невірної команди (помилка в слові, недопустима в даному контексті команда або невірно заданий параметр) Cisco IOS видасть відповідне повідомлення і вказівку імовірного місцезнаходження помилки в командному рядку. Ключове слово або невірний параметр в цьому випадку

позначаються символом “^” (тильда). Наступний приклад демонструє реакцію системи на невірно введене ключове слово “Ethernet”.

```
Router(config)#interface ethernat  
^Invalid input detected at ^ marker
```

Команди та ключові слова можна скорочувати до мінімально можливого – необхідно набрати кількість символів, яка є достатньою для однозначного трактування ключового слова чи команди. Якщо введена послідовність недостатня для однозначного трактування команди чи ключового слова – реакцією Cisco IOS на спробу виконати таку команду буде повідомлення, типу:

```
cisco(config)# Ambiguous command: "i"
```

Автозавершення – клавішею TAB можна завершити ввід команди, якщо кількість попередньо набраних символів команди задовольняє вище наведеній умові.

Для усунення необхідності повторного набору команд передбачено буфер історії команд, який надає можливість повторного використання введених раніше команд.

**Контексти Cisco IOS.** При роботі з командним рядком Cisco IOS передбачено декілька контекстів (режимів вводу команд). Поточний контекст ідентифікується символом запрошення вводу команди, який виводиться вслід за іменем маршрутизатора, наприклад Router> - контекст користувача; Router# - контекст адміністратора. Замість сигнатури "Router" виводиться назва маршрутизатора, якщо вона була наперед визначена за допомогою відповідної команди.

Контекст користувача – відкривається при підключенні до маршрутизатора і допускає виконання лише обмеженого набору основних контрольних команд, що не впливають на конфігурацію маршрутизатора. Якщо на протязі тривалого часу відсутні будь-які дії в контексті адміністратора, Cisco IOS автоматично переходить в контекст користувача.

Контекст адміністратора – відкривається командою **enable**, поданої в контексті користувача. Контекст адміністратора надає доступ до всіх без винятку команд (команди, що дозволяють отримати повну інформацію про конфігурацію маршрутизатора та його поточний стан, команди переходу в режим конфігурування, команди збереження та завантаження конфігурації). Зворотній перехід до контексту користувача відбувається по команді **disable** або по закінченні встановленого часу неактивності.

Контексти користувача та адміністратора можуть бути захищені паролями з метою запобігання несанкціонованого доступу незареєстрованих операторів, тому при вході до одного з цих контекстів може відбуватися запит пароля (Password:). При вводі пароля останній із міркувань безпеки на екрані терміналу не відображається. При роботі через сеанс TELNET пароль передається мережею у відкритому форматі. TELNET не вживає жодних засобів по забезпеченню захисту пароля від можливого перехоплення. Завершення сеансу роботи відбувається по команді **exit**.

Команди Cisco IOS чітко структуровані і доступні в різних контекстах і для успішної роботи з системою команд важливим є розуміння того, в якому контексті які команди є доступними. Для спрощення орієнтування в ієрархії команд вигляд рядка запрошення має унікальний вигляд. На рис.2.6 наведена проста схематична діаграма деяких контекстів Cisco IOS.

Кожна команда доступна лише на певному рівні ієрархії CLI (в певному контексті CLI). Наприклад, команди конфігурації не будуть доступними, поки інтерфейс не буде переведено на рівень глобального конфігурування командою **configure**.

В табл. 2.1 наведено перелік можливих контекстів та доступних команд системи команд.

Вихід з контексту глобального конфігурування до контексту адміністратора, а також вихід з будь-якого контексту до контексту верхнього рівня виконується командою **exit**. Комбінація CTRL+Z приводить до

переходу в контекст адміністратора з будь-якого підконтексту, до цього ж приводить команда end будь-якого підконтексту.

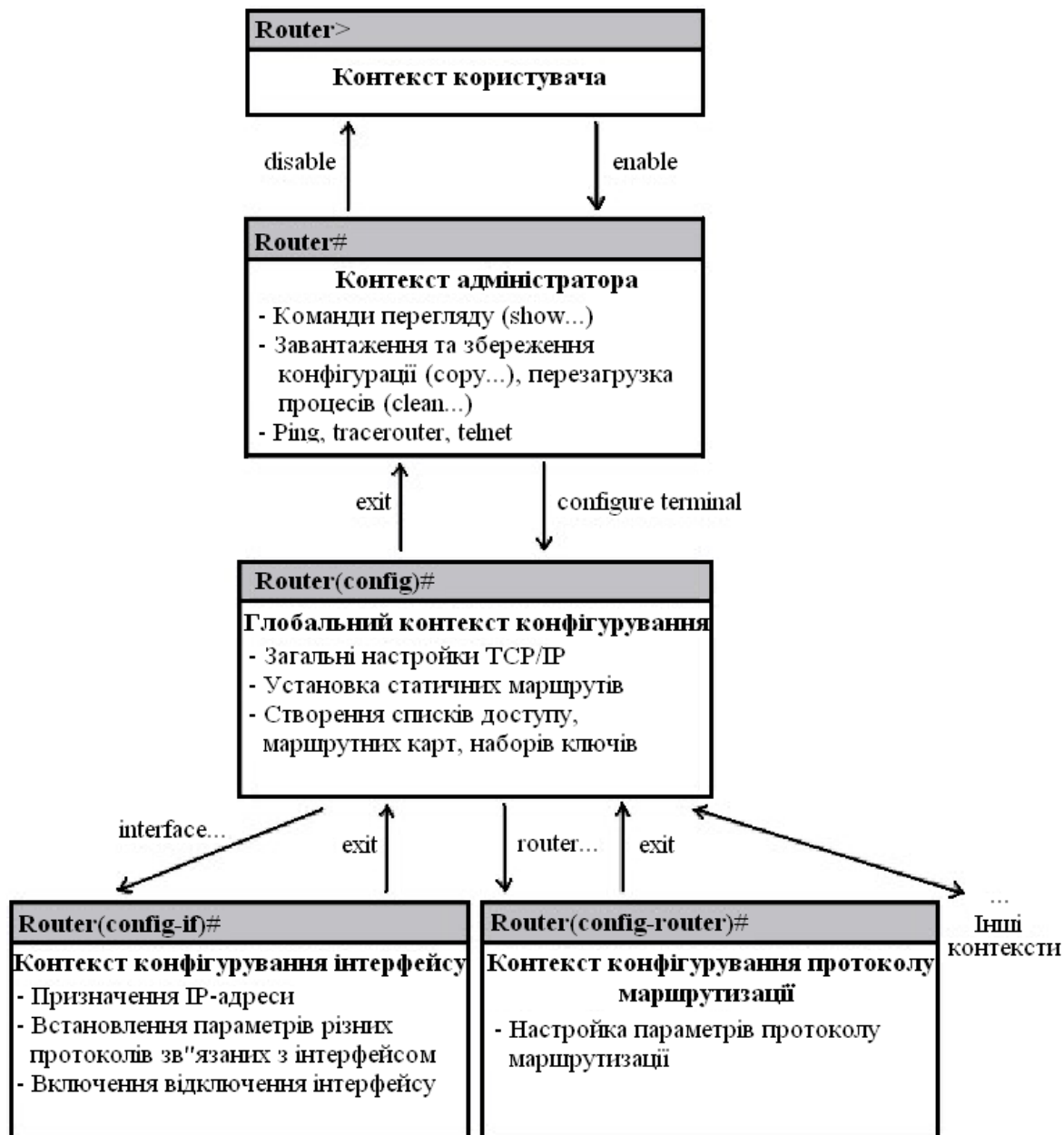


Рисунок 2.6 – Схематична ієрархія команд Cisco IOS

Відміна дії будь-якої команди реалізована за допомогою т.з. "негативних" команд – команд, яким передає префікс no, наприклад:

**Router(config-if)#shutdown** – вимикає інтерфейс  
**Router(config-if)#no shutdown** – включає інтерфейс.



Інколи при введенні негативних команд є потреба у вказуванні параметрів команд, дії яких вони відмінюють.

Таблиця 2.1 – Контексти та доступні команди системи команд Cisco IOS

Контексти	Опис
Router>	Режим користувача
Router#	Привілейований режим
Router(config)#	Режим глобального конфігурування
Router(config-if)#	Режим конфігурування інтерфейсу (контекст обраного інтерфейсу)
Router(config-router)#	Режим конфігурування маршрутизації
Router(config-line)#	Режим конфігурування віртуального терміналу

**Контекст адміністратора.** Команди конфігурування дозволяють маніпулювати поточним режимом роботи маршрутизатора шляхом зміни значень параметрів, які зберігаються в файлі конфігурації.

Маршрутизатор Cisco зберігає конфігурацію в двох копіях – файл поточної конфігурації (running-config) в RAM та файл стартової конфігурації (startup-config) в NVRAM. Файли конфігурації є текстовими файлами, що містять секції, кожна з яких відповідає одній із підсистем маршрутизатора; в секціях прописуються значення конкретних параметрів відповідних підсистем. При завантаженні Cisco IOS зчитує команди конфігурації з файлу startup-config (в NVRAM) до файлу running-config (в RAM). Поточна конфігурація є активною у процесі функціонування маршрутизатора.

Всі команди вступають в дію одразу ж після їх введення і прописуються до файлу поточної конфігурації (running-config) в RAM. Деякі настройки маршрутизатора та його окремих підсистем мають значення за замовчуванням. До файлу конфігурації прописуються лише ті значення параметрів, які відрізняються від значень, прийнятих за замовчуванням.

Контекст адміністратора містить команди перегляду файлів поточної та стартової конфігурації:

show running-config [options] – перегляд файлу поточної конфігурації;

show startup-config [options] – перегляд файлу стартової конфігурації.

Параметри [options] дозволяють керувати процесом виводу і дозволяють, наприклад, здійснювати вивід не всього файлу, а вмісту деякої окремої його секції.

Якщо маршрутизатор втрачить управління і буде перезавантажений, всі зміни, зафіксовані в running-config буде втрачено, якщо їх попередньо не було збережено до файлу стартової конфігурації (startup-config) в NVRAM. Для збереження змін у файлі стартової конфігурації слід користуватися командою:

**Router# copy running-config startup-config**

Конфігурація маршрутизатора може зберігатися на TFTP – сервері і завантажуватися з нього. Для цього необхідно вказувати IP – адресу TFTP – сервера та назву файлу, під якою буде збережено файл конфігурації. Команда збереження на TFTP має вигляд:

**copy <файл-джерело>TFTP://<IP – адреса TFTP >/[<назва файлу>]**

Якщо параметр <назва файлу> не буде вказано, Cisco IOS запропонує вказати його значення в процесі діалогу.

При збереженні однієї конфігурації поверх іншої можливі два варіанти: перезапис і злиття. При перезапису стара конфігурація попередньо видаляється, а при злитті – команди нової конфігурації дописуються до старої так, ніби вони вводилися вручну. При злитті конфігурацій можлива низка побічних ефектів, що має особливе значення при злитті списків доступу, оскільки порядок запису рядків списків має суттєве значення. Злиття може змінити цей порядок і суттєво спотворити роботу маршрутизатора.

Примусове перезавантаження маршрутизатора здійснюється командою:

**reload**

Якщо на момент перезавантаження виявлено факт попередньої зміни файлу поточної конфігурації `running-config`, Cisco IOS запропонує варіанти його збереження в файлі `startup-config` (або відмова від збереження).

**Контекст глобального конфігурування.** Перехід до контексту глобального конфігурування здійснюється з контексту адміністратора командою `configure`:

з терміналу: **`configure terminal`**;

з NVRAM: **`configure memory`**;

з мережі: **`configure network`**.

В контексті глобального конфігурування виконуються команди, які впливають на функціонування системи в цілому, а також команди переходу до контекстів конфігурування конкретних підсистем маршрутизатора. Контекст глобального конфігурування ідентифікується рядком запиту `(config)#` і допускає виконання наступних команд:

1) `hostname <назва маршрутизатора>` - встановлює назву маршрутизатора замість назви за замовчуванням "Router".

2) `[no] enable password <пароль>` - команда парольного доступу до контексту адміністратора, який буде запитуватися під час виконання команди `enable`. Пароль прописується до файлу поточної конфігурації і зберігається там

у відкритому (нешифрованому) вигляді. При відсутності цього пароля переключення до привілейованого режиму можна здійснити лише при використанні консолі, а з віртуального терміналу буде доступний лише контекст користувача.

3) `[no] enable secret <пароль>` - команда, за своєю дією аналогічна попередньо описаній, однак пароль зберігається в зашифрованому MD5 – алгоритмом вигляді і має вищий пріоритет виконання.

4) `[no] ip domain-lookup` – дозволити/заборонити звернення до DNS(Domain Name Service).

5) [no] cdp run – дозволяє/забороняє використання протоколу CDP (Cisco Discovery Protocol) виявлення безпосередньо підключеної апаратури Cisco, тобто доступної на каналному рівні. Протокол з періодичністю 60 с. опитує порти маршрутизатора на предмет наявності апаратури Cisco і заносить інформацію про виявлені пристрої до бази даних. Маршрутизатори до безпосередньо приєднаних мереж заносяться до таблиці маршрутизації автоматично одразу ж після конфігурування інтерфейсу, при умові, що цей інтерфейс працездатний (line protocol up). Для формування додаткових статичних маршрутів призначена команда:

6) [no] ip route <dest.address><dest.mask><next-hop>[options]

<destination address> - адреса цільової мережі

<destination mask> - маска цільової мережі

<next-hop> - адреса сусіднього маршрутизатора

< options> - додаткові параметри, наприклад – параметри метрики

В якості параметра <next-hop> можна вказувати:

- безпосередню адресу сусіднього (доступного на каналному рівні) маршрутизатора;
- адресу віддаленої мережі або віддаленого хоста (опосередкована маршрутизація);
- локальний інтерфейс.

Опосередкований маршрут вказує на запис в таблиці маршрутизації, в якому знаходиться прямий маршрут. Дозволяється формувати таким чином послідовності маршрутов будь-якої довжини. Локальний інтерфейс рекомендується вказувати лише для двоточкових інтерфейсів.

Статичні маршрути фіксуються в файлі стартової конфігурації, а до таблиці маршрутизації піднімаються тільки за умовою досяжності вказаного в них маршруту.

Для регулювання пріоритетами маршрутів слід користуватися параметром <адміндістанція>, який може приймати значення від 0 до 255. Рівень пріоритету зворотно пропорційний значенню адміністративної

дистанції і в таблицю маршрутизації з усіх активних маршрутів, що ведуть до даного префікса піднімається лише маршрут з найменшим значенням адміндистанції. За замовчуванням адміндистанція статичних маршрутів = 1.

Нульове значення зарезервоване системою Cisco IOS і не може бути використане в явному вигляді, однак неявно нульову адміндистанцію мають також маршрути до безпосередньо приєднаних мереж. Маршрути, які в якості адміндистанції містять значення 255, до таблиці маршрутів не піднімаються.

7) [no] ip default network <адреса віддаленої мережі> - дозволяє вказати маршрут за замовчуванням, відмінний від стандартного. Параметр <адреса віддаленої мережі > повинен бути статично описаний в таблиці маршрутизації. Можливим є визначення декількох маршрутів за замовчуванням – в цьому випадку при обранні маршруту Cisco IOS користується значенням адміністративної дистанції та метричною інформацією. Маршрути за замовчуванням в таблиці маршрутизації позначаються символом "\*".

Наведений нижче приклад демонструє використання маршруту в мережу 10.0.0.0 в якості маршруту за замовчуванням:

```
ip route 10.0.0.0 255.0.0.0 10.108.3.4
ip default-network 10.0.0.0
```

Cisco IOS має за замовчуванням зарезервований маршрут для використання його в якості маршруту за замовчуванням – 0.0.0.0/0. Cisco IOS надає можливість активації (деактивації) цього маршруту командою:

```
8) [no] ip classless
```

Команда ip classless активує зарезервований Cisco IOS маршрут за замовчуванням (0.0.0.0/0), а команда no ip classless деактивує цей маршрут. За замовчуванням цей маршрут активований, але не описаний.

**Лінії керування.** Налаштування ліній керування маршрутизаторів здійснюється окремо для кожної лінії в контексті обраної лінії, перехід до якого здійснюється з контексту глобального конфігурування командою:

## **line [aux | console | tty | vty] line-number [ending-line-number]**

Дана команда приводить до зміни поточного контексту на контекст обраної лінії керування, який ідентифікується зміною рядка запрошення на (config-line)#

В якості параметрів команди вказуються:

- aux – додатковий EIA/TIA-232 DTE – порт. Повинен задаватися, як відносна лінія 0. Додатковий порт може використовуватися для підтримки модема та асинхронних зв'язків;
- con – консольна термінальна лінія (DTE);
- tty – стандартна асинхронна лінія;
- vty – віртуальна термінальна лінія, що використовується для віддаленого доступу до консолі
- line-number – відносний номер останньої лінії (при конфігуруванні декількох ліній одночасно).

За замовчуванням маршрутизатор виводить діагностичні повідомлення тільки на консоль, а перенаправлення таких повідомлень на обрану лінію керування реалізується командою: **terminal monitor**.

Дія цієї команди відміняється командою: **no monitor**.

За замовчуванням маршрутизатор виводить системні повідомлення поверх вводу оператора і для продовження вводу оператор повинен пам'ятати, в якому місці його перервали. Для того, щоб дозволити після виводу кожного системного повідомлення вивід частини попередньо введеного оператором рядка, слід використовувати команду:

### **logging synchronous**

Якщо по завершенню деякого проміжку часу (інтервал неактивності) спостерігається відсутність вводу з терміналу, Cisco IOS розриває поточну сесію. Інтервал неактивності встановлюється командою:

**exec timeout <хвилини>[<секунди>]**

Будь-яка команда X, введена в контексті оператора або адміністратора, сприймається маршрутизатором, як команда telnet X. Це приводить до того,

що будь-який помилковий ввід примушує маршрутизатор опитувати сервер DNS для перетворення помилково введеного рядка в IP – адресу, що зумовлює затримки в роботі оператора. Уникнути таких затримок допомагає команда:

### **transport preffered none**

З міркувань безпеки, доступ до маршрутизатора через віртуальний термінал слід обмежити за допомогою пароля. Встановити пароль можна командою:

### **[no] password <текст пароля>**

Активація запиту пароля при в ході в Cisco IOS через віртуальний термінал виконується командою:

### **[no] login**

При відсутності парольного захисту контексту адміністратора використовується пароль захисту лінії CON, якщо цей пароль встановлено.

Слід зауважити, що в робочому режимі з міркувань безпеки віртуальні термінали потрібно заблокувати, а доступ до маршрутизатора здійснювати лише по консольній лінії або через термінальний сервер.

**Конфігурування інтерфейсів.** Конфігурування інтерфейсів здійснюється окремо для кожного інтерфейсу в контексті обраного інтерфейсу, перехід до якого здійснюється командою контексту глобального конфігурування:

### **interface <тип><номер>**

В якості параметру <тип> допускаються наступні слова: Ethernet, Fast Ethernet, Serial, Loopback, Null.

Вказана команда приводить до зміни поточного контексту на контекст конфігурування обраного інтерфейсу (config-if#).

На інтерфейсах Ethernet, окрім встановлення IP – адреси, як правило більше нічого робити не потрібно, однак Fast Ethernet може потребувати деяких примусових налаштувань дуплексного режиму або встановлення фіксованої швидкості (за замовчуванням ці параметри встановлюються

шляхом переговорів, однак в окремих випадках переговори можуть не дати необхідних результатів).

Послідовні інтерфейси за замовчуванням на фізичному рівні є інтерфейсами DTE, а на каналному рівні – інтерфейсами HDLC (фірмову модифікацію Cisco HDLC). Якщо інтерфейс переведено в режим DCE, для нього слід задавати тактову частоту синхронізації передачі даних.

Для надання фізичному інтерфейсу IP – адреси слід використовувати команду:

**ip address <IP-address><address-mask>**

де <IP-address> - IP – адреса інтерфейсу;

<address-mask> - маска підмережі.

В деяких випадках може бути необхідність встановлення ширини смуги пропускання командою:

**bandwidth <ширина-смуги-пропускання, кБіт/с>**

За замовчуванням bandwidth може мати наступні значення:

- для Ethernet 10000;
- для Fast Ethernet 100000;
- для Serial 1544.

Слід зауважити, що значення параметра bandwidth не впливає на фізичну швидкість передачі, а використовується деякими протоколами маршрутизації для оцінки маршруту.

Тип середовища передачі вказується командою:

**media-type <тип-середовища-передачі>**

Параметр <тип-середовища-передачі> може приймати значення:

- для Ethernet "10BASE-T";
- для Fast Ethernet "100BASE-T", "100BASE-TX".

Для послідовних інтерфейсів, які використовують функції DCE, необхідно вказати фізичну швидкість передачі даних. Це можна зробити командою:

**clock rate <фізична-швидкість-передачі, кБіт/с>**



Параметр <фізична-швидкість-передачі, кБіт/с> може приймати фіксовані значення, перелік яких можна попередньо проглянути, ввівши clock rate?.

Для послідовного інтерфейсу, що виконує функцію DTE також може бути вказаний цей параметр, однак він буде проігнорований Cisco IOS і жодного впливу на роботу інтерфейсу не матиме, оскільки обладнання DTE запозичує цей параметр від DCE.

За замовчуванням фізичні інтерфейси виключені (неактивні – administratively down). Для їх активації використовується команда:

### **[no] shutdown**

Ця команда переводить інтерфейс до стану manual up. Якщо зовнішнє обладнання вимкнено, то Cisco IOS автоматично переведе фізичний інтерфейс до стану manual down, а при активізації зовнішнього обладнання фізичний інтерфейс підніметься до стану manual up автоматично.

Для послідовних інтерфейсів іноді виникає необхідність використовувати протокол канального рівня, відмінний від протоколу за замовчуванням (HDLC). Cisco IOS надає можливість вказати тип використовуваного протоколу командою:

### **encapsulation <протокол>**

Параметр <протокол> може приймати фіксовані значення, для яких Cisco IOS передбачені зарезервовані ключові слова, наприклад PPP, Frame-Relay і т.п. Повний перелік значень параметра <протокол> доступний для перегляду командою encapsulation?.

Логічні інтерфейси конфігуруються командами, які наведені вище, за винятком того, що параметри media-type, clock rate та операція [no] shutdown для них не мають сенсу.

## **2.3 Програма Packet Tracer 5.3.2**

Cisco Packet Tracer – емулятор мережі передачі даних, який випускається компанією Cisco System. Програмні продукти Packet Tracer надають можливість створювати мережеві топології із широкого спектру маршрутизаторів і комутаторів Cisco, робочих станцій та мережевих з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Ця функція може бути виконана як для навчання, так і для роботи. Наприклад, щоб провести настройку мережі ще на етапі планування або щоб створити копію робочій мережі з метою усунування недоліків.

Загальний вигляд програми представлений на рис.2.7

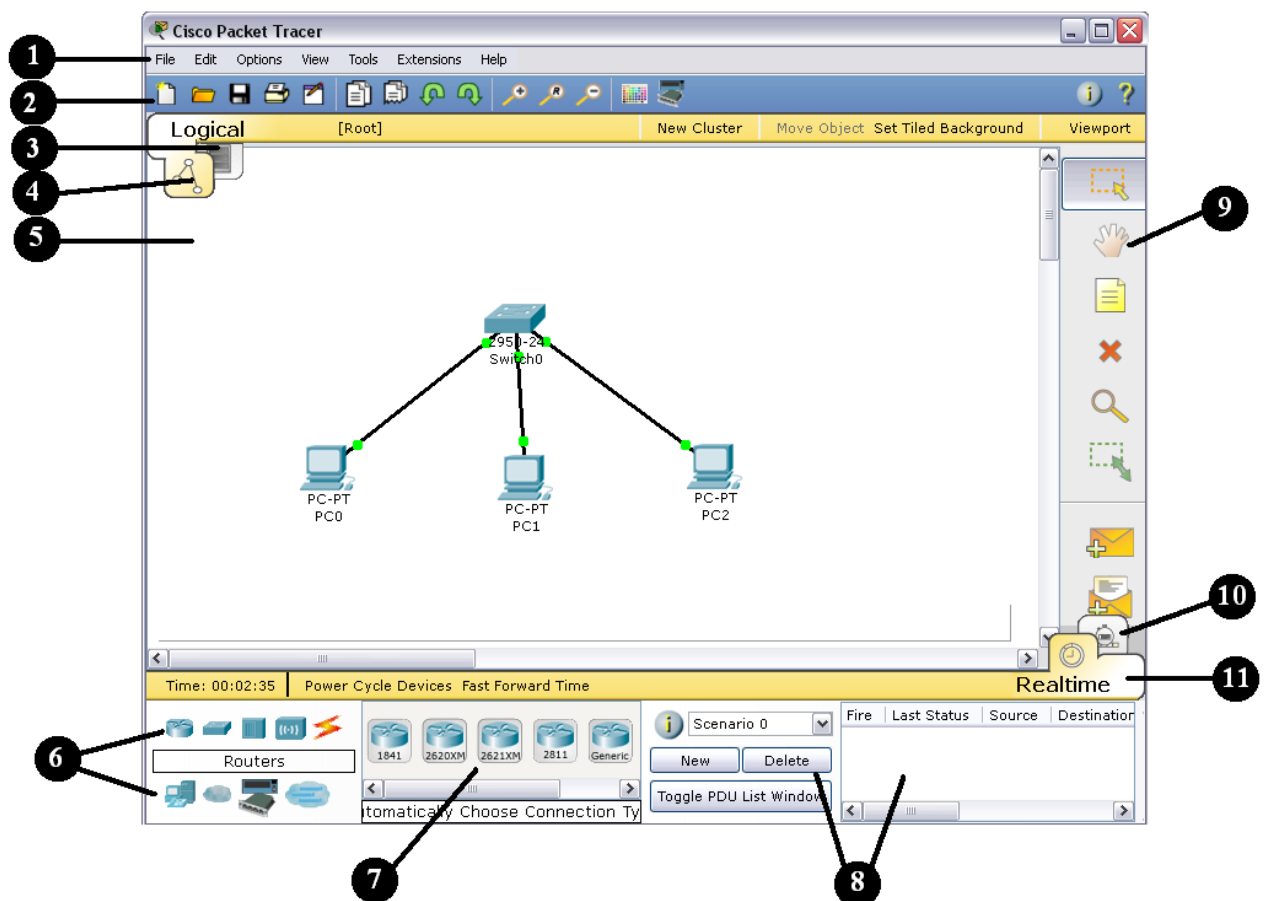


Рисунок 2.7 – Інтерфейс програми Packet Tracer

Робоча область вікна програми складається з наступних елементів:

1. **Menu Bar** – головне меню програми. Дозволяє детально налаштувати роботу програми. Панель містить меню File, Edit, Options, View, Tools, Extensions, Help.

2. **Menu Tool Bar** – піктографічне меню, містить графічні зображення ярликів для доступу к командам меню File, Edit, View і Tools, а також кнопку Network Information.

3. **Logical/Physical Workspace and Navigator Bar** – панель, яка надає можливість перемикає робочу область: фізичну чи логічну, а також дозволяє пересуватися між рівнями кластера.

4. **Logical Workspace and Navigator Bar** – режим побудови логічної топології мережі.

5. **Workspace** – область, в якій відбувається створення мережі, проводяться спостереження за симуляцією і проглядається різна інформація і статистика.

6. **Network Component Box** – це область, в якій вибираються устаткування і зв'язки для розміщення їх на робочому просторі. Вона містить області Device –Type Selection і Device-Specific Selection. Область Device – Type Selection містить доступні типи пристроїв і зв'язків, а область Device-Specific Selection змінюється в залежності від обраного пристрою.

7. **Device-Specific Selection** – область використовується для вибору конкретних устаткувань і з'єднань, необхідних для побудови в робочому просторі мережі. Вибір класу пристрою, яке буде елементом фізичної або логічної топології.

8. **User Created Packet Window** – вікно керує пакетами, які були створені в мережі під час симуляції сценарію.

9. **Common Tools Bar** – панель піктограм, яка забезпечує доступ до найбільш використовуваних інструментів програми: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU і Add Complex PDU.

10. **Simulation Bar** – пакетний аналізатор, містить кнопки Play Control і перемикач Event List.

11. **Realtime Bar** – панель для роботи в режимі реального часу, містить кнопки, що відносяться до Power Cycle Devices.

Для створення топології необхідно вибрати устаткування з панелі Network Component, а далі з панелі Device–Type Selection вибрати тип обраного устаткування. Після цього потрібно натиснути ліву кнопку миші в полі робочої області програми (Workspace). Також можна витягнути пристрій прямо з області Device–Type Selection, але при цьому буде обрана модель пристрою за замовчанням.

Для швидкого створення декількох екземплярів одного і того ж пристрою потрібно натиснути кнопку Ctrl і разом з нею натиснути на пристрій, який вже знаходиться в області Workspace. Після цього можна декілька разів натискати на робочій області для додавання копій пристрою.

В Packet Tracer представлені наступні типи устаткування:

- маршрутизатори;
- комутатори (в тому числі і мости);
- хаби і повторювачи;
- ПК, сервери, принтери, IP – телефони;
- бездротові пристрої: точки доступу і бездротовий маршрутизатор;
- інші пристрої – хмара, DSL – модем і кабельний модем.

Додамо необхідні елементи в робочу область програми так, як показано на рис.2.8.

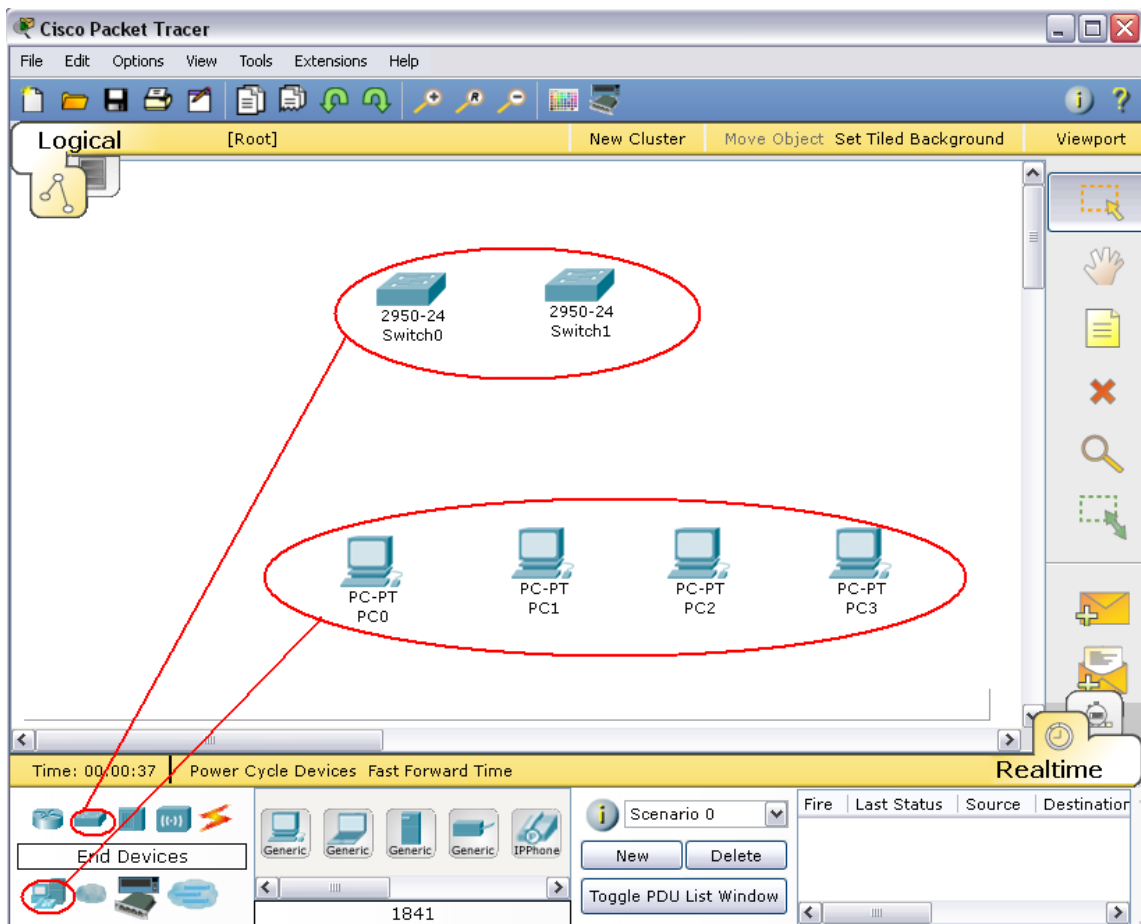


Рисунок 2.8 – Додавання елементів мережі

При додаванні кожного елемента користувач має можливість дати йому ім'я і установити параметри. Для цього необхідно натиснути на потрібний елемент лівою кнопкою миші (ЛКМ) і в діалоговому вікні устаткування перейти до вкладки **Config**.

Діалогове вікно властивостей кожного елемента має дві вкладки:

- Physical – містить графічний інтерфейс устаткування і дозволяє симулювати роботу з ним на фізичному рівні.

- Config – містить всі необхідні параметри для настройки устаткування і має зручний для цього інтерфейс.

Також в залежності від устаткування, властивості можуть мати додаткову вкладку для керування роботою обраного елемента: Desktop (якщо обране кінцеве устаткування) або CLI (якщо обраний маршрутизатор) і т.п.

Для видалення непотрібних устаткувань з робочої області програми використовується кнопка Delete (Del).

Додані елементи треба зв'язати за допомогою з'єднувальних зв'язків. Для цього необхідно вибрати вкладку Connections з панелі Network Component Box. Стануть доступними всі можливі типи з'єднань між устаткуваннями. Далі вибирається відповідний тип кабелю. Вказівник миші зміниться на курсор "connection" (має вигляд рознімання). Слід натиснути на першому пристрої і вибрати відповідний інтерфейс, к якому треба виконати з'єднання, а далі натиснути на другий пристрій, виконавши ту ж операцію. Можна також з'єднати за допомогою **Automatically Choose Connection Type**



 (автоматично з'єднує елементи в мережі). Між пристроями з'явиться кабельне з'єднання, а індикатори на кожному кінці покажуть статус з'єднання (для інтерфейсів які мають індикатор).









Рисунок 2.9 – Типи кабелю, що підтримуються в Packet Tracer

Packet Tracer підтримує широкий діапазон мережевих з'єднань. Вони описані в табл.2.2. Кожний тип кабелю може бути з'єднаний лише з певними типами інтерфейсів.

Таблиця 2.2 – Типи кабелю в Packet Tracer

Тип кабелю	Опис
 Console	Консольне з'єднання може бути виконане між ПК і маршрутизаторами або комутаторами. Для цього повинні виконуватися деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднання з обох сторін повинна бути однаковою, 7 біт даних (або 8 біт) для обох сторін, однаковий контроль парності, 1 або 2 стопових біта (але вони не обов'язково повинні бути однаковими), а потік даних може бути будь-яким для обох сторін.

 Copper Straight - through	Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв. Він повинен бути з'єднаний з наступними типами портів: мідний 10 Мбіт/с (Ethernet), мідний 100 Мбіт/с (Fast Ethernet) і мідний 1000 Мбіт/с (Gigabit Ethernet). Використовується для з'єднання типу ПК-комутатор, маршрутизатор-комутатор).
 Copper Cross - over	Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв. Використовується для з'єднання типу ПК-ПК, комутатор-комутатор, маршрутизатор-маршрутизатор, маршрутизатор-ПК).
 Fiber	Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт/с або 1000 Мбіт/с).
 Phone	З'єднання через телефонну лінію може бути здійснено тільки між пристроями, які мають модемні порти.
 Coaxial	Коаксіальне середовище використовується для з'єднання між коаксіальними портами, такими як кабельний модем, з'єднаний з хмарою Packet Tracer.
 Serial DCE and DTE	З'єднання через послідовні порти, часто використовуються для зв'язку WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на боці DCE – устаткування. Синхронізація DTE виконується за вибором. Сторону DCE можна визначити по маленькому малюнку «годинника» поряд з портом. При виборі типу з'єднання Serial DCE, перший пристрій, до якого застосовується з'єднання, становиться DCE – устаткуванням, а другий – автоматично стане стороною DTE. Можливе і зворотне розташування сторін, якщо обраний тип з'єднання Serial DTE.

Найбільш часто будемо використовувати два типи кабелю: прямий (Copper Straight-through) і перехресний кабель (Copper Cross – over). Щоб визначити тип кабелю RJ-45, треба положити два кінця кабелю разом, щоб побачити різнокольорові дроти, як це показано на рис. 2.10. На кінці кожного є вісім різнокольорових смужок або контактів. Якщо порядок слідування кольорових контактів співпадає, то такий кабель називається прямим (рис.2.5).

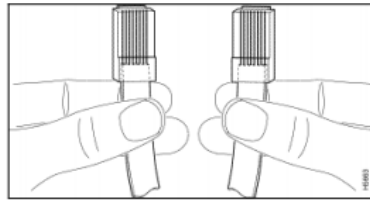
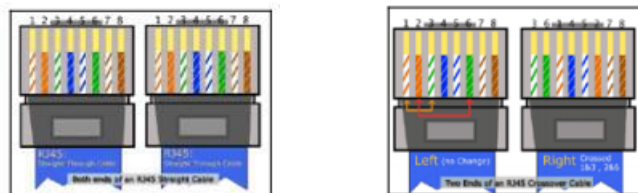


Рисунок 2.10 – Визначення типу кабелю RJ-45

Для того, щоб визначити який кабель слід використати для з'єднання, розділимо всі устаткування на два типи. Тип 1: мережеві адаптери комп'ютерів (LAN або Ethernet), WAN – порт маршрутизатора, рознімання Ethernet різних устаткувань (телевізори, тюнери та інш.). Тип 2: LAN- порти маршрутизаторів, LAN- порти ADSL модемів, всі порти концентраторів і комутаторів. При з'єднанні між собою двох пристроїв одного типу (наприклад, комп'ютер – комп'ютер або комутатор – комутатор) потрібен перехресний кабель, а при з'єднанні між собою двох пристроїв різного типу – прямий кабель (наприклад, комп'ютер – концентратор або комп'ютер – комутатор).



а) прямий кабель    б) перехресний кабель

Рисунок 2.11 – Вигляд прямого та перехресного кабелю

Після створення мережі її треба зберегти, вибравши пункт меню File->Save або іконку Save на панелі Main Tool Bar. Файл з збереженою топологією має розширення \*.pkt.

Packet Tracer надає можливість симулювати роботу с інтерфейсом командного рядка (ІКР) операційної системи IOS, встановленої на всіх комутаторах і маршрутизаторах компанії Cisco.



Підключившись до устаткування, можна працювати з ним так, як за консоллю реального пристрою. Стимулятор забезпечує підтримку практично усіх команд, що доступні на реальних пристроях.

Підключення до ІКР комутаторів або маршрутизаторів можна провести, клацнувши на необхідній пристрій і переключившись в вікно властивостей до вкладки CLI.

Для симуляції роботи командної строки на кінцевому устаткуванні (комп'ютері) необхідно во властивостях вибрати вкладку Desktop, а далі натиснути на ярлик Command Prompt.

**Робота з файлами в Packet Tracer.** Програма Packet Tracer дозволяє користувачеві зберігати конфігурацію деяких пристроїв, таких як маршрутизатори або комутатори в текстових файлах. Для цього необхідно перейти до властивостей даного пристрою і у вкладці Config натиснути на кнопку “Export...” для експорту конфігурації Startup Config або Running Config. Відкриється діалогове вікно для збереження необхідної конфігурації в файл, який буде мати розширення \*.txt. Текст файлу з конфігурацією пристрою running-config.txt (ім'я за замовчуванням) представляється аналогічним до тексту інформації, отриманому при використанні команди show running в IOS пристроях.

Слід відмітити, що конфігурація кожного устаткування зберігається в окремому текстовому файлі. Користувач також має можливість змінювати конфігурацію в збереженому файлі вручну за допомогою довільного текстового редактору. Для надання устаткуванню збережених або відредагованих налаштувань треба в вкладці Config натиснути кнопку “Load...” для завантаження необхідної конфігурації Startup Config або кнопку “Merge...” для завантаження конфігурації Running Config.

### **3. Порядок проведення лабораторної роботи**

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Виконати в Packet Tracer практичну частину лабораторної роботи.
4. Отримати у викладача варіант і виконати в Packet Tracer завдання для самостійної роботи.
5. Продемонструвати викладачу результати виконання завдання для самостійної роботи. Показати звіт про виконання команди ping з будь-якого комп'ютера на інший.
6. Оформити звіт.
7. Захистити звіт.

### 3.1 Практична частина лабораторної роботи

1. Додати на робочу область програми 2 комутатора Switch-PT. За замовчуванням вони мають ім'я – Switch0 і Switch1.
2. Додати 4 комп'ютера з іменами за замовчуванням PC0, PC1, PC2, PC3.
3. З'єднати устаткування в мережу Ethernet, як показано на рис.2.12.

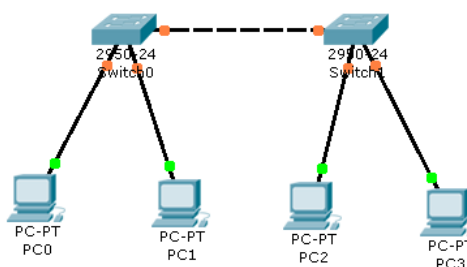


Рисунок 2.12 – Фізична топологія мережі для симуляції

4. Зберегти створену топологію, натиснувши кнопку Save (в меню File->Save).
5. Відкрити властивості устаткування PC0 натиснув на його зображенні. Перейти до вкладки Desktop і виконати симуляцію роботи run натиснувши Command Prompt.

6. Перелік команд можна отримати, якщо ввести ? і натиснути Enter. Для конфігурування комп'ютера слід скористатися командою ipconfig з командного рядка, наприклад, ipconfig 192.168.1.2 255.255.255.0

IP адресу і маску також можна вводити в зручному графічному інтерфейсі устаткування (рис.2.13). Поле DEFAULT GATEWAY – адреса шлюзу не важна, тому що мережа, що створюється не потребує маршрутизації.

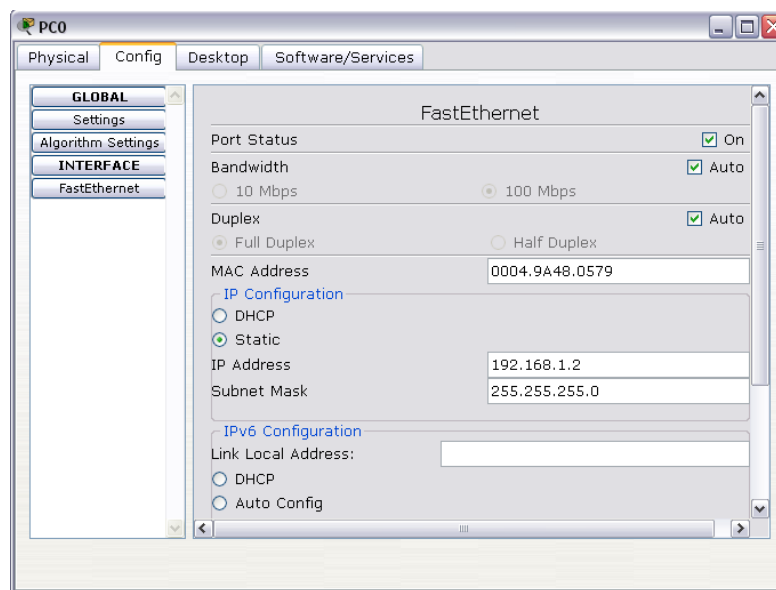


Рисунок 2.13 – Вкладка Config робочої станції PC0

Аналогічним способом слід налаштувати кожний комп'ютер, надавши їм IP-адреси з табл.2.3.

Таблиця 2.3 – Перелік IP-адрес для конфігурації мережі

Устаткування	IP ADDRESS	SUBNET MASK
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

7. На кожному комп'ютері переглянути назначені адреси командою ipconfig без параметрів.

8. Якщо всі пункти виконані вірно, то можна пропінгувати будь-який комп'ютер з будь-якого іншого комп'ютера. Наприклад, з комп'ютера PC3

виконати пінгування до комп'ютера PC0. Звіт про виконання команди ping наведений на рис.2.14.

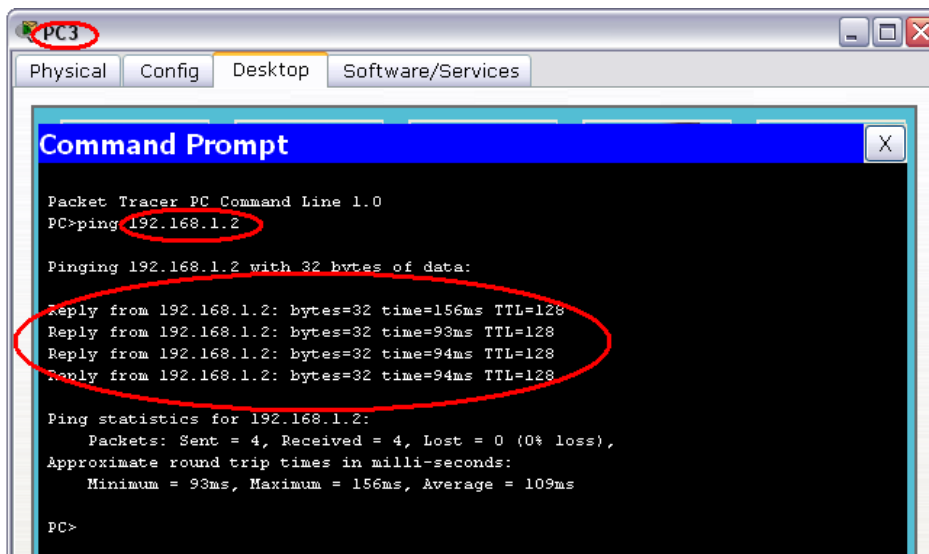
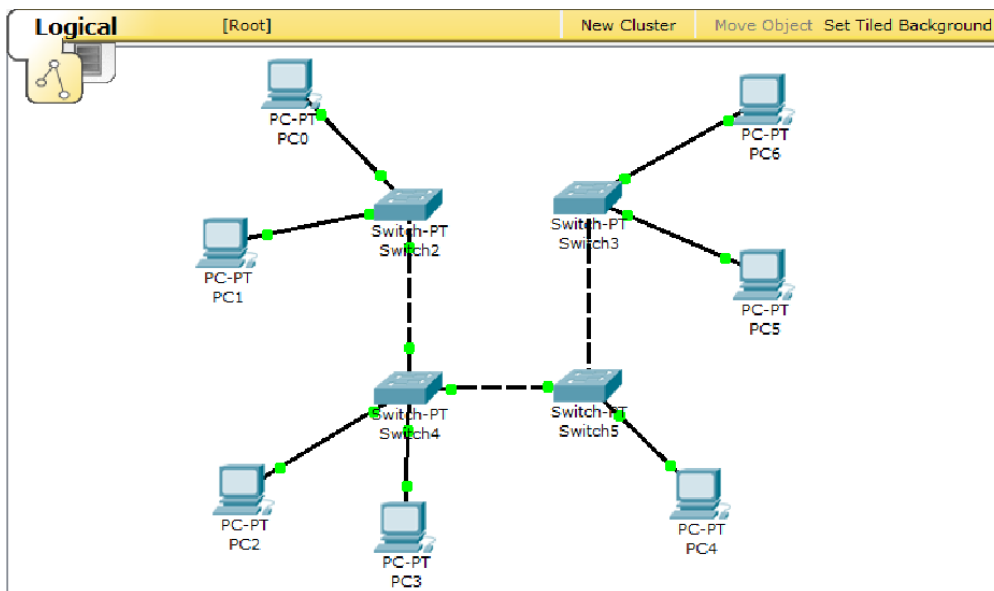


Рисунок 2.14 – Звіт про виконання команди ping між вузлами PC3 і PC0

#### 4. Варіанти індивідуальних завдань для самостійної роботи

##### 1. Створить топологію



**2. Призначте комп'ютерам адреси згідно варіанту (v=1-12). Наприклад, для варіанту 7 (v=7) і комп'ютер PC1 має IP ADDRESS 7.1.1.1**

Таблиця 2.4 – Варіанти для конфігурування комп'ютерів мережі

Устаткування	IP ADDRESS	SUBNET MASK
PC0	v.1.1.1	255.0.0.0
PC1	v.1.1.2	255.0.0.0
PC2	v.1.1.3	255.0.0.0
PC3	v.1.1.4	255.0.0.0
PC4	v.1.1.5	255.0.0.0
PC5	v.1.1.6	255.0.0.0
PC6	v.1.1.7	255.0.0.0

3. Призначте комп'ютерам різні ім'я.

4. Якщо все буде зроблено вірно, то стане можливим пропінгувати будь-який комп'ютер з іншого. Пропінгувати комп'ютери згідно варіанту, табл. 2.5

Таблиця 2.5 – Варіанти виконання команди ping для перевірки працездатності мережі

Варіант v	Ping з вузла	Ping до вузла	Варіант v	Ping з вузла	Ping до вузла
1	PC0	PC5	7	PC6	PC4
2	PC1	PC6	8	PC0	PC5
3	PC2	PC0	9	PC1	PC6
4	PC3	PC1	10	PC2	PC0
5	PC4	PC2	11	PC3	PC1
6	PC5	PC3	12	PC4	PC2

## 5. Контрольні питання

1. Які типи мережевих пристроїв і з'єднань можна використовувати в Packet Tracer?
2. Яким способом можна перейти до інтерфейсу командного рядка устаткування?
3. Як конфігурувати пристрої з іншого комп'ютера?
4. Як додати в топологію і налаштувати нове устаткування?

5. Як зберегти конфігурацію устаткування в \*.txt файл?

## **6. Перелік літератури**

### **Основна література**

1. Кузніченко С.Д. «Комп'ютерні мережі» Конспект лекцій. – Одеса: ОДЕКУ, 2018.– 175 с.
2. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: «Магнолія 2006», 2012.– 262с.
3. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. – К.:Київ ун-т ім. Б.Грінченка, 2011. – 291 с.

### **Додаткова література**

1. Паркер Т., К. Сиян TCP/IP. Для професіоналов. 3-е изд. - СПб.: Питер, 2004. - 859 с.: ил.
2. Снейдер И. Эффективное программирование TCP/IP. Библиотека программиста - СПб.: Питер, 2002. - 320 с.: ил.
3. Шамис В.А. Borland C++ Builder 6. Для професіоналов. - СПб.: Питер, 2004. - 798 с.: ил.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 672 с., ил.

## **7. Правила техніки безпеки та охорони праці**

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

## **8. Оформлення та захист звіту**

Звіт готується в електронному вигляді і роздруковується.

Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Титульна сторінка :
  - Найменування лабораторної роботи.
  - Відомості про виконавця, номер варіанту.
2. Мета роботи та завдання до лабораторної роботи.
3. Виконання *практичної частини лабораторної роботи* (п.3.1).
4. Опис побудови топології та приведення результатів виконання роботи (скріншот побудованої топології).
5. Скріншот виконання команди ping.
6. Виконання *практичної частини лабораторної роботи згідно варіанту* (п.4).
7. Опис побудови топології та приведення результатів виконання роботи (скріншот побудованої топології).
8. Скріншот виконання команди ping згідно варіанту.
9. Висновок за результатами роботи.
10. Контрольні питання та відповіді на них.

## ЛАБОРАТОРНА РОБОТА №3

### *Налаштування VLAN на комутаторах фірми Cisco*

#### 1. Мета роботи

**Метою лабораторної роботи** є навчитися конфігурувати порти доступу для VLAN на комутаторах фірми Cisco, а саме зібрати і протестувати мережу, логічна топологія

#### 2. Теоретичні відомості до лабораторної роботи

У даній лабораторній роботі будуть розглядатися практичні питання налаштування VLAN на комутаторах фірми Cisco, конкретно буде розглянуто налаштування портів доступу. Крім налаштування VLAN, також розглядаються основні навички роботи з обладнанням Cisco і симулятором мереж Packet Tracer.

##### 2.1 Опис access port та trunk port

###### Деякі позначення:

- **access port** – це порт, який належить до одного VLAN, і може передавати нетегірований інформаційний трафік;
- **trunk port** – це комутаційний порт, за допомогою якого може передаватися тегований трафік від одного або декількох VLAN.

Комутатори Cisco ранніх версій працювали з двома протоколами: 802.1Q, ISL. Другий з них відноситься до пропрієтарного протоколу, який застосовується в комутаційних платформах Cisco. Цей протокол дозволяє інкапсулювати фрейм з метою передачі даних про причетність до тієї чи іншої VLAN. Сучасні моделі цей протокол не підтримують, а працюють тільки з 802.1Q.



## 2.2 Налаштування Native Vlan на Cisco

Native VLAN – це поняття в стандарті 802.1Q, яке позначає VLAN на комутаторі, де всі кадри йдуть без тега, тобто трафік передається нетегірованим. За замовчуванням це VLAN 1. У деяких моделях комутаторів Cisco це можна змінити, вказавши інший VLAN як native.

Якщо комутатор отримує нетегіровані кадри на trunk порт, він автоматично зараховує їх до Native VLAN. І точно так само кадри, які генеруються з нерозподілених портів, при попаданні в trunk-порт зараховуються до Native VLAN.

Трафік, який належить іншим VLAN-ам, тегується із зазначенням відповідного VLAN ID всередині тега.

### ***Приклад налаштування VLAN 5 як native на комутаторі Cisco***

```
sw1 (config) # interface f0 / 10  
sw1 (config-if) # switchport trunk native vlan 5
```

Тепер весь трафік, що належить VLAN 5 передаватиметься через транковий інтерфейс нетегірованим, а весь нетегірований трафік, що прийшов на транковий інтерфейс буде промаркований як належить VLAN 5 (за замовчуванням VLAN 1).

З міркувань безпеки (наприклад, для захисту від VLAN Hopping) рекомендується в Trunk виконувати тегування навіть для native VLAN. Включити тегування фреймів для native VLAN глобально можна за допомогою команди **vlan dot1q tag native**, переглянути поточний статус тегування можна використовуючи команду **show vlan dot1q tag native**.

```
Switch (config) #no vlan dot1q tag native  
Switch # sho vlan dot1q tag native  
dot1q native vlan tagging is disabled
```

## 2.3 Налаштування Voice VLAN на Cisco

Більшість IP – телефонів, включаючи Cisco, мають маленький комутатор на 3 порти всередині IP – телефону. Телефон підключається «в розрив».



- перший порт підключається до комутатора;
- другий порт підключається до комп'ютера;
- внутрішній порт підключає сам телефон.

Між комутатором і телефоном є так званий " trunk ". Порт на телефоні, який підключається до комп'ютера, є портом доступу. Телефон передає весь трафік з комп'ютера на комутатор без будь-яких міток, непомічених. Трафік з самого телефону завжди буде позначатися, і в Trunk будуть дозволені тільки два вищезгаданих VLAN-а.

При основному знайомстві з налаштуванням VLAN-ів, створення голосового VLAN-а не складе для взагалі ніяких труднощів. Щоб налаштувати порт на комутаторі, де будуть використовуватися VLAN 10 і 11 необхідно:

1) спочатку створити необхідні VLAN-и:

```
MERION-SW1 (config) #vlan 10
```

```
MERION-SW1 (config-vlan) #name DATA
```

```
MERION-SW1 (config-vlan) #exit
```

```
MERION-SW1 (config) #vlan 11
```

```
MERION-SW1 (config-vlan) #name VOICE
```

```
MERION-SW1 (config-vlan) #exit
```

2) далі, налаштувати інтерфейс:

```
MERION-SW1 (config) #interface GigabitEthernet 0/1
```

```
MERION-SW1 (config-if) #switchport mode access
MERION-SW1 (config-if) #switchport access vlan 10
MERION-SW1 (config-if) #switchport voice vlan 11
MERION-SW1 (config-if) #exit
```

Після переключення даного порта в режим доступу слід налаштувати його для VLAN 10. Команда **switchport voice vlan** повідомляє комутатор, щоб він використовував VLAN 11 як голосовий VLAN.

Для того, щоб телефон зрозумів, який VLAN потрібно використовувати, використовуються два протоколи – Cisco Discovery Protocol (CDP) для телефонів Cisco і Link Layer Discovery Protocol (LLDP) для телефонів від інших вендорів.

## 2.4 Номери VLAN (VLAN ID)

Номери VLAN (VLAN ID) можуть бути в діапазоні від 1 до 4094:

- 1 – 1005 базовий діапазон (normal-range)
- 1002 – 1005 зарезервовані для Token Ring і FDDI VLAN
- 1006 – 4094 розширений діапазон (extended-range)

## 2.5 Параметри VLAN

При створенні або зміні VLAN можна задати наступні параметри:

- VLAN ID – Номер VLAN
- VLAN name (name) – Ім'я VLAN
- VLAN type (media) – Тип VLAN (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, або TrCRF, Token Ring, Token Ring-Net)
- VLAN state (state) – Стан VLAN (active або suspended)
- VLAN MTU (mtu) – Максимальний розмір блоку даних, який може бути переданий на каналному рівні

- SAID (said) – Security Association Identifier – ідентифікатор асоціації безпеки (стандарт IEEE 802.10)
- Remote SPAN (remote-span) – Створення VLAN для віддаленого моніторингу трафіку (Надалі в такий VLAN можна віддзеркалювати трафік з якого-небудь порту, і передати його через транк на інший комутатор, в якому з цього VLAN трафік відправити на потрібний порт з підключеним сніфера)
- Bridge identification number для TrBRF VLAN (bridge) – Ідентифікатор номера моста для функції TrBRF (Token Ring Bridge Relay Function). Мета функції – створення моста з кілець.
- Ring number для FDDI і TrCRF VLAN (ring) – Номер кільця для типів VLAN FDDI і TrCRF (Token Ring concentrator relay functions). TrCRF називають кільця, які включені в міст.
- Parent VLAN number для TrCRF VLAN (parent) – Номер батьківського VLAN для типу VLAN FDDI або Token Ring
- Spanning Tree Protocol (STP) type для TrCRF VLAN (stp type) – Тип протоколу сполучного дерева (STP) для VLAN типу TrCRF
- Translational VLAN number 1 (tb-vlan1) – Номер VLAN для первинного перетворення одного типу VLAN в інший
- Translational VLAN number 2 (tb-vlan2) – Номер VLAN для вторинного перетворення одного типу VLAN в інший

## 2.6 Значення за замовчуванням

VLAN ID	1
VLAN name	VLANxxxx, де xxxx чотири цифри номера VLAN (Наприклад: VLAN0003, VLAN0200 і т.д.)
SAID	100000 плюс VLAN ID (Наприклад: 100001 для VLAN 1, 100200 для VLAN 200 і т.д.)
VLAN MTU	1500
Translational VLAN number 1	0
Translational VLAN number 2	0

VLAN state	active
Remote SPAN	disabled

### 3 Порядок проведення лабораторної роботи

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Виконати в Packet Tracer практичну частину лабораторної роботи.
4. Продемонструвати викладачу результати виконання практичної частини лабораторної роботи.
5. Отримати у викладача варіант і виконати в Packet Tracer завдання для самостійної роботи.
6. Продемонструвати викладачу результати виконання завдання для самостійної роботи.
7. Оформити звіт.
8. Захистити звіт.

#### 3.1 Практична частина лабораторної роботи

В даній лабораторній роботі № 3, необхідно зконфігурувати порти доступу для VLAN на комутаторах фірми Cisco, а саме зібрати і протестувати мережу, логічна топологія якої представлена на рисунку 3.1

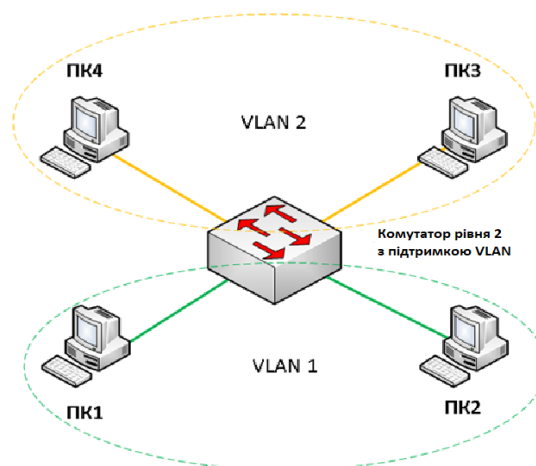


Рисунок 3.1 – Логічна топологія з комутатором рівня 2 та з підтримкою VLAN

Для досягнення поставленої мети нам знадобиться:

- в ідеальному випадку 1 комутатор фірми Cisco з підтримкою VLAN, 4 комп'ютери і 4 патчкорди;
- в більш реальному і найбільш підходящому варіанті, нам знадобиться комп'ютер з встановленим на нього програмним забезпеченням Cisco Packet Tracer.

Якщо є реальне обладнання, то підключаємо комп'ютери до перших чотирьох портів комутатора (далі вважаємо, що комп'ютер підключений до порту 1 – це ПК1, до порту 2 – ПК2 і т.д.). Включаємо комутатор і комп'ютери. Підключаємося з одного з комп'ютерів до комутатора через консольний кабель.

Якщо ж немає реального обладнання, то необхідно запустити Cisco Packet Tracer і зібрати в ньому наступну топологію (*при складанні враховуємо, що PC0 підключений до порту FastEthernet0/1, PC1 до порту FastEthernet0/2 і т.д*) рис. 3.2

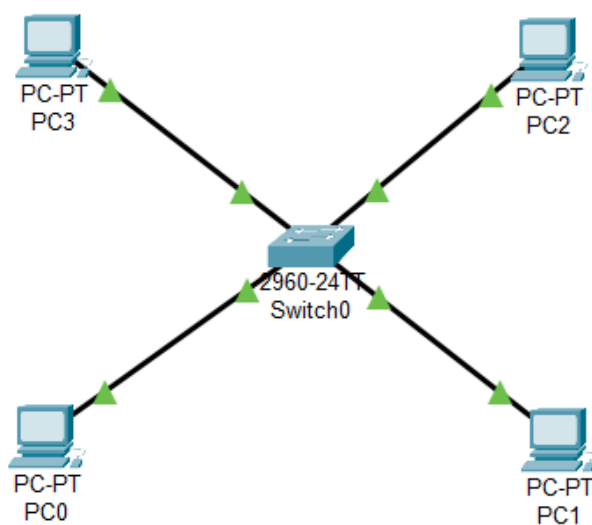


Рисунок 3.2 – Логічна топологія в Cisco Packet Tracer

Таблиця 3.1 – Таблиця розрахунку для задання адресації комутаторам VLAN

Кількість VLAN комутаторів	Кількість хостів в підмережі	IP-адреса		Маска
2	2	VLAN 1	192.168.1.1 192.168.1.2	/24
		VLAN 2	172.20.20.1 172.20.20.2	

Будемо вважати, що ПК 1 (PC 0) і ПК 2 (PC 1) знаходяться в VLAN 1 з адресацією 192.168.1.0 /24, ПК 3 (PC 2) і ПК 4 (PC 3) в VLAN 2 з адресацією 172.20.20.0 /24. Потрібно задати IP адреси комп'ютерів в Cisco Packet Tracer (для цього необхідно двічі клацнути лівою кнопкою миші по іконці комп'ютера в робочій області). Повинно відкритися вікно налаштування хоста, представлене нижче на рис. 3.3

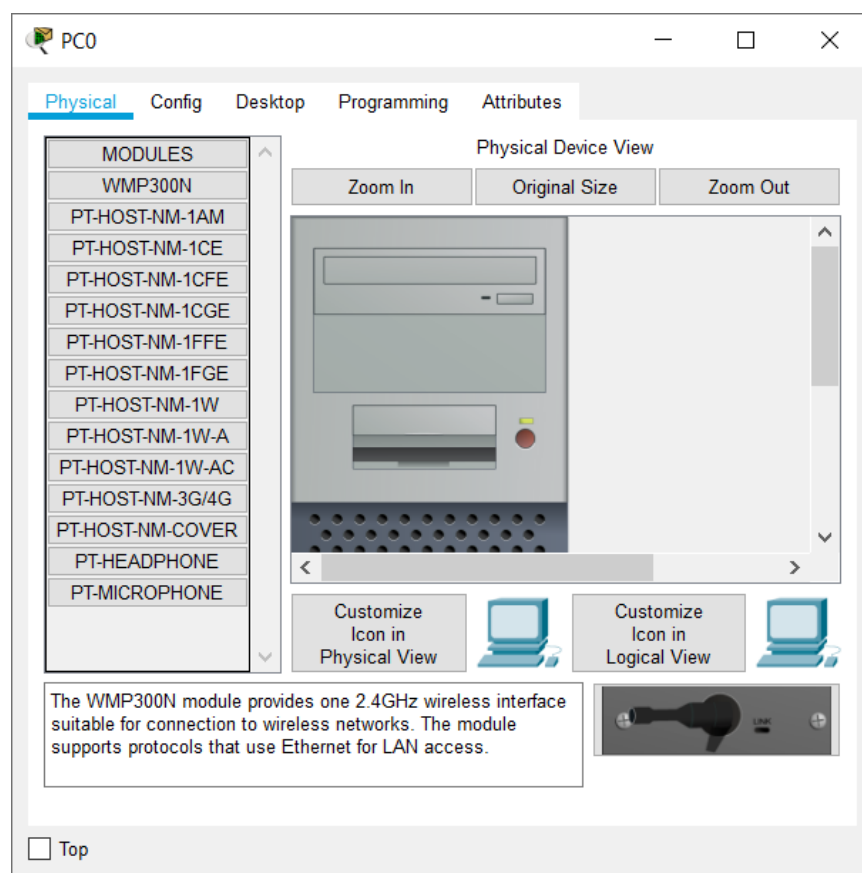


Рисунок 3.3 – Вікно налаштування хоста в Cisco Packet Tracer

Далі, потрібно перейти до вкладки Desktop, рис. 3.4

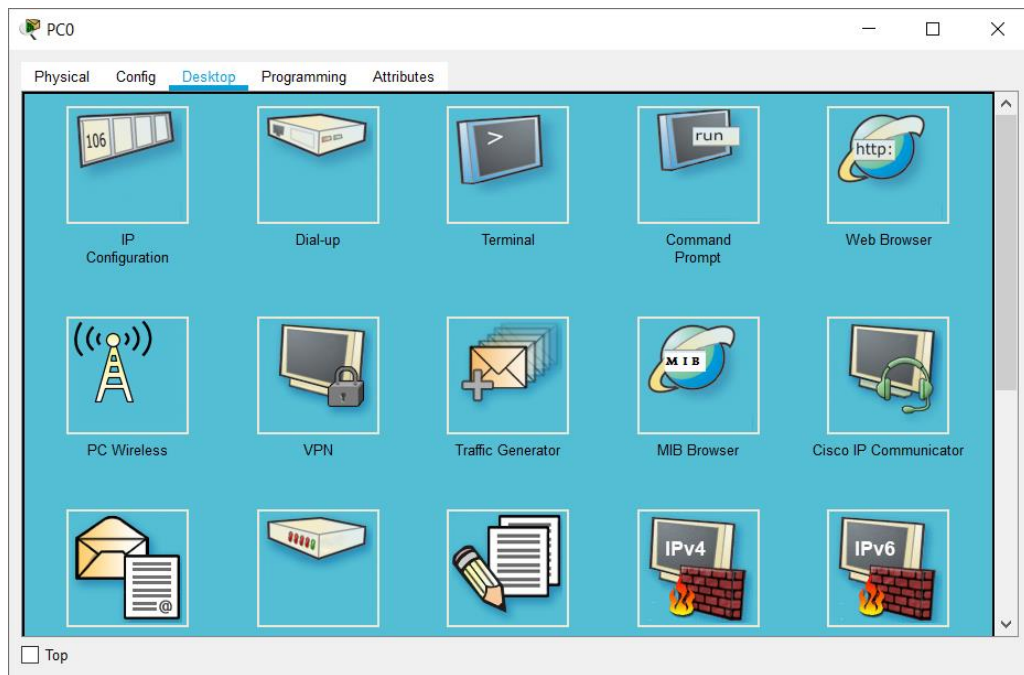


Рисунок 3.4 – Вкладки Desktop в ПЗ Cisco Packet Tracer

Клацнути на значок (іконку) IP Configuration (рис. 3.5)

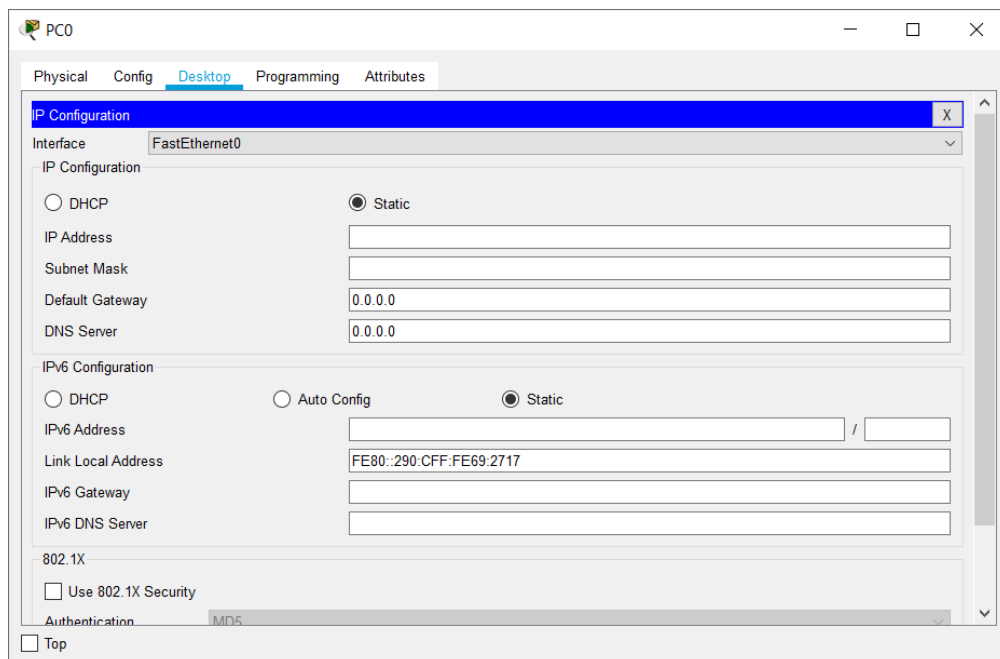


Рисунок 3.5 – Вікно конфігурації IP-адреси хоста



Потрібно переконаватися, що radiobutton знаходиться в положення **Static**. В поле IP Address введіть IP адресу комп'ютера PC0 – 192.168.1.1, в полі Subnet Mask введіть його маску – 255.255.255.0 (див.рис. 3.6)

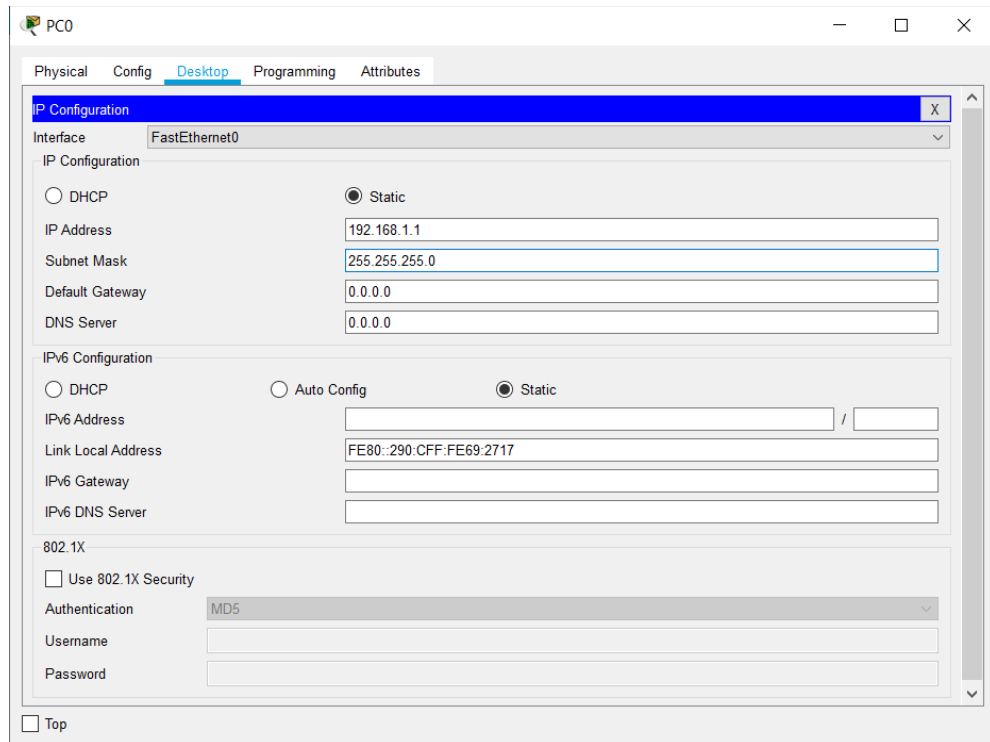


Рисунок 3.6 – Задання IP-адреси та маски підмережі в Cisco Packet Tracer

Після цього потрібно закрити вікно налаштувань даного хоста і аналогічним чином налаштувати ті, які залишилися – 3. Задати їм такі IP адреси: PC1 – 192.168.1.2/24, PC2 – 172.20.20.1/24, PC3 – 172.20.20.2/24.

Далі перевірити, як застосувалися введені налаштування (для цього знову двічі клацнути лівою кнопкою миші по одному із хостів, наприклад по PC0. У вікні вибрати пункт **Command Prompt** – потрапляємо у вікно консолі даного комп'ютера (дана дія аналогічно тому, якби виконувалося Пуск-Виконати-cmd на реальному комп'ютері)).

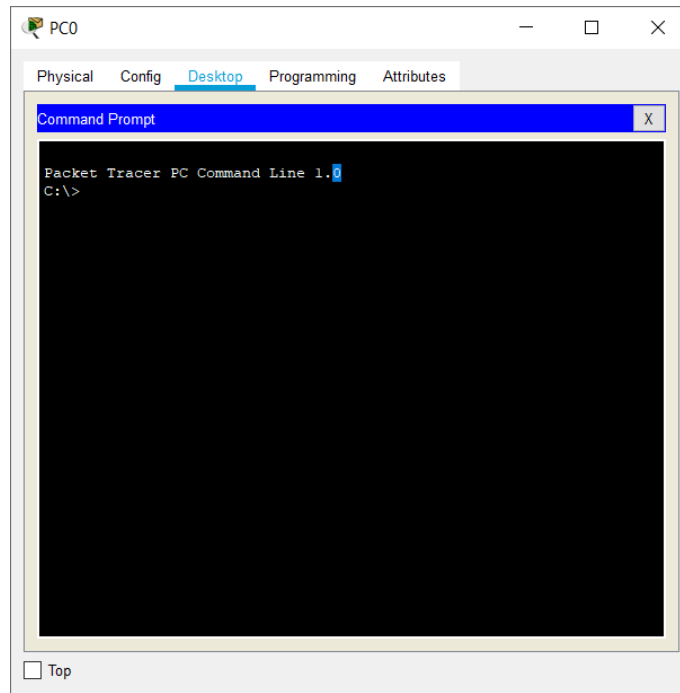


Рисунок 3.7 – Командний рядок в Packet Tracer

Для перевірки конфігурації хоста PC0 виконати команду **ipconfig**. Результат виконання команди на рисунку 3.8. При бажанні можна виконати аналогічну перевірку на інших хостах.

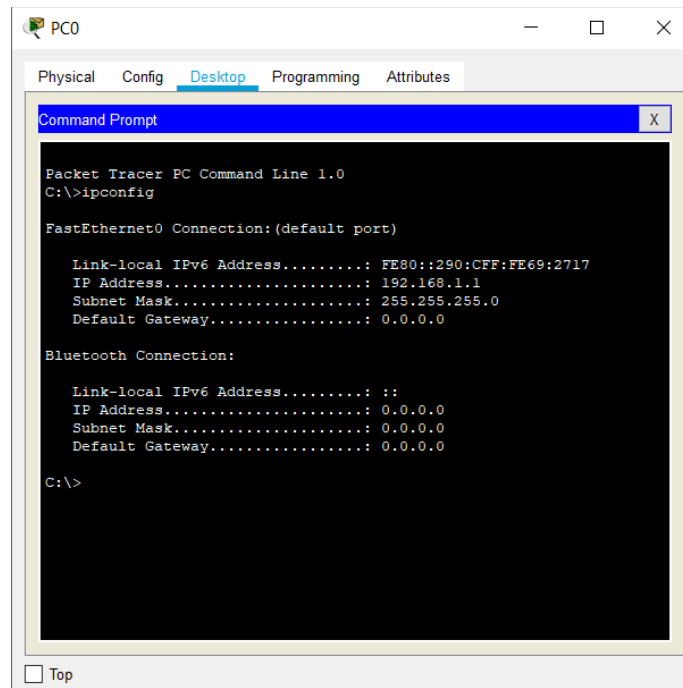


Рисунок 3.8 – Перевірка конфігурації хостів рядок

Перевірити зв'язність мережі, яку отримали. Для цього пропінгувати з PC0 комп'ютер PC1. З рис. 3.9 видно, що пінг успішно проходять.

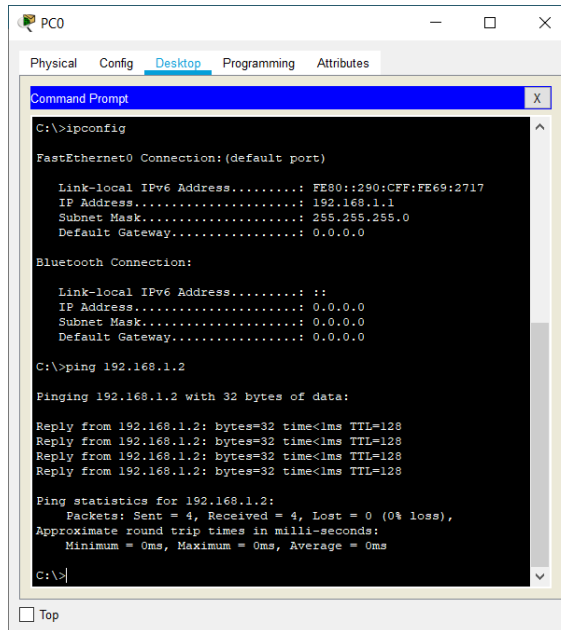


Рисунок 3.9 – Комп'ютер PC1 доступний в PC0

Далі спробуємо пропінгувати з PC0 комп'ютер PC2. Як видно на рис. 3.10 пінг не відбувається.

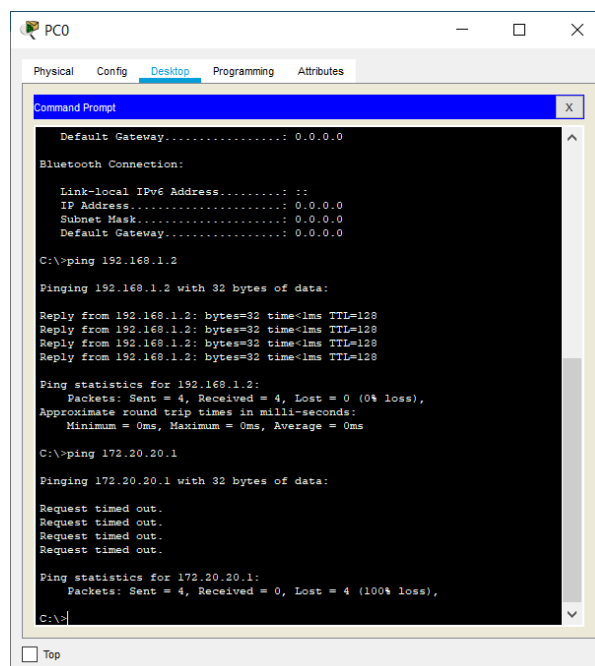


Рисунок 3.10 – Комп'ютер PC2 не доступний в PC0

Хоча в даному випадку всі чотири комп'ютери знаходяться в одному VLAN (за замовчуванням всі порти комутатора знаходяться в VLAN 1), всі вони не можуть бачити один одного, так як знаходяться в різних підмережах. Комп'ютери PC0 і PC1 знаходяться в підмережі 192.168.1.0, а комп'ютери PC2 і PC3 в підмережі 172.20.20.0.

VLAN потрібні для того щоб структурувати мережі на комутаторі і навести в них порядок, а також для того щоб було можливо здійснювати маршрутизацію між ними, адже здійснити маршрутизацію між мережами в тій конфігурації яку, на даний момент, отримали в Packet Tracer буде досить важко.

Далі необхідно перейти до налаштування комутатора. Для цього, відкрити його консоль (для того щоб це виконати в Packet Tracer двічі клацніть лівою кнопкою миші по комутатора в робочій області) рис. 3.11.

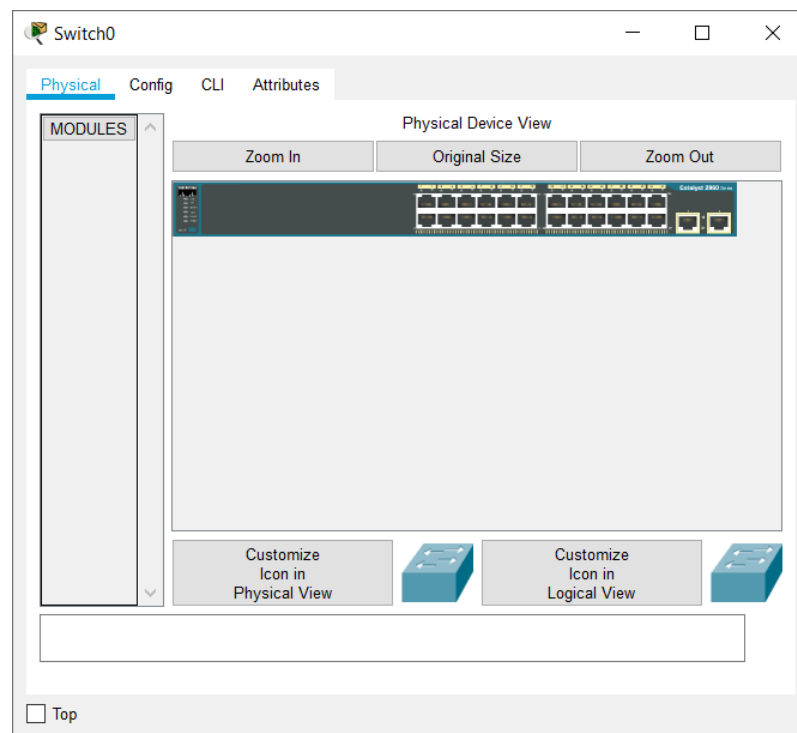


Рисунок 3.11 – Вікно налаштувань комутатора в Packet Tracer

У вікні, перейти на вкладку **CLI**, де буде вікно консолі. Натиснути Enter щоб приступити до введення команд. Інформація, яка в даний момент відображена на консолі, свідчить про те що інтерфейси FastEthernet0/1 –

FastEthernet0/4 успішно піднялися (тобто тепер вони знаходяться в робочому стані) див.рис. 3.12.

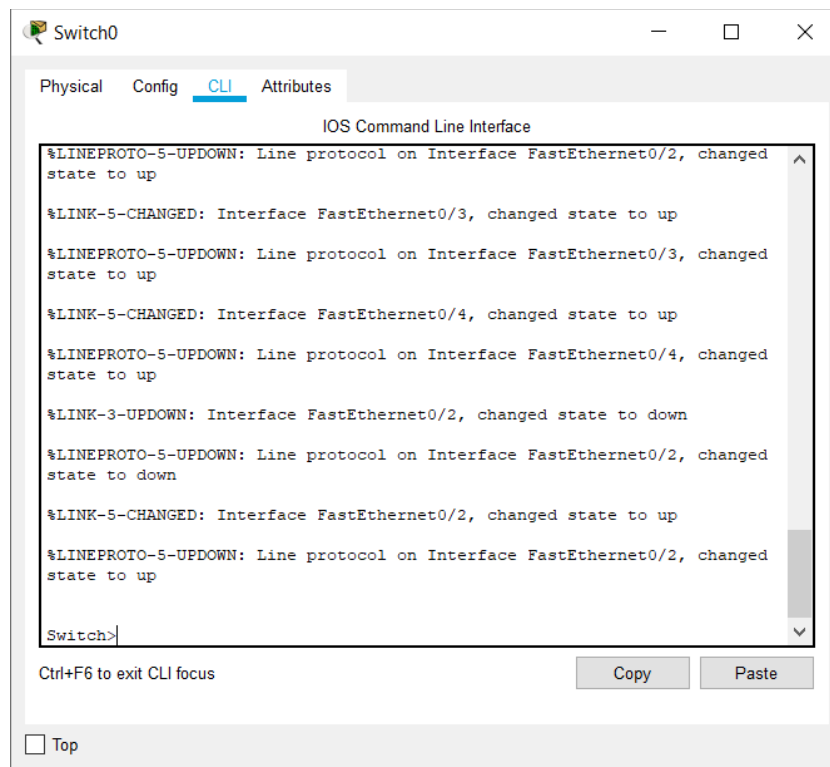


Рисунок 3.12 – Вікно консолі комутатора в Packet Tracer

Далі перейти в привілейований режим виконавши команду **enable**. Переглянути інформацію про існуючі на комутаторі VLAN-ах для цього виконати команду **show vlan brief** (можна просто **sh vl br**)

В результаті виконання команди на екрані з'явиться: номера vlan – перший стовпець, назва vlan – другий стовпець, стан vlan (працює він в даний момент чи ні) – третій стовпець, порти належать до даного vlan – четвертий стовпець. За замовчуванням на комутаторі існує п'ять VLAN-ів. Всі порти комутатора за замовчуванням належать VLAN 1. Решта чотири VLAN є службовими і використовуються не дуже часто (рис. 3.13).

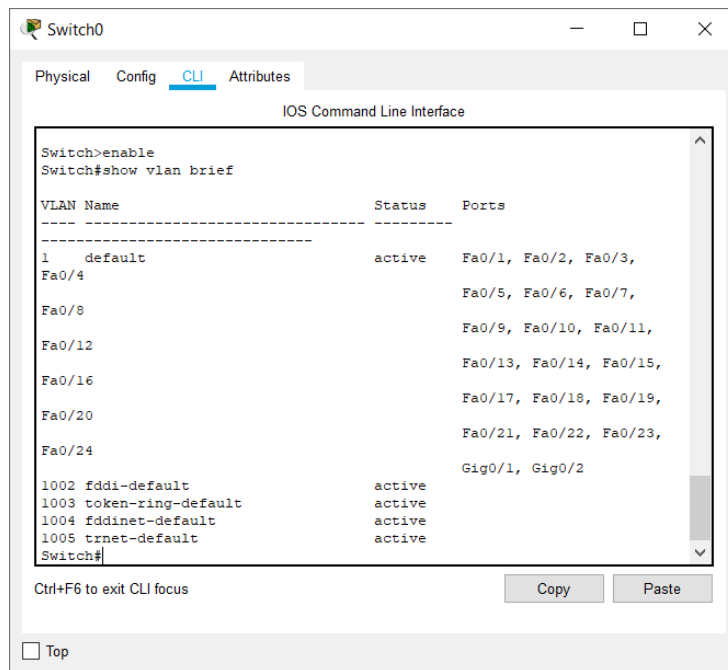


Рисунок 3.13 – Вікно команди show vlan brief в Packet Tracer

Для реалізації мережі, яка представлена на рис.5.1 необхідно, створити на комутаторі ще два VLAN. Для цього в привілейованому режимі виконати команду **config t** для переходу в режим конфігурації. Ввести команду **vlan 2** (даною командою ви створите на комутаторі vlan з номером 2). Показчик введення Switch (config) # зміниться на Switch (config-vlan) # це свідчить про те, що далі конфігуруватися буде не весь комутатор в цілому, а лише окремий VLAN, в даному випадку vlan номер 2.

Якщо використовувати команду «**vlan x**», де **x** номер VLAN, коли VLAN **x** – ще не створений на комутаторі, то він буде автоматично створений і відразу здійснюється перехід до його конфігурації. При перебуванні в режимі конфігурації VLAN, можлива зміна параметрів обраної віртуальної мережі, наприклад можна змінити її ім'я за допомогою команди **name**.

Для досягнення поставленої в даній лабораторній роботі завдання, треба зконфігурувати vlan 2 наступним чином:

- командою **vlan 2**, створюється на комутаторі новий vlan з номером 2  
*Switch (config) #vlan 2*

2. Команда **name subnet\_192** привласнює ім'я subnet\_192 віртуальної мережі номер 2

*Switch (config-vlan) #name subnet\_192*

3. Виконуючи команду **interface range fastEthernet 0/1-2** здійснюється перехід до конфігурації інтерфейсів fastEthernet 0/1 і fastEthernet 0/2 комутатора

*Switch (config) #interface range fastEthernet 0/1-2*

Ключове слово **range** в даній команді, вказує на те, що конфігурується не один єдиний порт, а цілий діапазон портів, в принципі її можна не використовувати, але тоді пункти 3 – 5 необхідно замінити на:

*Switch (config) #interface fastEthernet 0/1*

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

*Switch (config-if) #switchport access vlan 2*

*Switch (config) #interface fastEthernet 0/2*

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

*Switch (config-if) #switchport access vlan 2*

4. Команда **switchport mode access** конфігурує обраний порт комутатора, як порт доступу (access port)

*Switch (config-if-range) #switchport mode access*

5. Команда **switchport access vlan 2** вказує, що даний порт є портом доступу для vlan номер 2

*Switch (config-if-range) #switchport access vlan 2*

Для того, щоб переглянути результат конфігурації варто виконати команду **show vlan br** рис. 3.14:

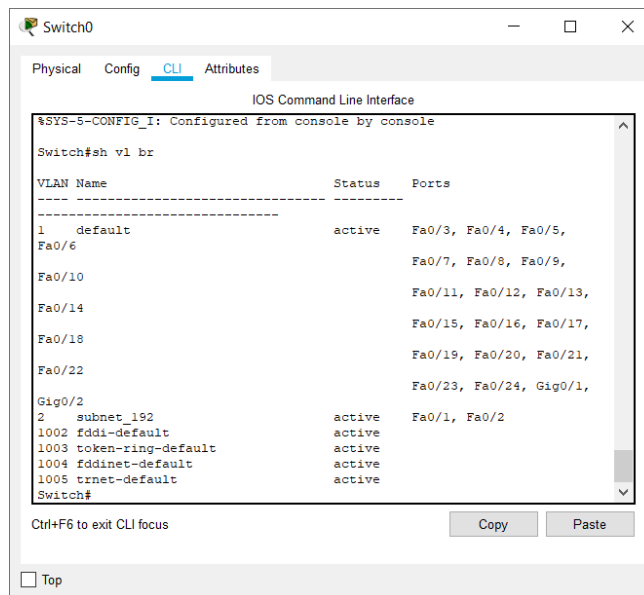


Рисунок 3.14 – Виконання команди show vlan br

З результату виконання даної команди представлено на рис. 3.14 видно, що на комутаторі з'явився ще один vlan з номером 2 і ім'ям subnet\_192, портами доступу якого є fastEthernet 0/1 і fastEthernet 0/2.

Далі аналогічним чином необхідно створити vlan 3 з ім'ям subnet\_172, і зробимо його портами доступу інтерфейси fastEthernet 0/3 і fastEthernet 0/4. Результат повинен вийти наступним (див.рис.5.15):

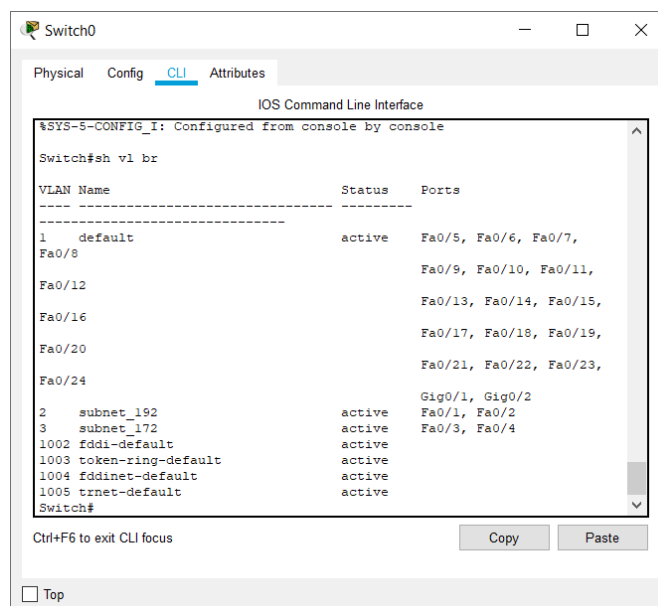


Рисунок 3.15 – Конфігурація VLAN на комутаторі Cisco



Наша мережа вже налаштована, залишилося лише її протестувати. Для цього, варто перейти в консоль комп'ютера PC0. Пропінгувати з нього інші 3 комп'ютери мережі.

Комп'ютер PC1 доступний, а комп'ютери PC2 і PC3 як і раніше не доступні – нічого не змінилося.

Для того, щоб переконатися та впевнитися, що конфігурація vlan дійсно працює – задамо комп'ютерам PC2 і PC3 IP адреси з мережі 192.168.1.0/24. Наприклад 192.168.1.3 і 192.168.1.4.

Після чого повторити спробу, пропінгувати з комп'ютера PC0 інші комп'ютери мережі. Як можна побачити нічого не змінилося, хоча всі чотири комп'ютера теоретично повинні знаходитися в одній підмережі 192.168.1.0/24 і бачити один одного, на практиці вони знаходяться в різних віртуальних локальних мережах і тому не можуть взаємодіяти між собою.

Якщо є бажання перевірити це ще раз, то можна перейти на комп'ютер PC 2 і пропінгувати інші комп'ютери. Доступним буде тільки PC3, так як вони разом знаходяться в одному vlan номер 3.

#### **4. Варіанти індивідуальних завдань для самостійної роботи**

1. Отримати у викладача варіант і розрахувати кількість підмереж згідно з даними табл. 3.2.

2. Побудувати схему мережі згідно результатів попереднього розрахунку.

3. Зконфігурувати стек протоколів кожного вузла мережі.

4. Задати ім'я комутатора, пароль на привілейований режим конфігурування, зберегти зміни у файлі стартової конфігурації.

5. За результатами роботи оформити звіт для другої частини.

Таблиця 3.2 – Варіанти завдання для виконання лабораторної роботи 3

Варіант	Кількість VLAN комутаторів	Кількість хостів в підмережі	IP-адреса	Маска
1	2	4	193.160.224.146, ... 178.136.197.66, ...	/24
2	2	3	213.200.38.11, ... 194.48.209.191, ...	/24
3	2	5	176.119.77.78, ... 212.178.13.87, ...	/24
4	2	3	185.6.187.200, ... 178.17.167.180, ...	/24
5	2	4	192.16.70.53, ... 178.133.91.122, ...	/24
6	2	4	188.163.100.96, ... 196.168.77.87, ...	/24
7	2	5	192.168.151.53, ... 178.136.197.66, ...	/24
8	2	3	181.191.106.32, ... 200.59.216.180, ...	/24
9	2	3	195.254.184.60, ... 212.22.94.36, ...	/24
10	2	4	217.117.77.54, ... 192.141.52.42, ...	/24
11	2	5	223.29.216.124, ... 178.151.88.22, ...	/24
12	2	3	194.187.48.30, ... 167.249.247.126, ...	/24

## 5. Контрольні питання

1. Що таке VLAN?
2. Яка команда привласнює ім'я створеному vlan?
3. Яка команда конфігурує обраний порт комутатора, як порт доступу?
4. Використання якого ключового слова, вказує на те, що конфігурується цілий діапазон портів, а не один єдиний порт?
5. Яка команда вказує, що даний порт є портом доступу для конкретного vlan?

## **6. Перелік літератури**

### **Основна література**

1. Кузніченко С.Д. «Комп'ютерні мережі» Конспект лекцій. – Одеса: ОДЕКУ, 2018.– 175 с.
2. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: «Магнолія 2006», 2012.– 262с.
3. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. – К.:Київ ун-т ім. Б.Грінченка, 2011. – 291 с.

### **Додаткова література**

1. Настройка VLAN в Cisco. URL: <https://linkas.ru/articles/vlan-v-cisco/>
2. Настройка VLAN на Cisco. URL: <https://network.msk.ru/blog/nastroyka-vlan-cisco>
3. Виртуальная реальность или что такое VLAN. URL : <http://www.netza.ru/2012/10/vlan-cisco-1.html>

## **7. Правила техніки безпеки та охорони праці**

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

## **8. Оформлення та захист звіту**

Звіт готується в електронному вигляді і роздруковується. Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Титульна сторінка :
  - Найменування лабораторної роботи.
  - Відомості про виконавця, номер варіанту.

2. Мета роботи та завдання до лабораторної роботи.
3. Таблицю розрахованих адрес підмереж.
4. Виконання *практичної частини лабораторної роботи* (п.3.1).  
Скріншот логічної структури мережі.
5. Лістинг команд конфігурування комутатора в Cisco IOS (з файлу \*.txt)
6. Лістинг командного рядка (CLI).
7. Опис та Скріншот виконання кожного з етапів.
8. Виконання *практичної частини лабораторної роботи згідно варіанту* (п.4)
9. Лістинг команд конфігурування комутатора в Cisco IOS (з файлу \*.txt)
10. Лістинг командного рядка (CLI).
11. Опис та Скріншот виконання кожного з етапів.
12. Висновок за результатами роботи.
13. Контрольні питання та відповіді на них.

## **ЛАБОРАТОРНА РОБОТА № 4**

### ***Конфігурування маршрутизаторів Cisco***

#### **1. Мета роботи**

**Метою лабораторної роботи** є ознайомлення студентів з прийомами роботи з мережною операційною системою Cisco IOS та отримання навичок конфігурування комутаційного обладнання та маршрутизаторів Cisco.

#### **2. Теоретичні відомості до лабораторної роботи**

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Фізична і логічна структуризація мережі за допомогою різних типів комунікаційного обладнання” і „Принципи роботи маршрутизаторів”. Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

##### **2.1 Конфігурування комутаторів і маршрутизаторів з командного рядка операційної системи IOS**

Розглянемо більш детально на прикладі конфігурування комутаторів і маршрутизаторів використання команд командного рядка операційної системи IOS.

При першому вході в мережевий пристрій користувач бачить командний рядок режиму користувача виду:

```
Switch>
```

Команди, доступні в режимі користувача є підмножиною команд, що доступні в привілейованому режимі. Ці команди дозволяють виводити на екран інформацію без зміни установок мереженого пристрою.

Щоб отримати доступ до повного набору команд, необхідно спочатку активізувати привілейований режим.

```
Press ENTER to start.  
Switch>  
Switch>enable  
Switch#  
Switch#disable  
Switch>
```

Тут і далі виведення мережевого пристрою буде даватися звичайним шрифтом, а виведення користувача **жирним** шрифтом.

Про перехід у цей режим буде свідчити поява в командному рядку запрошення у виді знака #. З привілейованого рівня можна отримати інформацію про настройки системи і отримати доступ до режиму глобального конфігурування і інших спеціальних режимів конфігурування, включаючи режими конфігурування інтерфейсу, підінтерфейсу, лінії, мережевого пристрою, карти маршрутів і т.п. Для виходу з системи IOS необхідно набрати на клавіатурі команду exit (вихід).

```
Switch>exit
```

Незалежно від того, як звертаються до мережевого пристрою: через консоль термінальної програми, що приєднана через ноль-модем до COM-порту мережевого пристрою, або в рамках сеансу протоколу Telnet, пристрій можна перевести в один з режимів. Нас цікавлять такі режими.

Режим користувача – це режим перегляду, в якому користувач може тільки переглядати певну інформацію про мережевий пристрій, але не може нічого змінювати. В цьому режимі запрошення має вигляд типу Switch>.

Привілейований режим – підтримує команди настройки і тестування, детальну перевірку мережевого пристрою, маніпуляцію з конфігураційними файлами і доступ в режим конфігурування. В цьому режимі запрошення має вигляд типу Switch#.

Команди в будь-якому режимі IOS розпізнає за першими унікальними символами. При натисненні табуляції IOS сам доповнить команду до повного імені.

При введенні в командному рядку будь-якого режиму імені команди і знака питання (?) на екран виводяться коментарі до команди. При введенні одного знака результатом буде список всіх команд режиму. На екран може виводиться багато екранів рядків, тому іноді знизу екрана буде з'являтися підказка – More -. Для продовження слід натиснути enter або пробіл.

Команди режиму глобального конфігурування визначають поведінку системи в цілому. Крім того, команди режиму глобального конфігурування включають команди переходу в інші режими конфігурування, які використовуються для створення конфігурацій, що потребують багаторядкових команд. Для входу в режим глобального конфігурування використовується команда привілейованого режиму `configure`. При введенні цієї команди слід вказати джерело команд конфігурування: `terminal` (термінал), `memory` (енергонезалежна пам'ять або файл), `network` (сервер `tftp` (Trivial ftp – спрощений ftp) в мережі). За замовчуванням команди вводяться з терміналу консолі. Наприклад

```
Switch# configure terminal
Switch(config)#(commands)
Switch(config)#exit
Switch#
```

Команди для активізації частинного виду конфігурації повинні передувати командам глобального конфігурування. Так для конфігурації інтерфейсу, на можливість якої вказує запрошення `Switch(config-if)#`, спочатку вводиться глобальна команда для визначення типу інтерфейсу і номер його порту:

```
Switch# conf t
Switch(config)# interface type port
Switch(config-if)# (commands)
Switch(config-if)# exit
Switch(config)# exit
```

Для обмеження доступу до системи використовуються паролі. Команда **line console** встановлює пароль на вхід на термінал консолі:

```
Switch(config)# line console 0
Switch(config-line)# login
```

```
Switch(config-line)# password Cisco
```

Команда **line vty 0 4** встановлює парольний захист на вхід за протоколом Telnet:

```
Switch(config)# line vty 0 4
Switch(config-line)# login
Switch(config-line)# password cisco
```

Команда **enable password** обмежує доступ до привілейованого режиму:

```
Switch#conf t
Switch(config)# enable password пароль
```

Далее

```
Ctrl-Z
```

```
Switch#ex
```

...

Press RETURN to get started

```
Switch>en
```

```
Password: пароль
```

```
Switch#
```

Тут пароль **пароль** – послідовність латинських символів.

Для встановлення на мережевому інтерфейсі IP адреси використовується команда:

```
Router(config-if)#ip address [ip-address][subnet-mask],
Router(config-if)#no shut
```

Команда `no shut` (скорочення від `no shutdown`) використовується для того, щоб інтерфейс був активним (без цієї команди можливе довільне тимчасове відключення інтерфейсу). Зворотна команда – `shut`, вимкне інтерфейс.

Важливо мати можливість контролю вірності функціонування і стану мережевого пристрою в будь-який момент часу. Для цього служать команди:

Таблиця 4.1 – Show команди

Команда	Опис
<code>show version</code>	Виводить на екран дані про конфігурації апаратної частини системи, версії програмного забезпечення, імена і джерела файлів конфігурування і завантажені образи
<code>show running-config</code>	Показує зміст активної конфігурації



show interfaces	Показує дані про всі інтерфейси на пристроях
show protocols	Виводить дані про протоколи третього мережевого рівня.

### 3. Порядок проведення лабораторної роботи

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Виконати в Packet Tracer практичну частину лабораторної роботи.
4. Отримати у викладача варіант і виконати в Packet Tracer завдання для самостійної роботи.
5. Продемонструвати викладачу результати виконання завдання для самостійної роботи. Показати звіт про виконання команди ping з будь-якого комп'ютера на інший.
6. Оформити звіт.
7. Захистити звіт.

#### 3.1 Практична частина лабораторної роботи

Реалізуємо поділ мережі на підмережі використовуючи програму Packet Tracer. Нехай адміністратор виконав розбиття мережі 192.168.8.0/24 на 6 підмереж. Використовуючи адреси 4-х перших підмереж, представимо їх логічну структуру за допомогою програми. Адреси підмереж наведені в табл. 4.2.

Таблиця 4.2 – Адреси підмереж

Адреса мережі	Широкомовний адрес	Адреси хостів
192.168.8.32	192.168.8.63	<b>від</b> 192.168.8.33 <b>до</b> 192.168.8.62
192.168.8.64	192.168.8.95	<b>від</b> 192.168.8.65 <b>до</b> 192.168.8.94
192.168.8.96	192.168.8.127	<b>від</b> 192.168.8.97 <b>до</b> 192.168.8.126
192.168.8.128	192.168.8.159	<b>від</b> 192.168.8.129 <b>до</b> 192.168.8.158

1. Побудуємо мережу з 4-ма підмережами (див. рис. 4.1). Використовуйте модель маршрутизатора за замовчуванням – Generic.
2. Сконфігуруємо стек протоколів кожного вузла мережі відповідно з даними табл.4.3.
3. Здійснімо тестування мережі, використовуючи команду ping.

Таблиця 4.3 – Параметри стеку TCP/IP для вузлів мережі

Пристрій	IP-адреса	Маска	Шлюз
PC1	192.168.8.33	255.255.255.224	192.168.8.62
PC2	192.168.8.65	255.255.255.224	192.168.8.94
PC3	192.168.8.97	255.255.255.224	192.168.8.126
PC4	192.168.8.129	255.255.255.224	192.168.8.158
Server1	213.33.168.60	255.255.255.0	213.33.168.254
Router0(порт 0/0)	192.168.8.62	255.255.255.224	
Router0(порт 1/0)	192.168.8.94	255.255.255.224	
Router0(порт 6/0)	192.168.8.126	255.255.255.224	
Router0(порт 7/0)	192.168.8.158	255.255.255.224	
Router0(порт 8/0)	213.33.168.254	255.255.255.0	

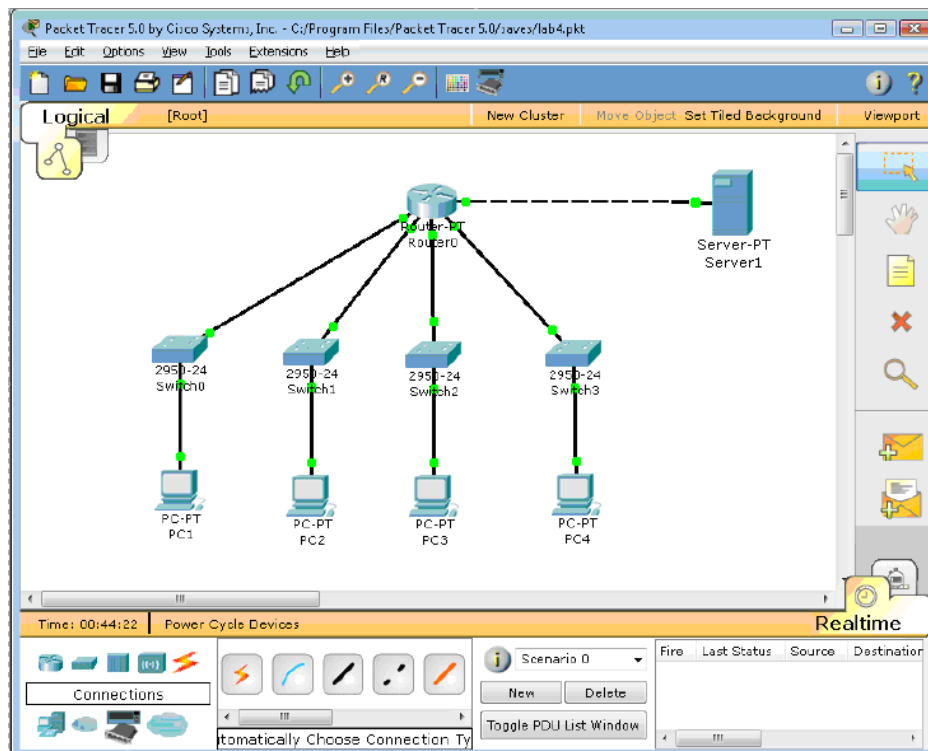


Рисунок 4.1 – Конфігурація мережі з 4-ма підмережами

Нижче приведений порядок конфігурування маршрутизатора за допомогою CLI Cisco IOS.

1. Для вибору мережевого пристрою Router0 натисніть в робочій області програми на його зображення. Відкриється вікно налаштувань мережевого пристрою. Вибираємо вкладку CLI для керування маршрутизатором.

2. В середині екрану ви побачите:

Continue with configuration dialog? [yes/no]:

Введіть “no” і натисніть клавішу <Enter>.

З’явиться запрошення виду:

Router>

Це означає, що ви підключені до мережевого пристрою і знаходитесь в командному рядку режиму користувача. Тут “Router” – це імя мережевого пристрою, а “>” позначає режим користувача.

3. Далі введіть команду enable, щоб потрапити в привілейований режим.

```
Router> enable
```

```
Router#
```

4. Перегляньте список доступних команд в привілейованому режимі:

```
Router#?
```

5. Перейдемо в режим конфігурації:

```
Router# config terminal
```

```
Router(config)#
```

6. Ім'я хосту мережевого пристрою використовується для локальної ідентифікації. Коли ви входите до мережевого пристрою, ви бачите ім'я хосту перед символом режиму (“>” або “#”). Це ім'я може бути використано для визначення місця знаходження. Встановіть “ Router0” как ім'я вашого мереженого пристрою.

```
Router(config)# hostname Router0
```

```
Router0(config)#
```

7. Пароль доступу дозволяє контролювати доступ в привілейованому режимі. Це дуже важливий пароль, тому що в привілейованому режимі можна вносити зміни в конфігурації пристрою. Встановіть пароль доступу “cisco”

```
Router0(config)#enable password cisco
```

8. Випробуємо цей пароль. Вийдіть з мережевого пристрою і спробуйте зайти в привілейований режим:

```
Router0>en
```

```
Password:*****
```

```
Router0#
```

Тут знаки: \*\*\*\*\* - це ваш введений пароль. Ці знаки на екрані не видно.

### 3.1.1 Основні Show команди

Перейдіть до контексту користувача командою disable. Введіть команду для перегляду всіх доступних show команд.

```
Router0>show ?
```

1. Команда show version використовується для отримання типу платформи мережевого пристрою, версії операційної системи, імені файла

образу операційної системи, часу роботи системи, об'єму пам'яті, кількості інтерфейсів і реєстру конфігурації.

2. Можна побачити часи

```
Router0>show clock
```

3. В флеш-пам'яті мережевого пристрою зберігається файл-образ операційної системи Cisco IOS. На відміну від операційної пам'яті, в реальних устаткуваннях флеш-пам'ять зберігає файл-образ навіть при перебої живлення.

```
Router0>show flash
```

4. Інтерфейс командного рядка мереженого пристрою за замовчуванням зберігає 10 останніх введених команд

```
Router0>show history
```

5. Дві команди дозволяють повернутися до команд, що були введені раніше. Натисніть на стрілку вгору або <ctrl>P.

6. Дві команди дозволяють перейти до наступної команди, яка зберігається в буфері. Натисніть на стрілку вниз або <ctrl>N.

7. Можна побачити список хостів і IP-адреси всіх їх інтерфейсів:

```
Router0>show hosts
```

8. Наступна команда виводить детальну інформацію про кожний інтерфейс:

```
Router0>show interfaces
```

9. Команда

```
Router0>show sessions
```

Виведе інформацію про кожну telnet сесію.

10. Команда

```
Router0>show terminal
```

показує параметри конфігурації терміналу.

11. Список всіх користувачів, приєднаних до пристрою по термінальних лініях можна побачити, використовуючи команду:

```
Router0>show users
```

12. Команда

```
Router0>show controllers
```

показує стан контролерів інтерфейсів.

13. Перейдемо до привілейованого режиму

```
Router0>en
```

14. Введіть команд для перегляду всіх доступних show команд.

```
Router0# show ?
```

Привілейований режим включає до себе всі show команди контексту користувача і ряд нових.

15. Подивимося активну конфігурацію в пам'яті мереженого пристрою.

```
Router0# show running-config
```

Активна конфігурація автоматично не зберігається і буде втрачена в разі перебою живлення. Для продовження перегляду наступної сторінки конфігурації натисніть на клавішу пробіл.

16. Наступна команда дозволяє переглянути поточний стан протоколів третього рівня

```
Router0# show protocols
```

### 3.1.2 Конфігурація інтерфейсів

Розглянемо команди, які дозволяють вмикати (піднімати) інтерфейси мережевого пристрою та переводити їх в стан UP.

1. На мережевому пристрої Router0 увійдемо в контекст конфігурації

```
Router0#conf t
```

```
Router0(config)#
```

2. Щоб настроїти Ethernet інтерфейс, треба зайти в контекст конфігурації інтерфейсу:

```
Router0(config)#interface FastEthernet 0/0
```

```
Router0(config-if)#
```

3. Переглянемо усі доступні в цьому контексті команди

```
Router0(config-if)#?
```

Для виходу в контекст глобальної конфігурації наберіть exit. Знову увійдіть в контекст конфігурації інтерфейсу:

```
Router0(config)#int fa0/0
```

Ми використали скорочене ім'я інтерфейсу.

4. Встановимо IP адресу Ethernet інтерфейсу

```
Router0(config-if)#ip address 192.168.8.62 255.255.255.224
```

5. Увімкнемо цей інтерфейс

```
Router0(config-if)#no shutdown
```

6. Додамо до інтерфейсу опис:

```
Router0(config-if)#description Ethernet interface on Router 0
```

Щоб побачити опис цього інтерфейсу, перейдіть в привілейований режим і виконайте команду show interface.

```
Router0(config-if)#end
```

```
Router0# show interface
```

7. Після того, як виконано конфігурування усіх інтерфейсів можна переглянути активну конфігурацію пристрою і переконатися, що з'явилися призначені IP - адреси

```
Router0# show running-config
```

8. Перегляньте детальну IP інформацію про кожний інтерфейс та переконайтеся, що інтерфейси, що були сконфігуровані, перейшли до стану UP

```
Router0# show ip interface
```

Коротку інформацію можна отримати командою **show ip interface brief**

```
Router0# show ip in bri
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	194.138.33.62	YES	manual	up	up
FastEthernet1/0	194.138.33.94	YES	manual	up	up
Serial2/0	unassigned	YES	unset administratively	down	down
Serial3/0	unassigned	YES	unset administratively	down	down
FastEthernet4/0	unassigned	YES	unset	down	down
FastEthernet5/0	unassigned	YES	unset administratively	down	down
FastEthernet6/0	194.138.33.126	YES	manual	up	up
FastEthernet7/0	194.138.33.158	YES	manual	up	up
FastEthernet8/0	213.33.168.254	YES	manual	up	up
FastEthernet9/0	unassigned	YES	unset administratively	down	down

#### 4. Варіанти індивідуальних завдань для самостійної роботи

1. Отримати у викладача варіант і розрахувати кількість підмереж згідно з даними табл.4.4.
2. Побудувати схему мережі згідно результатів попереднього розрахунку.
3. Сконфігурувати стек протоколів кожного вузла мережі.
4. Задати ім'я маршрутизатора, пароль на привілейований режим конфігурування, зберегти зміни у файлі стартової конфігурації.
5. За результатами роботи оформити звіт для другої частини.

Таблиця 4.4 – Варіанти завдання до другої частини лабораторної роботи

Варіант	IP-адреса	Маска	Завдання
1	194.138.33.0	/24	Розбити мережу на 4 підмережі
2	192.168.45.0	/24	Розбити мережу на 3 підмережі
3	82.207.118.0	/24	Розбити мережу на 5 підмережі
4	113.45.25.0	/24	Розбити мережу на 6 підмережі
5	164.34.24.0	/24	Розбити мережу на 5 підмережі
6	155.150.100.0	/24	Розбити мережу на 4 підмережі
7	164.90.34.0	/24	Розбити мережу на 3 підмережі
8	197.230.100.0	/24	Розбити мережу на 5 підмережі
9	87.217.118.0	/24	Розбити мережу на 6 підмережі
10	182.207.120.0	/24	Розбити мережу на 4 підмережі
11	105.23.47.0	/24	Розбити мережу на 6 підмережі
12	97.13.45.0	/24	Розбити мережу на 3 підмережі

#### 5. Контрольні питання

1. Які є контексти вводу команд в командному рядку?



2. Як перемикається між контекстами вводу команд в командному рядку?
3. Яку роль виконує клавіша табуляції при вводі команд?
4. Як увійти до режиму глобальної конфігурації, активізувати частинний вигляд конфігурації та вийти з цих режимів?
5. Як орієнтуватися в командах, що були введені раніше, і повторювати їх?
6. Як задати ім'я хоста?
7. Яку інформацію можна переглянути командами show в контексті користувача?
8. Яку інформацію можна переоглянути командами show в привілейованому режимі, але неможна переглянути в режимі користувача?
9. Як підняти інтерфейс і визначити його стан?
10. Як призначити IP адресу на інтерфейсі і переконатися, що вона призначена?
11. Яка команда задає пароль на конфігурацію мережевого пристрою?

## **6. Перелік літератури**

### **Основна література**

1. Кузніченко С.Д. «Комп'ютерні мережі» Конспект лекцій. – Одеса: ОДЕКУ, 2018.– 175 с.
2. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: «Магнолія 2006», 2012.– 262с.
3. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. – К.:Київ ун-т ім. Б.Грінченка, 2011. – 291 с.

### **Додаткова література**

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб.: Питер, 2010. – 944 с.: ил.

2. Коломоец Г.П. Организация компьютерных сетей: учебное пособие. Запорожье: КПУ– 156 с.

3. Кравец, О.Я. Практикум по вычислительным сетям и телекоммуникациям : учебное пособие / О. Я. Кравец. – Изд. 2-е, перераб. и доп. – Воронеж: Научная книга, 2006. – 156 с.

## **7. Правила техніки безпеки та охорони праці**

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

## **8. Оформлення та захист звіту**

Звіт готується в електронному вигляді і роздруковується. Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Титульна сторінка :
  - Найменування лабораторної роботи.
  - Відомості про виконавця, номер варіанту.
2. Мета роботи та завдання до лабораторної роботи.
3. Виконання *практичної частини лабораторної роботи* (п.3.1).
4. Таблицю розрахованих адрес підмереж.
  - 5. Опис побудови топології та приведення результатів виконання роботи (Скріншот логічної структури мережі).
6. Таблицю з параметрами стеку TCP/IP для вузлів мережі.
7. Лістинг команд конфігурування маршрутизатора в Cisco IOS (з файлу \*.txt).
8. Скріншот виконання команди `show ip interface brief`.
9. Скріншот виконання команди `ping` між будь-якими двома вузлами мережі
10. Скріншот завантаження HTTP сторінки на будь-який вузол з серверу.
  - 11. Виконання практичної частини лабораторної роботи згідно варіанту (п.4)
12. Таблицю розрахованих адрес підмереж.
  - 13. Опис побудови топології та приведення результатів виконання роботи (Скріншот логічної структури мережі).
14. Таблицю з параметрами стеку TCP/IP для вузлів мережі.

15. Лістинг команд конфігурування маршрутизатора в Cisco IOS (з файлу \*.txt).
16. Скріншот виконання команди `show ip interface brief`.
17. Скріншот виконання команди `ping` між будь-якими двома вузлами мережі
18. Скріншот завантаження HTTP сторінки на будь-який вузол з серверу.
19. Висновок за результатами роботи.
20. Контрольні питання та відповіді на них.

## ЛАБОРАТОРНА РОБОТА № 5

### *З'єднання з мережевими пристроями Cisco.*

#### *Статична маршрутизація*

### 1. Мета роботи

**Метою лабораторної роботи** є ознайомлення студентів з прийомами роботи з мережною операційною системою Cisco IOS та отримання навичок налаштування статичної маршрутизації на маршрутизаторах Cisco.

### 2. Теоретичні відомості до лабораторної роботи

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Принципи роботи маршрутизаторів” і „Статична і динамічна маршрутизація”. Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

#### 2.1 Cisco Discovery Protocol (CDP)

CDP дозволяє пристроям обмінюватися основною інформацією конфігурування. CDP буде працювати без настройки будь-якого протоколу. За замовчуванням CDP включений на всіх інтерфейсах. CDP працює на другому (канальному) рівні моделі OSI, тому він не є маршрутизованим протоколом і працює тільки з безпосередньо підключеними пристроями. Протокол CDP зв'язує фізичне середовище передачі даних більш низького рівня з протоколами більш високого мережевого рівня, тому пристрої, що підтримують різні протоколи третього рівня, можуть впізнавати один одного.

Під час запуску пристрою протокол CDP запускається автоматично. Після цього він може автоматично визначити сусідні пристрої, на яких також

виконується протокол CDP. Серед знайдених пристроїв будуть не тільки ті, які працюють з протоколом IP.

CDP дозволяє адміністраторам мати доступ до даних про інший мережевий пристрій, до якого є безпосереднє з'єднання.

Для виводу інформації про сусідні пристрої, що виявлені за протоколом CDP, використовується сімейство команд **show cdp**. Воно виводить наступні дані по кожному порту і кожному пристрою, що з'єднаний з ним: ідентифікатори пристроїв, список адрес, ідентифікатор порту, перелік функціональних можливостей, апаратну платформу пристрою.

## 2.2 Команди ping і traceroute

Для діагностики можливості встановлення зв'язку в мережах використовуються протоколи типу запит-відповідь або протокол луна-пакетів. Результати роботи такого протоколу можуть допомогти в оцінці надійності путі до іншого пристрою, величин затримок в цілому і між проміжними пристроями. Для того щоб така команда працювала, необхідно, щоб не тільки локальний мережевий пристрій знав як потрапити до пункту призначення, але і щоб пристрій в пункті призначення знав, як дістатися до джерела.

Команда ping посилає ICMP(Internet Control Message Protocol) луна-пакети для верифікації з'єднання. У наведеному нижче прикладі час проходження одного луна-пакету перевищило заданий, про що свідчить точка (.) в інформації, що виведена, а чотири пакета пройшли успішно, про що свідчить знак оклику (!).

```
Switch> ping 172.16.101.1
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2
seconds:
.!!!!
Success rate is 80 percent, round-trip min/avg/max = 6/6/6
ms
```

Таблиця 5.1 – Результати команди ping

Символ	Значення
!	Успішний прийом луна-відповіді
.	Перевищений час очікування
U	Пункт призначення недосяжний
C	Перевантаження мережі
I	Виконання команди перервано адміністратором
?	Невідомий тип пакету
&	Пакет перевищив значення параметру часу життя TTL пакету

Команди traceroute показує адреси проміжних інтерфейсів (хопов) на шляху пакетів в пункт призначення.

```
Switch> traceroute 172.16.101.1
```

Розширена версія команди ping підтримується тільки в привілейованому режимі (контекст адміністратора). Для того, щоб увійти в розширений режим, необхідно в рядку підказки до Extended commands ввести букву «у» (Yes).

Команда в режимі діалогу опитує значення параметрів. Важливо відмітити, що ця команда дозволяє, знаходячись на одному пристрої, перевіряти зв'язок між мережевими інтерфейсами на інших пристроях.

```
Router# ping
Protocol [ip]:
Target IP address: 2.2.2.0
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Sweep range of sizes [n]:
```

### 2.3 Команда telnet

Протокол віртуального терміналу telnet, що входить до складу протоколів TCP/IP, дозволяє встановити з'єднання між мережевим пристроєм telnet клієнта і мережевим пристроєм telnet сервера, що забезпечує можливість роботи в режимі віртуального терміналу. Telnet використовується для віддаленого керування мережевим пристроєм або для перевірки зв'язку на рівні додатків. Успішне встановлене telnet – з'єднання дозволяє керувати віддаленим пристроєм так, наче ви знаходитесь за його консоллю. Мережеві пристрої Cisco здібні підтримувати одночасно до п'яти вхідних сеансів протоколу telnet.

## 2.4 Маршрутизація

Протоколи маршрутизації – це правила за якими здійснюється обмін інформації про шляхи передачі пакетів між маршрутизаторами. Протоколи характеризуються часом збіжності, втратами і масштабіруемістю. В даний час використовується декілька протоколів маршрутизації. Кожний протокол має свої достоїнства і недоліки.

Одна з головних задач маршрутизатора полягає в визначенні найкращого шляху до заданого адресата. Маршрутизатор визначає шляхи (маршрути) до адресатів або із статичної конфігурації, введеної адміністратором, або динамічно на основі маршрутної інформації, отриманої від інших маршрутизаторів. Маршрутизатори обмінюються маршрутною інформацією за допомогою протоколів маршрутизації. Маршрутизатор зберігає таблиці маршрутів в оперативній пам'яті. Таблиця маршрутів – це список найкращих відомих доступних маршрутів. Маршрутизатор використовує цю таблицю для прийняття рішення, куди направляти пакет. Для перегляду таблиці маршрутів слід використовувати команду **show ip route**. Навіть, якщо на якомусь маршрутизаторі X не задавались ніякі команди маршрутизації, тоді він все одно буде таблицю маршрутів для безпосередньо приєднаних до нього мереж, наприклад:

...

```
C 192.168.4.0/24 is directly connected, Ethernet0
10.0.0.0/16 is subnetted, 3 subnets
C 10.3.0.0 is directly connected, Serial0
C 10.4.0.0 is directly connected, Serial1
C 10.4.0.0 is directly connected, Ethernet1
```

Маршрут на безпосередньо приєднані мережі відображається на інтерфейс маршрутизатора, до якого вони приєднані. Тут /24 позначає маску 255.255.255.0, а /16 – 255.255.0.0.

Таблиця маршрутів відображає мережеві префікси (адреси мереж) на вихідні інтерфейси. Коли X одержує пакет, призначений для 192.168.4.46, він шукає префікс 192.168.4.0/24 в таблиці маршрутів. Згідно таблиці пакет буде направлений на інтерфейс Ethernet0. Якщо X отримує пакет для 10.3.21.5 он направить його на Serial0.

Ця таблиця показує чотири маршруту для безпосередньо приєднаних мереж. Вони мають мітку C. Маршрутизатор X відкидає всі пакети, що спрямовані до мереж, які не вказані в таблиці маршрутів. Для спрямування пакетів до інших адресатів необхідно в таблицю включити додаткові маршрути. Нові маршрути можуть бути додані двома методами:

Статична маршрутизація – адміністратор вручну визначає маршрути до мереж призначення.

Динамічна маршрутизація – маршрутизатори дотримуються правил, що визначаються протоколами маршрутизації, для обміну інформацією про маршрути і вибору найкращого шляху.

Статичні маршрути не змінюються самим маршрутизатором. Динамічні маршрути змінюються самим маршрутизатором автоматично при отриманні інформації про зміну маршрутів від сусідніх маршрутизаторів. Статична маршрутизація споживає мало обчислювальних ресурсів і корисна в мережах, які не мають декілька шляхів до адресату призначення. Якщо від маршрутизатора до маршрутизатора є тільки один шлях, то часто використовують статичну маршрутизацію.

Для конфігурації статичної маршрутизації Cisco використовують дві версії команди ip route



Перша версія

**ip route АдресаМережіПризначення МаскаМережіПризначення Інтерфес**

Команда вказує маршрутизатору, що всі пакети, які призначені для АдресаМережіПризначення-МаскаМережіПризначення слід направляти на свій інтерфейс Інтерфес. Якщо інтерфейс Інтерфес – типа Ethernet, то фізичні (MAC) адреси вихідних пакетів будуть широкомовними.

Друга версія

**ip route АдресаМережіПризначення МаскаМережіПризначення Адреса**

Команда вказує маршрутизатору, що всі пакети, які призначені для АдресаМережіПризначення-МаскаМережіПризначення, слід направляти на той свій інтерфейс, з якого досяжна IP адреса Адреса. Як правило, **Адреса** це адреса наступного хопу по шляху до АдресаМережіПризначення. Вихідний інтерфейс і фізичні адреси вихідних пакетів визначаються маршрутизатором за своїми ARP таблицями на підставі IP адрес Адреса. Наприклад

```
ip route 10.6.0.0 255.255.0.0 serial1 (1)  
ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2)
```

Перший приклад відображає мережевий префікс 10.6.0.0/16 на локальний інтерфейс маршрутизатора Serial1. Наступний приклад відображає мережевий префікс 10.7.0.0/16 на IP адресу 10.4.0.2 наступного хопу по шляху до 10.7.0.0/16. Обидві ці команди додадуть статичні маршрути в таблицю маршрутизації (мітка S):

```
S 10.6.0.0 via serial1  
S 10.7.0.0 [1/0] via 10.4.0.2
```

Коли інтерфейс падає, всі статичні маршрути, що відображаються на цей інтерфейс, видаляються з таблиці маршрутов. Якщо маршрутизатор не може більше знайти адресу наступного хопу по шляху до адреси, вказаної в статичному маршруті, то маршрут виключається з таблиці.

Зауважимо, що для мереж типа Ethernet рекомендується завжди використовувати формулу (2) команди ip route. Ethernet інтерфейс на маршрутизаторі, як правило, з'єднаний з декількома Ethernet інтерфейсами інших пристроїв в мережі. Вказівка в команді ip route IP адреси дозволить маршрутизатору вірно сформувати фізичну адресу вихідного пакету по своїм ARP таблицям.

## 2.5 Маршрутизація за замовчуванням

Зовсім не обов'язково, щоб кожний маршрутизатор обслуговував маршрути до всіх можливих мереж призначення. Замість цього маршрутизатор зберігає маршрут за замовчуванням або шлюз останнього пристановища (last resort). Маршрут за замовчуванням використовується, коли маршрутизатор не може поставити у відповідність мережі призначення рядок в таблиці маршрутів. Маршрутизатор повинен використовувати маршрут за замовчуванням для відсилання пакетів іншому маршрутизатору. Наступний маршрутизатор буде мати маршрут до цієї мережі призначення або мати свій маршрут за замовчуванням до третього маршрутизатора і т.д. В кінцевому рахунку, пакет буде маршрутизований на маршрутизатор, який має маршрут до мережі призначення.

Маршрут за замовчуванням може бути статично введений адміністратором або динамічно отриманий з протоколу маршрутизації.

Так як всі IP адреси належать мережі 0.0.0.0 з маскою 0.0.0.0, то в найпростішому випадку треба використовувати команду

```
ip route 0.0.0.0 0.0.0.0 [адреса наступного хопу | вихідний  
інтерфейс]
```

Ручне завдання маршруту за замовчуванням на кожному маршрутизаторі підходить для простих мереж. В складних мережах необхідно організувати динамічний обмін маршрутами за замовчуванням.

## 2.6 Інтерфейс петля

На мережевих пристроях можна створювати інтерфейси не зв'язані з реальними каналами для передачі даних і призначати на них IP адреси з масками. Такі інтерфейси називають петлями (loopback). Це чисто програмний інтерфейс, який тільки емулює роботу фізичного інтерфейсу. Він може використовуватися для віддаленого адміністрування і його функціонування не буде залежати від стану фізичних інтерфейсів, він буде завжди піднятий і доступний для будь-яких сесій. Петлі корисні при поетапному проектуванні мереж. Якщо до якогось реального мережевого інтерфейсу маршрутизатора в подальшому буде приєднана підмережа, то з початку на маршрутизаторі створюється loopback, налаштовується в плані взаємодії з іншими ділянками мережі і лише потім змінюється на реальний інтерфейс. Інтерфейс петля з'являється після команди `interface loopbackN` або скорочено `int IN`, де N ціле невід'ємне число – номер петлі.

Наприклад

```
Router(config)# int loopback 10  
Router(config-if)#ip address 1.1.1.1 255.0.0.0
```

## 2.7 Команда trace

Команда `trace` є ідеальним засобом для з'ясування того, куди відправляються дані в мережі. Ця команда використовує ту ж технологію протоколу ICMP, що і команда `ping`, тільки замість перевірки наскрізного зв'язку між відправником і одержувачем, вона перевіряє кожний крок на шляху. Команда `trace` використовує здатність маршрутизаторів генерувати повідомлення про помилки при перевищенні пакетом свого встановленого часу життя (Time To Live, TTL). Ця команда посилає декілька пакетів і виводить на екран дані про час проходження туди і назад для кожного з них. Перевага команді `trace` полягає в тому, що вона показує черговий досягнутий

маршрутизатор на шляху до пункту призначення. Це дуже потужний засіб для локалізації відмов на шляху від відправника до одержувача.

Таблиця 5.2 – Варіанти відповідей утиліти trace

Символ	Значення
<b>!H</b>	Зондуєчий пакет був прийнятий маршрутизатором, але не переадресований, що звичайно буває через список доступу
<b>R</b>	Протокол недосяжний
<b>N</b>	Мережа недосяжна
<b>U</b>	Порт недосяжний
<b>*</b>	Перевищення межі очікування

### 3. Порядок проведення лабораторної роботи

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Виконати в Packet Tracer практичну частину лабораторної роботи.
4. Отримати у викладача варіант і виконати в Packet Tracer завдання для самостійної роботи.
5. Продемонструвати викладачу результати виконання пунктів 8 і 9 завдання для самостійної роботи.
6. Оформити звіт.
7. Захистити звіт.

#### 3.1 Практична частина лабораторної роботи

1. Створіть в Packet Tracer топологію, зображену на рис.2.1 з використанням моделі маршрутизатора за замовчуванням – Generic. Назвіть пристрої так, як на схемі: Router 1, Router 2 і Router 4.

Чорна лінія означає Ethernet з'єднання. Червона – послідовне з'єднання. Для створення послідовного з'єднання обираємо послідовне з'єднання точка-точка (serial cable). Обираємо другий пристрій. Визначаємо,

який маршрутизатор буде виконувати функції DCE пристрою. Цій пристрій задає синхронізацію. В емуляторі для нього необхідно буде визначити частоту синхронізації.

Збережіть топологію.

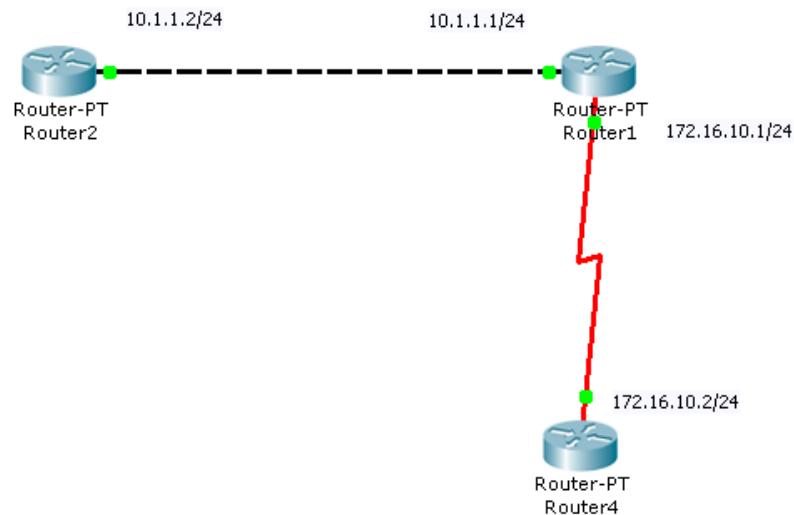


Рисунок 5.1 – Топологія мережі для моделювання

2. Командою `hostname` змініть імена маршрутизаторів. Задайте конфігурацію їх інтерфейсів відповідно з рисунком. Увімкніть інтерфейси. Конфігурацію послідовних інтерфейсів виконайте в наступній послідовності:

2.1 Зайдемо на Router1. Перевіримо, яким пристроєм виступає маршрутизатор для послідовної лінії зв'язку: кінцевим пристроєм DTE (data terminal equipment) або пристроєм зв'язку DCE (data circuit).

```
Router1#show controllers s2/0
```

Якщо бачити - **....DCE cable....** - , то цей маршрутизатор є пристроєм зв'язку і він повинен задавати частоту синхронізації тактових імпульсів, що використовуються при передачі даних. Частота обирається з певного ряду частот.

```
Router1#conf t
Router1(config)#int s2/0
Router1(config-if)#clock rate ?
Обираємо частоту 64000
```

```
Router1(config-if)#clock rate 64000
```

і підіймаємо інтерфейс

```
Router1(config-if)#no shut
```

2.2 Перейдемо до маршрутизатора Router 4. Піднімімо на ньому інтерфейс serial2/0. Коли інтерфейси на двох кінцях послідовного з'єднання включені, на екрані з'явиться повідомлення про зміну стану інтерфейсу на активний.

2.3 Перевіримо на кожному пристрої, що інтерфейси, які були сконфігуровані, знаходяться в стані UP.

```
Router1#sh int s2/0
Router1#sh int fa0/0
Router2#sh int fa0/0
Router4#sh int s2/0
```

3. На кожному пристрої подивіться вашу активну конфігурацію і переконайтеся, що там з'явилися призначені IP адреси.

```
Router1#show running-config
Router2#show running-config
Router4#show running-config
```

4. Подивіться детальну IP інформацію про кожний інтерфейс і переконайтеся, що інтерфейси, які були сконфігуровані, перейшли у стан UP

```
Router1#show ip interface
Router2#show ip interface
Router4#show ip interface
```

5. Скорочену інформацію можна отримати командою **show ip interface brief**

```
Router1#show ip in bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.1.1.1 YES manual up up
FastEthernet1/0 unassigned YES unset administratively down down
Serial2/0 172.16.10.1 YES manual up up
```

```

Serial3/0 unassigned YES unset administratively down down
FastEthernet4/0 unassigned YES unset administratively down down
FastEthernet5/0 unassigned YES unset administratively down down
Router2#show ip in bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.1.1.2 YES manual up up
FastEthernet1/0 unassigned YES unset administratively down down
Serial2/0 unassigned YES unset administratively down down
Serial3/0 unassigned YES unset administratively down down
FastEthernet4/0 unassigned YES unset administratively down down
FastEthernet5/0 unassigned YES unset administratively down down
Router4#show ip in bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
FastEthernet1/0 unassigned YES unset administratively down down
Serial2/0 172.16.10.2 YES manual up up
Serial3/0 unassigned YES unset administratively down down
FastEthernet4/0 unassigned YES unset administratively down down
FastEthernet5/0 unassigned YES unset administratively down down

```

## 2.8.1 Протокол CDP

1. На маршрутизаторі Router1 введемо команду для виводу стану всіх інтерфейсів на яких працює CDP.

```
Router1#show cdp interface
```

Треба переконатися, що обидва інтерфейсу підняти і посилають CDP пакети.

```

FastEthernet0/0 is up, line protocol is up
Sending CDP packets every 60 seconds
holdtime is 180 seconds
Serial2/0 is up, line protocol is up
Sending CDP packets every 60 seconds
holdtime is 180 seconds

```

2. Переконавшись, що мережевий пристрій посилає і одержує CDP-оновлення, можемо використовувати CDP для отримання інформації про безпосередньо підключені пристрої. Введіть команду

```

Router1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source
Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Router2 Fas 0/0 121 R PT1000 Fas 0/0
Router4 Ser 2/0 129 R PT1000 Ser 2/0

```

Як можна побачити, маршрутизатор Router1 з'єднаний з інтерфейсом Fas 0/0 (**Port ID**) маршрутизатора (**Capability**) Router2 (**Device ID**) серії 1000 (**Platform**) через інтерфейс Fas 0/0 (**Local Intrfce**) і з інтерфейсом Ser 2/0 маршрутизатора Router4 серії 1000 через інтерфейс Ser 2/0.

4. На Router1 введіть команду для більш детальної інформації про сусідів

```
Router1#show cdp neighbors detail
```

Ця команда показує по одному пристрою за раз. Вона використовується для відображення адресної інформації мережевого рівня. В даний момент цей рівень у нас не налаштований, тому поле Entry address(es) порожнє. Команда також виводить інформацію про версію IOS.

4. На Router1 введіть команду, щоб дізнатися інформацію про пристрій Router 4

```
Router1#show cdp entry Router4
```

Ця команда дає ту ж саму інформацію що і show cdp neighbors detail, але для одного конкретного пристрою. Пам'ятайте, що імена хостів чутливі до регістру.

5. На пристрої Router1 введіть команду, щоб побачити, як часто Router1 посилає сусідам оновлення CDP і як довго у сусідів вони повинні зберігатися.

```

Router1#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds

```



Sending CDPv2 advertisements is enabled

Для економії смуги пропускання низько швидкісних пристроїв CDP можна відключити

```
Router1(config)# no cdp run
```

і знову вимкнути для усього пристрою

```
Router1(config)# cdp run
```

6. Іноді необхідно відключити CDP для певного інтерфейсу, наприклад при його вузькій смуги пропускання або в цілях безпеки. На пристрої Router1 відключити CDP на інтерфейсі FastEthernet 0/0.

```
Router1(config)#interface fa0/0
```

```
Router1(config-if)#no cdp enable
```

```
Router1(config)#Ctrl-Z
```

```
Router1(config)#show cdp interface
```

В отриманому виводі ви не побачите відомостей про FastEthernet 0/0.

## 2.8.2 Команди ping і traceroute

1. Підключимося до пристрою Router1. Пропінгуємо безпосередньо приєднаний інтерфейс FastEthernet 0/0 на пристрої Router2

```
Router1#ping 10.1.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/28/32 ms
```

Спробуємо пропінгувати інтерфейс Serial 2/0 на пристрої Router4

```
Router1#ping 172.16.10.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
```

Успішно.

2. Перейдемо на Router2. Спробуйте пропінгувати адрес 10.1.1.1 безпосередньо приєднаного FastEthernet 0/0 інтерфейсу на пристрої Router1. Успішно.

Перейдемо на Router4. Спробуйте пропінгувати адрес 172.16.10.1 безпосередньо приєднаного інтерфейсу Serial 2/0 на пристрої Router1. Успішно.

Спробуємо пропінгувати інтерфейс FastEthernet 0/0 на пристрої Router1:

```
Router4#ping 10.1.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

Невдача.

Спробуємо пропінгувати адресу 10.1.1.2 FastEthernet 0/0 інтерфейсу на пристрої Router2. Невдача.

3. Повернемося на Router2. Спробуємо пропінгувати адресу 172.16.10.1 інтерфейсу Serial 2/0 на пристрої Router1. Невдача. Спробуємо пропінгувати адресу 172.16.10.2 інтерфейсу Serial 2/0 на пристрої Router4. Невдача.

Невдачі спіткали нас тому, що ми не налаштували на маршрутизаторах маршрутизацію!

4. Зайдіть на пристрій Router1. Визначте шляхи проходження пакетів на Router2

```
Router1# traceroute 10.1.1.2
```

```
і Router4
```

```
Router1# traceroute 172.16.10.2
```

Ви повинні побачити по одному хопу.

5. Виконайте команду розширеного пінга від адреси 10.1.1.2 до адреси 172.16.10.2

```
Router1#ping
...
Target IP address: 172.16.10.2
...
Extended commands [n]: y
Source address: 10.1.1.2
...
```

### 2.8.3 Telnet

Будьте уважні: емулятор має обмежену підтримку telnet.

1. Увійдіть на пристрій Router1. Нам необхідно, щоб мережений пристрій приймав telnet-сесії і був захищений паролем. Кожна так звана лінія в мережевому пристрої потенційно представляє активну telnet-сесію, яку пристрій може підтримувати. Наші мережеві пристрої підтримують до 5 ліній, призначені на віртуальні термінали vty. Ми використовуємо всі 5 ліній

```
Router1(config)#line vty 0 4
Router1(config-line)#
```

2. Далі повідомимо мережевому пристрою, що нам знадобиться пароль входу в систему.

```
Router1(config-line)#login
Router1(config-line)#password parol
```

3. Увійдемо на пристрій Router2 і встановимо telnet – з'єднання з пристроєм Router1. Для цього ми використовуємо IP адресу його інтерфейсу FastEthernet 0/0

```
Router2#telnet 10.1.1.1
```

4. Ми побачимо запрошення ввести пароль. Введіть пароль parol і натисніть <enter>. Зауважте, що ім'я мережевого пристрою змінилося на Router1, тому що ми встановили telnet – з'єднання з Router1. Команда

```
Router1>show user
* 67 vty 0 idle 00:00:00 10.1.1.2
```

покаже, що з'єднання здійснено від адреси 10.1.1.2 пристрою Router2.

На секунду натисніть одночасно клавіші <Ctrl>+<Shift>+6, потім відпустить і зразу натисніть клавішу x. Ім'я мережевого пристрою змінилося знову на Router2. Тобто зараз ми на пристрої Router2.

```
Router1#<Ctrl>+<Shift>+<6> потім x
Router2#
```

5. Введіть команду show sessions. Це дозволить побачити всі активні telnet – сесії. Щоб відновити telnet – сесію визначте номер сесії, яку ви хочете відновити (у нашому випадку є тільки одна з номером 1) і введіть команду resume 1.

```
Router2#show sessions
Conn Host Address Byte Idle Conn Name
* 1 10.1.1.1 10.1.1.1 0 1 10.1.1.1
Router2#resume 1
Router1#
```

6. Ім'я хоста знову змінилося на Router1. Натисніть комбінацію <Ctrl>+<Shift>+<6> і клавішу x, щоб повернутися назад на Router2.

```
Router1#<Ctrl>+<Shift>+<6> потім x
Router2#
```

7. Закрийте сесію

```
Router2#disconnect 1
Closing connection to 10.1.1.1 [confirm]
```

## 2.8.4 Протокол ARP

1. Приєднайтеся до маршрутизатора Router1 і подивіться його ARP таблицю

```
Router1#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.1 - 0002.4AD6.5391 ARPA FastEthernet0/0
```

Вона містить тільки один рядок про MAC адресу свого Ethernet інтерфейсу з IP адресою 10.1.1.1.

2. Приєднайтеся до маршрутизатора Router2 і подивіться його ARP таблицю. Вона містить тільки один рядок про MAC адресу свого Ethernet інтерфейсу з IP адресою 10.1.1.2

```
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.2 - 0001.C779.8AB5 ARPA FastEthernet0/0
```

3. Пропінгуйте Ethernet інтерфейс маршрутизатора Router1

```
Router2# ping 10.1.1.1
```

4. Знову подивіться ARP таблицю. Вона містить вже два рядка. З'явився запис про MAC адресу Ethernet інтерфейсу Router1 з IP адресою 10.1.1.1.

```
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.1 2 0002.4AD6.5391 ARPA FastEthernet0/0
Internet 10.1.1.2 - 0001.C779.8AB5 ARPA FastEthernet0/0
```

5. Приєднайтеся до маршрутизатора Router2 і подивіться його ARP таблицю. Вона містить вже два рядки

```
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.1 - 0002.4AD6.5391 ARPA FastEthernet0/0
Internet 10.1.1.2 4 0001.C779.8AB5 ARPA FastEthernet0/0
```

З'явився запис про MAC адресу Ethernet інтерфейсу маршрутизатора Router2 з IP адресою 10.1.1.2. Чому, адже ми не слали від Router1 ніяких IP пакетів? Тому що Router1 для відповіді на пінг від Router2 повинен був знати про MAC адресу Ethernet інтерфейсу маршрутизатора Router2 з IP адресою 10.1.1.2, і він сформував ARP пакет для його отримання.

## 2.8.5 Статичні маршрути

Раніше ми не могли з маршрутизаторів Router2 і Router4 пропінговати деякі інтерфейси через відсутність маршрутизації. виправимо це.

1. Приєднайтеся до маршрутизатора Router2. Ми не могли пінговати адреси 172.16.10.1 і 172.16.10.2. Подивіться таблицю маршрутизації.

```
Router2#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,  
B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS  
inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

Ми бачимо безпосередньо приєднані мережі. Нема маршруту до мережі 172.16.10.0/24. Додамо маршрут до мережі 172.16.10.0/24 через адресу 10.1.1.1 найближчого хопу на шляху до цієї мережі:

```
Router2(config)#ip route 172.16.10.0 255.255.255.0 10.1.1.1
```

Тут і далі 172.16.10.0/24 – це скорочений запис – визначення підмережі 172.16.10.0 з маскою 255.255.255.0. У масці 255.255.255.0 міститься 24 одиниці, що і позначається /24.

2. Успішно пропінгуємо Serial інтерфейс Router1

```
Router2#ping 172.16.10.1
```

Знову подивимося таблицю маршрутів

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

172.16.0.0/24 is subnetted, 1 subnets

S 172.16.10.0 [1/0] via 10.1.1.1

3. Але ми не зможемо пропінгувати Serial інтерфейс Router4

```
Router2#ping 172.16.10.2
```

Чому? Тому що ICMP пакети пінгів не знають, як їм повернутися назад від Router4, оскільки на Router4 не прописані маршрути.

4. Приєднайтеся до маршрутизатора Router4. Подивіться таблицю маршрутів

```
Router4#show ip route
```

```
172.16.0.0/24 is subnetted, 1 subnets
с 172.16.10.0 is directly connected, Serial2/0
```

Нема маршруту до мережі 10.1.1.0/24. Додамо маршрут до мережі 10.1.1.0/24 через адресу 172.16.10.1 найближчого хопа на шляху до цієї мережі:

```
Router4(config)#ip route 10.1.1.0 255.255.255.0 172.16.10.1
```

Знову подивимося таблицю маршрутів

```
10.0.0.0/24 is subnetted, 1 subnets
s 10.1.1.0 [1/0] via 172.16.10.1
172.16.0.0/24 is subnetted, 1 subnets
с 172.16.10.0 is directly connected, Serial2/0
```

5. Зараз всі мережеві інтерфейси в мережі пінгуються з кожного мережевого пристрою. Перевірте це.

## 2.8.6 Маршрутизація за замовчуванням

Мережеві пристрої Router2 і Router4 мають тільки по одному виходу у зовнішній світ: через інтерфейси з адресами 10.1.1.1 і 172.16.10.1, відповідно. Тому можна не визначати на які підмережі ми маршрутизуємо пакети і використовувати маршрутизацію за замовчуванням.

1. Спочатку видалимо старі маршрути

```
Router2(config)#no ip route 172.16.10.0 255.255.255.0 10.1.1.1
Router4(config)# no ip route 10.1.1.0 255.255.255.0 172.16.10.1
```

2. Далі призначимо маршрути за замовчуванням

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
Router4(config)# ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

3. Подивіться таблицю маршрутів на всіх пристроях.

```
Router2#sh ip route
```

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
с 10.1.1.0 is directly connected, FastEthernet0/0
s* 0.0.0.0/0 [1/0] via 10.1.1.1
```

```
Router4#sh ip route
```

```
Gateway of last resort is 172.16.10.1 to network 0.0.0.0
```

```
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.10.0 is directly connected, Serial2/0
S* 0.0.0.0/0 [1/0] via 172.16.10.1
```

4. Всі мережеві інтерфейси в мережі пінгуються з кожного мережевого пристрою. Перевірте це.

### 2.8.7 Loopback

1. Визначимо інтерфейс петлю на пристрої Router4

```
Router4(config)# int loopback 0
Router4(config-if)# ip address 1.1.1.1 255.255.255.0
```

2. Пропишемо до пристрою Router1 маршрут на мережу петлі

```
Router1(config)# ip route 1.1.1.0 255.255.255.0 172.16.10.2
```

3. Приєднаємося до пристрою Router2 і пропінгуємо створену петлю

```
Router2#ping 1.1.1.1
```

**Збережіть проект і конфігурацію кожного роутера окремо в текстовий файл.**

## 4. Варіанти індивідуальних завдань для самостійної роботи

1. Побудувати в Packet Tracer топологію, що представлена на рис.5.2. Використовувати необхідні маршрутизатори. В мережі шість підмереж, кожний маршрутизатор підключений до трьох підмереж.

2. На кожному маршрутизаторі підійміть інтерфейси, що використовуються, і подивіться сусідів командою `show cdp neighbors`. Зробіть скріншот.

3. Призначте інтерфейсам мережі адреси згідно рис.5.2 і табл.5.3, в котрих *v* – це номер варіанту. Всі маски 255.255.255.0. Не забудьте призначити шлюзи за замовчуванням для комп'ютерів згідно таблиці.

4. Перевірте факт призначення адрес шляхом виконання на кожному маршрутизаторі команд `show running-config` і `show ip interface brief`. Для комп'ютерів використовуйте команду `ipconfig`.



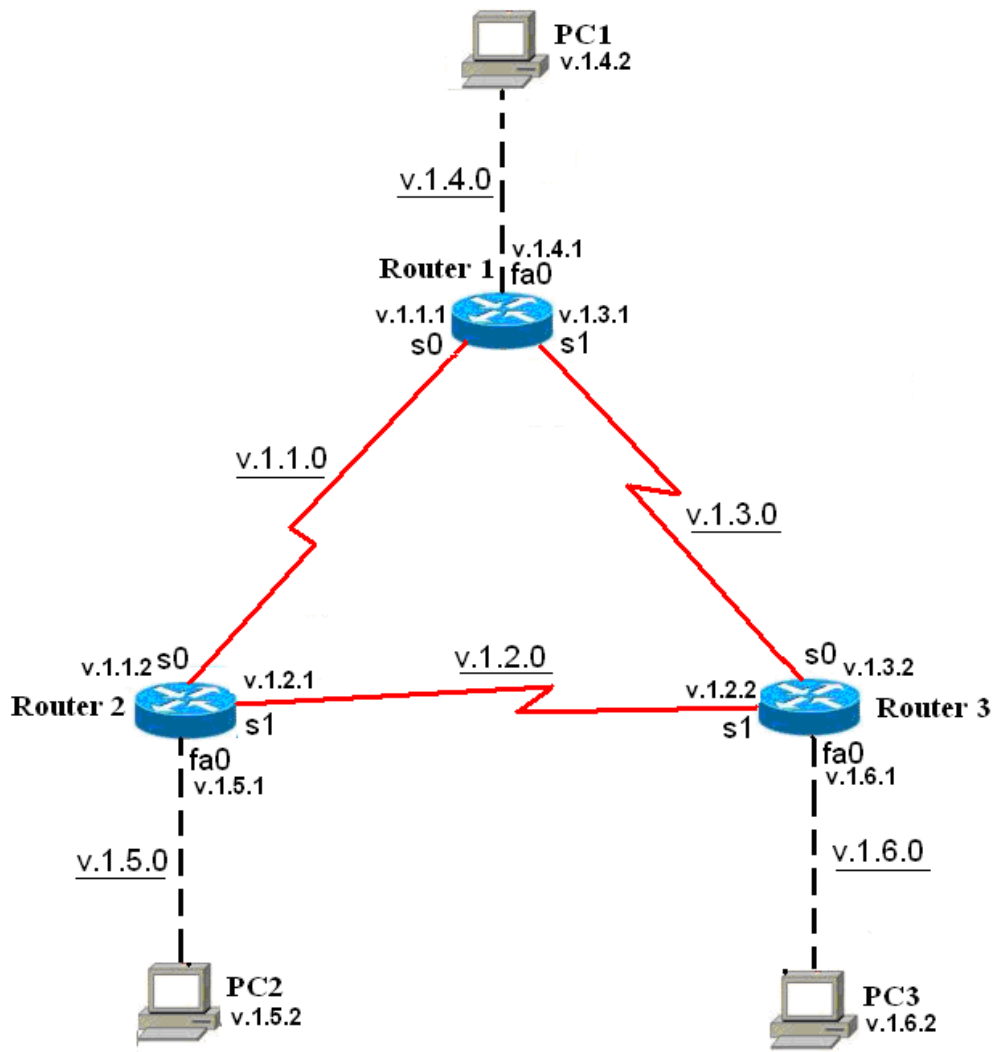


Рисунок 5.2 – Топологія мережі для виконання самостійної роботи

Таблиця 5.3 – Адреси інтерфейсів

Адреси підмереж	v.1.1.0	v.1.2.0	v.1.3.0	v.1.4.0	v.1.5.0	v.1.6.0
Router1	S0:v.1.1.1		S1:v.1.3.1	E0:v.1.4.1		
Router2	S0:v.1.1.2	S1:v.1.2.1			E0:v.1.5.1	
Router3		S0:v.1.2.2	S1:v.1.3.2			E0:v.1.6.1
PC1				E0:v.1.4.2		
PC2					E0:v.1.5.2	
PC3						E0:v.1.6.2

Перевірте правильність призначення адрес шляхом виконання на кожному маршрутизаторі команд ping до безпосередніх сусідів. Наприклад, на маршрутизаторі Router1 виконайте

```
Router1#ping v.1.1.2
```

```
Router1#ping v.1.3.2
```

```
Router1#ping v.1.4.2
```

6. Поставимо перед собою завдання зв'язати між собою комп'ютери PC1, PC2 і PC3. Для цього здійсимо на маршрутизаторах настройку статичної маршрутизації. В кожному маршрутизаторі пропишемо маршрути на віддалені Ethernet мережі. Для вирішення поставленого завдання маршрутизувати пакети на віддалені мережі послідовних з'єднань не треба.

У кожного маршрутизатора є по два маршруту на віддалені Ethernet мережі. Всього треба прописати шість статичних маршрутів.

Щоб з маршрутизатора Router1 досягти віддалену Ethernet мережу v.1.5.0/24, пакети можна направляти на IP адресу v.1.1.2 найближчого зовнішнього інтерфейсу на шляху в цю мережу. Це зробить команда

```
Router1(config)#ip route v.1.5.0 255.255.255.0 v.1.1.2
```

Задайте інші п'ять команд маршрутизації.

7. На кожному маршрутизаторі подивіться таблицю маршрутизації командою show ip route. Зробіть скріншоти.

8. На кожному маршрутизаторі зробіть скріншоти розширених пінгів

a) на маршрутизаторі Router1 від PC2 до PC3

b) на маршрутизаторі Router2 від PC1 до PC3

c) на маршрутизаторі Router3 від PC1 до PC2

Наприклад, результат розширеного пінгу на маршрутизаторі Router1 від PC2 до PC3 для варіанта 12 (v=12) має вигляд:

```
Router1#ping
Protocol [ip]:
Target IP address: 12.1.6.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```

Extended commands [n]: y
Source address or interface: 12.1.5.2
% Invalid source
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.6.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 62/62/63 ms

```

9. На кожному комп'ютері зробіть скріншоти виконання команд трасіровки `tracert` інших комп'ютерів. Всього шість скріншотів. Наприклад, трасіровка з PC1 на PC2 для варіанта 12 (v=12)

```

PC>tracert 12.1.5.2
Tracing route to 12.1.5.2 over a maximum of 30 hops:
 0  17 ms  31 ms  32 ms  12.1.4.1
 1  47 ms  63 ms  63 ms  12.1.1.2
 2  94 ms  94 ms  78 ms  12.1.5.2
Trace complete.

```

10. Збережіть проект

## 5. Контрольні питання

1. Що таке CDP, для чого він служить і як їм користуватися?
2. Яку інформацію повертає команда `ping`?
3. Чи можна, знаходячись на одному пристрої, попарно пропінгувати всі пристрої в мережі?
4. Для чого служить команда `tracert`?
5. Для чого служить протокол `telnet`?
6. Яким пристроєм може виступати маршрутизатор для послідовної лінії зв'язку?
7. На якому пристрої при послідовному з'єднанні можна встановлювати частоту синхронізації?
8. Чому можуть не проходити пінги між пристроями?

9. Як призупинити і відновити telnet – сесію?
10. Як закрити telnet з'єднання?
11. Як відправник дізнається MAC адресу одержувача?
12. Як подивиться ARP таблицю?
13. Коли в ARP таблиці з'являються нові рядки?
14. Що таке таблиця маршрутів? Якщо адміністратор не налаштує ніяких маршрутів, то що вона буде містити?
15. Чим статична маршрутизація відрізняється від динамічної?
16. Які дві форми завдання статичної маршрутизації ви знаєте?
17. Як в команді маршрутизації визначається мережа призначення?
18. Чому для мереж типу Ethernet рекомендується завжди використовувати форму (2) команди маршрутизації?
19. Поясніть значення полів в командах маршрутизації.
20. Чому в якості поля Адреса рекомендують використовувати адресу наступного хопу по шляху до мережі призначення?
21. Коли використовується маршрутизація за замовчуванням?
22. Коли використовується інтерфейс петля?
23. Як працює команда трасіровки?

## **6. Перелік літератури**

### **Основна література**

1. Кузніченко С.Д. «Комп'ютерні мережі» Конспект лекцій. – Одеса: ОДЕКУ, 2018.– 175 с.
2. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: «Магнолія 2006», 2012.– 262с.
3. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. – К.:Київ ун-т ім. Б.Грінченка, 2011. – 291 с.

### **Додаткова література**

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб.: Питер, 2010. – 944 с.: ил.
2. Коломоец Г.П. Организация компьютерных сетей: учебное пособие. – 156 с.

3. Кравец, О.Я. Практикум по вычислительным сетям и телекоммуникациям : учебное пособие / О. Я. Кравец. – Изд. 2-е, перераб. и доп. – Воронеж: Научная книга, 2006. – 156 с.

## **7. Правила техніки безпеки та охорони праці**

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

## **8. Оформлення та захист звіту**

Звіт готується в електронному вигляді і роздруковується. Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Титульна сторінка :
  - Найменування лабораторної роботи.
  - Відомості про виконавця, номер варіанту.
2. Мета роботи та завдання до лабораторної роботи.
3. Виконання *практичної частини лабораторної роботи* (п.3.1).
4. Опис побудови топології та скріншот топології, створеної при виконанні практичної частини
5. Конфігурації трьох маршрутизаторів з .txt файлів, створених при виконанні практичної частини.
6. Виконання практичної частини лабораторної роботи згідно варіанту (п.4).
7. Опис побудови топології та скріншот топології для свого варіанту з вказаними адресами.
8. Таблиця конфігурації згідно свого варіанту.
9. Конфігурації трьох маршрутизаторів з .txt файлів, створених при виконанні завдання для самостійної роботи.
10. Всі скріншоти, що вказані в завданні для самостійної роботи.
11. Висновок за результатами роботи.
12. Контрольні питання та відповіді на них.