Дрогобицький державний педагогічний університет

імені Івана Франка

АННА КАРПИН, ДМИТРО КАРПИН, ОЛЕГ НАУМ

Комп’ютерні мережі:

методичні рекомендації до виконання лабораторних робіт

Навчально-методичний посібник

Дрогобич, 2025

УДК

К

Рекомендовано до друку вченою радою
Дрогобицького державного педагогічного університету імені Івана Франка
(протокол № 11 від 25.09.2025 року)

Рецензенти:
І. Нищак – доктор педагогічних наук, професор, професор кафедри технологічної та професійної освіти Дрогобицького державного педагогічного університету імені Івана.
Франка.
М. Лучкевич – кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних систем та мереж Національного університету "Львівська політехніка".

Відповідальний за випуск: **Віталій Гольський** – доцент, завідувач кафедри фізики та інформаційних систем Дрогобицького державного педагогічного університету імені Івана Франка.

Карпин Анна Василівна, Карпин Дмитро Степанович, Наум Олег Миколайович «Комп'ютерні мережі:методичні рекомендації до виконання лабораторних робіт»: Навчально-методичний посібник – Дрогобич: ДДПУ ім. І. Франка, 2025. – 120 с.

Навчально-методичний посібник «Комп'ютерні мережі: методичні рекомендації до виконання лабораторних робіт» містить практичні завдання, спрямовані на формування прикладних навичок роботи з мережевим обладнанням та програмними засобами. У посібнику розглянуто основи налаштування мережевих інтерфейсів, маршрутизації, служби IP-адресації (DHCP, DNS), сегментації мереж (VLAN), електронної пошти, а також інструменти моделювання мереж у середовищі Cisco Packet Tracer. Кожна лабораторна робота супроводжується теоретичними відомостями, детальними інструкціями з виконання та контрольними запитаннями, що сприяє кращому розумінню матеріалу та його практичному засвоєнню. Посібник орієнтований на студентів та забезпечує системне освоєння основ комп'ютерних мереж через виконання покрокових сценаріїв реальних мережевих конфігурацій. Бібліографія 20 назв.

ЗМІСТ

ВСТУП

Сучасні цифрові технології стрімко розвиваються і разом з ними зростає роль практичних навичок у роботі з комп’ютерними мережами. Уміння налаштовувати, адмініструвати й аналізувати роботу мережевого обладнання є критично важливими для майбутніх фахівців з інформаційних технологій. Саме лабораторні роботи дозволяють перейти від теоретичного розуміння до реального застосування знань у змодельованих або наближених до реальних умовах, формуючи професійні компетентності через практику.

Посібник «Комп'ютерні мережі: методичні вказівки до виконання лабораторних робіт» покликаний дати студентам можливість власноруч налаштовувати мережі, створювати топології, аналізувати трафік, працювати з основними мережевими службами (DHCP, DNS, електронна пошта, VLAN тощо) та засвоювати принципи маршрутизації й сегментації. Практичні завдання розроблено з урахуванням сучасних підходів до моделювання мереж з використанням Cisco Packet Tracer і базових налаштувань Windows.

Матеріали цього посібника сприяють розвитку критичного мислення, навичок пошуку і виправлення помилок у конфігураціях, а також здатності приймати технічно обґрунтовані рішення в умовах змінного цифрового середовища. Завдяки поєднанню інструкцій, варіативних завдань і контрольних запитань посібник забезпечує комплексну підготовку студентів до реальних викликів у сфері комп’ютерних мереж.

«Комп'ютерні мережі: методичні вказівки до виконання лабораторних робіт» забезпечує такі компетентності як:

загальні компетентності:

- здатність застосовувати знання в практичних ситуаціях;
- навички використання інформаційних і комунікаційних технологій;
- здатність до абстрактного мислення, аналізу та синтезу;
- здатність вчитися і оволодівати сучасними знаннями;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність працювати в команді;

- здатність діяти соціально відповідально та свідомо;
- здатність приймати обґрунтовані рішення;

фахові компетентності:

- здатність нести відповідальність за прийняття рішень у непередбачуваних умовах. − здатність використовувати у професійній діяльності основні положення, методи, принципи фундаментальних та прикладних наук.
- здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище.

програмні результати навчання:

- володіти інформацією чинних нормативно-правових документів, законодавства, галузевих стандартів професійної діяльності в установах та організаціях галузі освіти. − доносити зрозуміло і недвозначно професійні знання, обґрунтування і висновки до фахівців і широкого загалу державною та іноземною мовами.
- аналізувати та оцінювати ризики, проблеми у професійній діяльності й обирати ефективні шляхи їх вирішення.
- самостійно планувати й організовувати власну професійну діяльність і діяльність здобувачів освіти.
- відшуковувати, обробляти, аналізувати та оцінювати інформацію, що стосується професійної діяльності, користуватися спеціалізованим програмним забезпеченням та сучасними засобами зберігання та обробки інформації.
- емпатійно взаємодіяти, відповідати за прийняття рішень в межах своєї компетенції, дотримуватися стандартів професійної етики.

«Комп'ютерні мережі: методичні вказівки до виконання лабораторних робіт» укладені згідно із робочою програмою навчальної дисципліни «Комп'ютерні мережі» (затверджена науково-методичною радою Дрогобицького державного педагогічного університету імені Івана Франка, протокол № 8 від 27 серпня 2025 року). Також у посібнику є питання для самоконтролю.

ЛАБОРАТОРНА РОБОТА № 1
РОЗРАХУНОК КОМП'ЮТЕРНИХ ПІДМЕРЕЖ

Мета роботи: навчитися планувати адресний простір у сучасних IP-мережах, виконувати розрахунок підмереж із використанням CIDR, визначати маски, кількість вузлів і діапазони адрес, аналізувати приналежність IP-адрес до однієї підмережі.

Теоретичні відомості:

У сучасних комп'ютерних мережах все частіше застосовується безкласова адресація (CIDR), яка дозволяє ефективно використовувати обмежений простір IPv4-адрес. CIDR-позначення, як-от 192.168.1.0/24, дає змогу точно вказати кількість біт, які відповідають за адресу мережі, і таким чином створювати підмережі з різною кількістю хостів залежно від потреб. Це особливо важливо в умовах глобального дефіциту IPv4-адрес та широкого використання віртуальних і хмарних інфраструктур, де точне планування адресного простору забезпечує масштабованість і контрольованість мережі.

Для визначення приналежності IP-адреси до підмережі використовується побітова операція AND між адресою та маскою. Кількість адрес у підмережі обчислюється за формулою 2^n-2, де n — кількість біт, відведених під хости (одна адреса зарезервована для самої мережі, інша — для широкомовного повідомлення). Використання CIDR дозволяє зменшити кількість широкомовних доменів, покращити продуктивність, і зберігає гнучкість в об'єднанні різних логічних сегментів мережі — що критично важливо для IoT, корпоративних VPN, SD-WAN і хмарних сервісів.

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

Таблиця 1.1 Класи мереж

Клас	Призначення	Найменша IP-адреса	Найбільша IP-адреса
A	Великі мережі, провайдери, дата-центри	1.0.0.0	126.255.255.255

Клас	Призначення	Найменша IP-адреса	Найбільша IP-адреса
B	Середні мережі, університети, компанії	128.0.0.0	191.255.0.0
C	Невеликі мережі, локальні організації	192.0.0.0	223.255.255.0
D	Багатоадресна передача (multicast)	224.0.0.0	239.255.255.255
E	Резерв, дослідження, експериментальні	240.0.0.0	254.255.255.255

У сучасних IP-мережах для призначення адрес хостам переважно використовуються діапазони, що походять з історичних класів A, B і C. При цьому класи як такі майже не застосовуються — їх замінила CIDR-адресація, яка дає більшу гнучкість. Однак знання про класову структуру важливе для розуміння основ. Адреси типу `127.x.x.x` (переважно `127.0.0.1`) зарезервовані для loopback-інтерфейсу — вони використовуються лише всередині пристрою для тестування TCP/IP-стека, локального взаємозв'язку процесів і діагностики. Такий трафік ніколи не покидає пристрій і не передається в мережу.

Адреси з діапазону `224.0.0.0–239.255.255.255` (клас D) використовуються для multicast-трансляцій, наприклад у потоковому відео, IPTV, VoIP. Діапазон `240.0.0.0–254.255.255.255` (клас E) зарезервований для експериментальних цілей і не використовується в практичних конфігураціях. Адреси з нулями (`0.0.0.0`) або з усіма одиницями в хостовій частині (наприклад, `192.168.1.255`) виконують спеціальні функції — це широкомовні (broadcast) адреси, їх не призначають хостам.

Для локальних, ізольованих від Інтернету мереж, сучасні стандарти визначають приватні діапазони IP-адрес, які не маршрутизуються у глобальній мережі: `10.0.0.0/8` (колишній клас A), `172.16.0.0–172.31.255.255/12` (B) і `192.168.0.0–192.168.255.255/16` (C). Усі хости в одній локальній мережі повинні мати однакову мережеву частину адреси (визначену маскою підмережі) та унікальну хостову частину. Такий поділ дозволяє точно і ефективно керувати IP-адресацією всередині корпоративних, навчальних або домашніх мереж.

У сучасних IP-мережах **маска підмережі** визначає межу між частиною IP-адреси, що відноситься до мережі, та частиною, що ідентифікує хост-пристрій. Це 32-бітове значення, представлене у вигляді чотирьох октетів (наприклад, `255.255.255.0`). Маска дозволяє визначити кількість хостів у підмережі та виконує ключову функцію в маршрутизації — зокрема, дозволяє маршрутизатору визначити, до якої мережі належить пакет. У контексті IPv4, де адресний простір обмежений, використання масок є одним із найважливіших інструментів управління мережею.

У мережевій топології кожна IP-адреса виконує одну з трьох функцій: адресу мережі, адресу інтерфейсу (хоста) або широкомовну адресу. Наприклад, у мережі `192.168.1.0/24`, адреса `192.168.1.0` є адресою самої мережі, а `192.168.1.255` — широкомовною. IP-адресація забезпечує комунікацію в межах і між мережами, а широкомовлення (broadcast) дозволяє одному пристрою надсилати повідомлення всім іншим у межах підмережі, що особливо важливо на початкових етапах обміну даними, наприклад, для ARP-запитів.

У класичній схемі IP-адресації застосовувалися фіксовані маски для класів A, B і C. Проте ця модель виявилась неефективною: наприклад, клас C підтримує лише до 254 хостів, а клас B — понад 65 тисяч, що призводить до втрати значної кількості адрес. Щоб уникнути таких втрат, у сучасних мережах застосовується **CIDR (Classless Inter-Domain Routing)** — безкласова адресація. Вона дозволяє використовувати будь-яку кількість бітів для мережевої частини адреси, що забезпечує точніше планування підмереж. CIDR-нотація виглядає як IP-адреса зі слешем: наприклад, `192.168.1.0/26` означає, що 26 бітів відведено під мережу, а решта — під хости.

Завдяки CIDR адміністратори можуть створювати підмережі з різною кількістю пристроїв відповідно до потреб. Наприклад, маска `255.255.255.240` (або `/28`) дозволяє створити підмережу з 16 адресами, з яких 14 придатні для використання хостами. Формула для визначення максимальної кількості хостів виглядає як 2^n-2, де n — кількість бітів, відведених під хостову частину. Віднімаються 2 адреси: одна для самої мережі, інша — для широкомовної трансляції.

Розбиття мережі на підмережі дозволяє покращити масштабованість і безпеку, а також знизити рівень трафіку. Воно дає змогу створювати логічні групи пристроїв (робочі групи, сегменти VLAN), ефективно управляти маршрутизацією, скорочувати розмір широкомовних доменів та полегшувати адміністрування. У комплексі з DHCP, NAT та VLAN підмережування стає базовим інструментом у проєктуванні сучасних корпоративних мереж, дата-центрів, хмарної інфраструктури та IoT-систем.

Хід роботи

Алгоритм визначення знаходження двох вузлів в одній підмережі такий:

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

Приклад 1.

Визначити, чи розміщені вузли А і В в одній підмережі. IP- адреси комп'ютера А і комп'ютера В відповідно рівні: 172.45.87.20 та 172.46.15.230, маска підмережі 255.254.0.0.

Розв’язання:

Комп'ютер А:

Десятковий вигляд:	Двійковий вигляд:
IP-адреса:	
172.45.87.20	*10101100.00101101.01010111.00010100*
Маска підмережі:	
255.254.0.0	*11111111.11111110.00000000.00000000*
AND(2)	*10101100.00101100.00000000.00000000*
AND(10)	172. 44. 0. 0

Комп'ютер B:

Десятковий вигляд:	Двійковий вигляд:
IP-адреса:	
172.46.15.230	*10101100.00101110.00001111.11100110*
Маска підмережі:	
255.254.0.0	*11111111.11111110.00000000.00000000*

AND(2)	*10101100.00101110.00000000.00000000*			
AND(10)	172.	46.	0.	0

Не співпадіння номерів підмереж вузлів A та B, отриманих в результаті побітової операції AND, означає, що ці вузли знаходяться в різних підмережах. Отже, між ними не можна встановити пряме з'єднання без застосування шлюзів.

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

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

Приклад 2.

Визначити маску підмережі, що відповідає діапазону IP-адрес 192.168.20.1 – 192.168.23.254.

Розв’язання:

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

початкова адреса:

192.168.20.1 *11000000.10101000.00010100.00000001*

кінцева адреса:

192.168.23.254 *11000000.10101000.00010111.11111110*

2) Визначимо маску:

маска підмережі: **11111111.11111111.11111**00.00000000

3) Подамо отриману маску у десятковій системі числення:

маска підмережі: *255.255.252.0*

Отже, маска підмережі, що відповідає діапазону IP-адрес 192.168.20.1 – 192.168.23.254 дорівнює 255.255.*252*.0.

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

1. Переведіть номер і маску підмережі у двійковий вигляд.
2. На основі маски визначте кількість біт, значення яких рівне нулю, і позначте їх літерою K; ці нульові біти використовуються для адресації вузлів; біти, що відповідають за номер підмережі, рівні одиниці.
3. Загальна кількість адрес мережі рівна 2K, але з цього числа слід виключити адресу мережі та широкосповіщальну адресу, що складаються з усіх нулів та всіх одиниць відповідно. Отже, загальна кількість вузлів підмережі буде дорівнювати 2K – 2.
4. Щоб отримати початкову IP-адресу підмережі, потрібно біти IP-адреси (справа), що відповідають нульовим бітам у масці, заповнити нулями, а крайній правий біт встановити в одиницю. Отримана адреса буде першою з допустимих адрес певної підмережі.
5. Щоб отримати кінцеву IP-адресу підмережі, потрібно біти IP-адреси (справа), що відповідають нульовим бітам у масці, заповнити одиницями, а крайній правий біт встановити в нуль. Отримана адреса буде останньою з допустимих адрес певної підмережі.

Приклад 3.

Визначити кількість і діапазон адрес вузлів у підмережі, якщо її номер дорівнює 192.168.160.0, а маска – 255.255.224.0.

Розв’язання:

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

номер підмережі: 192.168.160.0 11000000.10101000.10100000.00000000

маска підмережі: 255.255.224.0 11111111.11111111.11100000.00000000

K = 14.

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

3) Визначаємо початкову адресу підмережі:

початкова адреса: 11000000.10101000.10100000.00000001 192.168.160.1

маска підмережі: 11111111.11111111.11100000.00000000 255.255.224.0

4) Визначаємо кінцеву адресу підмережі:

кінцева адреса: 11000000.10101000.10111111.11111110 192.168.191.254

маска підмережі: 11111111.11111111.11100000.00000000 255.255.224.0

Отже, для підмережі 192.168.160.0 з маскою 255.255.224.0 кількість можливих адрес дорівнює 16382, а діапазон можливих адрес – 192.168.160.1–192.168.191.254.

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

1. Визначаємо загальну кількість вузлів у мережі (2K – 2).
2. Для визначення кількості вузлів у підмережі загальну кількість вузлів у мережі потрібно поділити на задану (орієнтовну) кількість вузлів у проектованій мережі. Далі потрібно знайти число, що кратне числу 2 і при цьому розміщене якнайближче до значення загальної кількості вузлів у мережі, але не більше останнього. Після цього подати його у вигляді 2N, де N – кількість бітів, які потрібно виділити під номер вузла, інші біти виділяються під маску.
3. Визначаємо нову маску підмережі.
4. Щоб визначити кількість підмереж, потрібно кількість вузлів у мережі поділити на кількість вузлів у підмережі.
5. Щоб отримати діапазони IP-адрес підмереж, до початкової адреси додаємо кількість вузлів у підмережі, включаючи адресу підмережі та широкосповіщальну адресу. Кожна наступна підмережа відраховується від адреси попередньої підмережі шляхом додавання одиниці до адреси вузла. Цю дію потрібно повторити стільки разів, скільки є підмереж.

Приклад 4.

Організації виділена мережа класу С: 198.51.42.0/24. Визначити маски підмереж, кількість можливих адрес підмереж та діапазони IP-адрес цих підмереж, якщо в кожній підмережі кількість вузлів повинна бути близько 50.

Розв'язання:

1) Визначаємо загальну кількість вузлів у мережі.

З умови видно, що маска містить 24 одиниці, тобто 255.255.255.0, з яких під номер вузла відводиться 8 біт, тобто мережа може включати $2^8 - 2 = 254$ вузли;

2) Визначаємо реальну кількість вузлів у підмережі, нову адресу та маску мережі.

Кількість вузлів у підмережі має бути числом, що кратне числу 2 (за умовою кількість вузлів дорівнює 50). Визначимо число кратне числу 2, яке найближче до 50:

$2^5 = 32$, а $|50-32|=18$;

$2^6 = 64$, а $|50-64|=14$.

Отже, найближчим числом, що відповідає критерію є $2^6 = 64$.

Крім того, повинна виконуватися вимога, що кількість вузлів у підмережі має бути не більше значення загальної кількості вузлів у мережі: $50 < (\mathbf{2^6 = 64}) \leq 254$. Тому для номера вузла потрібно виділити 6 біт (число, що є степенем двійки), тому маску потрібно розширити на 2 біта – з 24 до 26 біт.

3) Визначаємо кількість підмереж:

$254 : 64 = 4$.

Отримали 4 підмережі.

4) Визначаємо діапазони IP-адрес підмереж.

Оскільки під маску відводиться 26 бітів, то вона буде мати такий вигляд: 11111111.11111111.11111111.11000000, тобто 255.255.255.192.

При цьому кількість можливих адрес у кожній підмережі дорівнюватиме 64.

Тоді діапазони IP-адрес всіх підмереж будуть такі:

198.51.42.0 -198.51.42.63;
198.51.42.64 -198.51.42.127;

198.51.42.128-198.51.42.191;
198.51.42.192-198.51.42.255;

Отже, отримаємо маску підмережі 255.255.255.192, 64 можливі адреси і 4 діапазони IP-адрес підмережі.

Завдання для індивідуальної роботи

1. Визначити, чи розміщені вузли А і В в одній підмережі згідно свого варіанту (табл. 1.2, завдання 1).
2. Визначити маску підмережі, що відповідає вказаному діапазону IP-адрес згідно зі своїм варіантом (табл. 1.2, завдання 3).
3. Визначити кількість і діапазон адрес вузлів у підмережі за її номером та маскою згідно зі своїм варіантом (табл. 1.2, завдання 2).
4. Організації виділена мережа класу С. Визначити маску, кількість вузлів та діапазони IP-адрес підмереж згідно зі своїм варіантом (табл. 1.2, завдання 4).

Таблиця 1.2 Варіанти завдань

№ в-ту	Завдання 1	Завдання 2	Завдання 3	Завдання 4
1	IP-адреси комп'ютерів А і В відповідно: 172.24.207.54 та 172.40.121.89, маска підмережі: 255.254.0.0.	Діапазон IP 192.168.102.6 – 192.168.106.233	IP 192.168.214.0, маска – 255.255.252.0	Мережа класу С: 220.150.116.0/24 Кількість вузлів ~ 60.
2	IP-адреси комп'ютерів А і В відповідно: 172.17.12.49 та 172.48.97.226, маска підмережі: 255.240.0.0.	Діапазон IP 192.168.68.87 – 192.168.71.201	IP 192.168.233.0, маска – 255.255.255.224	Мережа класу С: 210.2.61.0/24. Кількість вузлів ~ 200.
3	IP-адреси комп'ютерів А і В відповідно: 172.30.218.30 та 172.19.209.20, маска підмережі: 255.224.0.0	Діапазон IP 192.168.69.73 – 192.168.71.207	IP 192.168.219.0, маска – 255.255.254.0	Мережа класу С: 199.203.121.0/24 Кількість вузлів ~ 150.
4	IP-адреси комп'ютерів А і В відповідно:	Діапазон IP 192.168.98.5 – 192.168.102.163	IP 192.168.31.0, маска – 255.255.252.0	Мережа класу С: 204.75.103.0/24.

№ в-ту	Завдання 1	Завдання 2	Завдання 3	Завдання 4
	172.43.63.168 та 172.20.96.62, маска підмережі: 255.240.0.0.			Кількість вузлів ~ 100.
5	IP-адреси комп'ютерів A і B відповідно: 172.31.43.111 та 172.41.134.27, маска підмережі: 255.240.0.0.	Діапазон IP 192.168.197.25 – 192.168.198.253	IP 192.168.210.0, маска – 255.255.254.0	Мережа класу C: 210.98.111.0/24 Кількість вузлів ~ 50.
6	IP-адреси комп'ютерів A і B відповідно: 172.46.211.239 та 172.48.204.188, маска підмережі: 255.248.0.0.	Діапазон IP 192.168.14.56 – 192.168.16.151	IP 192.168.206.0, маска – 255.255.240.0	Мережа класу C: 204.110.63.0/24. Кількість вузлів ~ 80.
7	IP-адреси комп'ютерів A і B відповідно: 172.26.68.162 та 172.31.3.107, маска підмережі: 255.240.0.0.	Діапазон IP 192.168.29.58 – 192.168.32.152	IP 192.168.105.0, маска – 255.255.254.0	Мережа класу C: 222.140.235.0/24 Кількість вузлів ~ 120.
8	IP-адреси комп'ютерів A і B відповідно: 172.44.12.248 та 172.21.4.192, маска підмережі: 255.255.0.0.	Діапазон IP 192.168.95.55 – 192.168.98.177	IP 192.168.224.0, маска – 255.255.255.192.	Мережа класу C: 212.113.201.0/24 Кількість вузлів ~ 80.
9	IP-адреси комп'ютерів A і B відповідно: 172.41.76.43 та 172.36.121.203, маска підмережі: 255.248.0.0.	Діапазон IP 192.168.173.66 – 192.168.174.169	IP 192.168.99.0, маска – 255.255.255.128	Мережа класу C: 200.66.114.0/24 Кількість вузлів ~ 150.
10	IP-адреси комп'ютерів A і B відповідно: 172.16.73.7 та 172.23.40.154, маска підмережі: 255.248.0.0.	Діапазон IP 192.168.188.32 – 192.168.192.204	IP 192.168.206.0, маска – 255.255.240.0	Мережа класу C: 195.23.10.0/24 Кількість вузлів ~ 50.
11	IP-адреси комп'ютерів A і B відповідно: 172.27.255.111 та	Діапазон IP 192.168.6.14 – 192.168.9.174	IP 192.168.182.0, маска – 255.255.254.0	Мережа класу C: 214.87.201.0/24 Кількість вузлів ~ 10.

№ в-ту	Завдання 1	Завдання 2	Завдання 3	Завдання 4
	172.47.180.46, маска підмережі: 255.192.0.0.			
12	IP-адреси комп'ютерів A і B відповідно: 172.27.140.55 та 172.46.106.196, маска підмережі: 255.255.0.0	Діапазон IP 192.168.209.55 – 192.168.211.249	IP 192.168.190.0, маска – 255.255.252.0.	Мережа класу C: 203.45.55.0/24 Кількість вузлів ~ 120.
13	IP-адреси комп'ютерів A і B відповідно: 172.50.19.201 та 172.29.36.194, маска підмережі: 255.254.0.0	Діапазон IP 192.168.136.65 – 192.168.138.226	IP 192.168.145.0, маска – 255.255.255.128	Мережа класу C: 197.162.220.0/24 Кількість вузлів ~ 10.
14	IP-адреси комп'ютерів A і B відповідно: 172.17.81.129 та 172.33.177.71, маска підмережі: 255.224.0.0.	Діапазон IP 192.168.200.71 – 192.168.203.241	IP 192.168.171.0, маска – 255.255.255.0	Мережа класу C: 214.49.214.0/24 Кількість вузлів ~ 100.
15	IP-адреси комп'ютерів A і B відповідно: 172.37.90.62 та 172.37.26.75, маска підмережі: 255.252.0.0.	Діапазон IP 192.168.9.50 – 192.168.10.208	IP 192.168.86.0, маска – 255.255.255.128	Мережа класу C: 207.37.88.0/24 Кількість вузлів ~ 200.
16	IP-адреси комп'ютерів A і B відповідно: 172.43.115.91 та 172.24.230.56, маска підмережі: 255.252.0.0.	Діапазон IP 192.168.45.11 – 192.168.49.206	IP 192.168.95.0, маска – 255.255.240.0	Мережа класу C: 218.208.142.0/24 Кількість вузлів ~ 50.
17	IP-адреси комп'ютерів A і B відповідно: 172.29.140.93 та 172.49.207.169, маска підмережі: 255.240.0.0.	Діапазон IP 192.168.56.82 – 192.168.58.209	IP 192.168.69.0, маска – 255.255.252.0	Мережа класу C: 200.34.45.0/24 Кількість вузлів ~ 20.
18	IP-адреси комп'ютерів A і B відповідно: 172.16.254.239 та 172.28.80.90,	Діапазон IP 192.168.124.43 – 192.168.129.223	IP 192.168.194.0, маска – 255.255.255.224	Мережа класу C: 217.184.162.0/24 Кількість вузлів ~20.

№ в-ту	Завдання 1	Завдання 2	Завдання 3	Завдання 4
	маска підмережі: 255.252.0.0			
19	IP-адреси комп'ютерів A і B відповідно: 172.40.95.254 та 172.31.241.223, маска підмережі: 255.252.0.0	Діапазон IP 192.168.204.77 – 192.168.207.221	IP 192.168.15.0, маска – 255.255.255.128	Мережа класу C: 214.76.166.0/24 Кількість вузлів ~ 100.
20	IP-адреси комп'ютерів A і B відповідно: 172.50.186.12 та 172.43.210.203, маска підмережі: 255.254.0.0.	Діапазон IP 192.168.84.8 – 192.168.86.164	IP 192.168.77.0, маска – 255.255.255.224	Мережа класу C: 197.184.202.0/24. Кількість вузлів ~ 80.
21	IP-адреси комп'ютерів A і B відповідно: 172.35.7.60 та 172.48.10.19, маска підмережі: 255.248.0.0	Діапазон IP 192.168.158.93 – 192.168.161.253	IP 192.168.77.0, маска – 255.255.252.0	Мережа класу C: 220.53.166.0/24 Кількість вузлів ~ 30.
22	IP-адреси комп'ютерів A і B відповідно: 172.43.141.90 та 172.22.211.219, маска підмережі: 255.254.0.0	Діапазон IP 192.168.217.93 – 192.168.218.239	IP 192.168.83.0, маска – 255.255.240.0	Мережа класу C: 209.155.128.0/24 Кількість вузлів ~ 120.
23	IP-адреси комп'ютерів A і B відповідно: 172.36.139.138 та 172.44.92.141, маска підмережі: 255.252.0.0	Діапазон IP 192.168.49.57 – 192.168.51.220	IP 192.168.50.0, маска – 255.255.255.224	Мережа класу C: 213.209.211.0/24 Кількість вузлів ~ 150.
24	IP-адреси комп'ютерів A і B відповідно: 172.17.18.254 та 172.17.212.174, маска підмережі: 255.255.0.0	Діапазон IP 192.168.165.30 – 192.168.169.186	IP 192.168.197.0, маска – 255.255.254.0	Мережа класу C: 204.70.230.0/24 Кількість вузлів ~ 100.
25	IP-адреси комп'ютерів A і B відповідно: 172.47.147.225 та 172.25.55.6,	Діапазон IP 192.168.96.82 – 192.168.100.182	IP 192.168.122.0, маска – 255.255.252.0	Мережа класу C: 198.63.195.0/24 Кількість вузлів ~ 20.

№ в-ту	Завдання 1	Завдання 2	Завдання 3	Завдання 4
	маска підмережі: 255.224.0.0			
26	IP-адреси комп'ютерів A і B відповідно: 172.32.155.80 та 172.23.72.194, маска підмережі: 255.224.0.0.	Діапазон IP 192.168.249.87 – 192.168.251.190	IP 192.168.90.0, маска – 255.255.255.192	Мережа класу C: 221.51.24.0/24 Кількість вузлів ~ 10.
27	IP-адреси комп'ютерів A і B відповідно: 172.34.45.74 та 172.16.24.213, маска підмережі: 255.192.0.0.	Діапазон IP 192.168.240.28 – 192.168.244.209	IP 192.168.175.0, маска – 255.255.255.128	Мережа класу C: 196.188.18.0/24 Кількість вузлів ~ 200.
28	IP-адреси комп'ютерів A і B відповідно: 172.45.36.128 та 172.27.218.210, маска підмережі: 255.254.0.0	Діапазон IP 192.168.63.43 – 192.168.65.231	IP 192.168.1.0, а маска – 255.255.240.0	Мережа класу C: 210.14.204.0/24 Кількість вузлів ~ 100.
29	IP-адреси комп'ютерів A і B відповідно: 172.33.27.170 та 172.28.159.156, маска підмережі: 255.252.0.0	Діапазон IP 192.168.146.93 – 192.168.148.157	IP 192.168.182.0, маска – 255.255.255.192	Мережа класу C: 208.125.164.0/24 Кількість вузлів ~ 60.
30	IP-адреси комп'ютерів A і B відповідно: 172.18.195.185 та 172.37.229.185, маска підмережі: 255.240.0.0	Діапазон IP 192.168.181.4 – 192.168.183.178	IP 192.168.82.0, маска – 255.255.255.224	Мережа класу C: 214.94.159.0/24 Кількість вузлів ~ 10.

Звіт має містити:

1. Мета роботи
2. Розв’язання усіх 4 завдань
3. Висновки

Контрольні запитання:

1. Що таке підмережа і для чого вона використовується у комп’ютерних мережах?
2. Що таке маска підмережі? Яку функцію вона виконує?
3. Як за маскою підмережі визначити кількість доступних IP-адрес для хостів?
4. Чому з формули 2n2^n2n потрібно віднімати 2 при обчисленні кількості хостів у підмережі?
5. Що таке адреса мережі та широкомовна (broadcast) адреса?
6. У чому полягає перевага CIDR перед класовою адресацією?
7. Які правила потрібно враховувати при плануванні IP-адрес для підмереж у великих організаціях?
8. Як визначити діапазон IP-адрес у підмережі?
9. Яка мінімальна маска підмережі дозволяє мати щонайменше 50 хостів?
10. Що відбудеться, якщо дві підмережі матимуть перекриття адресних діапазонів?

ЛАБОРАТОРНА РОБОТА № 2
ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ В CISCO PACKET TRACER

Мета роботи: Навчитися проектувати базову топологію комп'ютерної мережі з використанням програмного середовища Cisco Packet Tracer, налаштовувати мережеві пристрої (ПК, комутатори, маршрутизатори), виконувати перевірку з'єднань та діагностику з використанням PING і PDU.

Теоретичні відомості:

Cisco Packet Tracer — це програмне середовище моделювання мереж, створене компанією Cisco. Воно дозволяє створювати віртуальні мережі з використанням пристроїв Cisco, таких як маршрутизатори, комутатори, сервери та роутери, і симулювати реальні процеси передачі даних. Packet Tracer підтримує протоколи TCP/IP, DHCP, DNS, FTP, ICMP, HTTP та інші, а також дозволяє користувачу аналізувати мережеву поведінку на різних рівнях OSI-моделі.

Для проєктування мережі в Cisco Packet Tracer використовуються віртуальні пристрої, які підключаються один до одного через мережеві інтерфейси. Кожному пристрою може бути призначена статична IP-адреса або налаштовано автоматичне отримання через DHCP. Після побудови мережі користувач може перевірити її працездатність за допомогою інструментів, таких як ping, traceroute або додавання PDU.

Програмне середовище підтримує як графічний режим налаштування (через вкладки Config і Desktop), так і командний інтерфейс CLI. Це дозволяє моделювати роботу справжніх пристроїв Cisco IOS. Packet Tracer також дає можливість переглядати таблиці ARP, маршрутизації, використовувати мережеві сервіси (DHCP, DNS, HTTP тощо), що забезпечує максимально наближений до реальності досвід побудови та діагностики мереж.

Після запуску програми Cisco Packet Tracer відкриється головне вікно програми.

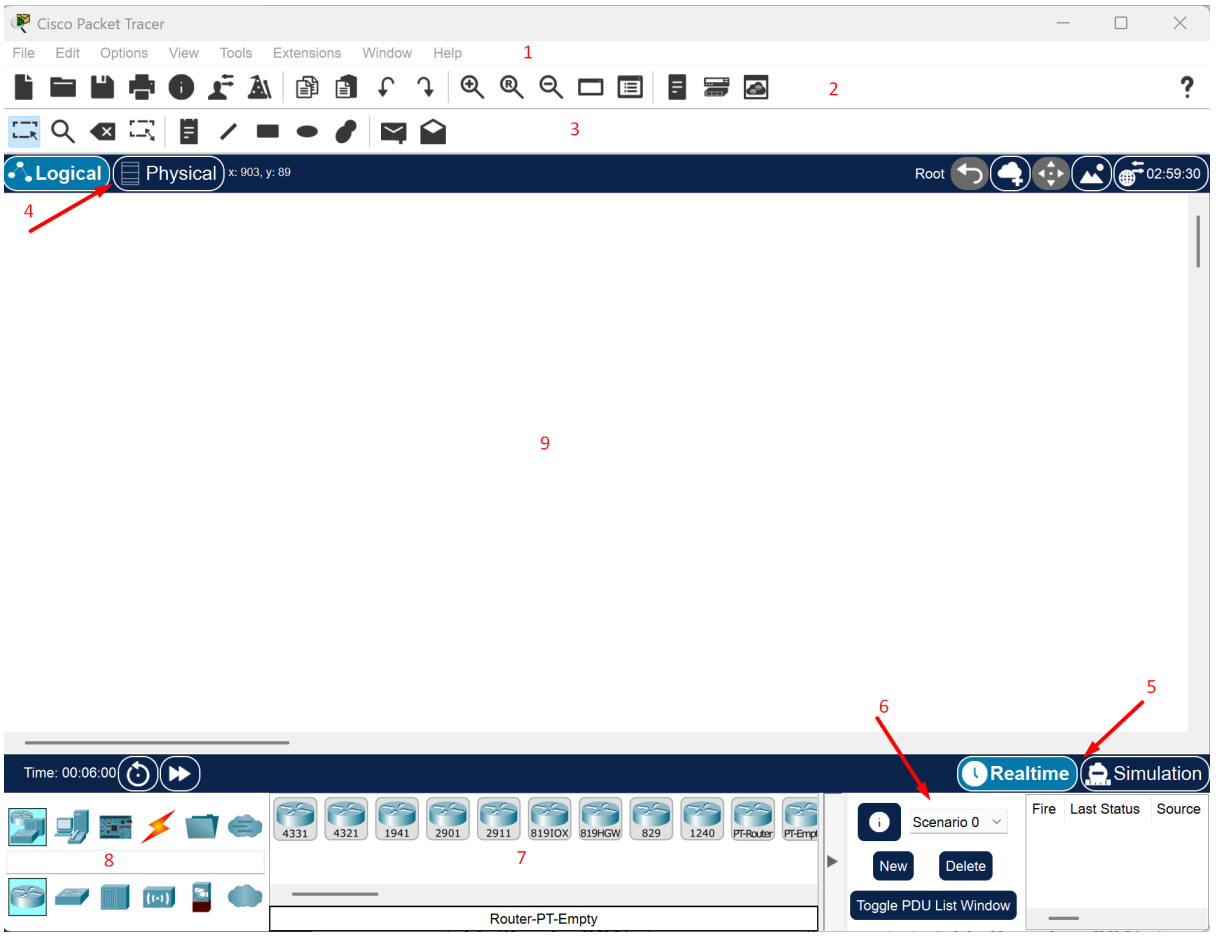


Рисунок 2.1 Головне вікно Cisco Packet Tracer

Головне вікно програми Cisco Packet Tracer, показане на рис. 2.1, складається з таких частин:

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

Для того щоб додати пристрій у проєкт мережі, потрібно послідовно виконати такі кроки (рис. 2.2). А саме:

- на панелі типів пристроїв вибрати піктограму потрібного пристрою (1);

- на панелі кінцевих пристроїв вибрати необхідний пристрій (2);
- додати вибраний пристрій у проєкт, натиснувши лівою кнопкою миші у робочій області (3).

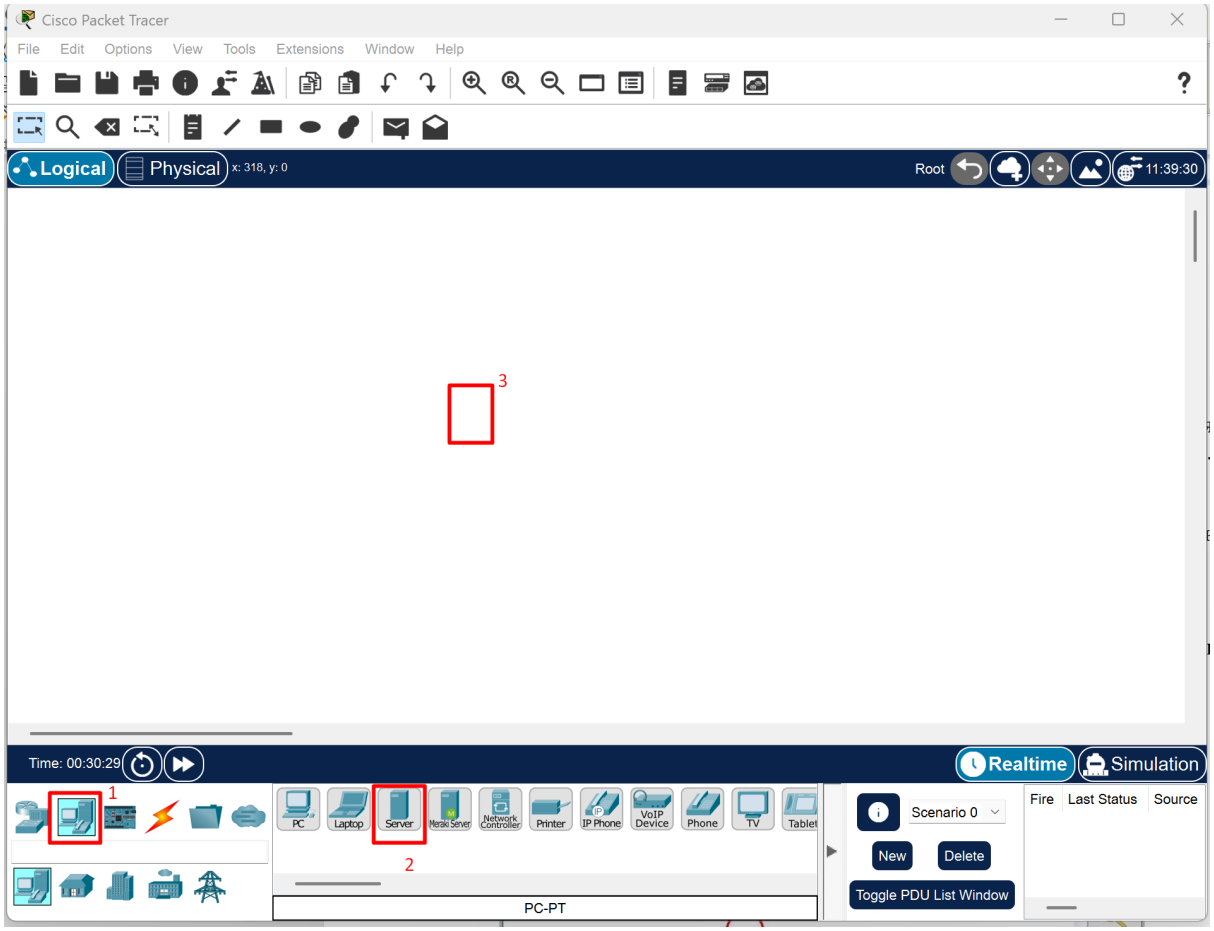


Рис. 2.2 Додавання пристрою у робочу область

Якщо натиснути лівою кнопкою миші на будь який пристрій у робочій області, то відкривається вікно його налаштувань. Кожен пристрій містить свої підпункти, такі як Physical, Config, Services, Desktop, Programming, Attributes та ін.

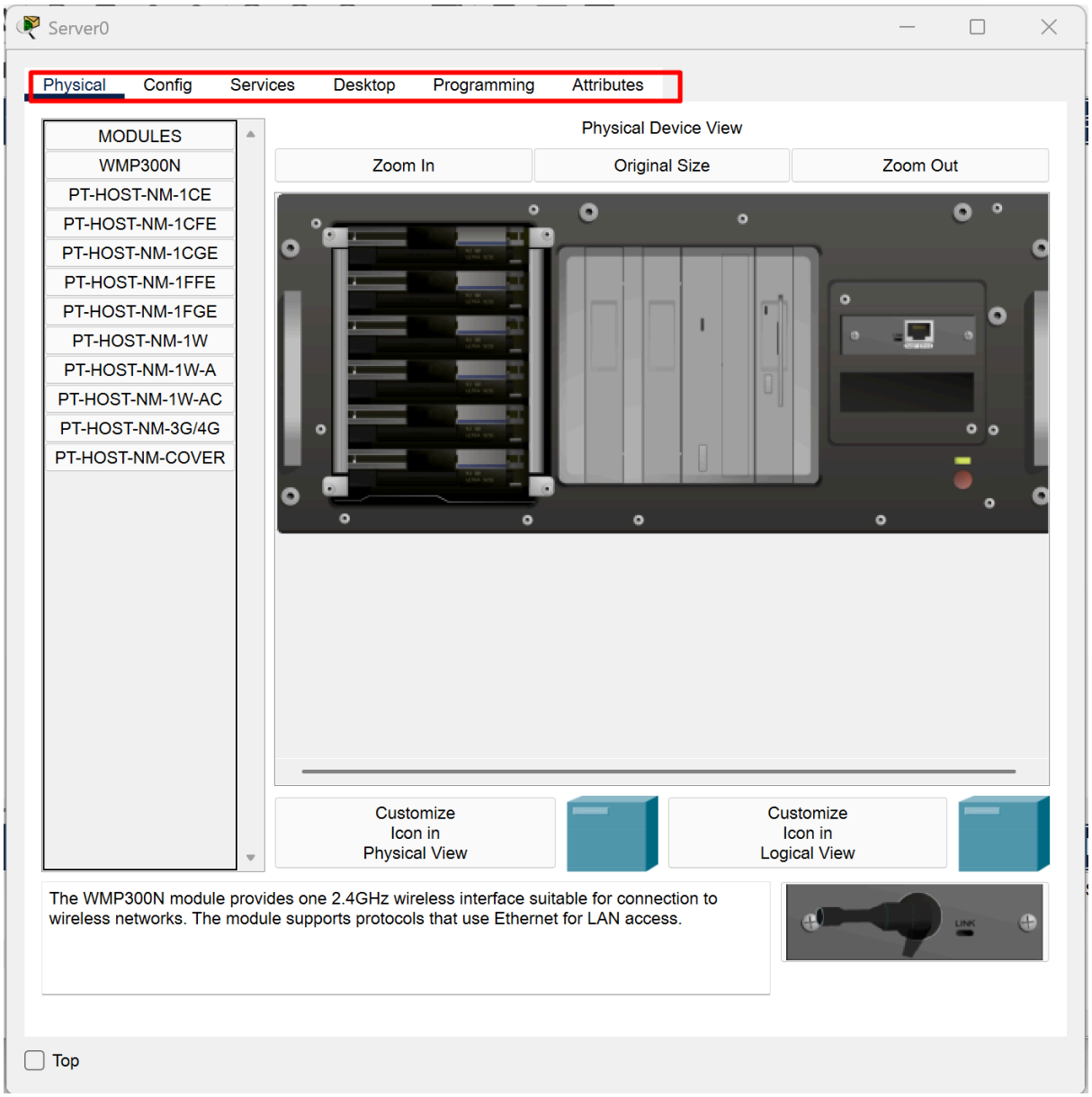


Рис. 2.3 Вікно налаштувань пристрою Сервер

На закладці **Physical** є змога встановлювати певні модулі у вільні роз'єми (рис. 2.4). Крім того, вільні роз'єми можуть бути закриті фальш панелями.

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

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

Видалення вже встановленого модуля з пристрою виконується шляхом перетягування зображення цього модуля (3) лівою кнопкою миші з пристрою у місце зовнішнього вигляду модуля (2).

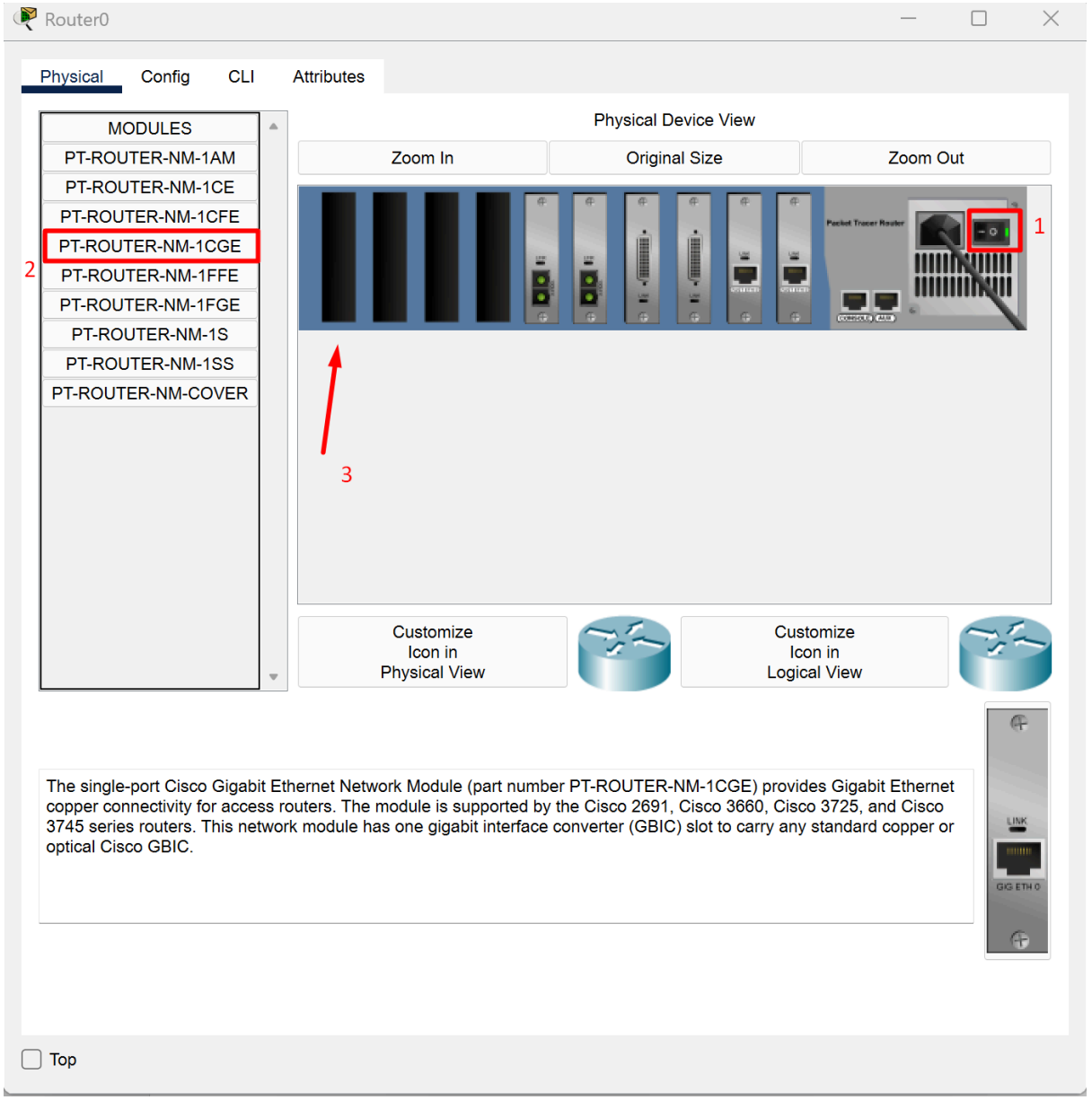


Рис. 2.4 Схема встановлення нового модуля у роутер

Закладка **CLI** надає доступ до консолі Console0 комутатора (рис. 2.5).

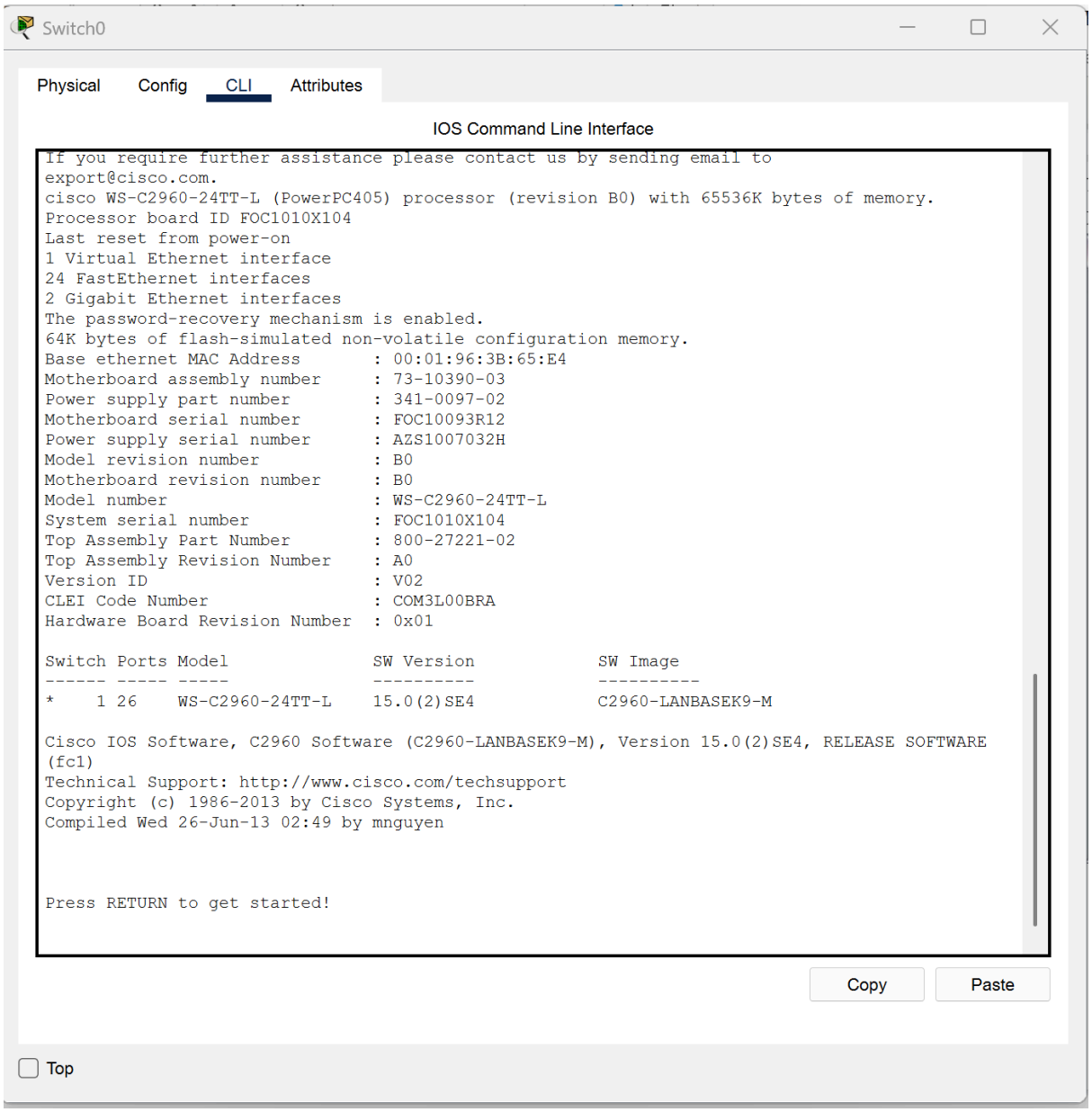


Рис. 2.5 Консоль комутатора

Вміст вікна параметрів кінцевих пристроїв залежить від самого пристрою. Параметри мережевих інтерфейсів для певного кінцевого пристрою встановлюються за допомогою меню **Settings** (рис. 2.6) та меню **FastEthernet** (рис. 2.7) на закладці **Config** відповідного кінцевого пристрою.

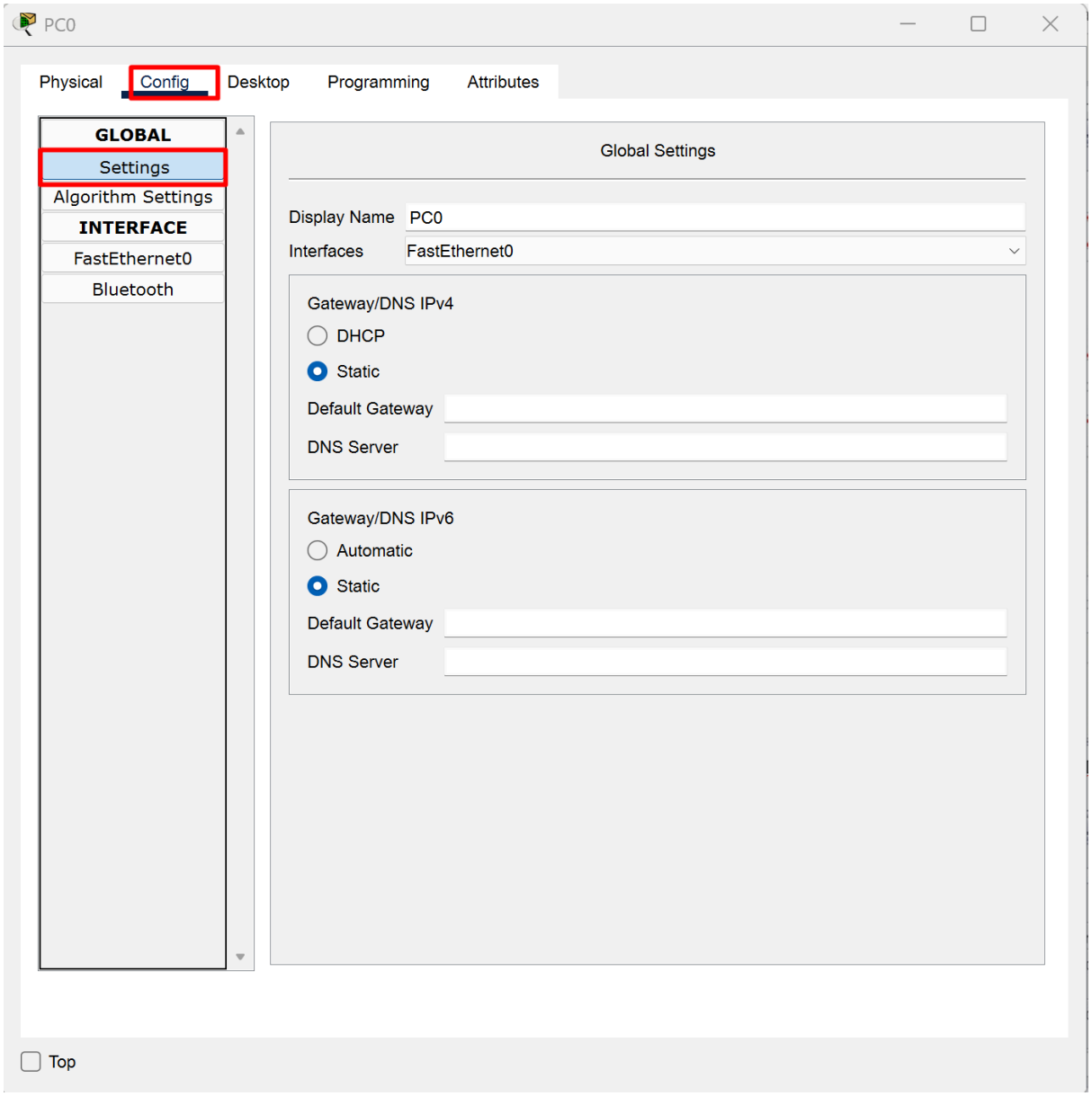


Рис. 2.6 Меню Settings закладки Config робочої станції

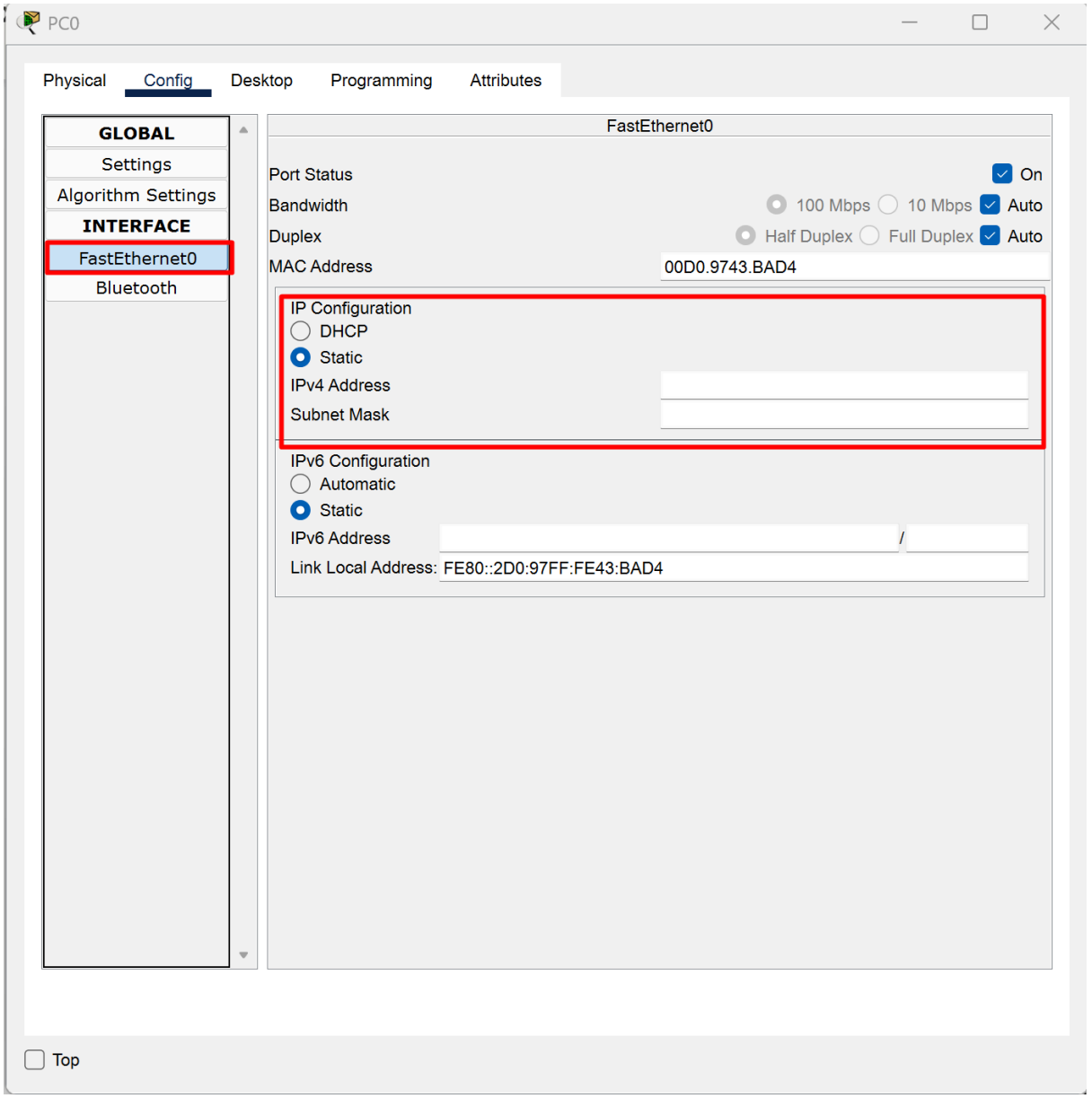


Рис. 2.7 Меню FastEthernet закладки Config робочої станції

Крім того, на закладці **Config** певні пристрої мають додаткове меню **SERVICES** (сервіси), за допомогою якого налаштовується лише необхідна для тестування базова функціональність, як-от служби HTTP, DHCP, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP.

Також мережеві налаштування кінцевого пристрою задають у вікні його параметрів, використовуючи пункт **IP Configuration** на закладці **Desktop** (рис. 2.8). Сам вміст вікна **IP Configuration** подано на рис. 2.9.

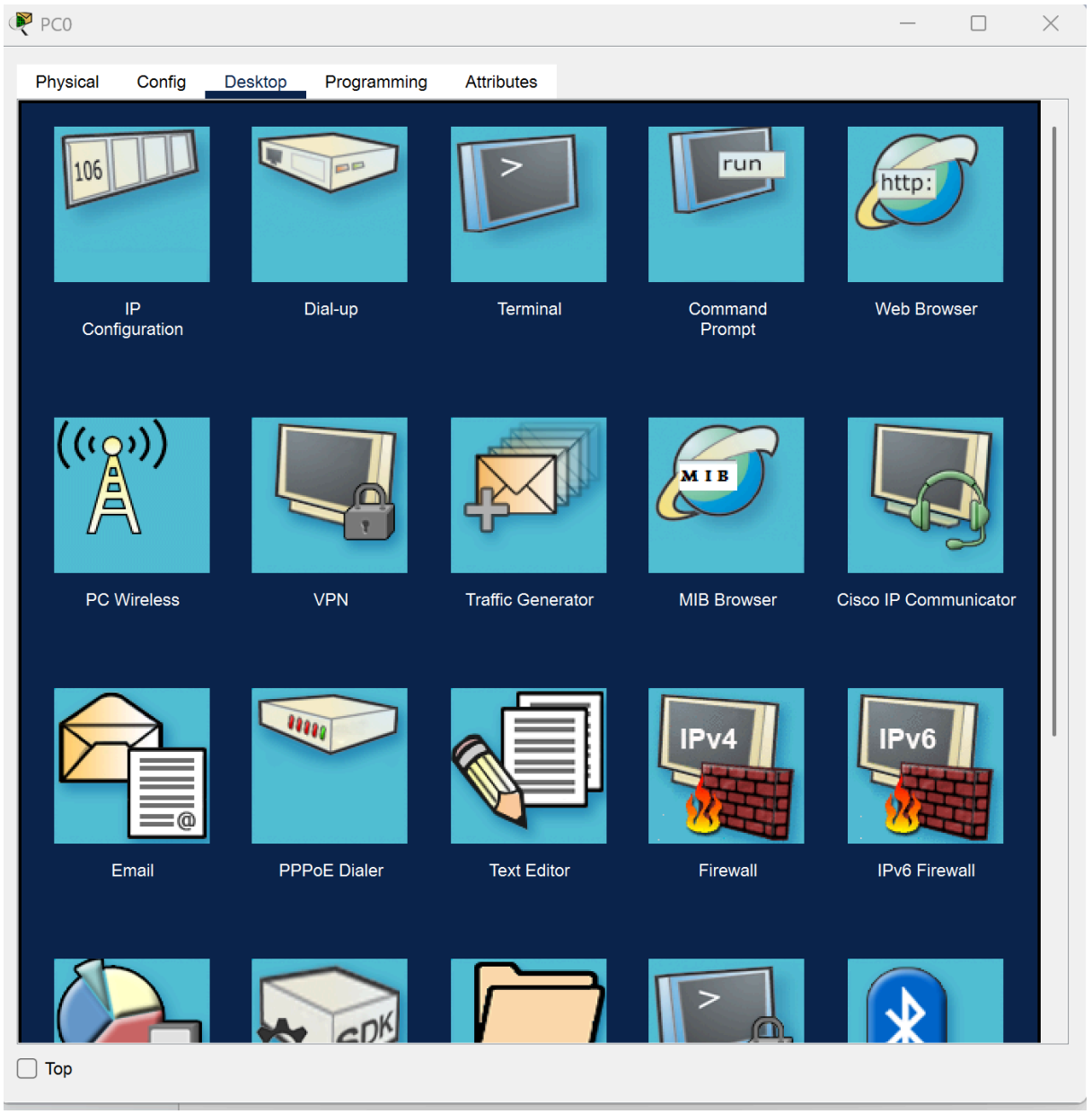


Рис. 2.8 Закладка Desktop робочої станції

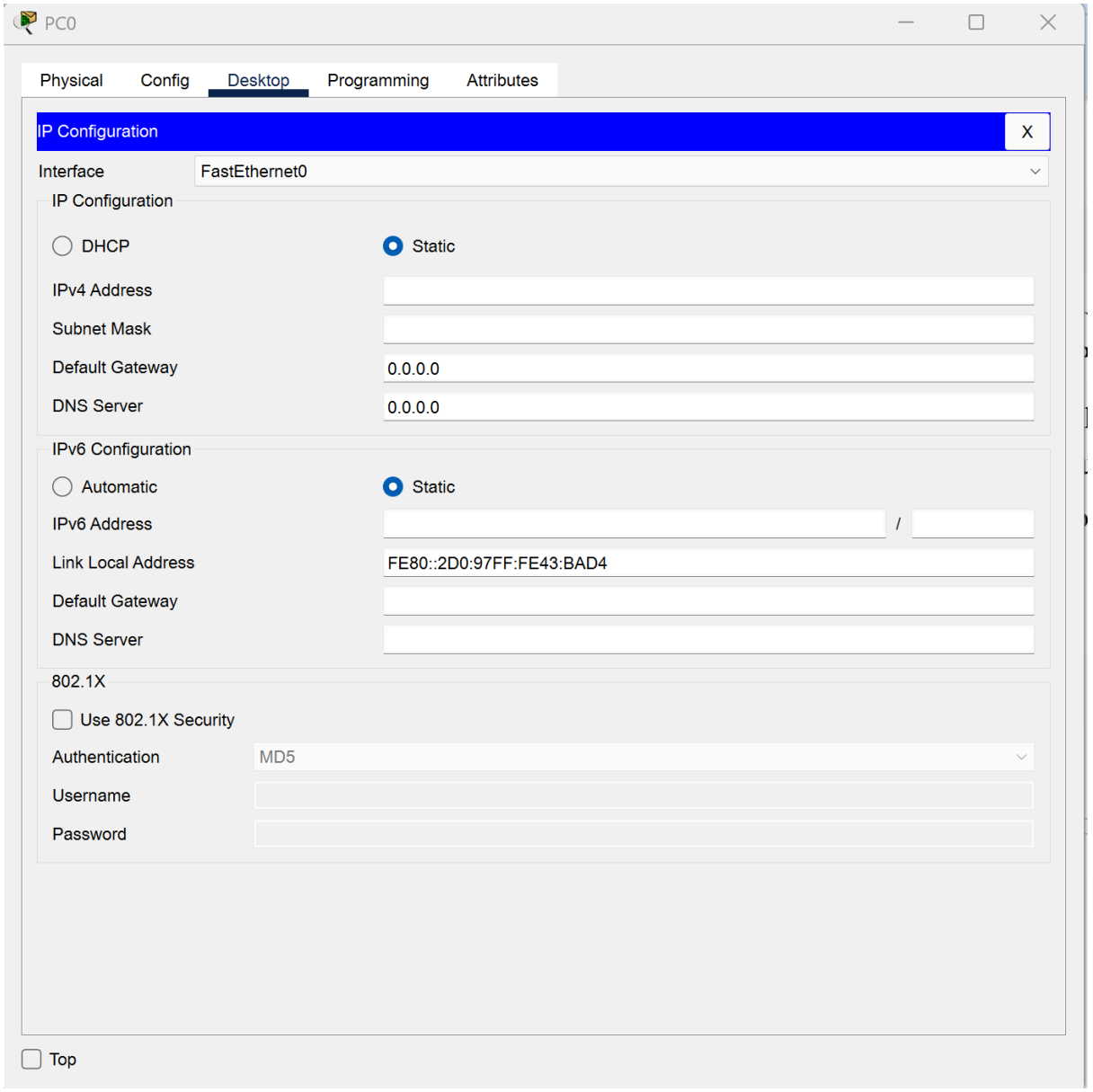


Рис. 2.9 Вікно IP Configuration робочої станції

У наступних лабораторних роботах будемо розглядати кожен пристрій окремо і всі налаштування до нього.

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

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

1. **Automatic Connection** (*Automatically choose connection type*)

Packet Tracer самостійно підбирає відповідний кабель залежно від типів портів.

2. **Console Cable** (*Console*)

Підключення між **ПК (RS-232 порт)** і **консольним портом (Console)** на маршрутизаторі або комутаторі.

Використовується для первинної CLI-конфігурації пристрою.

3. **Copper Straight-Through Cable**

   Прямий Ethernet-кабель.

   Використовується для з'єднання:

   - ПК ↔ комутатор
   - маршрутизатор ↔ комутатор
   - сервер ↔ комутатор

4. **Copper Cross-Over Cable**

   Перехресний Ethernet-кабель.

   Використовується для з'єднання:

   - ПК ↔ ПК
   - маршрутизатор ↔ маршрутизатор
   - комутатор ↔ комутатор

   (у сучасному обладнанні часто не потрібен завдяки Auto-MDIX)

5. **Fiber Optic Cable**

   Волоконно-оптичний кабель.

Для підключення пристроїв із портами **GigabitEthernet (Fiber)**, зазвичай між маршрутизаторами або високошвидкісними комутаторами.

6. **Phone Cable**

Використовується для **VoIP телефонів**, **POTS**-пристроїв або аналогових з'єднань (наприклад, факсів).

7. **Coaxial Cable**

Для симуляції мереж старого зразка або для **кабельних модемів** (Cable Modem → CMTS).

8. **Serial DCE/DTE Cable**

Послідовне з'єднання між маршрутизаторами.

Один інтерфейс має бути DCE — на ньому задається тактова частота (наприклад, `clock rate 64000`).

Як з’єднати два пристрої? Спочатку переносимо два пристрої у робочу область (рис 2.10). Тоді вибираємо з панелі типів пристроїв меню кабелі (1), далі після цього на панелі кінцевих пристроїв вибираємо необхідний тип кабелю лівою кнопкою миші (2) і перетягуємо його до необхідного пристрою.

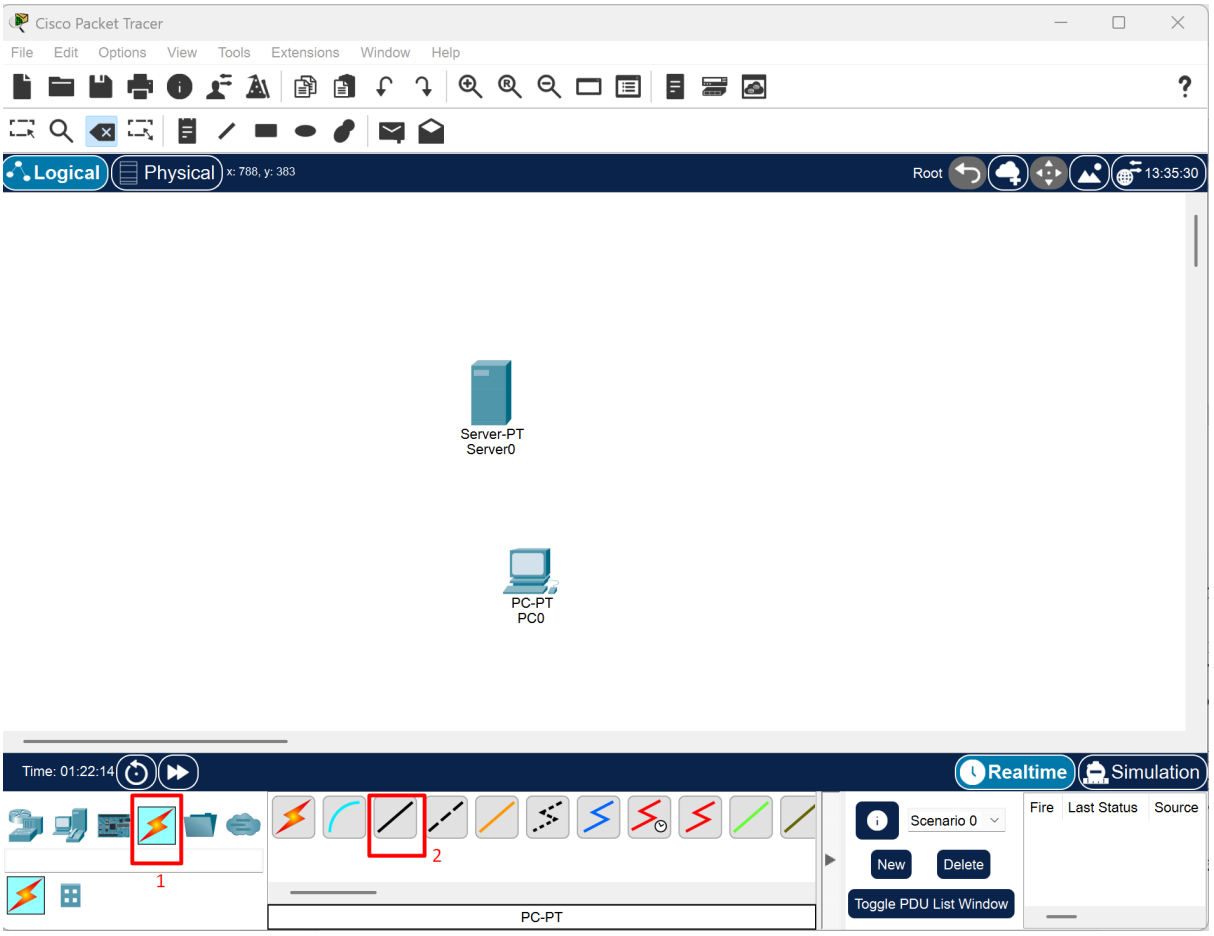


Рис. 2.10 Вибір кабелю для з’єднання

Після цього обираємо тип інтерфейсу FastEthernet0 на одному пристрої (рис 2.11) та обираємо інший пристрій лівою кнопкою миші та знову обираємо тип інтерфейсу FastEthernet0 (рис 2.12). З'єднання пристроїв відбулося. Для того щоб воно було коректним, перед цим необхідно налаштувати пристрої. Коли індикатори обох пристроїв стануть зеленими, значить все працює коректно.

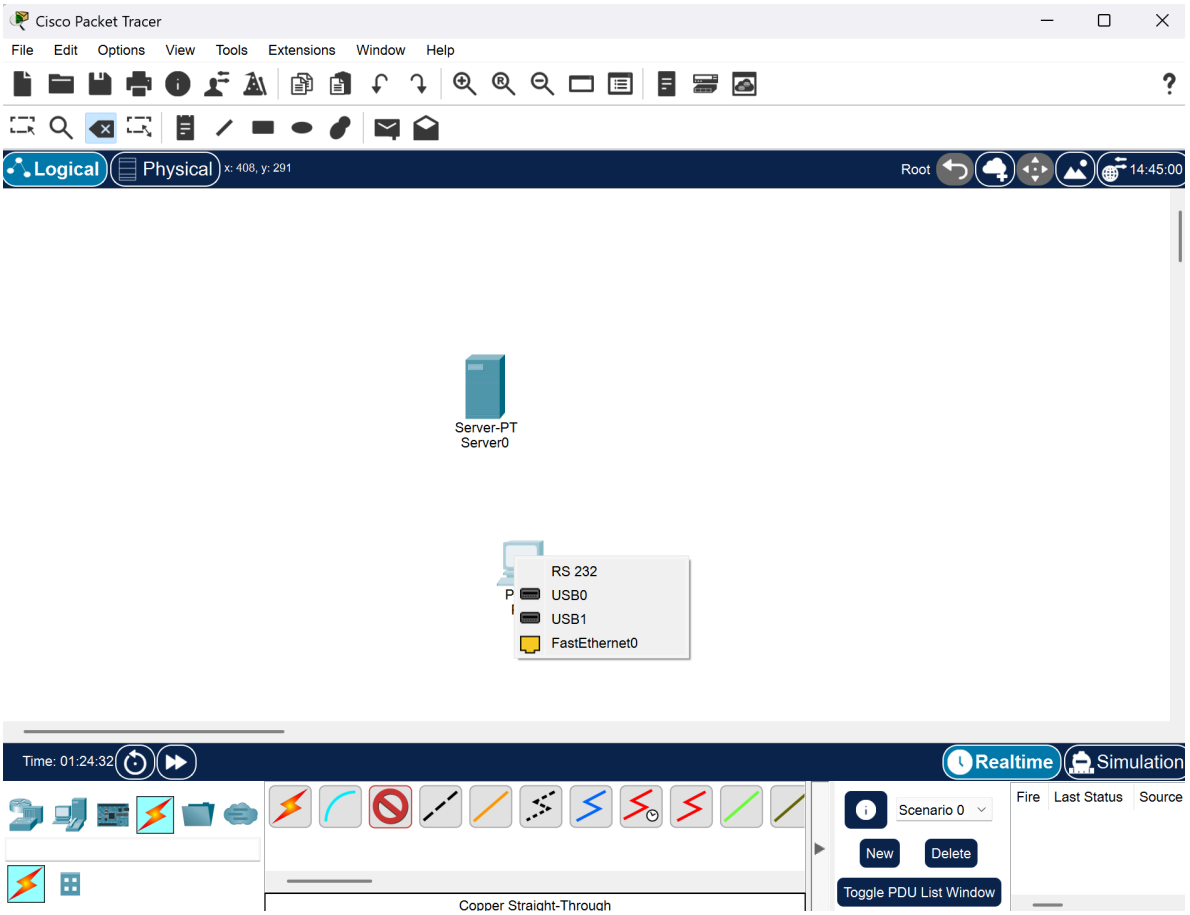


Рис. 2.11 Перетягування кабелю до одного пристрою

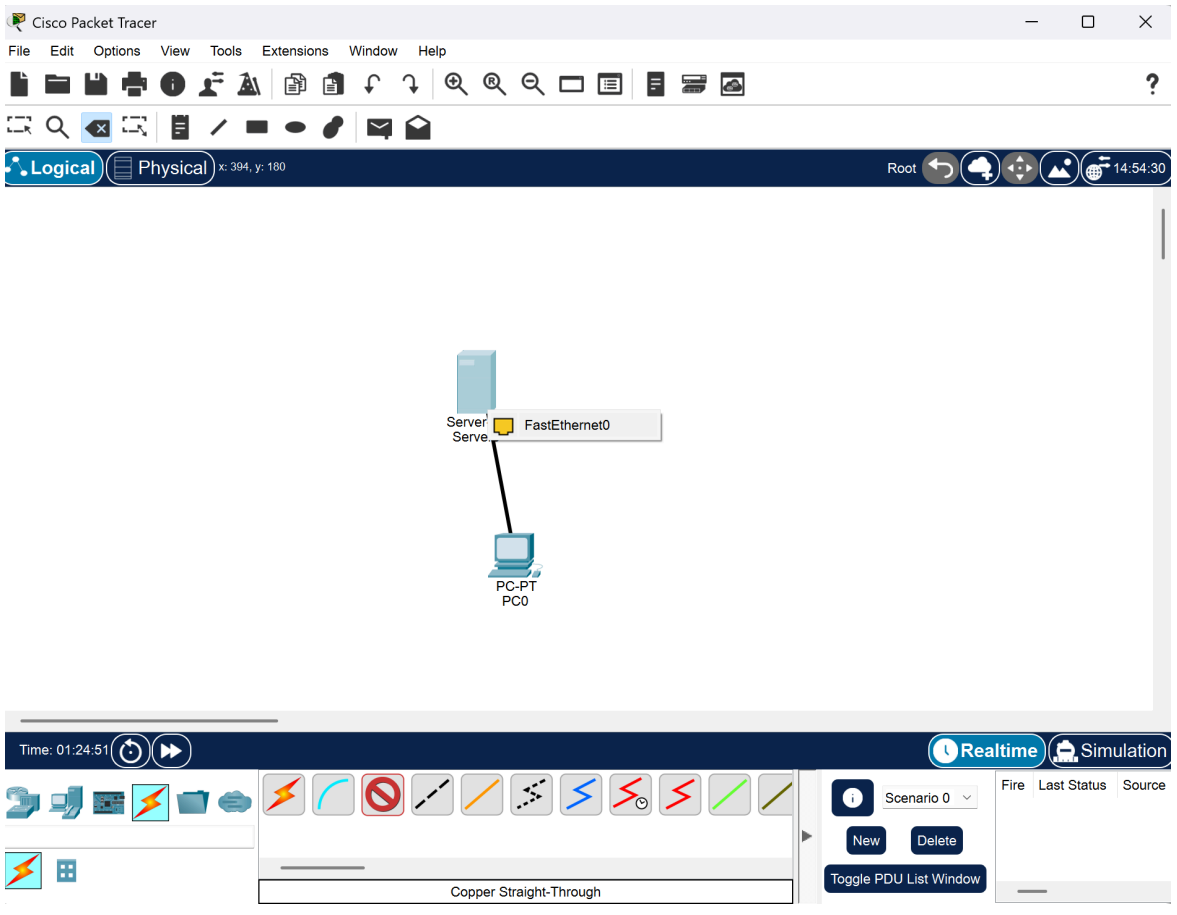


Рис. 2.12 З'єднання другого пристрою

Перед перевіркою з'єднання двох вузлів мережі (джерела та приймача), наприклад двох робочих станцій, що з'єднані з комутатором, джерелу та приймачу потрібно встановити IP-адреси та маску з однієї підмережі. Після цього потрібно переконатись, що в цей момент часу встановлений режим **Realtime** (реального часу); якщо ні, то встановити його, вибравши відповідну піктограму у правому нижньому куті вікна Cisco Packet Tracer. На панелі інструментів вибрати режим формування простих пакетів для перевірки роботи мережі за допомогою ехо-пакетів, скориставшись піктограмою **Add Simple PDU** (рис 2.13.) . Далі потрібно послідовно вибрати джерело і приймач ping-запиту. Для цього слід навести курсор і натиснути лівою кнопкою миші спочатку на PC0 (джерело ping-запиту), а потім перемістити курсор на PC1 (приймач ping-запиту) і натиснути лівою кнопкою миші на ньому.

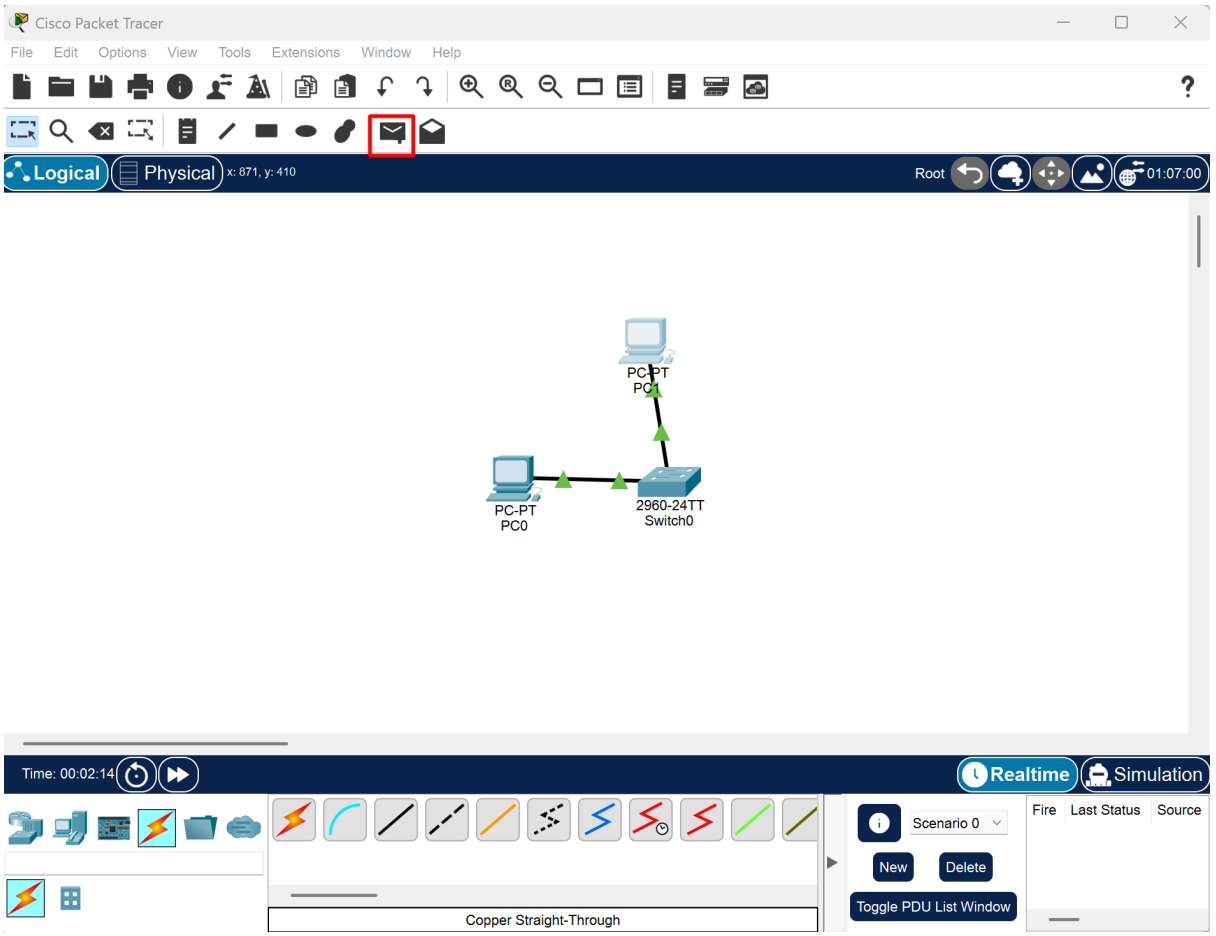


Рис. 2.13 Вибір ехо-пакетів

Так як всі мережеві інтерфейси та з'єднання налаштовані правильно (про що свідчать зелені індикатори стану), то ping-запит повинен виконуватись успішно. У вікні управління пакетами **User Created Packet Window** з'явиться відповідний

запис. Запис **Successful** у полі **Last Status** свідчить про успішне виконання ping-запиту від PC0 до PC1 (рис 2.14).

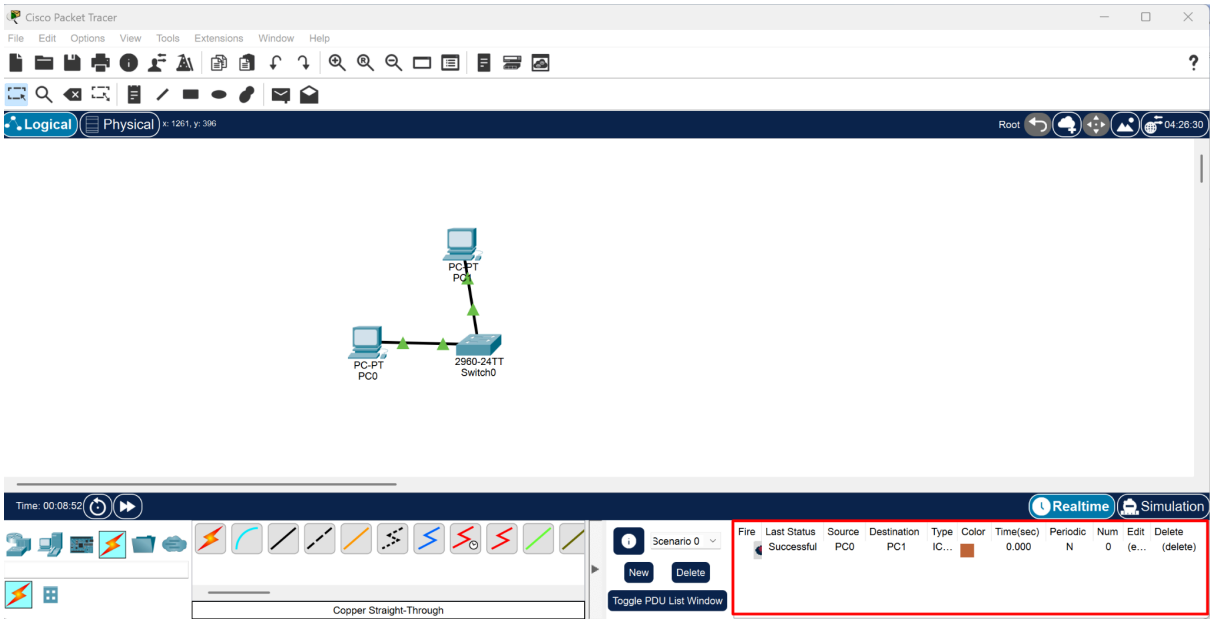


Рис. 2.14 Вікно управління пакетами User Created Packet Window

Також перевірити “видимість” пристроїв можна через командний рядок. Для цього на пристрої заходимо на закладку **Desktop** і вибираємо пункт **Command Prompt**.

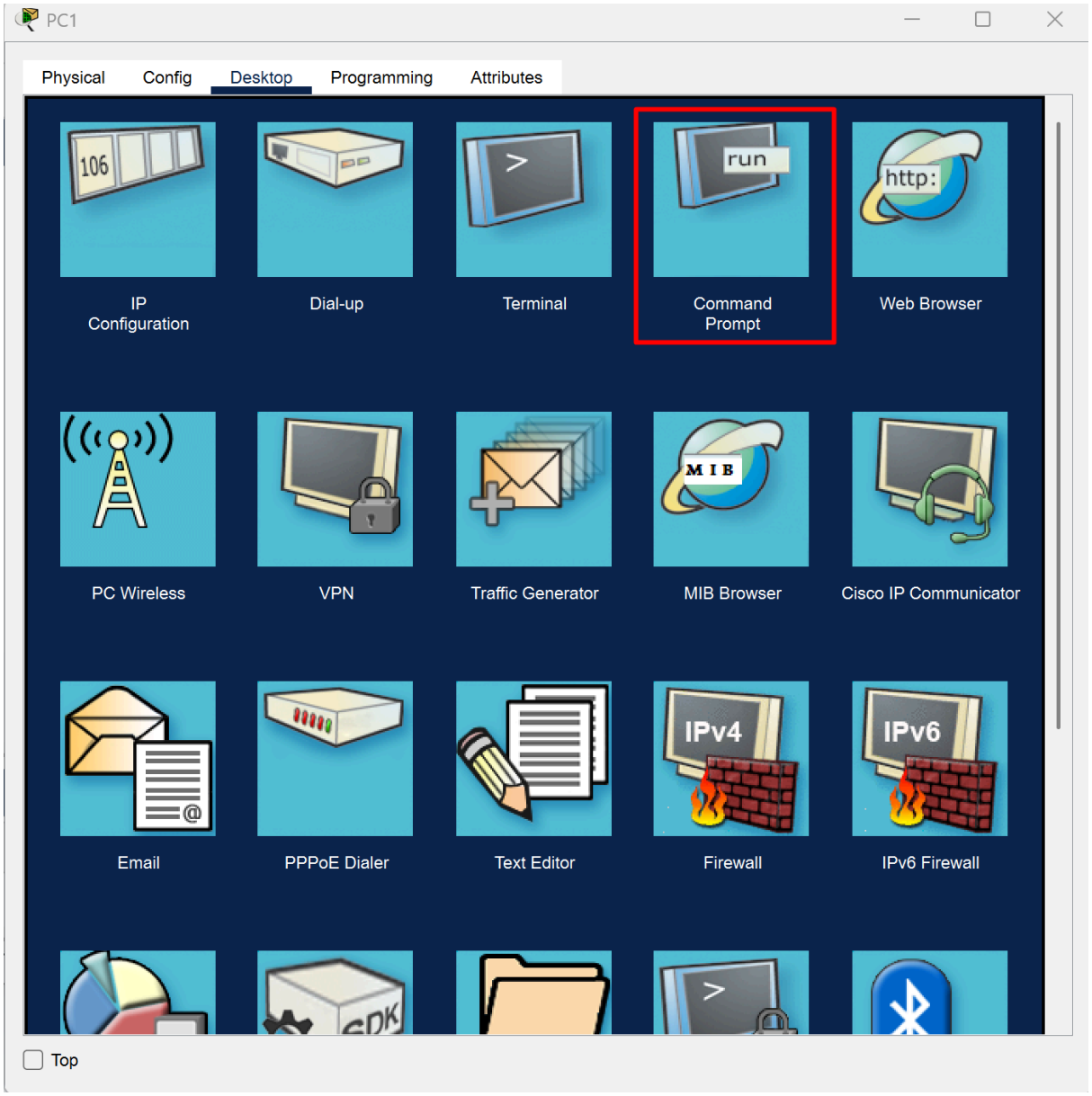


Рис. 2.15 Пункт Command Prompt закладки Desktop робочої станції

У цьому вікні є змога виконувати всі команди, пов'язані з налаштуванням та тестуванням мережі, як і в повноцінній командній стрічці операційної системи.

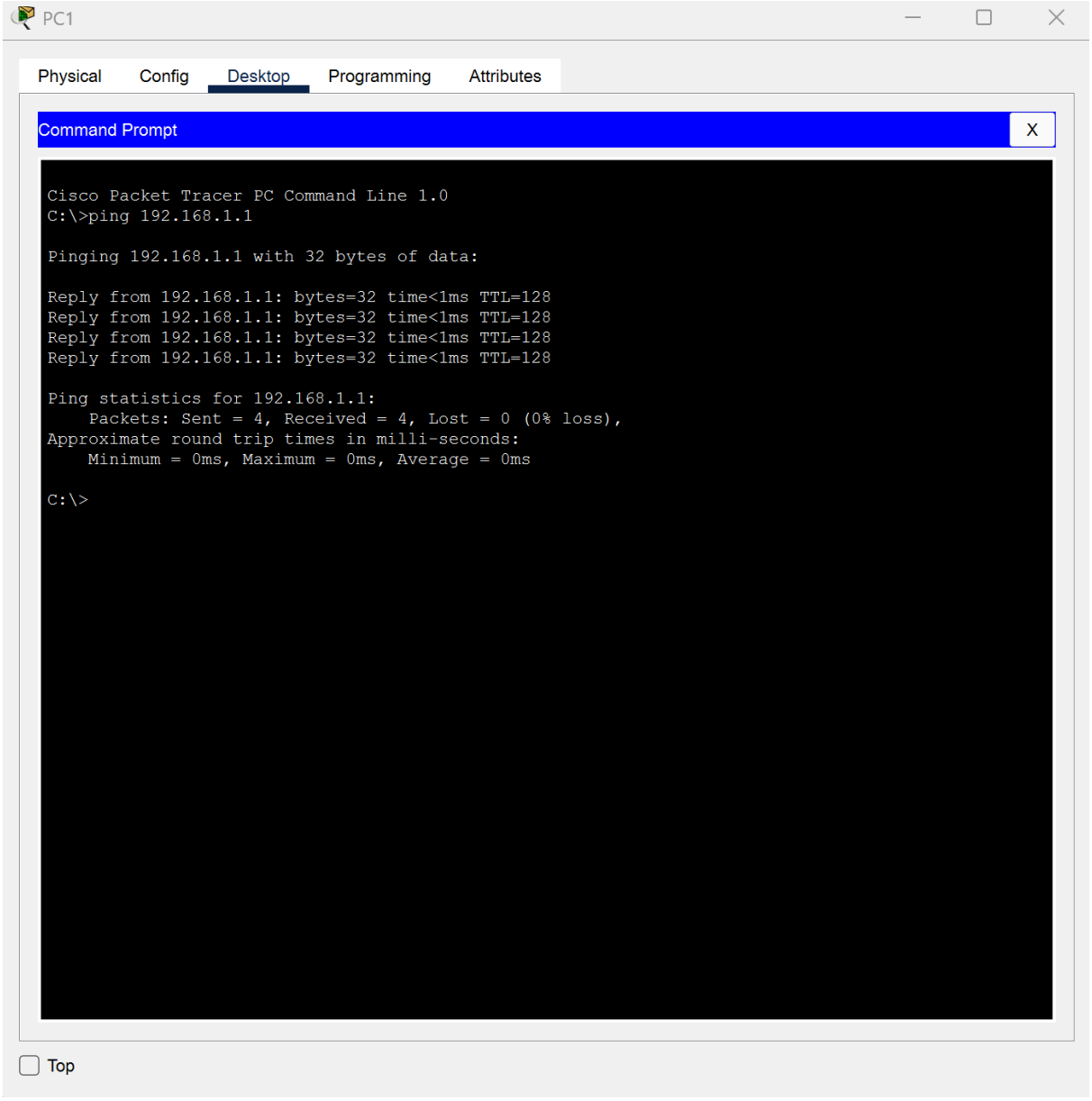


Рис. 2.16. Вікно Command Prompt закладки Desktop робочої станції

Завдання для індивідуальної роботи

1. Запустіть програму і створіть новий проєкт мережі. Назвіть проєкт.
2. Додайте у проєкт кінцеві пристрої – декілька робочих станцій, ноутбуків та сервер.
3. Змініть кінцевим пристроям, доданим у п.2, стандартні імена і налаштуйте IP-адреси згідно з варіантом з таблиці 2.1.

Таблиця 2.1. Варіанти індивідуальних завдань

Варіант	Адреса підмережі	Маска підмережі
1	192.168.10.0	255.255.255.0

Варіант	Адреса підмережі	Маска підмережі
2	192.168.20.0	255.255.254.0
3	192.168.30.0	255.255.252.0
4	192.168.40.0	255.255.255.0
5	192.168.50.0	255.255.254.0
6	192.168.60.0	255.255.252.0
7	192.168.70.0	255.255.255.0
8	192.168.80.0	255.255.254.0
9	192.168.90.0	255.255.252.0
10	192.168.100.0	255.255.255.0
11	192.168.10.0	255.255.254.0
12	192.168.20.0	255.255.252.0
13	192.168.30.0	255.255.255.0
14	192.168.40.0	255.255.254.0
15	192.168.50.0	255.255.252.0
16	192.168.60.0	255.255.255.0
17	192.168.70.0	255.255.254.0
18	192.168.80.0	255.255.252.0
19	192.168.90.0	255.255.255.0
20	192.168.100.0	255.255.254.0
21	192.168.10.0	255.255.252.0
22	192.168.20.0	255.255.255.0
23	192.168.30.0	255.255.254.0
24	192.168.40.0	255.255.252.0
25	192.168.50.0	255.255.255.0
26	192.168.60.0	255.255.254.0
27	192.168.70.0	255.255.252.0
28	192.168.80.0	255.255.255.0
29	192.168.90.0	255.255.254.0
30	192.168.100.0	255.255.252.0

1. Додайте у проєкт комутатор і з'єднайте всі пристрої за топологією “зірка”.

2. Використовуючи ехо-пакети, перевірте доступність різних вузлів мережі.
3. Збережіть проєкт мережі.

Звіт має містити:

1. Мета роботи
2. Скріншот схеми мережі
3. Таблиця IP-адрес пристроїв
4. Скріншот результатів перевірки ехо-пакетами
5. Висновки

Контрольні запитання:

1. Що таке Cisco Packet Tracer і які його основні можливості?
2. Які типи мережевих пристроїв доступні для використання в Cisco Packet Tracer?
3. Які є основні типи кабелів у Cisco Packet Tracer? Для яких пристроїв вони використовуються?
4. Як призначити статичну IP-адресу в Cisco Packet Tracer?
5. Яка різниця між вкладками **Config** та **CLI** на мережевих пристроях?
6. Як перевірити з’єднання між пристроями в Cisco Packet Tracer?
7. Що таке PDU в Packet Tracer? Як його використовувати?
8. Для чого використовується команда **ping** і що означає її результат?
9. Які сервіси можна активувати на сервері у Cisco Packet Tracer?
10. У чому полягає різниця між логічним та фізичним режимом перегляду мережі у Packet Tracer?

ЛАБОРАТОРНА РОБОТА № 3
СТВОРЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ CISCO PACKET TRACER ІЗ СЕРВЕРОМ ТА АВТОМАТИЧНОЮ АДРЕСАЦІЄЮ

Мета роботи: Закріпити навички побудови комп'ютерної мережі у Cisco Packet Tracer та навчитися: використовувати сервер, налаштовувати DHCP, перевіряти підключення між кількома пристроями, користуватись базовими службами, як HTTP і DNS.

Теоретичні відомості:

Локальна мережа (Local Area Network, **LAN**) — це система взаємопов'язаних комп'ютерів, які знаходяться в межах обмеженої території (наприклад, офісу, навчального закладу чи будинку) та мають можливість обміну даними. Основними пристроями для створення LAN є комутатори (Switch), маршрутизатори (Router), сервери та клієнтські пристрої (ПК, ноутбуки тощо).

Сервер — це спеціалізований комп'ютер або пристрій, що надає ресурси чи послуги іншим комп'ютерам у мережі (клієнтам). У межах цієї лабораторної роботи сервер виконує такі функції:

- DHCP-сервера — для автоматичної видачі IP-адрес;
- DNS-сервера — для перетворення доменних імен у IP-адреси;
- HTTP-сервера — для надання вебсторінок клієнтам.

DHCP (Dynamic Host Configuration Protocol) використовується для автоматичного надання IP-адрес та інших мережевих параметрів (маски підмережі, шлюзу, DNS) пристроям у мережі. Це дозволяє комп'ютерам, смартфонам, принтерам та іншим пристроям швидко отримувати доступ до мережі без необхідності ручного налаштування. DHCP особливо корисний у великих мережах, де ручне введення параметрів для кожного пристрою було б надто трудомістким і призводило б до помилок або конфліктів IP-адрес.

Завдяки DHCP адміністратори економлять час і зменшують ризик помилок, пов'язаних із неправильним введенням налаштувань. Система забезпечує гнучкість:

пристрої можуть переміщуватись між мережами, вмикатись і вимикатись — і все одно отримуватимуть коректні параметри. Це робить DHCP ключовим елементом сучасних комп’ютерних мереж.

DNS (Domain Name System) — це система, яка перетворює зрозумілі для людини доменні імена, такі як *google.com* або *myserver.local*, на числові IP-адреси, які використовують комп’ютери для зв’язку між собою. Завдяки DNS користувачі можуть відкривати вебсайти або звертатися до серверів, вводячи прості імена замість складних чисел. Система працює як телефонна книга для інтернету: вона знаходить відповідну IP-адресу за заданим ім’ям.

DNS є важливим компонентом будь-якої комп’ютерної мережі, включно з локальними. Він спрощує доступ до ресурсів і дозволяє уникати запам’ятовування IP-адрес. У локальних мережах DNS використовується для іменування серверів, принтерів або інших пристроїв, що полегшує їх пошук і використання. Без DNS мережеві сервіси були б менш зручними та потребували б більше технічних знань від користувачів.

У цій лабораторній DNS використовується для локальної маршрутизації імен у мережі Packet Tracer.

HTTP — це протокол передачі гіпертексту, який використовується для обміну вебсторінка між клієнтами та вебсервер. Коли користувач у браузері вводить адресу (доменне ім’я), запит надсилається до HTTP-сервера, який відповідає вмістом вебсторінки. У Packet Tracer HTTP-сервер може імітувати базову вебсторінку.

IP-адресація — це процес присвоєння унікальних ідентифікаторів (IP-адрес) пристроям у мережі. Існують два основні типи IP-адрес:

- Статична — налаштовується вручну;
- Динамічна — надається автоматично за допомогою DHCP.

У лабораторній роботі використовується динамічна адресація для ПК і статична для сервера та маршрутизатора.

Маршрутизатор (Router) з’єднує різні мережі, забезпечує маршрутизацію пакетів та виступає як шлюз за замовчуванням для клієнтів. Шлюз — це пристрій, через який трафік мережі направляється до інших мереж або інтернету.

Для того щоб перевірити доступність пристроїв у мережі можна використати такі способи:

- **Ping** — надсилає ICMP-пакет для перевірки наявності з’єднання;
- **Web Browser** — перевірка роботи HTTP-сервера;
- **NSLookup** (в Packet Tracer – через DNS-перевірку) — для тестування роботи DNS.

Хід роботи

Для прикладу створюємо новий проєкт в Cisco Packet Tracer. У робочу область переносимо 1 сервер, 1 комутатор (Switch 2960), 1 маршрутизатор (Router), 3 ПК. З’єднуємо сервер і комп’ютери з комутатором через FastEthernet, використовуючи скручену пару.

Додайте Gigabit Ethernet-модуль PT-ROUTER-NM-1CGE до роутера для підключення мережі. Для цього натисніть на роутер та зайдіть у вкладку *Physical*. Спершу необхідно вимкнути роутер. На рис. 3.1 вмикач позначено під номером 1. Тоді вибрати необхідний модуль (під номером 2) і перетягнути у вільне гніздо (номер 3). Після встановлення модуля увімкнути роутер.

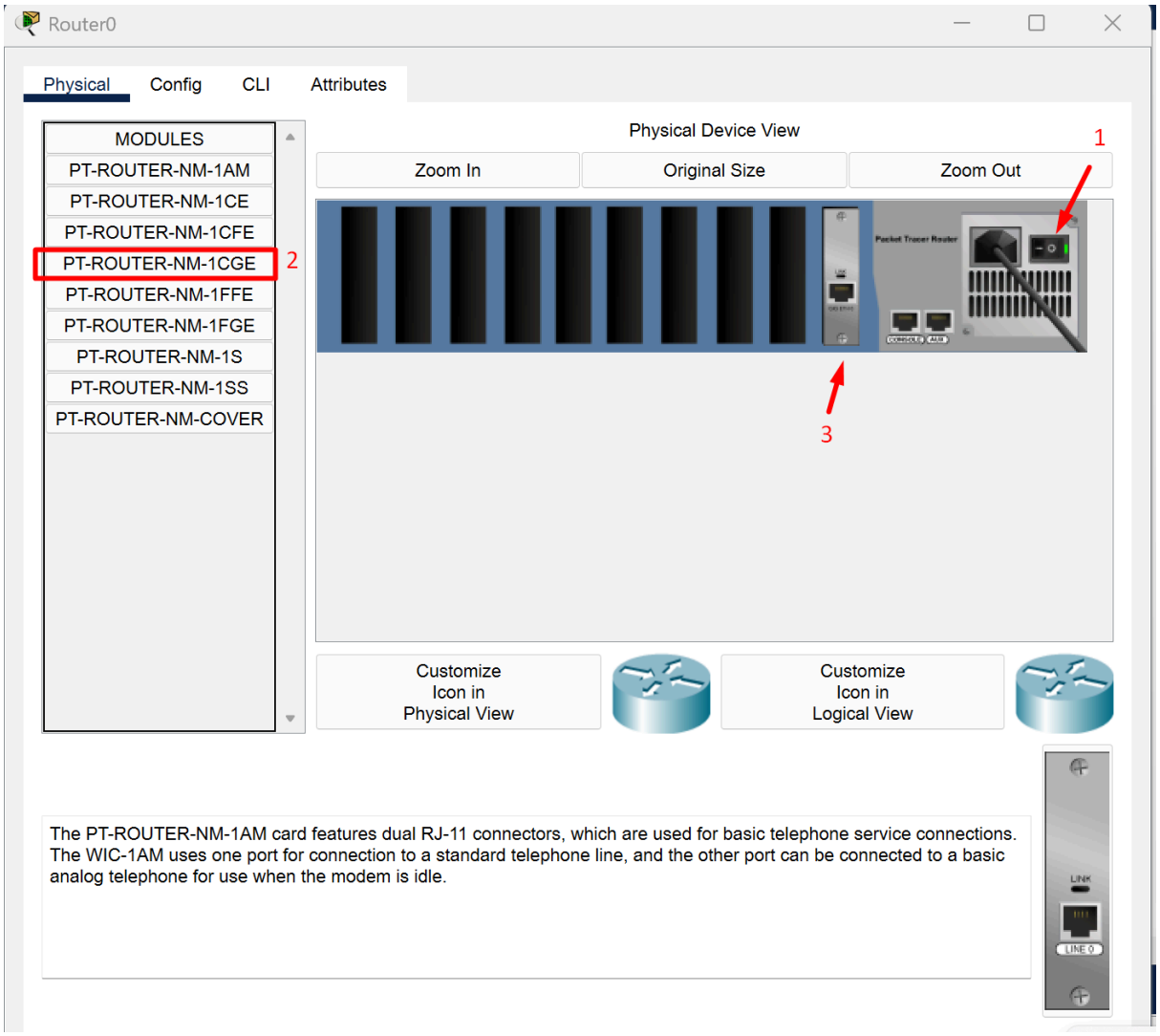


Рис. 3.1 Додавання модуля до роутера

Після встановлення необхідного модуля з'єднуємо роутер з комутатором через GigabitEthernet, використовуючи скручену пару.

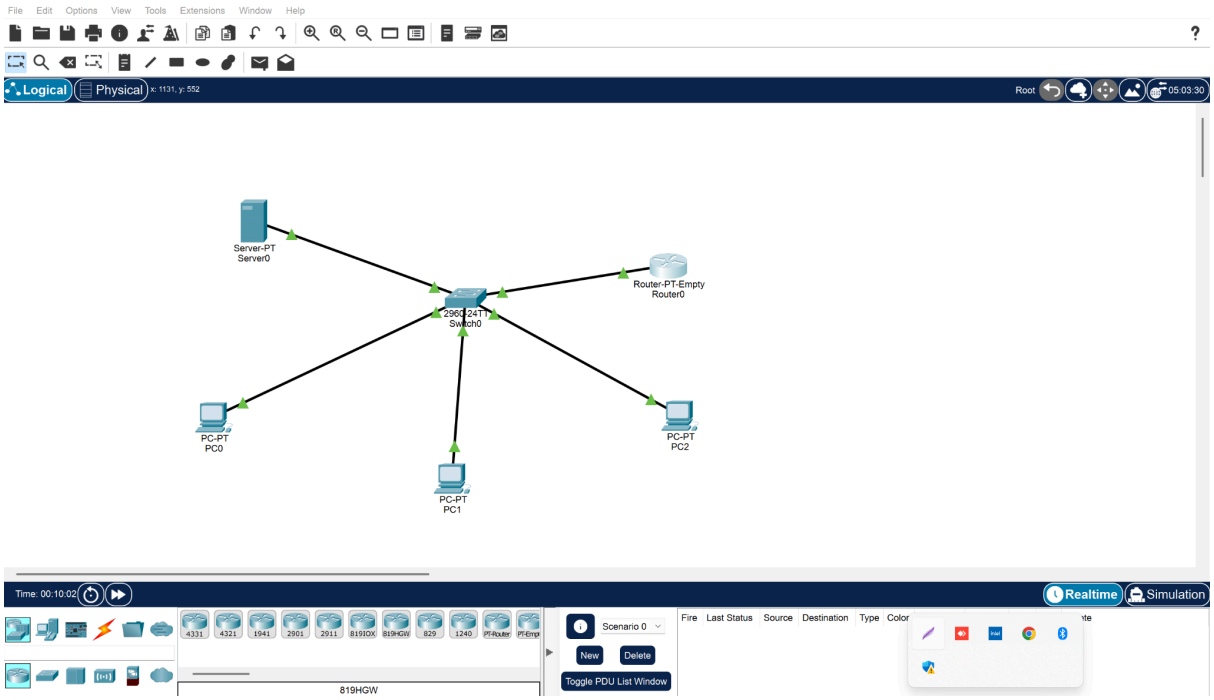


Рис. 3.2 Схема мережі

Налаштовуємо сервер:

Заходимо на вкладку `Config → FastEthernet0`: в поле IP пишемо IP-адресу сервера `192.168.10.1` та маску: `255.255.255.0`.

Далі вкладка `Services → DHCP`: в поле `Default Gateway` пишемо `Gateway IP 192.168.50.254`, в поле `DNS Server` пишемо IP-адресу сервера `192.168.10.1`, в поле `Start IP` Address пишемо IP з якого розпочнеться роздача `192.168.10.100` та в полі `Maximum Number of Users` пишемо максимальну кількість користувачів, тут `100`. Все це змінюємо у створеному пулі `serverPool` і зберігаємо зміни кнопкою `Save`, потім `ON` (рис. 3.3).

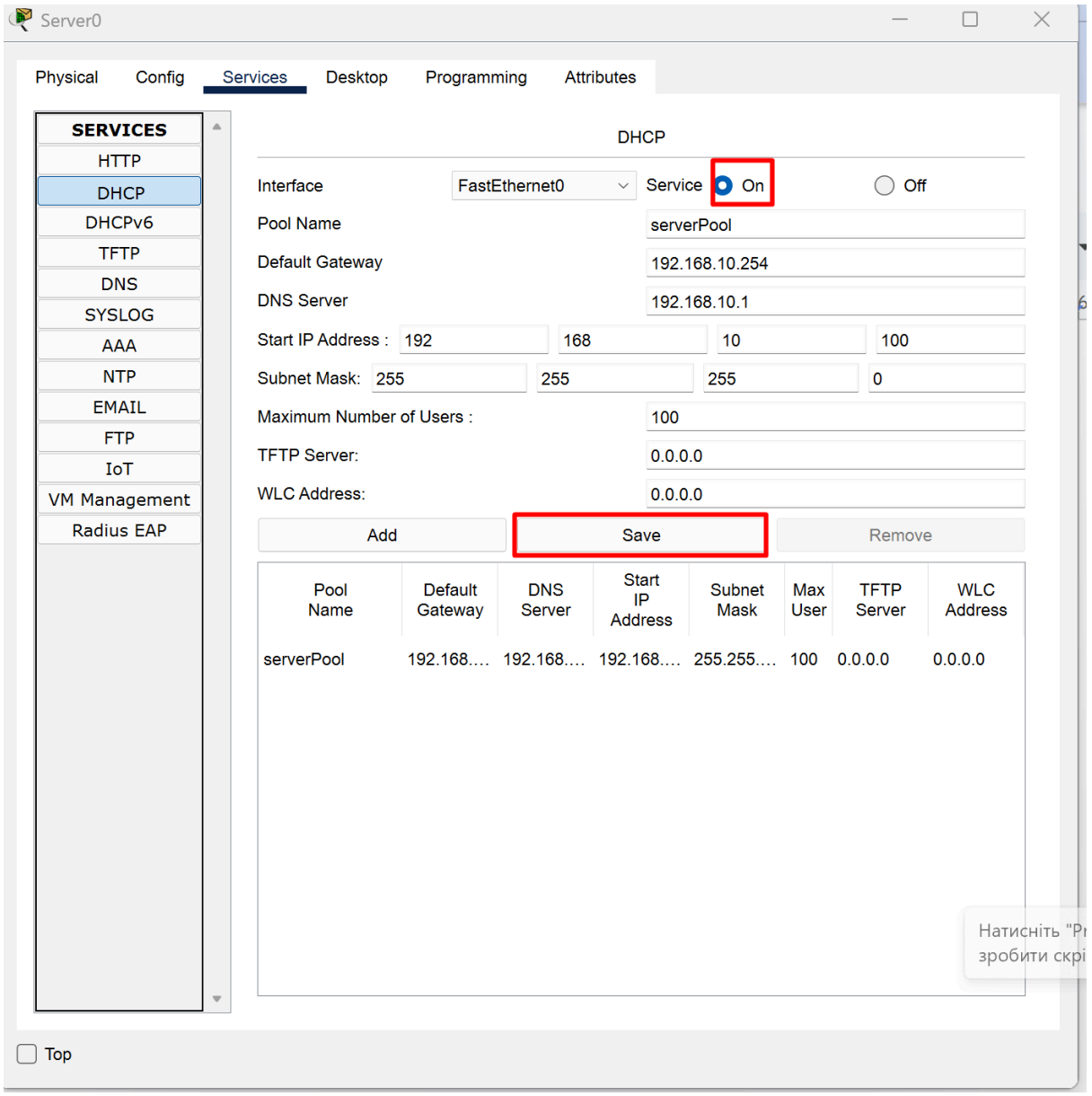


Рис. 3.3 Налаштування DHCP на сервері

Наступною обираємо вкладку *Services* → HTTP та ставимо перемикач на перемикач ON (рис. 3.4).

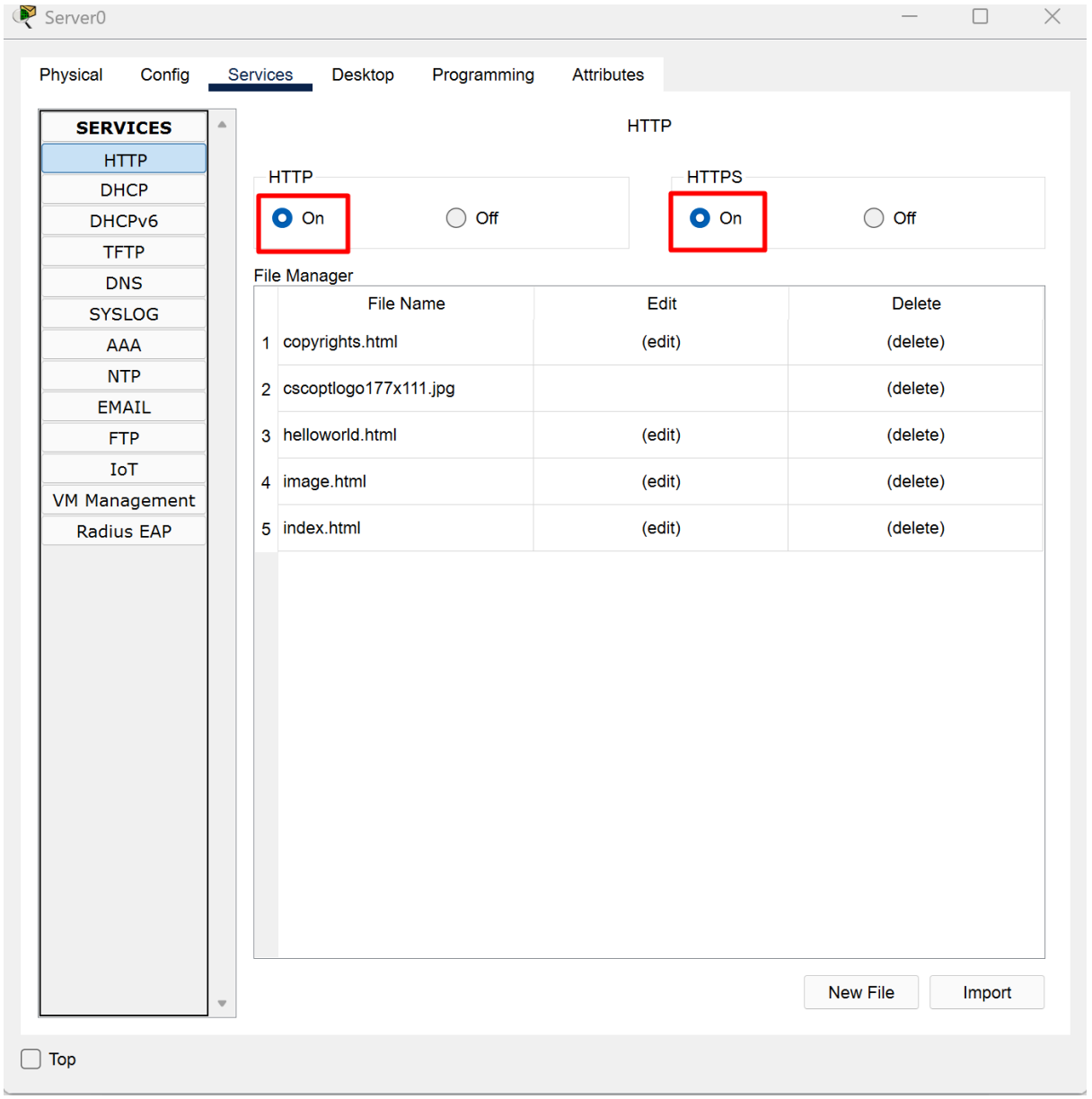


Рис. 3.4 Схема включення HTTP на сервері

Після цього обираємо вкладку *Services* → DNS. У полі Name записуємо ім'я DNS `myserver.local`, а в полі Address пишемо IP-адресу сервера `192.168.10.1` та натискаємо кнопку ADD, тоді перемикач ON (рис. 3.5).

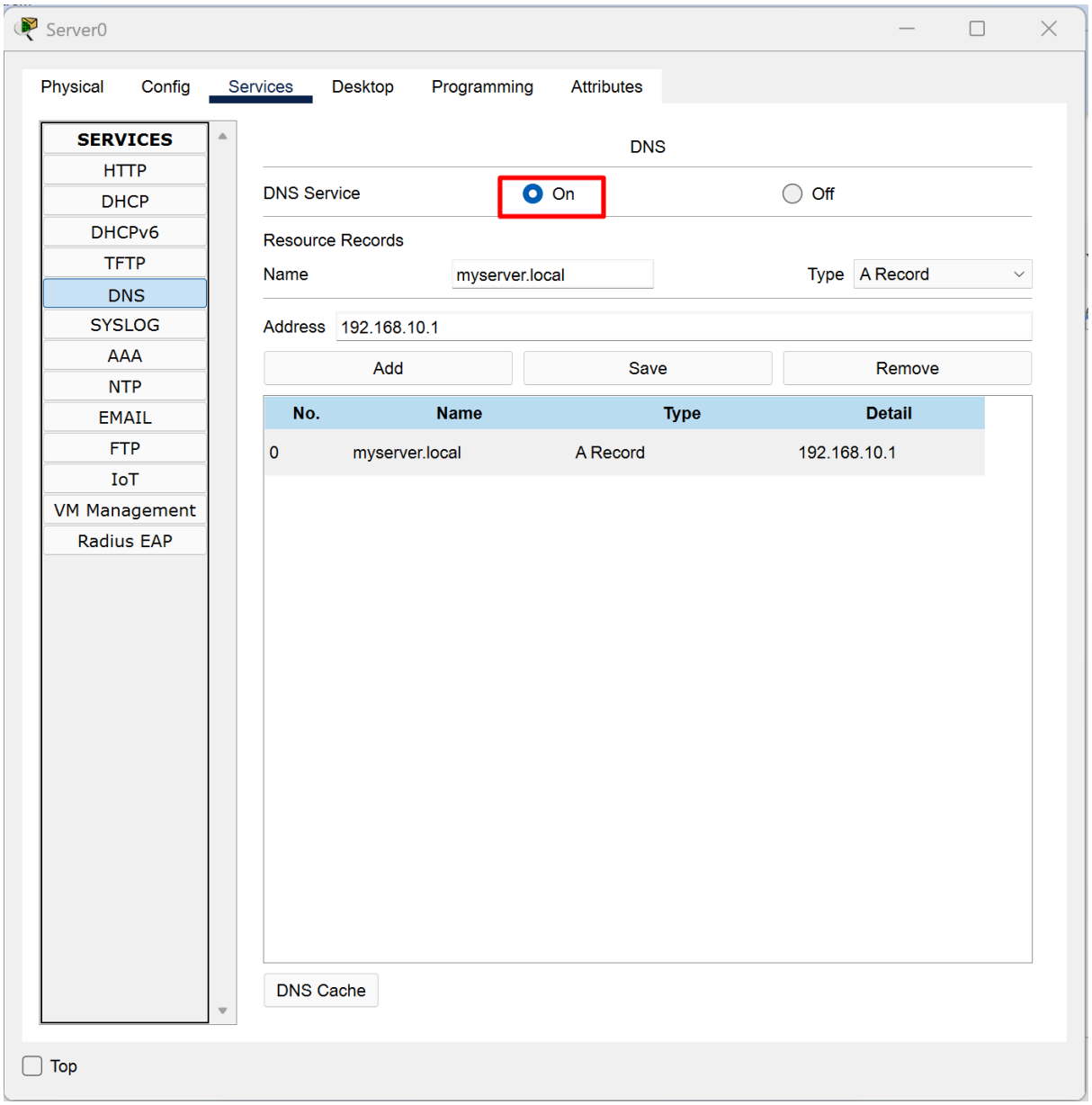


Рис. 3.5 Налаштування DNS на сервері

Налаштовуємо роутер:

Заходимо у вкладку *Config* → GigabitEthernet0/0 та в полі IPv4 Address записуємо Gateway IP `192.168.10.254`, в поле Subnet Mask: `255.255.255.0`. Не забудьте увімкнути порт On (рис. 3.6).

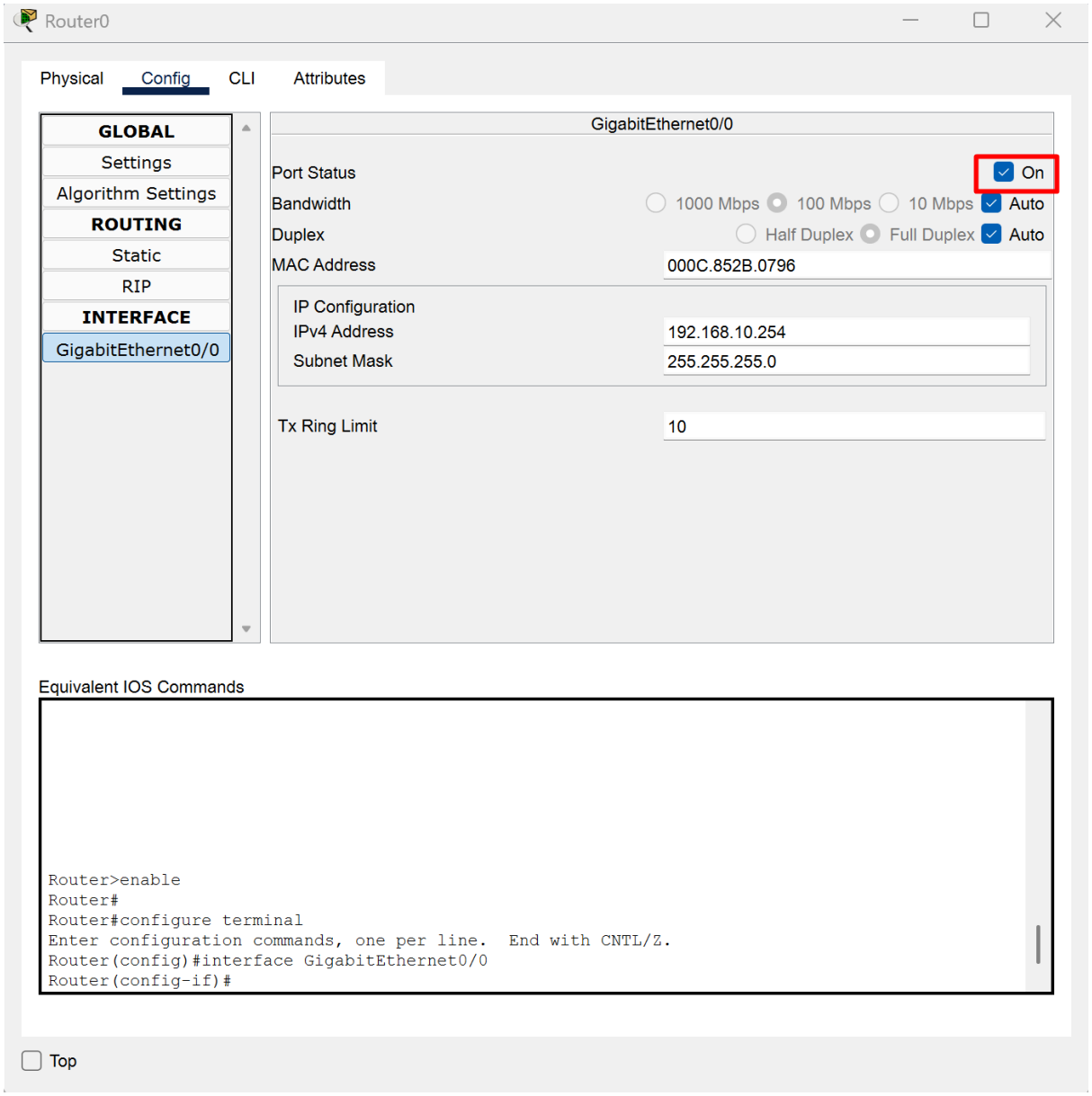


Рис. 3.6 Налаштування IP на роутері

Наступні налаштування робимо для всіх ПК. Заходимо на вкладку *Desktop* → IP Configuration → DHCP. Перевіряємо отримання адреси (рис. 3.7).

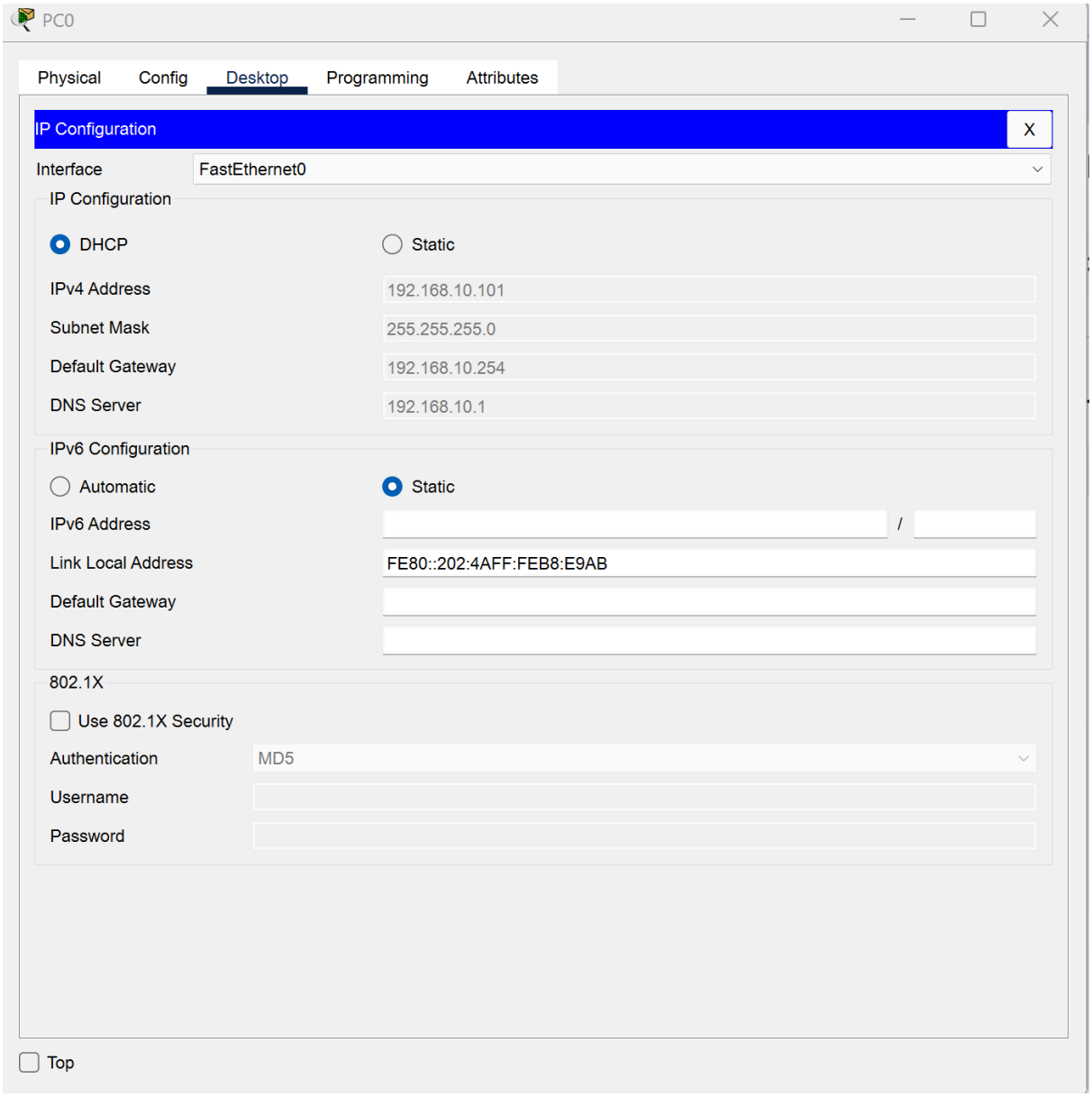


Рис. 3.7 Отримана IP адреса на комп'ютері

Наступним кроком робимо перевірку. Заходимо на ПК, обираємо вкладку *Desktop* → Command Promt і пишемо команду *ping* `192.168.10.1` для перевірки з'єднання з сервером (рис 3.8).

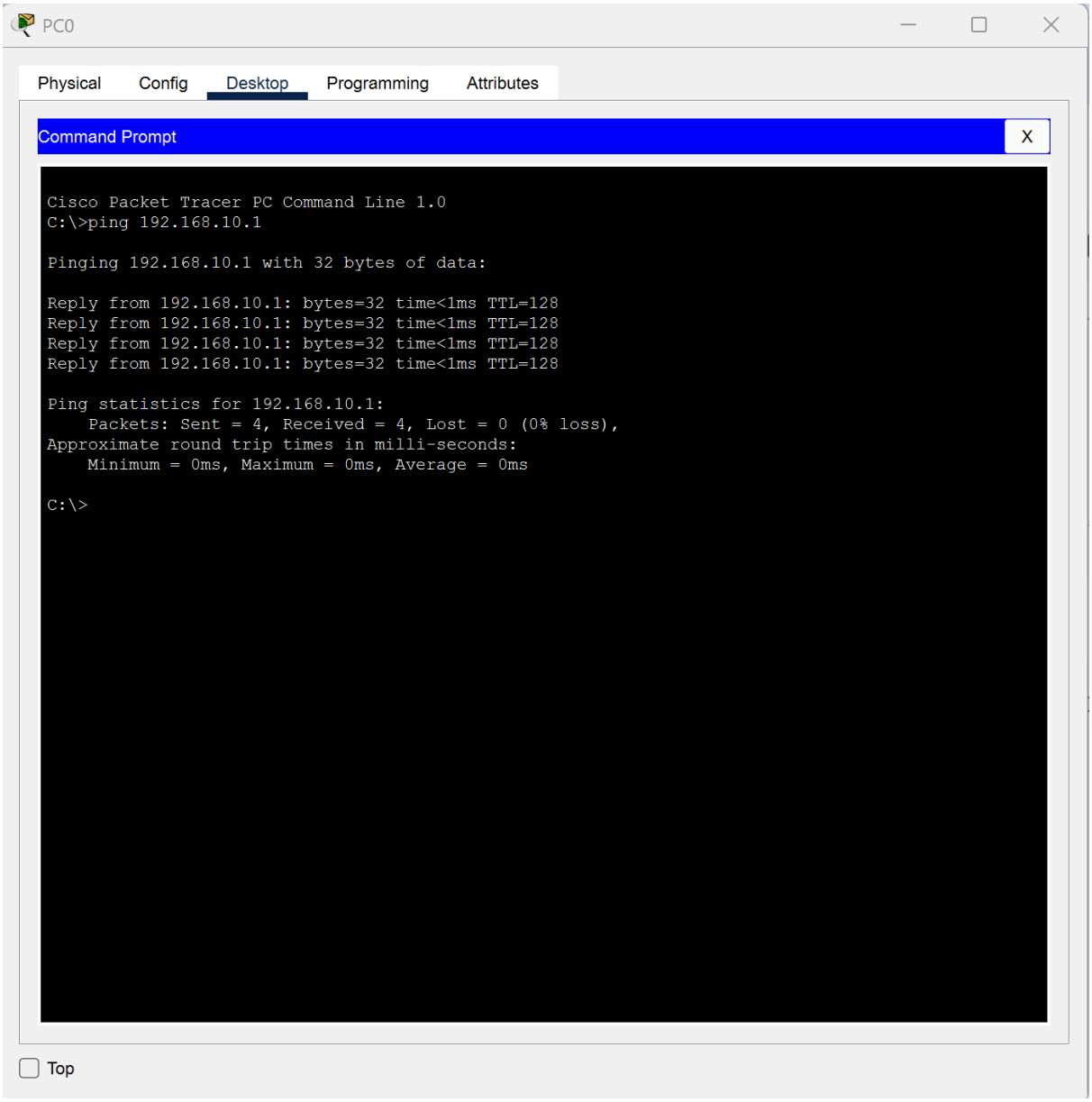


Рис. 3.8 Виконання PING - запиту до сервера з ПК

Знову заходимо на ПК, обираємо вкладку *Desktop* → Web Browser і у полі URL пишемо DNS-ім'я, в цьому випадку `myserver.local` та натиснути кнопку Go (рис 3.9).

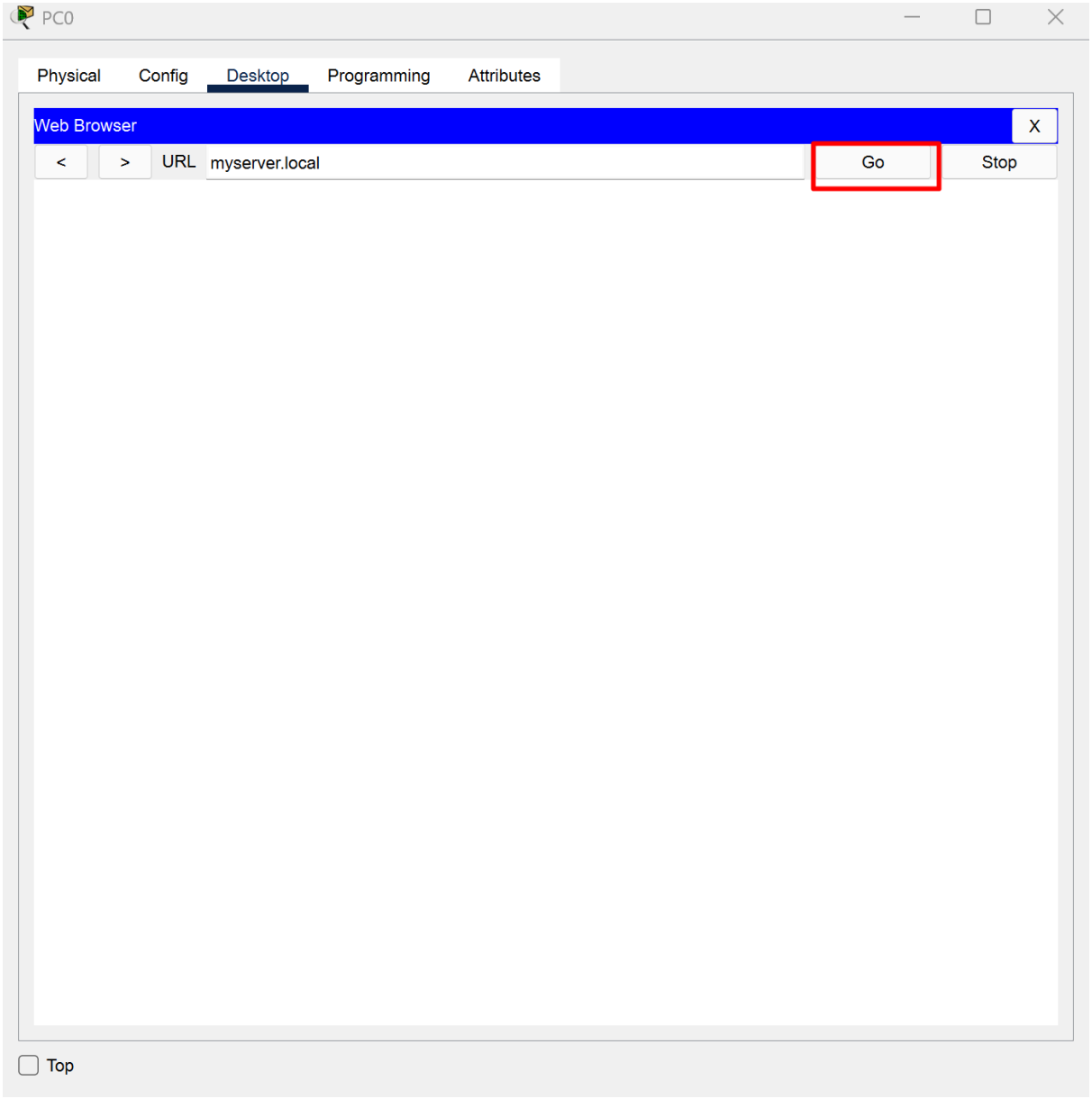


Рис. 3.9 Схема введення DNS-імені

Якщо всі налаштування виконані правильно, то відкриється початкова сторінка, що означає:

- DNS-запит успішно перетворив myserver.local на `192.168.10.1`;
- HTTP-сервер на цій адресі відповідає;
- з'єднання між ПК і сервером працює.

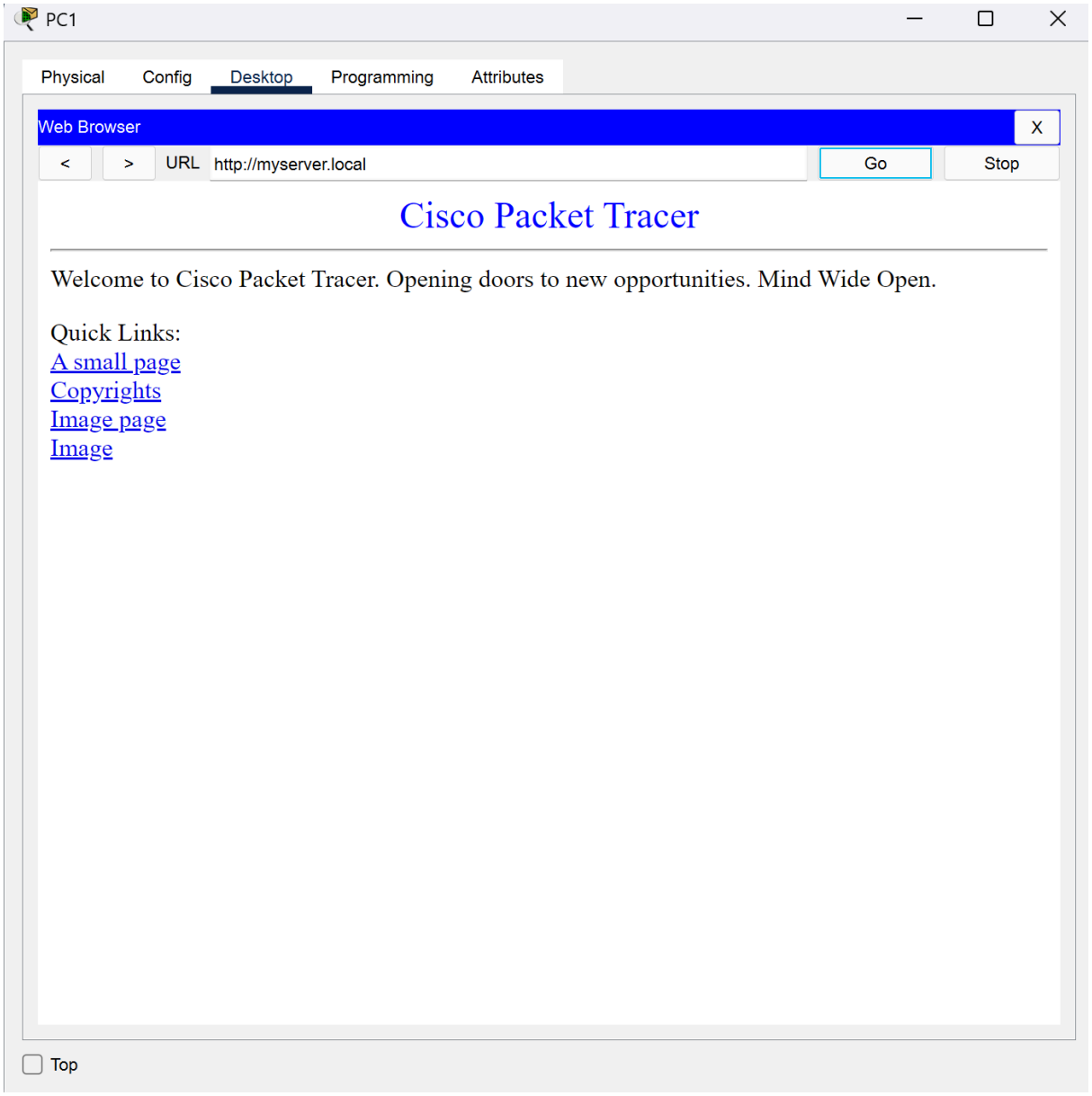


Рис. 3.10 Доступ до HTTP-сервера

Завдання для індивідуальної роботи

1. Створіть новий проєкт та назвіть його.
2. Додайте в робочу область Cisco Packet Tracer 1 сервер, 1 комутатор (Switch 2960), 1 маршрутизатор (Router), 3 ПК, 2 ноутбуки.
3. Об’єднайте всі пристрої за допомогою витої пари. Порти підключення роутера і комутатора – GigabitEthernet, решти пристроїв з комутатором - FastEthernet.
4. Зробіть налаштування сервера, роутера та комп’ютерів відповідно до свого варіанту з таблиці 3.1.

Таблиця 3.1

Варіант	IP-адреса сервера	DNS-ім’я	Gateway IP	DHCP Start IP
1	192.168.5.1	classroom.local	192.168.5.254	192.168.5.100
2	192.168.20.1	labserver.local	192.168.20.254	192.168.20.100
3	192.168.30.1	netserver.local	192.168.30.254	192.168.30.100
4	192.168.40.1	alpha.local	192.168.40.254	192.168.40.100
5	192.168.50.1	delta.local	192.168.50.254	192.168.50.100
6	10.0.0.1	intranet.local	10.0.0.254	10.0.0.100
7	172.16.0.1	webhost.local	172.16.0.254	172.16.0.100
8	192.168.60.1	beta.local	192.168.60.254	192.168.60.100
9	192.168.70.1	omega.local	192.168.70.254	192.168.70.100
10	192.168.80.1	testlab.local	192.168.80.254	192.168.80.100
11	192.168.90.1	node.local	192.168.90.254	192.168.90.100
12	192.168.100.1	edu.local	192.168.100.254	192.168.100.100
13	192.168.110.1	data.local	192.168.110.254	192.168.110.100
14	192.168.120.1	printer.local	192.168.120.254	192.168.120.100
15	192.168.130.1	access.local	192.168.130.254	192.168.130.100
16	10.1.1.1	media.local	10.1.1.254	10.1.1.100
17	172.20.0.1	studio.local	172.20.0.254	172.20.0.100
18	192.168.140.1	dev.local	192.168.140.254	192.168.140.100
19	192.168.150.1	files.local	192.168.150.254	192.168.150.100
20	192.168.160.1	config.local	192.168.160.254	192.168.160.100
21	192.168.170.1	vpn.local	192.168.170.254	192.168.170.100
22	192.168.180.1	info.local	192.168.180.254	192.168.180.100
23	192.168.190.1	storage.local	192.168.190.254	192.168.190.100
24	192.168.200.1	project.local	192.168.200.254	192.168.200.100
25	10.10.10.1	debug.local	10.10.10.254	10.10.10.100
26	172.25.0.1	sim.local	172.25.0.254	172.25.0.100
27	192.168.210.1	dnsserver.local	192.168.210.254	192.168.210.100
28	192.168.220.1	gateway.local	192.168.220.254	192.168.220.100
29	192.168.230.1	example.local	192.168.230.254	192.168.230.100
30	192.168.240.1	backend.local	192.168.240.254	192.168.240.100

1. Отримайте динамічні адреси для своїх ПК.
2. Зробіть пінгування до сервера з цих же ПК.
3. Перевірте доступ до HTTP-сервера.
4. Збережіть проєкт.

Звіт має містити:

1. Мета роботи
2. Скріншот схеми мережі
3. Таблиця IP-адрес (включно з DHCP)
4. Скріншоти налаштувань сервера, роутера та отриманих динамічних IP кожного ПК.
5. Результати ping і доступ до HTTP-сервера
6. Висновки

Контрольні запитання:

1. Що таке DHCP і які його переваги?
2. Для чого потрібен DNS у локальній мережі?
3. Яка різниця між статичною та динамічною IP-адресацією?
4. Що таке шлюз за замовчуванням?
5. Як перевірити, що комп’ютери мають з’єднання між собою?

ЛАБОРАТОРНА РОБОТА № 4
НАЛАШТУВАННЯ ВІРТУАЛЬНИХ МЕРЕЖ В CISCO PACKET TRACER

Мета роботи: Ознайомитися з принципами створення та налаштування віртуальних локальних мереж (VLAN) у середовищі Cisco Packet Tracer; набути практичних навичок конфігурування VLAN на керованих комутаторах, зрозуміти переваги використання VLAN у корпоративних мережах для підвищення безпеки, масштабованості та керованості інфраструктури.

Теоретичні відомості:

У сучасних мережах VLAN (Virtual Local Area Network) — це технологія, що дозволяє логічно об’єднати пристрої в одну мережу незалежно від їхнього фізичного розташування. Завдяки VLAN пристрої, які підключені до різних комутаторів або портів, можуть належати до одного широкомовного домену, немовби вони з’єднані безпосередньо. Це досягається за рахунок ізоляції трафіку на канальному рівні OSI, що дозволяє адміністратору гнучко розподіляти ресурси, незалежно від топології.

Основні переваги VLAN включають сегментацію мережі, покращену безпеку, контроль над широкомовним трафіком і підвищену ефективність управління. Кожен VLAN функціонує як окремий логічний сегмент, що зменшує обсяг непотрібних широкомовних повідомлень (broadcast) і дозволяє створювати захищені середовища для окремих відділів, сервісів або типів користувачів. У типовій конфігурації всі порти комутатора належать до VLAN1, однак за допомогою налаштування керованих комутаторів можна створювати довільну кількість віртуальних сегментів.

VLAN ідентифікуються за допомогою числових тегів — VLAN ID (VID), відповідно до стандарту IEEE 802.1Q. Устаткування підтримує ідентифікатори у діапазоні від 1 до 4094, причому деякі значення зарезервовані: наприклад, 1002–1005 для застарілих технологій Token Ring і FDDI. VLAN поділяються на дві категорії: стандартні (normal-range, від 1 до 1005) і розширені (extended-range, від 1006 до 4094). Це дає змогу масштабувати інфраструктуру до сотень віртуальних мереж у великих підприємствах і дата-центрах.

Налаштування VLAN виконується тільки на керованих комутаторах — через консоль, SSH, Telnet або веб-інтерфейс. Порти комутатора при цьому поділяються на два типи: **access-порти** — для підключення кінцевих пристроїв (ПК, принтерів тощо), і **trunk-порти** — для передачі трафіку одразу з кількох VLAN між комутаторами або між комутатором і маршрутизатором. Такий підхід забезпечує високу гнучкість, масштабованість і безпечний розподіл ресурсів у рамках корпоративної мережі.

Хід роботи

Налаштування VLAN в одному комутаторі

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

Перші два комп'ютери з'єднаємо у `Vlan2`, а інші два – у `Vlan3` (рис. 4.1), оскільки за замовчуванням всі порти комутатора належать `Vlan1`.

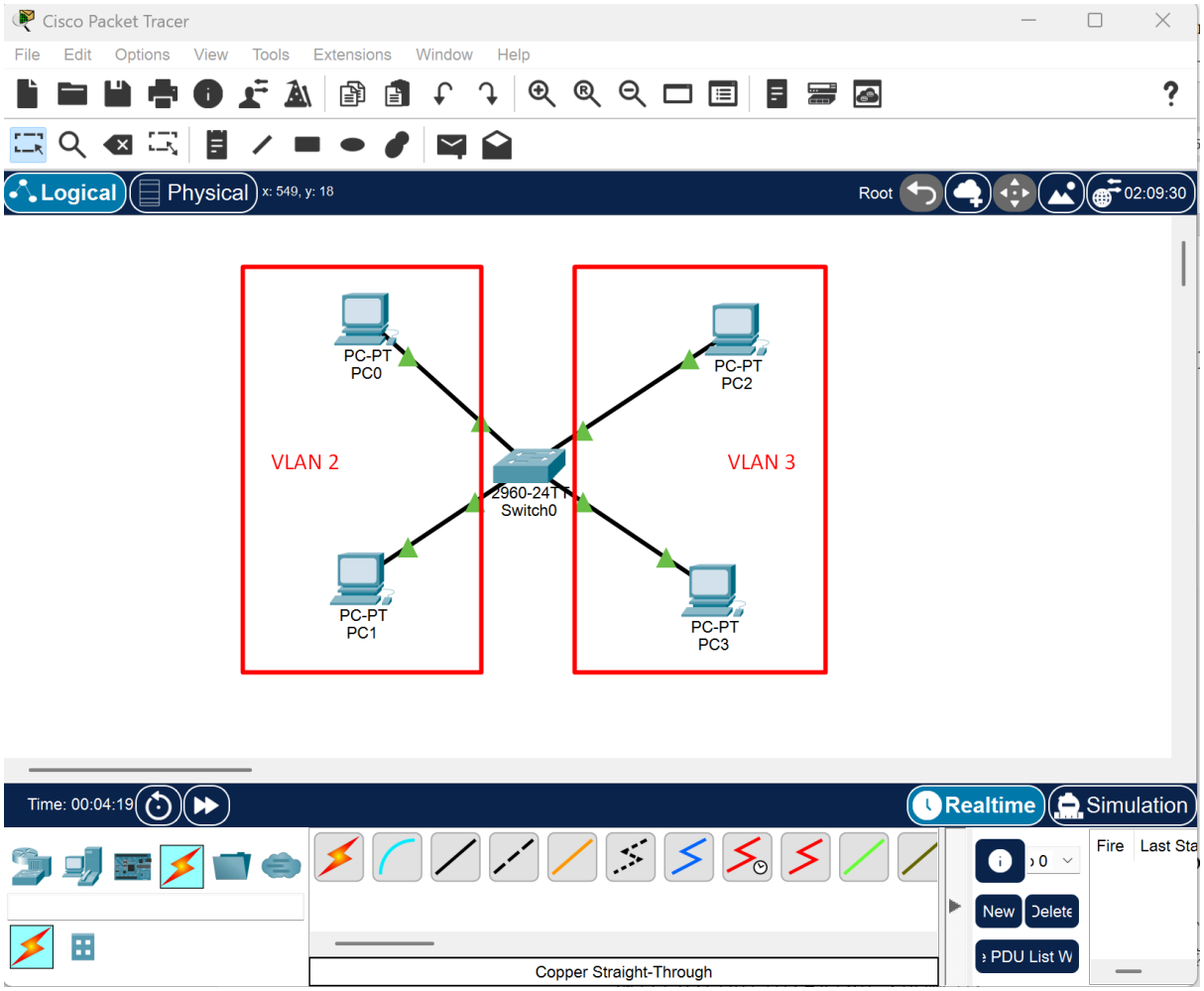


Рис 4.1. Проєкт мережі з одним комутатором

Для того щоб відкрити налаштування комутатора клацаємо по ньому лівою кнопкою миші і переходимо на закладку **CLI**. Заходимо спочатку у привілейований режим:

```
Switch>enable
```

а потім у режим глобальних налаштувань:

```
Switch#conf t
```

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

```
Switch(config)#vlan <номер>
```

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

Після цього відбудеться перехід у режим налаштування Vlan, який має вигляд

```
Switch(config-vlan)#,
```

в якому потрібно визначити назву цього Vlan.

Назва Vlan задається командою

```
Switch(config-vlan)#name <назва>
```

де `<назва>` – назва нового Vlan, наприклад, `arhiv`.

Виходимо з режиму налаштування Vlan

```
Switch(config-vlan)#exit
```

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

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

Налаштування певного інтерфейсу комутатора виконується командою:

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

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

Визначимо цей порт як Access-порт:

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

і визначаємо його у цей же Vlan:

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

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

Виходимо з режиму налаштування інтерфейсу

```
Switch(config-if)#exit
```

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

Щоб переглянути всі налаштування Vlan, у привілейованому режимі виконуємо команду

```
Switch#show vlan
```

На екрані відображається інформація про наявні віртуальні сегменти та порти, що їм належать.

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

Для перегляду основних відомостей про віртуальні сегменти у привілейованому режимі скористаємось командою

```
Switch#show vlan brief,
```

результат якої подано на рис. 4.2.

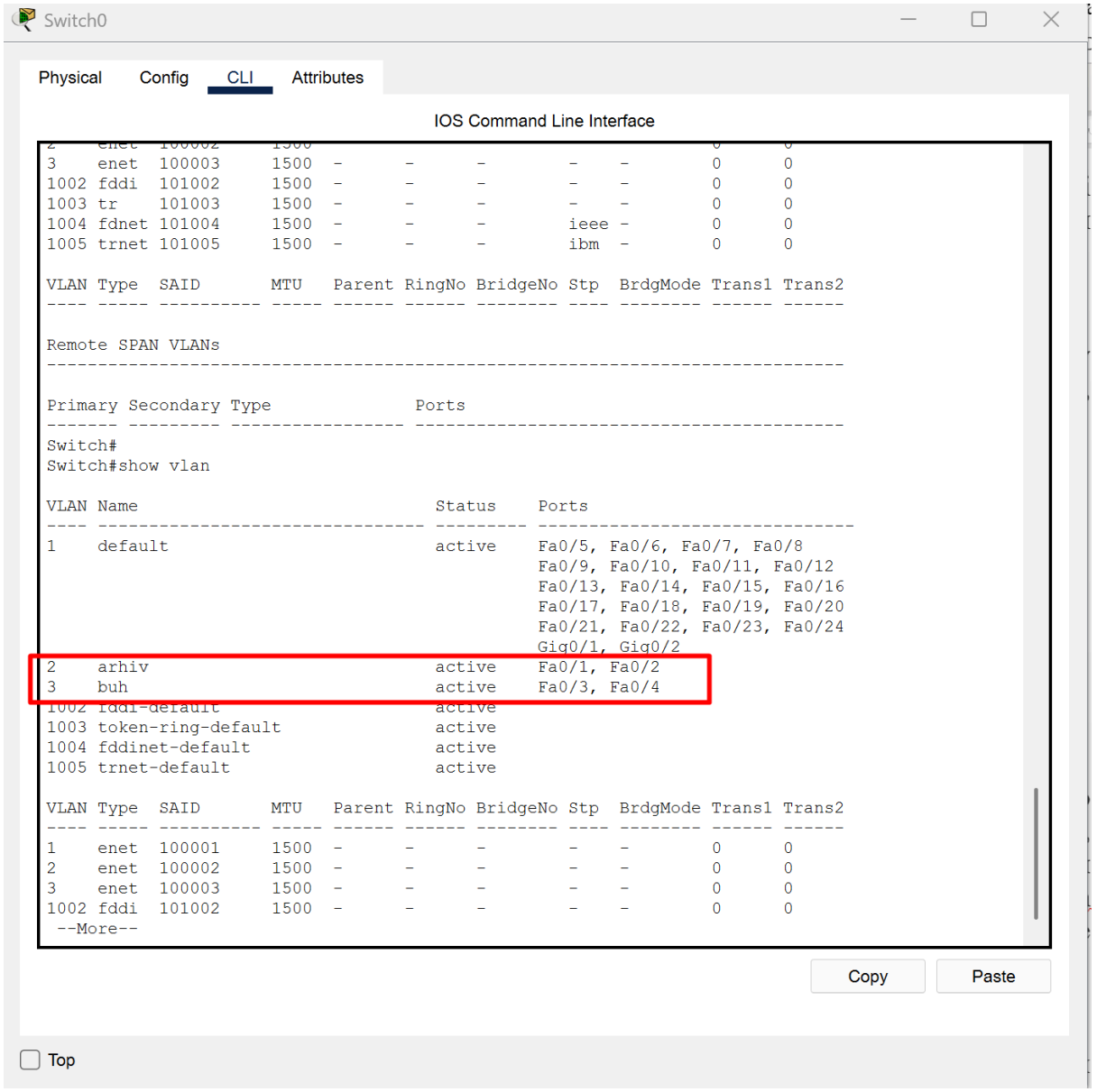


Рис 4.2. Схема різних VLAN в одному комутаторі

Щоб перевірити роботу VLAN всім комп'ютерам мережі необхідно встановити IP-адреси з одного діапазону. Наприклад, `192.168.1.1-192.168.1.4`. Тоді за допомогою exo-пакетів або ping-запитів перевірити з'єднання між комп'ютерами спільної та різних Vlan. Якщо всі налаштування правильні, то комп'ютери з одного Vlan будуть бачити один одного, але не будуть бачити комп'ютери з іншого Vlan (рис 4.3).

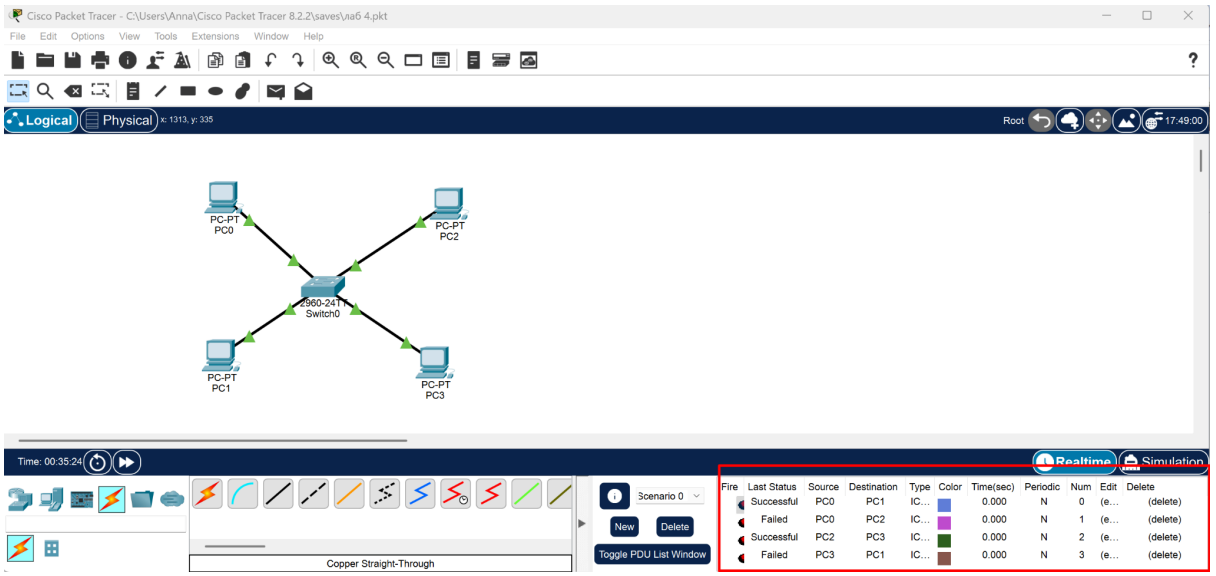


Рис 4.3. Схема виконання ехо-пакетів

Налаштування VLAN у двох комутаторах

Відкриваємо проєкт мережі з одним комутатором і виділяємо 4 комп'ютери та комутатор, копіюємо та вставляємо копію у проєкт. Таким чином в робочій області є 8 комп'ютерів і 2 комутатори (серія 2960). З'єднуємо комутатори перехресною скрученою парою через порти GigabitEthernet (рис. 4.4).

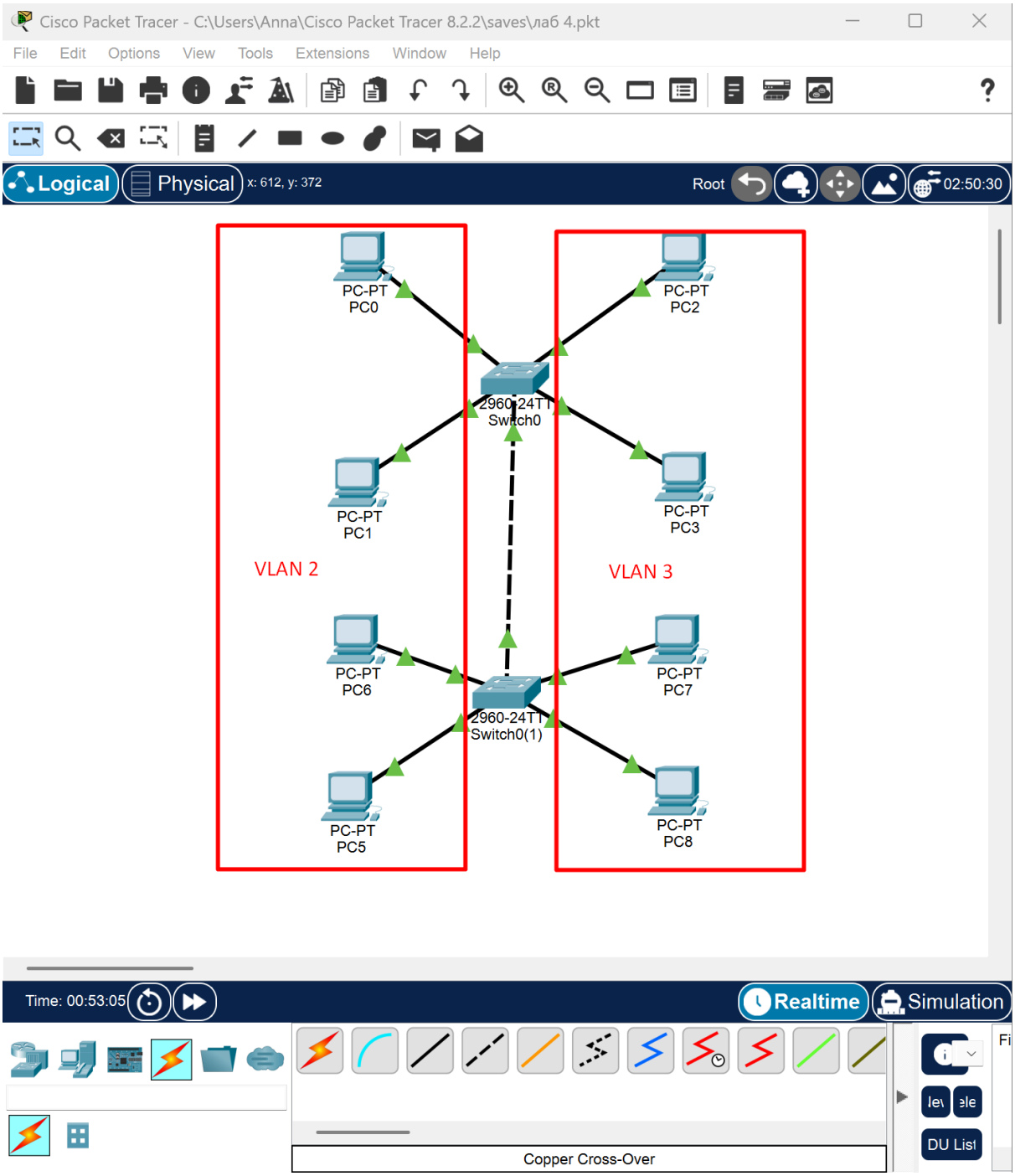


Рис 4.4. Проєкт мережі з двома комутаторами

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

Переглянемо налаштування другого комутатора за допомогою команди

```
Switch#show run
```

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

Отже, комп'ютери PC0, PC1, PC5 та PC6 з'єднані у `Vlan2`, а комп'ютери PC2, PC3, PC7 та PC8 – у `Vlan3` (рис. 4).

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

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

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

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

Далі вказуємо режим використання цього порту:

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

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

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

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

Зберігаємо налаштування комутатора командою

```
Switch#wr mem
```

Аналогічні дії виконуємо для відповідного порту другого комутатора.

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

Завдання для індивідуальної роботи

1. Запустіть програму і створіть новий проєкт мережі. Назвіть проєкт.

2. Додайте у проєкт кінцеві пристрої – 5 робочих станцій і комутатор (2960), з’єднайте їх.

3. Змініть кінцевим пристроям, доданим у п.2, стандартні імена і налаштуйте IP-адреси згідно з варіантом з таблиці 4.1.

Таблиця 4.1.

Варіант	Адреса підмережі	Маска підмережі
1	192.168.10.0	255.255.255.0
2	192.168.20.0	255.255.254.0
3	192.168.30.0	255.255.252.0
4	192.168.40.0	255.255.255.0
5	192.168.50.0	255.255.254.0
6	192.168.60.0	255.255.252.0
7	192.168.70.0	255.255.255.0
8	192.168.80.0	255.255.254.0
9	192.168.90.0	255.255.252.0
10	192.168.100.0	255.255.255.0
11	192.168.10.0	255.255.254.0
12	192.168.20.0	255.255.252.0
13	192.168.30.0	255.255.255.0
14	192.168.40.0	255.255.254.0
15	192.168.50.0	255.255.252.0
16	192.168.60.0	255.255.255.0
17	192.168.70.0	255.255.254.0
18	192.168.80.0	255.255.252.0
19	192.168.90.0	255.255.255.0
20	192.168.100.0	255.255.254.0
21	192.168.10.0	255.255.252.0
22	192.168.20.0	255.255.255.0
23	192.168.30.0	255.255.254.0
24	192.168.40.0	255.255.252.0
25	192.168.50.0	255.255.255.0
26	192.168.60.0	255.255.254.0
27	192.168.70.0	255.255.252.0
28	192.168.80.0	255.255.255.0
29	192.168.90.0	255.255.254.0
30	192.168.100.0	255.255.252.0

4. Створіть Vlan 2, Vlan 3 та Vlan 4.
5. У Vlan 2 включіть комп'ютери PC0 та PC1, у Vlan 3 – комп'ютери PC2, PC3, а у Vlan 4 – комп'ютер PC4.
6. За допомогою ping-запиту перевірте коректність налаштувань всіх Vlan.
7. Виділіть всі комп'ютери та комутатор, скопіюйте і вставте копії в робочу область проєкту.
8. Для копій комп'ютерів змініть імена на PC6, PC7, PC8, PC9, PC10 відповідно, а також змініть їхні IP-адреси (продовжіть IP-адресацію).
9. З'єднайте комутатори перехресною скрученою парою через порт GigabitEthernet.
10. Налаштуйте комутатори для передавання всіх Vlan через відповідні фізичні з'єднання.
11. За допомогою ping-запиту перевірити коректність налаштувань всіх Vlan.
12. Збережіть проєкт мережі.

Звіт має містити:

1. Мета роботи
2. Скріншот схеми мережі з одним комутатором
3. Таблиця IP-адрес пристроїв
4. Скріншот результатів перевірки exo-пакетами з одним комутатором
5. Скріншот схеми мережі з двома комутаторами
6. Таблиця IP-адрес пристроїв
7. Скріншот результатів перевірки exo-пакетами з двома комутаторами
8. Висновки

Контрольні запитання:

1. Що таке VLAN і яку функцію вона виконує у комп’ютерних мережах?
2. Які переваги дає використання VLAN у порівнянні з фізичним розділенням мереж?
3. Що таке широкомовний (broadcast) домен і як VLAN впливає на його межі?

4. Які типи портів використовуються в конфігурації VLAN і чим вони відрізняються?
5. Для чого призначені trunk-порти та в яких випадках їх потрібно використовувати?
6. Чому VLAN 1 за замовчуванням використовується на всіх портах і чим це може бути небезпечно?
7. Які методи доступу використовуються для налаштування VLAN на керованому комутаторі?

ЛАБОРАТОРНА РОБОТА № 5
НАЛАШТУВАННЯ З'ЄДНАННЯ З КОМУТАТОРОМ В CISCO PACKET TRACER

Мета роботи: Набути практичних навичок з первинного налаштування керованого комутатора в середовищі Cisco Packet Tracer; опанувати конфігурування IP-адреси для інтерфейсу VLAN1, зміну імені пристрою, встановлення паролів для консолі, Telnet/SSH-доступу та режиму enable; навчитися шифрувати паролі, зберігати конфігурацію комутатора, перевіряти доступність з ПК, а також розуміти роль базових налаштувань у забезпеченні керованості мережі.

Теоретичні відомості:

У сучасних комп'ютерних мережах керовані комутатори (managed switches) відіграють ключову роль, забезпечуючи не лише передачу кадрів на канальному рівні, а й гнучке адміністрування, сегментацію трафіку, безпеку та моніторинг. Щоб здійснювати віддалене керування комутатором, необхідно попередньо виконати базове налаштування — призначити IP-адресу, активувати інтерфейс VLAN1, встановити паролі доступу та, за потреби, увімкнути протоколи віддаленого керування (наприклад, Telnet або SSH).

Інтерфейс VLAN1 є логічним інтерфейсом, який використовується для керування пристроєм у мережі. Саме на нього призначається IP-адреса комутатора, що дозволяє отримати до нього доступ з інших пристроїв — наприклад, із персонального комп'ютера через утиліту Telnet або SSH-клієнт. Без призначеної IP-адреси пристрій неможливо адмініструвати віддалено, навіть якщо він фізично під'єднаний до мережі.

Для базового налаштування комутатора в Cisco Packet Tracer зазвичай використовують консольний доступ, який моделюється через вкладку CLI (Command Line Interface). Після підключення консольного кабелю до порту Console, адміністратор переходить у привілейований режим (`enable`), потім у режим конфігурації (`configure terminal`), змінює ім'я пристрою (`hostname`), встановлює паролі (`enable secret, line console 0, line vty 0 4`), активує інтерфейс

VLAN1 (`interface vlan 1`) та задає IP-адресу з маскою (`ip address`). Обов’язково потрібно активувати інтерфейс командою `no shutdown`, зберегти конфігурацію (`write` або `copy running-config startup-config`) і перевірити з’єднання за допомогою `ping`.

Дуже важливо шифрувати паролі командою `service password-encryption` — це базова вимога безпеки, навіть для локального доступу. Для доступу по мережі зручно використовувати Telnet, який вмикається за допомогою команд `line vty 0 4`, `login`, `password`, а також, за потреби, `transport input telnet`. У продуктивних мережах зазвичай надається перевага SSH як безпечнішому протоколу, однак у Packet Tracer реалізація SSH обмежена, тому для ознайомлення використовується Telnet.

Після успішного налаштування комутатора адміністратор може підключитися до нього з ПК, використовуючи утиліту Telnet через вкладку `Desktop → Terminal` або Command Prompt. Важливим кроком є перевірка доступності пристрою за допомогою команди `ping`, яка свідчить про коректне IP-з’єднання між вузлами.

Таким чином, первинна конфігурація комутатора забезпечує можливість централізованого керування, спрощує адміністрування мережі, є основою для подальшої конфігурації VLAN, безпеки, моніторингу та інших сервісів. Навички з налаштування базових параметрів комутатора є фундаментальними для адміністраторів мереж Cisco та обов’язковими для сертифікації рівня CCNA.

Підключення до комутатора через консоль

У робочій області Cisco Packet Tracer розміщуємо два комп'ютери і комутатор (серія 2960). Використовуючи консольний кабель, з'єднуємо комп'ютер через порт RS-232 та комутатор через порт Консоль (рис.5.1).

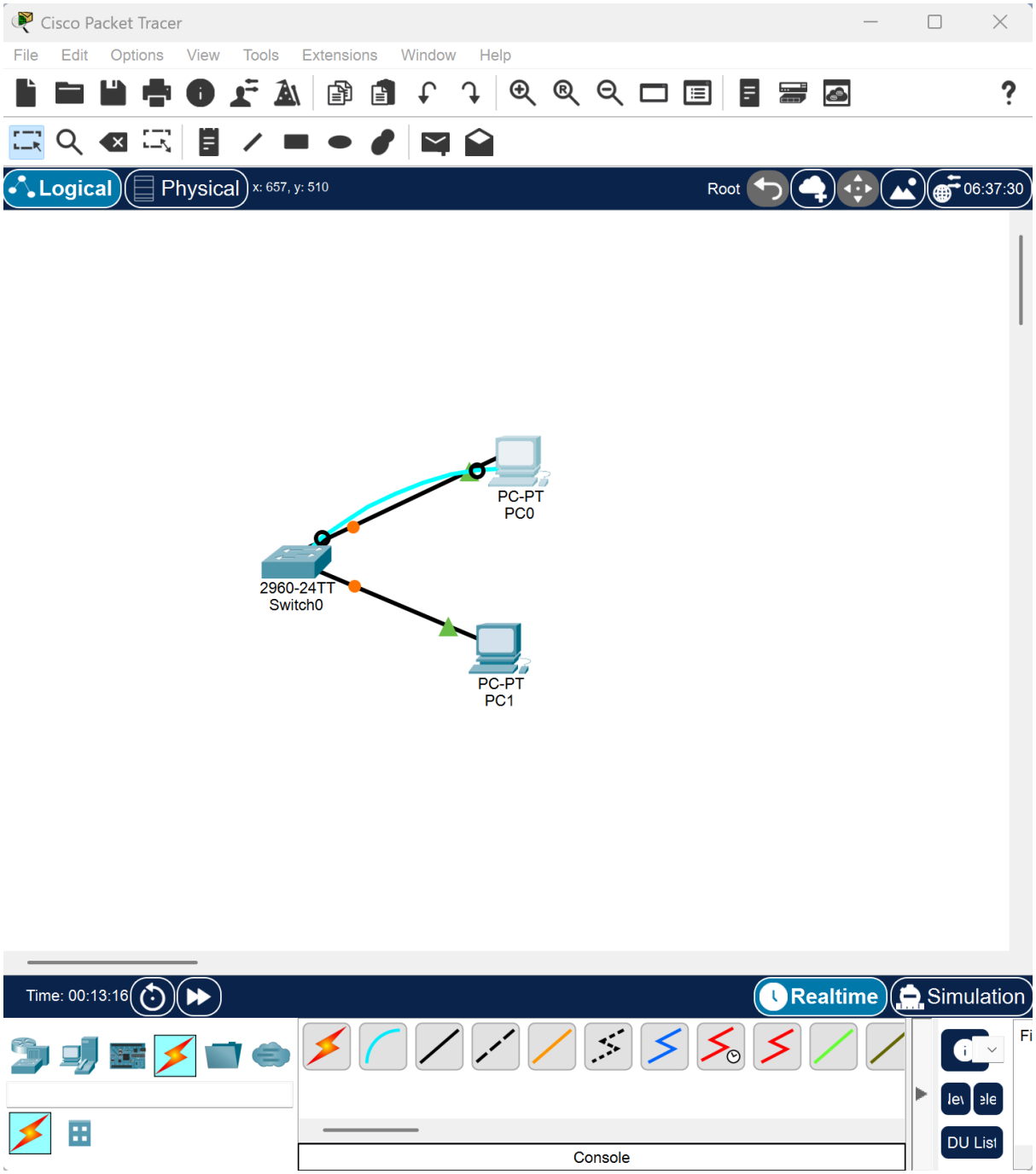


Рис. 5.1. Проєкт мережі

Далі потрібно зайти в налаштування комп'ютера, перейти на закладку **Desktop** і вибрати пункт **Terminal**. На екрані монітора відобразиться вікно **Terminal Configuration** (рис. 5.2), в якому потрібно вказати параметри порту термінального з'єднання. Значення цих параметрів потрібно залишити без змін і натиснути кнопку **OK**.

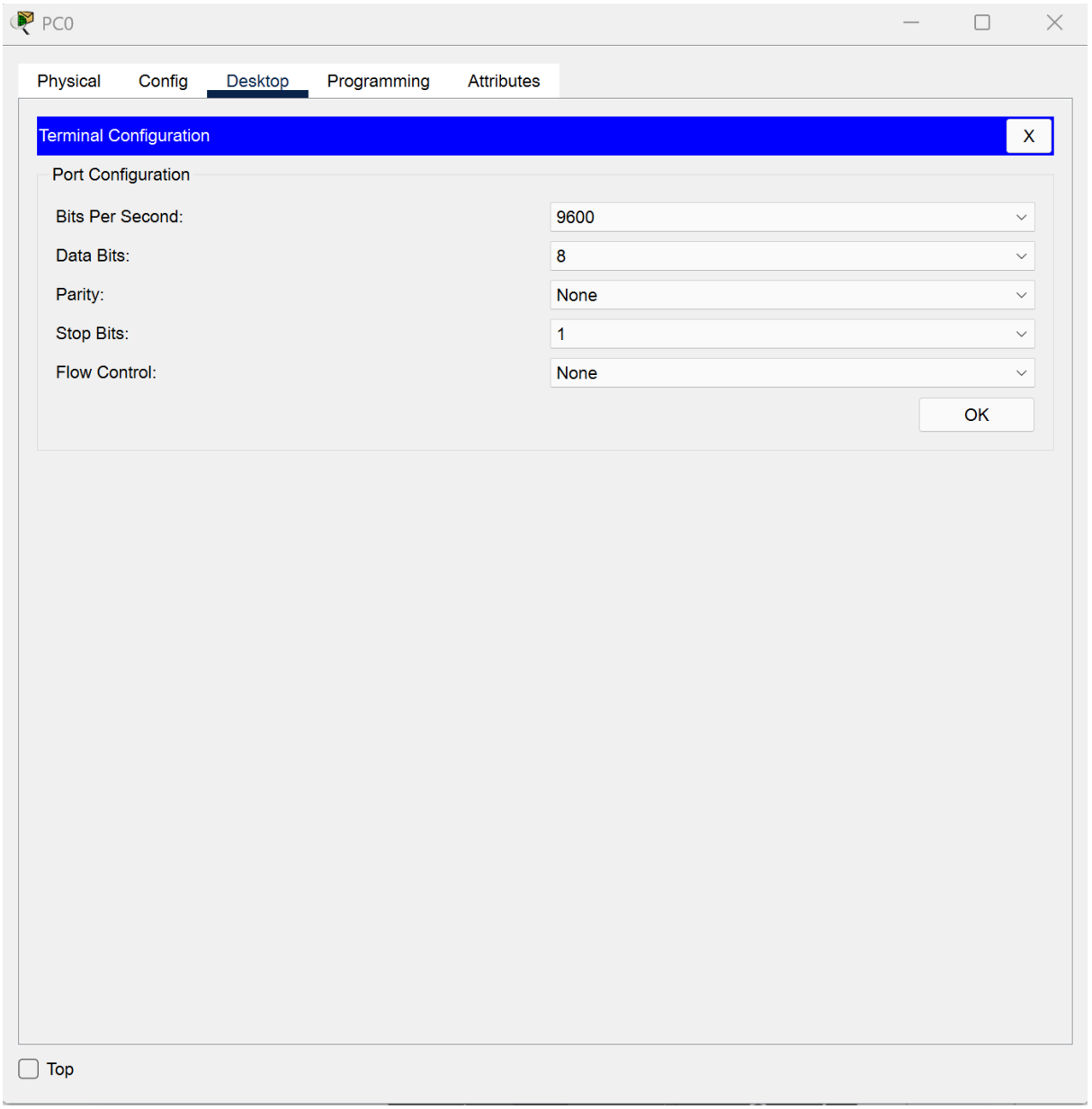


Рис. 5.2. Вікно Terminal Configuration

Після цього відкриється вікно **Terminal** (рис. 5.3), призначене для налаштування комутатора.

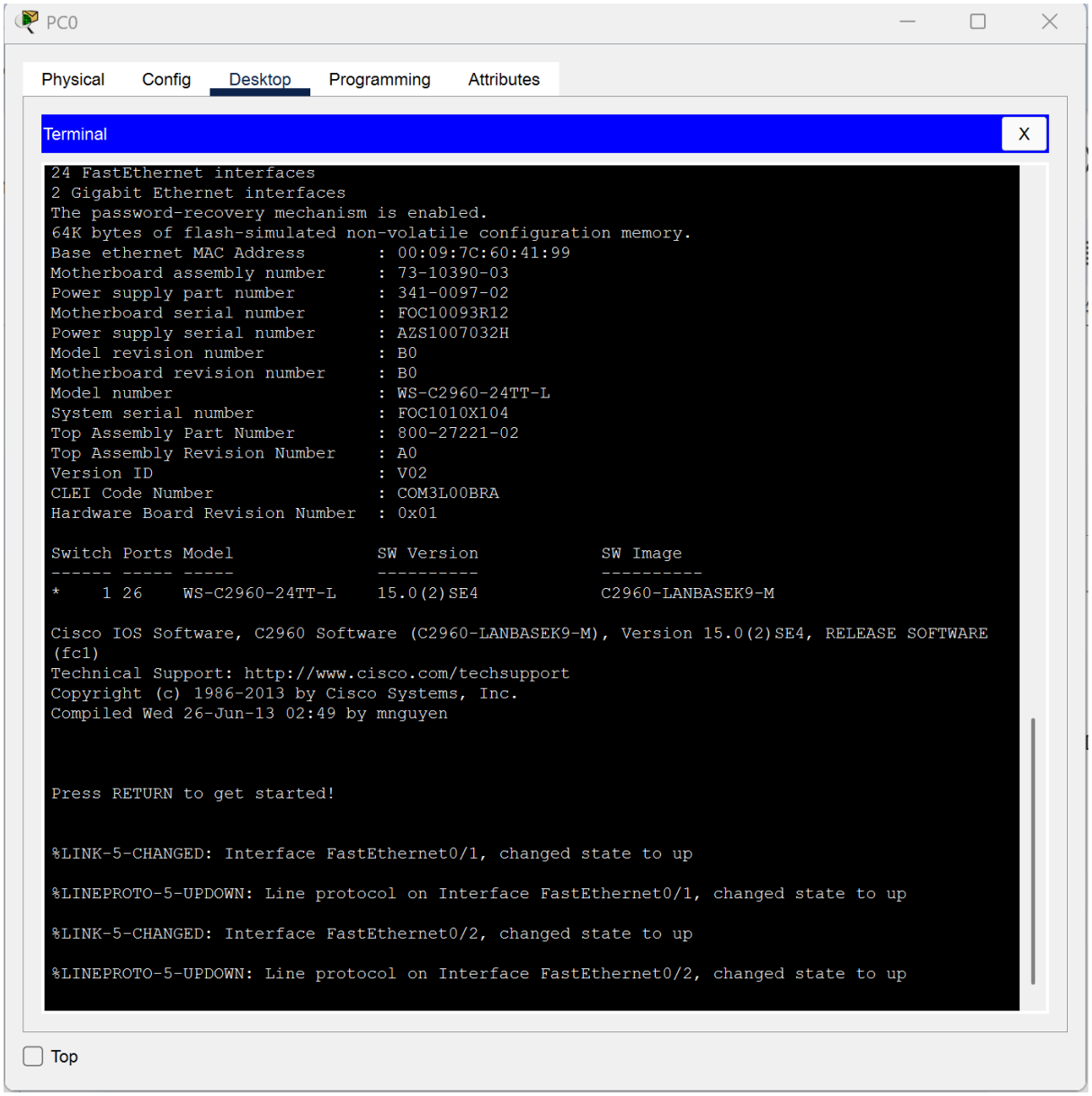


Рис. 5.3. Вікно Terminal

Щоб переглянути список доступних команд у поточному режимі командного рядка, слід виконати команду:

```
Switch>?
```

Для переходу з користувацького режиму до привілейованого використовується команда:

```
Switch>enable
```

Символ # у запрошенні (Switch#) вказує, що ви перебуваєте у привілейованому режимі, тоді як символ > (Switch>) свідчить про перебування в користувацькому режимі. Такий поділ на рівні доступу необхідний для забезпечення безпеки та обмеження змін конфігурації.

Щоб повернутися з привілейованого режиму до звичайного, використовується команда:

```
Switch#disable або Switch#exit
```

Для виходу одразу з усіх рівнів конфігурації можна скористатися командою:

```
Switch#end
```

Для перегляду поточних налаштувань комутатора слід скористатися командою:

```
Switch#show running-config
```

або скорочено:

```
Switch#show run
```

Перед початком конфігурації пристрою необхідно перейти в режим глобального налаштування за допомогою команди:

```
Switch#configure terminal
```

або скорочено:

```
Switch#conf t
```

Щоб отримати підказки щодо можливих параметрів будь-якої команди, можна додати знак питання після неї. Наприклад, для перегляду підкоманд `show`:

```
Switch#show ?
```

Встановлення паролю на привілейований режим

Щоб забезпечити базовий рівень безпеки мережевого обладнання, необхідно задати пароль для входу в привілейований режим доступу. Це можна зробити за допомогою команди:

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

Однак цей пароль за замовчуванням зберігається у відкритому вигляді, тому його варто зашифрувати. Для цього спочатку потрібно активувати механізм шифрування командою:

```
Switch(config)#service password-encryption
```

Після цього рекомендується встановити альтернативний, більш захищений пароль через команду:

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

У конфігурації пристрою саме пароль, заданий через `enable secret`, має вищий пріоритет. Це означає, що при вході в привілейований режим буде використовуватись саме він, навіть якщо `enable password` також задано.

Створення користувача

Для створення облікового запису користувача в локальній базі даних комутатора використовується команда такого формату:

```
Switch(config)#username <ім'я_користувача> privilege <рівень>
password <пароль>
```

У цій команді `<ім'я_користувача>` вказує логін нового користувача, `<рівень>` визначає рівень привілеїв у межах від 0 до 15 (де 15 — максимальний рівень доступу), а `<пароль>` — це пароль, який буде використовуватись для автентифікації. Така конфігурація дозволяє задавати індивідуальні параметри доступу для кожного користувача до керованого пристрою.

Встановлення авторизації на з'єднання через консоль

Для налаштування авторизації доступу через консоль необхідно перейти в режим конфігурації термінальних ліній за допомогою команди:

```
Switch(config)#line console <номер>
```

У більшості випадків використовується номер **0**, тобто команда має вигляд `line console 0`. Перелік доступних номерів можна переглянути, виконавши команду:

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

Щоб увімкнути авторизацію з використанням облікових записів, збережених у локальній базі даних пристрою, потрібно задати команду:

```
Switch(config-line)#login local
```

Це забезпечить, що при підключенні до пристрою через консоль користувач повинен буде ввести логін і пароль, задані раніше в конфігурації.

Встановлення IP-адреси комутатора

Перегляд поточної конфігурації комутатора, включаючи фізичні інтерфейси (FastEthernet, GigabitEthernet) та логічні інтерфейси (наприклад, VLAN), виконується з привілейованого режиму за допомогою команди:

```
Switch#show run
```

За замовчуванням усі порти комутатора належать до VLAN1. Щоб налаштувати IP-адресу для логічного інтерфейсу комутатора, необхідно перейти в режим глобальної конфігурації, а потім у режим конфігурації інтерфейсу VLAN1 за допомогою команди:

```
Switch(config)#interface Vlan1
```

Далі виконується призначення IP-адреси та маски підмережі:

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

Наприклад:

```
Switch(config-if)#ip address 192.168.0.1 255.255.255.0
```

Щоб активувати інтерфейс VLAN1 (він за замовчуванням може бути вимкнений), потрібно виконати команду:

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

У відповідь комутатор має вивести повідомлення типу:

```
Interface Vlan1, changed state to up
```

що означає успішне ввімкнення інтерфейсу та його готовність до роботи.

Встановлення типу віддаленого з’єднання та увімкнення авторизації

Щоб налаштувати віртуальний термінальний доступ (VTY) до комутатора, необхідно перейти до режиму конфігурації термінальних ліній за допомогою команди:

```
Switch(config)#line vty 0 4
```

Тут `vty` означає віртуальний термінал, а числа 0–4 визначають діапазон ліній, які будуть налаштовані. Наступним кроком є вказання дозволеного протоколу доступу — наприклад, Telnet:

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

Щоб забезпечити автентифікацію користувача з локальної бази даних пристрою, необхідно задати:

```
Switch(config-line)#login local
```

Після завершення конфігурації слід вийти з режиму налаштування командою:

```
Switch(config-line)#end
```

А для збереження всіх внесених змін у постійну пам’ять комутатора — використати команду:

```
Switch#write memory
```

або скорочено:

```
Switch#wr mem
```

Перевірка налаштувань комутатора

Щоб перевірити IP-адресу комутатора та доступність з локальної мережі, необхідно підключити комп’ютер до комутатора кабелем типу «скручена пара», призначити комп’ютеру IP-адресу з того самого підмережевого діапазону, в якому знаходиться IP-адреса комутатора, і здійснити перевірку з’єднання за допомогою команди `ping`.

Для перевірки можливості віддаленого доступу через протокол Telnet слід відкрити командний рядок (наприклад, у вкладці Desktop → Command Prompt) на підключеному ПК і ввести команду:

```
telnet <IP-адреса комутатора>
```

Після цього з’явиться запит на введення імені користувача та пароля. Якщо вказані облікові дані вірні, буде встановлено з’єднання, і користувач отримає доступ до режиму конфігурації комутатора на відповідному рівні привілеїв.

Хід роботи

В проєкті мережі рис 5.1. розставляємо IP-адреси комп’ютерам: `192.168.1.1` та `192.168.1.2`. IP-адреса комутатора (VLAN1) буде 192.168.1.254.

1. Через закладку **Desktop на ПК** вибираємо пункт **Terminal**. Входимо в режим глобальної конфігурації:

   ```
   Switch > enable
   Switch # conf t
   ```

2. Далі потрібно зробити заборону небажаних пошуків в DNS.

Для цього вимкніть пошук в DNS, щоб запобігти спробі комутатора перетворювати введені невірні команди таким чином, як ніби вони є іменами вузлів.

```
Switch (config) # no ip domain-lookup
```

3. Налаштування паролів привілейованого режиму

Встановлюємо незашифрований пароль cisco на вхід в привілейований режим.

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

4. Створення власного користувача

Створюємо власного користувача з найнижчим пріоритетом.

```
Switch(config)#username Student privilege 15 password 1234
```

5. Налаштування доступу до консолі

```
Switch(config)#line console 0
Switch(config-line)# password cisco
Switch(config-line)#login
Switch(config-line)#exit
```

6. Налаштування пароля на доступ по telnet або ssh

Лінії vty (virtual terminal line) потрібні для віддаленого адміністрування пристроєм по telnet або ssh. Встановлюємо пароль cisco на лінії vty.

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

7. Налаштування імені комутатора

Встановлюємо для комутатора ім'я командою «hostname».

```
Switch(config)#hostname S1
```

8. Шифрування паролів

Зашифровуємо всі поточні і наступні паролі.

```
S1(config)# service password-encryption
```

9. Налаштування інтерфейсу керування комутатором

```
S1(config) # interface vlan 1
S1(config-if) # ip address 192.168.1.254 255.255.255.0
S1(config-if) # no shutdown
```

10. Збереження конфігурації комутатора в NVRAM

```
S1# wr mem
```

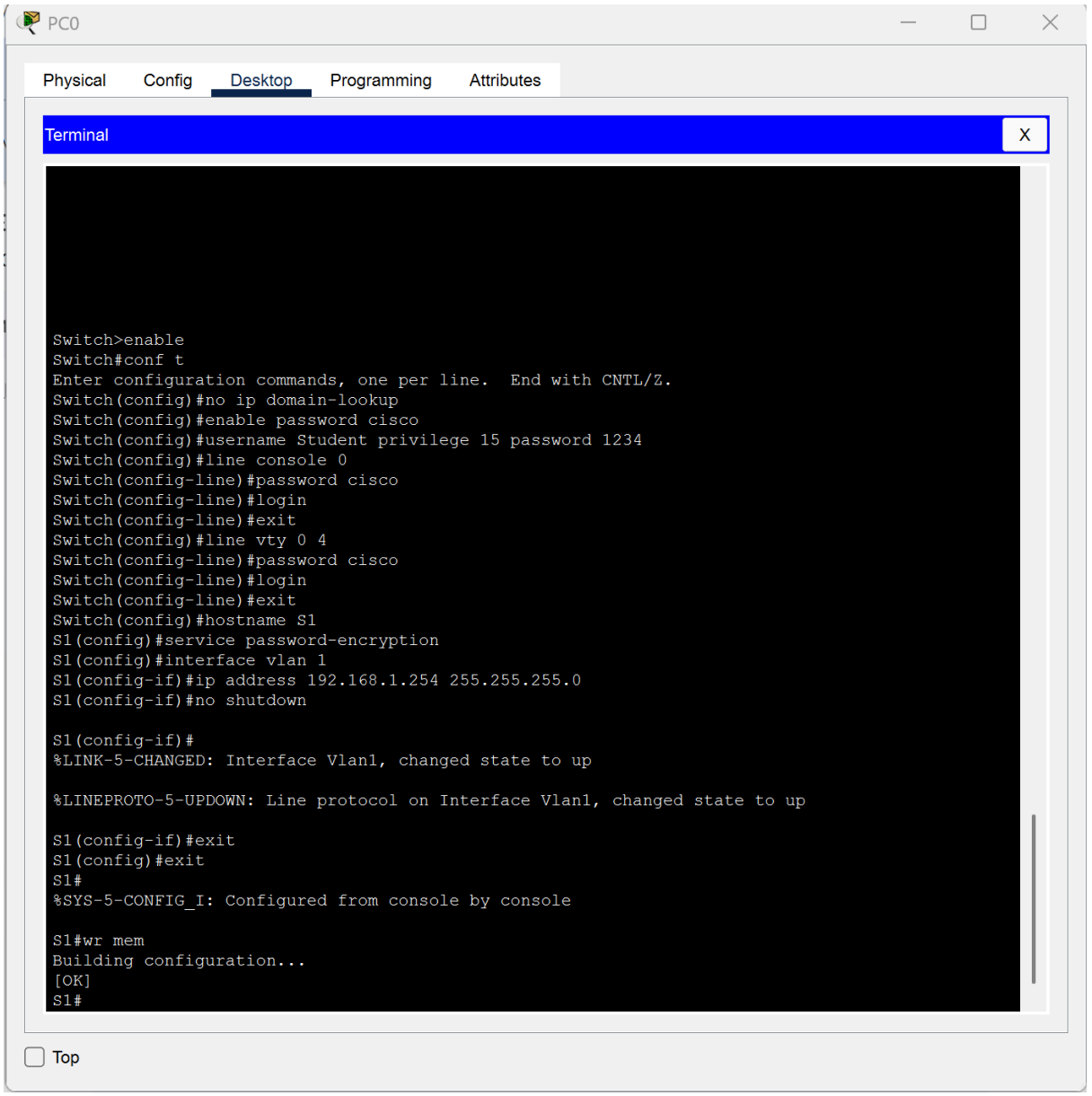


Рис 5.4. Вигляд вікна Terminal

11. Перевірка підключення до мережі

На вкладці Desktop вибираємо додаток Command Prompt (Командний рядок). З командного рядка надсилаємо ping-запит на IP-адресу комп'ютера PC1.

```
PC> ping 192.168.1.2
```
(рис. 5.5)

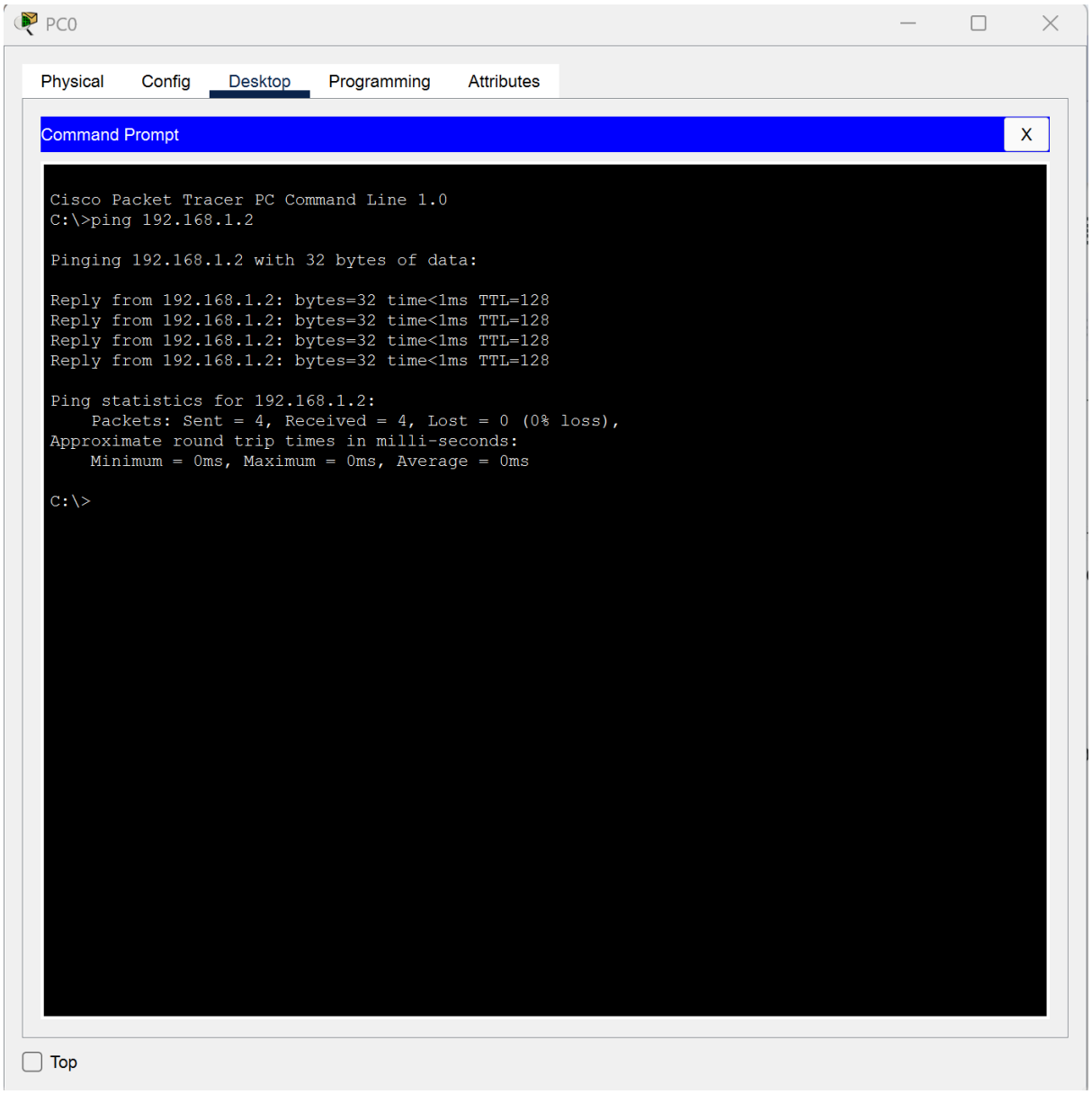


Рис 5.5. Виконання ping-запиту з комп'ютером

З командного рядка надсилаємо ping-запит на IP-адресу комутатора.

```
PC> ping 192.168.1.254
```

12. Для перевірки віддаленого підключення до комутатора через адресу управління SVI в командному рядку вводимо команду «telnet ip-адреса».

    telnet 192.168.0.100 (рис 5.6)

Варто зауважити, що після того як введено команду і відбулось з'єднання з'являється повідомлення про те, щоб ввести пароль. Коли пароль вводиться, його не видно. Після того як він введений натискаємо Enter. Якщо пароль введений вірно, з'явиться рядок з іменем комутатора S1.

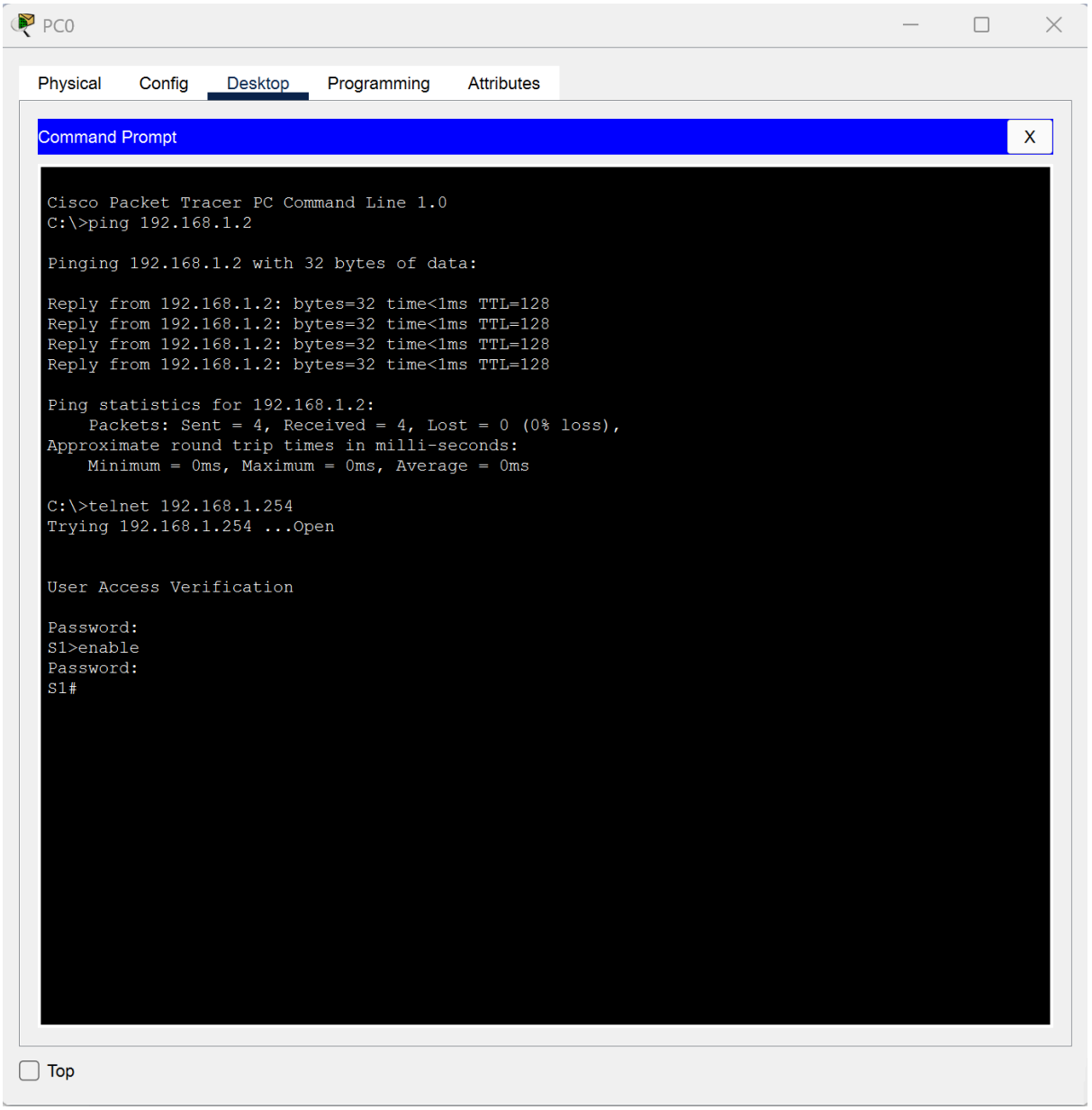


Рис 5.6. Виконання ping-запиту по telnet

Завдання для індивідуальної роботи

1. Запустіть програму і створіть новий проєкт мережі. Назвіть проєкт.

2. Додайте у проєкт кінцеві пристрої – 2 робочих станцій і комутатор (2960), з’єднайте їх.

3. Змініть кінцевим пристроям, доданим у п.2, стандартні імена і налаштуйте IP-адреси згідно варіанту з таблиці 5.1.

Таблиця 5.1.

Варіант	IP-адреса комутатора (VLAN1)	IP-адреса ПК0	IP-адреса ПК1	Ім’я комутатора
1	192.168.164.100	192.168.164.1	192.168.164.2	S1
2	192.168.29.100	192.168.29.1	192.168.29.2	S2
3	192.168.7.100	192.168.7.1	192.168.7.2	S3
4	192.168.190.100	192.168.190.1	192.168.190.2	S4
5	192.168.71.100	192.168.71.1	192.168.71.2	S5
6	192.168.63.100	192.168.63.1	192.168.63.2	S6
7	192.168.58.100	192.168.58.1	192.168.58.2	S7
8	192.168.36.100	192.168.36.1	192.168.36.2	S8
9	192.168.189.100	192.168.189.1	192.168.189.2	S9
10	192.168.27.100	192.168.27.1	192.168.27.2	S10
11	192.168.174.100	192.168.174.1	192.168.174.2	S11
12	192.168.190.100	192.168.190.1	192.168.190.2	S12
13	192.168.229.100	192.168.229.1	192.168.229.2	S13
14	192.168.140.100	192.168.140.1	192.168.140.2	S14
15	192.168.23.100	192.168.23.1	192.168.23.2	S15
16	192.168.152.100	192.168.152.1	192.168.152.2	S16
17	192.168.109.100	192.168.109.1	192.168.109.2	S17
18	192.168.9.100	192.168.9.1	192.168.9.2	S18
19	192.168.8.100	192.168.8.1	192.168.8.2	S19
20	192.168.24.100	192.168.24.1	192.168.24.2	S20
21	192.168.56.100	192.168.56.1	192.168.56.2	S21
22	192.168.60.100	192.168.60.1	192.168.60.2	S22
23	192.168.130.100	192.168.130.1	192.168.130.2	S23
24	192.168.155.100	192.168.155.1	192.168.155.2	S24
25	192.168.7.100	192.168.7.1	192.168.7.2	S25
26	192.168.144.100	192.168.144.1	192.168.144.2	S26
27	192.168.51.100	192.168.51.1	192.168.51.2	S27
28	192.168.184.100	192.168.184.1	192.168.184.2	S28
29	192.168.167.100	192.168.167.1	192.168.167.2	S29
30	192.168.180.100	192.168.180.1	192.168.180.2	S30

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

Звіт має містити:

1. Мета роботи
2. Скріншот схеми мережі
3. Скріншот встановлення IP-адрес
4. Скріншот вікна Telnet з виконанням завдань
5. Скріншот виконання ping-запитів
6. Скріншот виконання запиту telnet
7. Висновки

Контрольні запитання:

1. Які режими доступу до комутатора існують у Cisco IOS? Як між ними перемикатися?
2. Яка роль інтерфейсу VLAN1 у налаштуванні комутатора?
3. Як призначити IP-адресу для керування комутатором? Навіщо потрібна команда `no shutdown`?
4. Чим відрізняється `enable password` від `enable secret`? Чому варто використовувати саме `enable secret`?
5. Для чого використовується команда `service password-encryption`?

6. Як створити обліковий запис користувача в локальній базі комутатора?
7. Яка команда дозволяє активувати авторизацію через локальну базу даних для консольного доступу?
8. Що таке VTY-лінії і як їх налаштовують для доступу по Telnet?
9. Як перевірити доступність комутатора з комп’ютера в мережі?
10. У чому полягає різниця між командами `write memory`, `copy running-config startup-config` і `show running-config`?
11. Як перевірити, які команди доступні в поточному режимі командного рядка?
12. Який тип кабелю потрібно використовувати для підключення ПК до комутатора?
13. Що таке `hostname` в конфігурації комутатора і як його змінити?
14. Чому важливо налаштовувати паролі доступу навіть у навчальному середовищі?
15. Як перевірити результат налаштування за допомогою ping та Telnet?

ЛАБОРАТОРНА РОБОТА № 6
НАЛАШТУВАННЯ ПОШТОВИХ СЕРВЕРІВ У ДВОХ ПІДМЕРЕЖАХ І ОРГАНІЗАЦІЯ ОБМІНУ ПОВІДОМЛЕННЯМИ

Мета роботи: Ознайомитися з принципом роботи електронної пошти у розподілених мережах; навчитися створювати і налаштовувати поштові сервери в ізольованих підмережах, працювати з протоколами SMTP та POP3, організовувати маршрутизацію між підмережами та здійснювати взаємний обмін повідомленнями між клієнтами різних доменів.

Теоретичні відомості:

У сучасному цифровому світі електронна пошта (email) залишається однією з найважливіших технологій для обміну повідомленнями. Вона дозволяє користувачам швидко надсилати й отримувати текстові повідомлення, файли та мультимедійні вкладення через комп’ютерні мережі, зокрема Інтернет. Концепція електронної пошти багато в чому повторює традиційну пошту: ми використовуємо "адреси", "вкладення", "скриньки" та "доставку", хоча все це реалізовано в цифровій формі.

Основні переваги електронної пошти залишаються актуальними: простота адресування (username@domain), підтримка форматованого тексту, можливість додавати файли та універсальна сумісність. Електронна пошта є платформонезалежною, дозволяє взаємодіяти між різними поштовими системами, а передача повідомлень зазвичай здійснюється безпосередньо між серверами. Попри зручність, електронна пошта також має недоліки — зокрема, спам, фішинг, затримки доставки, обмеження розміру вкладень та ризики конфіденційності.

З розвитком технологій еволюціонували і протоколи передачі пошти. Надсилання електронних листів зазвичай відбувається через SMTP (Simple Mail Transfer Protocol) — простий протокол передачі пошти, що працює у мережах TCP/IP. Він визначає правила, за якими поштові сервери надсилають листи одне одному та приймають їх від користувачів. Однак SMTP вимагає налаштування безпеки, оскільки застаріле використання без аутентифікації створює ризики для спуфінгу та несанкціонованої розсилки.

Для отримання листів сучасні поштові клієнти (наприклад, Outlook, Thunderbird, мобільні поштові застосунки) використовують IMAP або POP3. Протокол POP3 (Post Office Protocol, версія 3) дозволяє завантажити листи з сервера на пристрій і зазвичай видаляє їх із сервера після отримання. Натомість IMAP (Internet Message Access Protocol) зберігає повідомлення на сервері та дозволяє синхронізувати поштову скриньку на кількох пристроях одночасно. Обидва протоколи широко підтримуються провайдерами електронної пошти, зокрема Gmail, Outlook, Yahoo тощо.

Сьогодні популярні поштові сервіси також інтегрують додаткові функції безпеки (наприклад, TLS/SSL шифрування, SPF/DKIM/DMARC автентифікацію) та інструменти боротьби з небажаною поштою. Електронна пошта стала ключовим інструментом у комунікації, як в особистому, так і в корпоративному середовищі, а її інфраструктура постійно вдосконалюється відповідно до викликів сучасної цифрової епохи.

Хід роботи

1. Додаємо в робоче поле 4 ПК, 2 сервери, 2 комутатори (2960) та роутер (1941). Підключаємо ПК і сервер до комутатора за допомогою витої пари через порти підключення FastEthernet, а роутер і комутатор через порт GigabitEthernet. Топологія моделі мережі представлена на рис. 6.1.

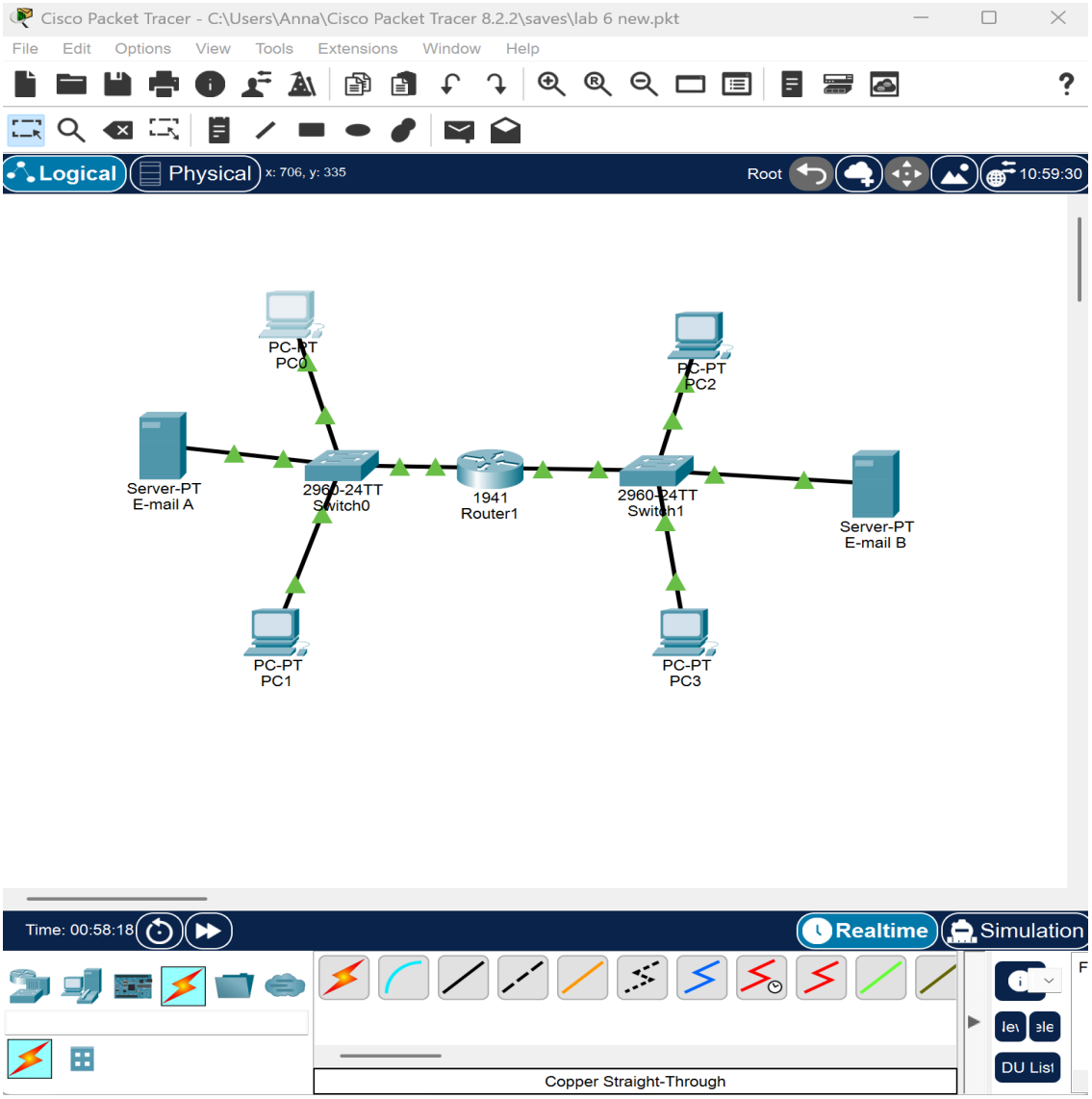


Рис. 6.1. Проєкт мережі.

2. Налаштуємо елементи мережі. Маємо такі вхідні дані.

Мережа А	***Маска А***	***Мережа Б***	***Маска Б***	***Домен А***	***Домен Б***	***Користувачі (по 2)***
10.31.0.0	*255.255.255.192*	*192.168.31.0*	*255.255.255.224*	*india.com*	*vietnam.net*	*Mumbai, Delhi / Hanoi, Haiphong*

Щоб налаштувати сервер А, відкриємо його властивості, переходимо на вкладку *Config* і в підменю *INTERFACE* вибираємо модуль *FastEthernet0*. У поле *IP Address* ведемо другу зарезервовану IP-адресу мережі – *10.31.0.2*, а в поле *Subnet Mask* – маску мережі 255.255.192. Після цього включимо цей модуль – *Port Status* в *On*. Далі налаштуємо сервіс *EMAIL*.

Переходимо на вкладку *Services* та вибираємо підменю *EMAIL*. Для ввімкнення перемикачі *SMTP Service* і *POP3 Service* встановимо в положення *On*.

Призначаємо доменне ім'я поштовому серверу - в поле *Domain Name* введемо, наприклад, *india.com*. Натискаємо кнопку *Set*, щоб зберегти ім'я домену. Далі створюємо два облікові записи користувачів. Для цього потрібно в поле *User* ввести ім'я облікового запису, а в поле *Password – пароль*. Для додавання запису до бази даних, натиснемо кнопку "+". Таким чином, створюємо ще два записи: *Mumbai* з паролем 123 і *Delhi* з паролем 123 (рис. 6.2).

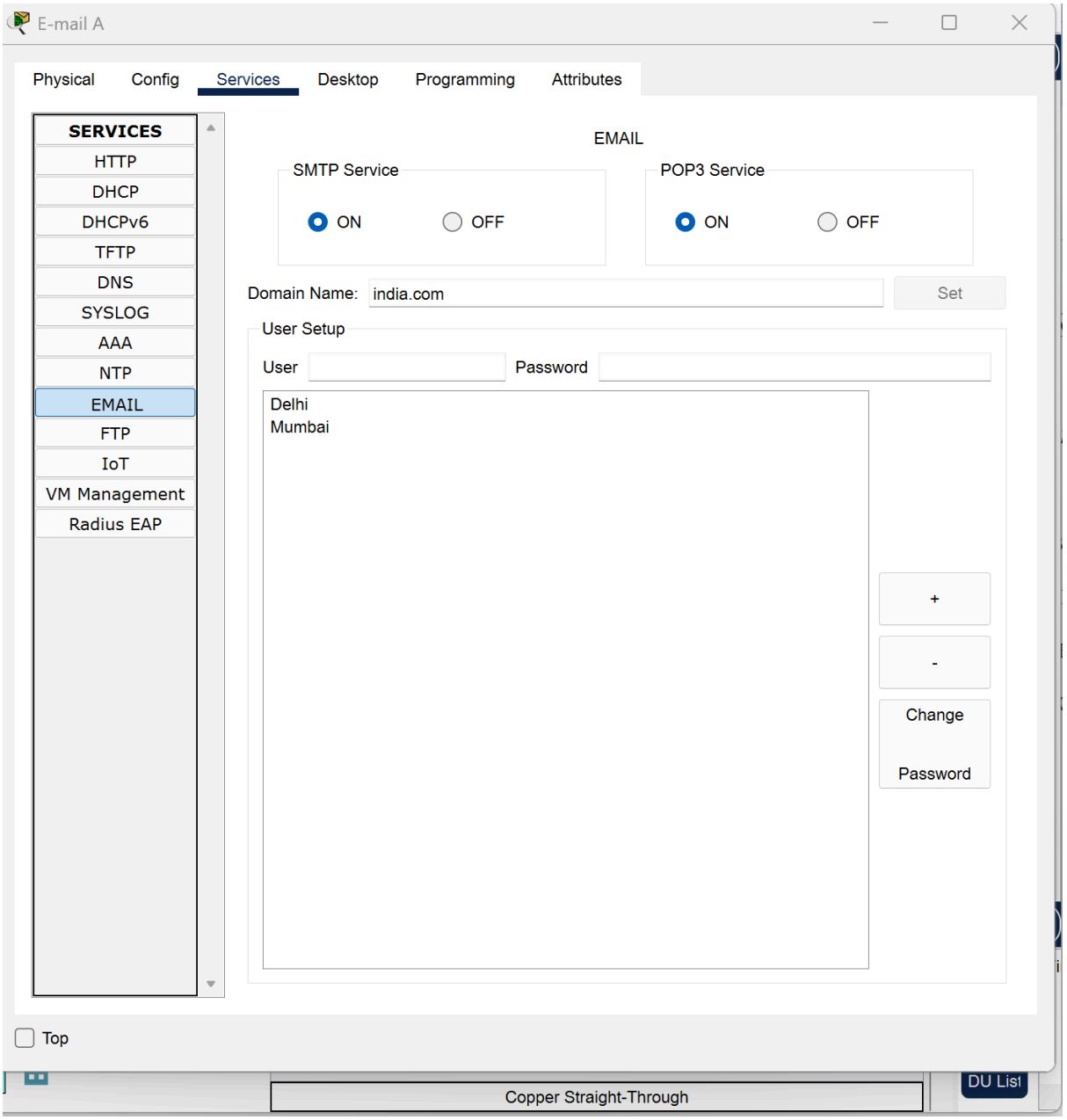


Рис. 6.2. Вікно налаштування Email на сервері

Аналогічно робимо налаштування на сервері B відповідно до вхідних даних.

Так як нам потрібно буде пересилати листи з однієї підмережі в іншу, необхідно налаштувати DNS сервер. Можемо не додавати новий сервер, а зробити налаштування у вже існуючому, наприклад на сервері А. Для цього заходимо на вкладку *Servis → DNS*. Ставимо перемикач в положення ***ON***. Додаємо два записи ***Records***:

Запис 1:
Name: `india.com`
Address: *IP-адреса сервера Email A (наприклад* `10.31.0.2`*)*
Add
Запис 2:
Name: `vietnam.net`
Address: *IP-адреса сервера Email B (наприклад* `192.168.31.2`*)*
Add

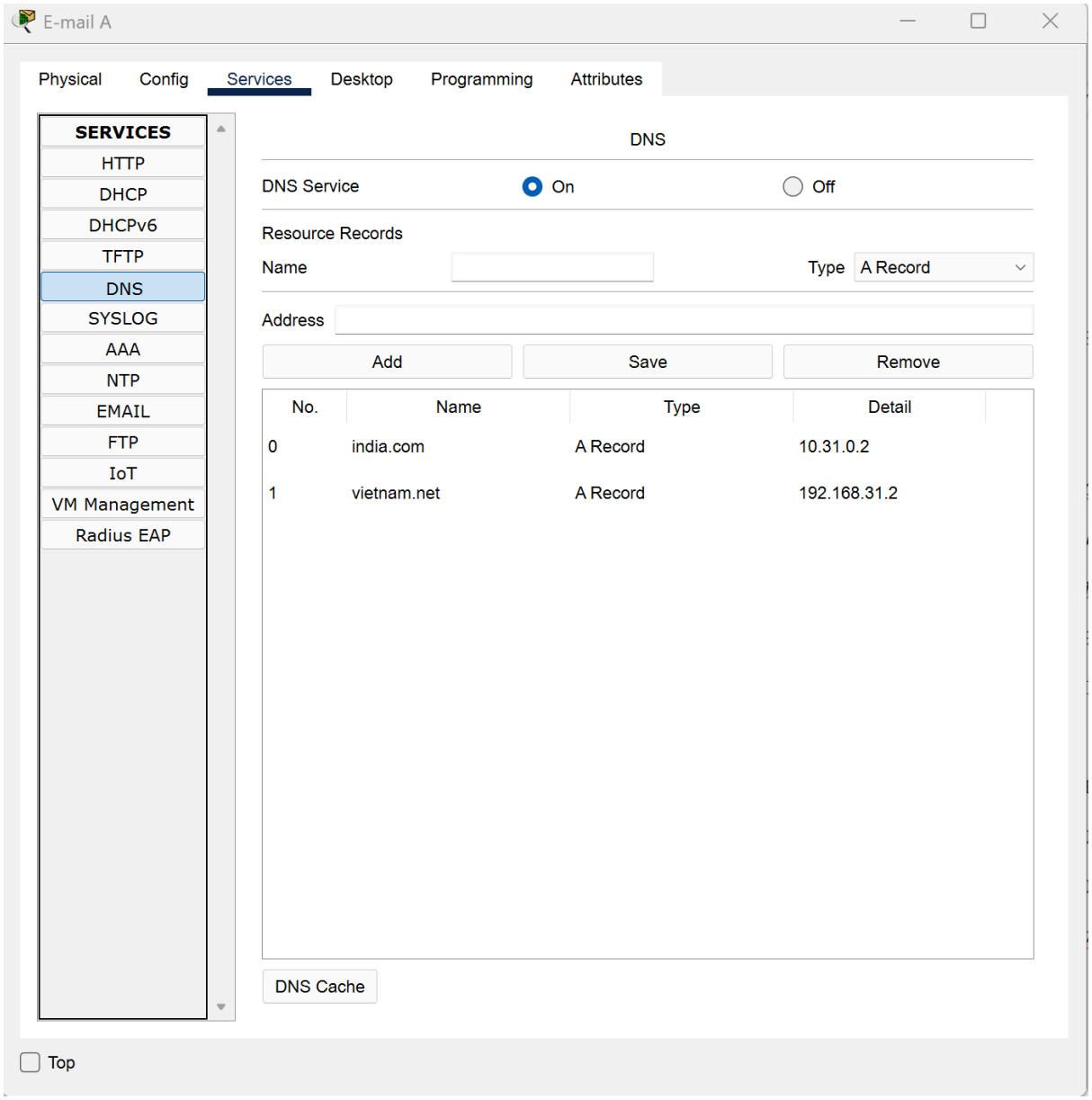


Рис. 6.3. Вікно налаштування DNS на сервері

Наступним кроком на сервері прописуємо *Default Gateway та DNS Server.* Для цього заходимо на вкладку `Config →Settings`. У поле Default Gateway записуємо IP роутера з боку сервера A, а в поле DNS Server IP сервера на якому створювали DNS (рис 6.4).

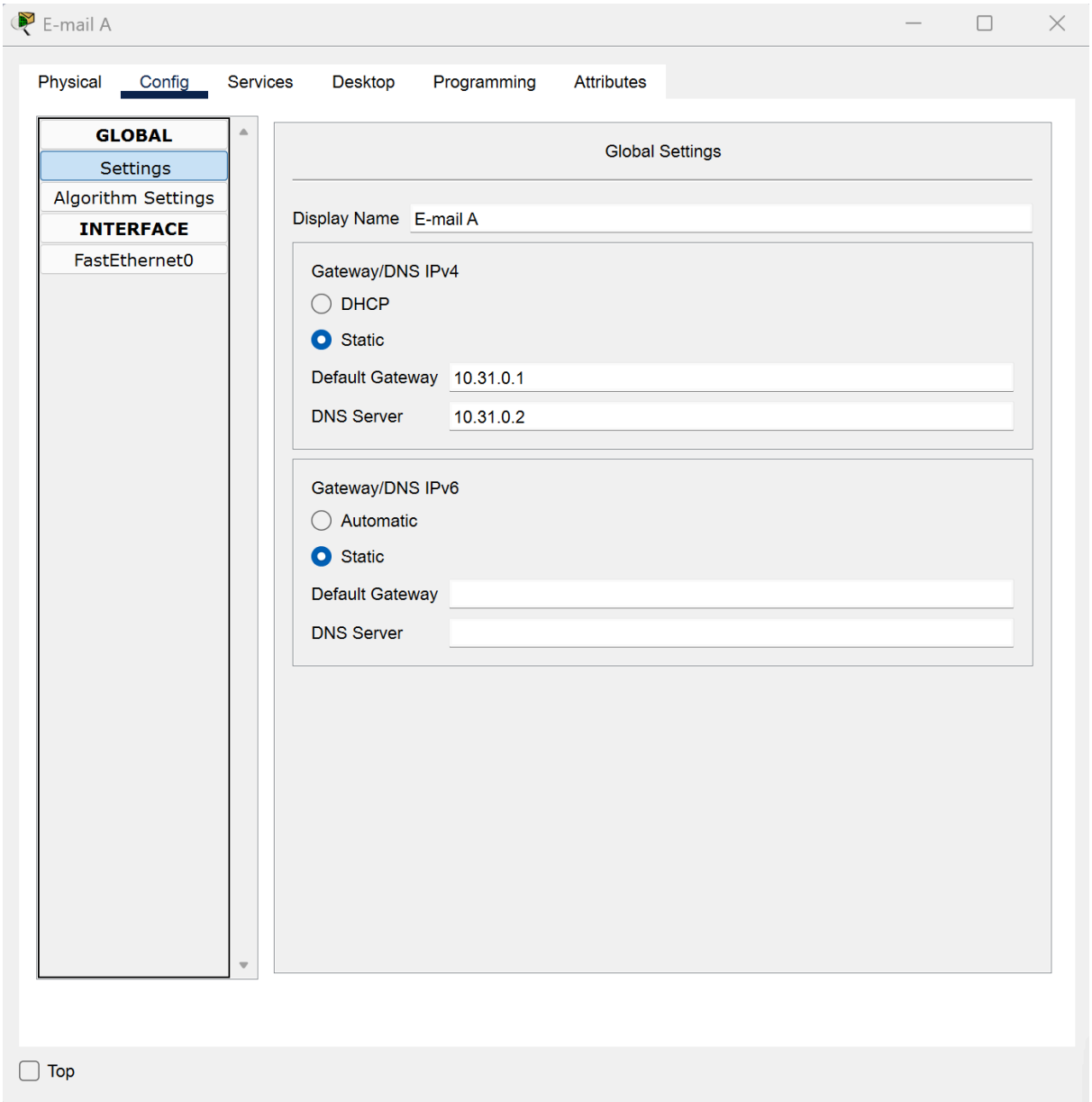


Рис. 6.4. Вікно налаштування Settings на сервері

Так як у роутері вже встановлені потрібні модулі, необхідно їх тільки налаштувати. Для цього заходимо у властивості роутера Config →GigabitEthernet0/0. Записуємо IP-адресу та маску мережі A, вмикаємо перемикач ***ON.*** Ті ж діє робимо з GigabitEthernet0/1 і записуємо IP та маску мережі B (рис 6.5).

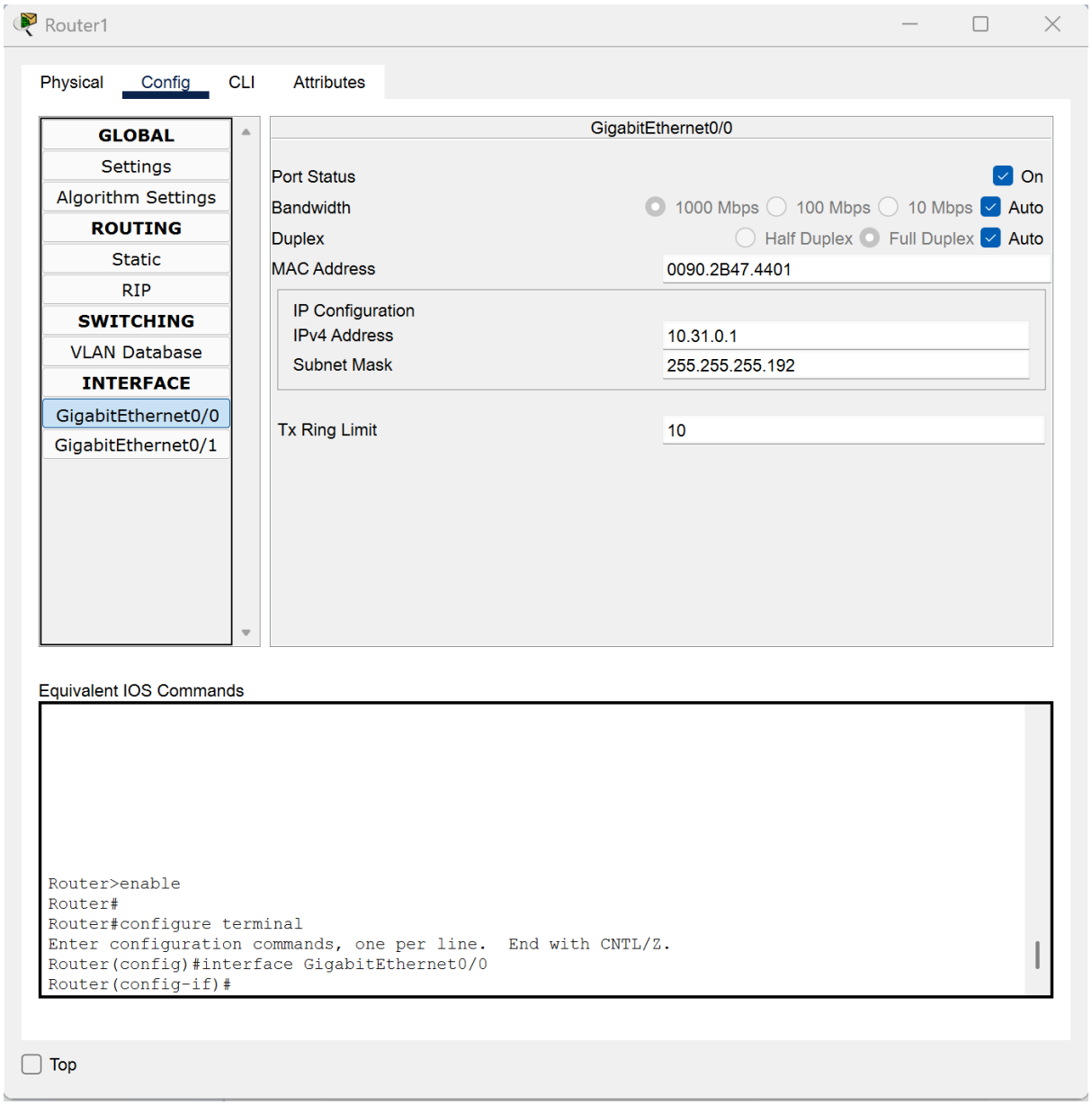


Рис. 6.5. Вікно налаштування роутера

Особливу увагу слід звернути на те, щоб були ввімкнені інтерфейси маршрутизатора:

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

Якщо це не зроблено, то заходимо на вкладку CLI і прописуємо:

```
Router(config)# interface gig0/0
Router(config-if)# ip address 10.31.0.1 255.255.255.192
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface gig0/1
```

```
Router(config-if)# ip address 192.168.31.1 255.255.255.224
Router(config-if)# no shutdown
```

Після цього переходимо до налаштувань ПК. Два ПК, що входять в мережу А налаштовуємо так: IP адреси та маски з мережі А, у поле Default Gateway записуємо IP маршрутизатора з боку А, а в поле DNS Server записуємо IP сервера DNS , тобто сервера А (рис 6.6).

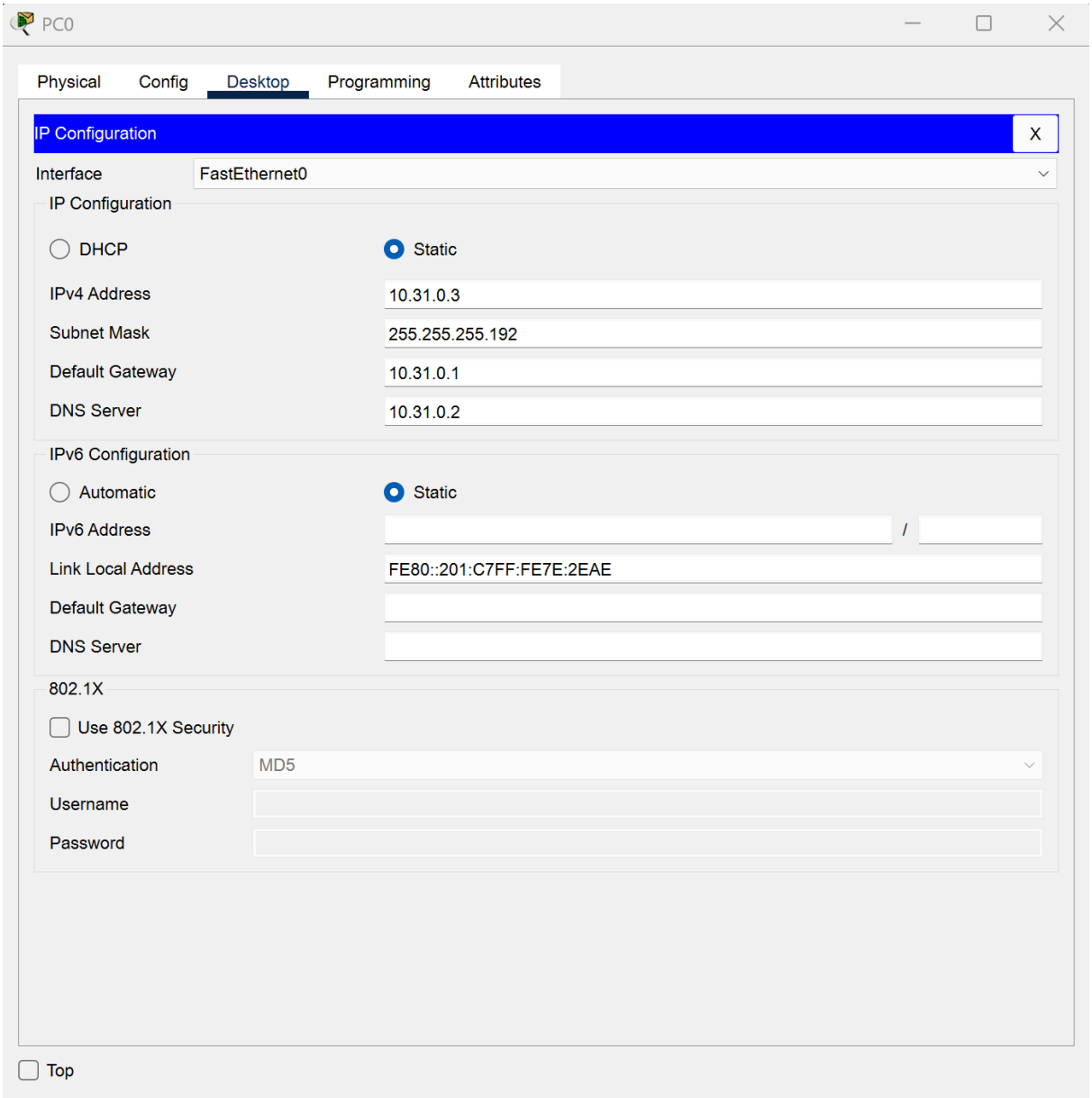


Рис. 6.6. Вікно налаштування ПК мережі А

Інші два ПК, що входять в мережу В налаштовуємо так: IP адреси та маски з мережі В, у поле Default Gateway записуємо IP маршрутизатора з боку В, а в поле DNS Server записуємо IP сервера DNS , тобто сервера А (рис 6.7).

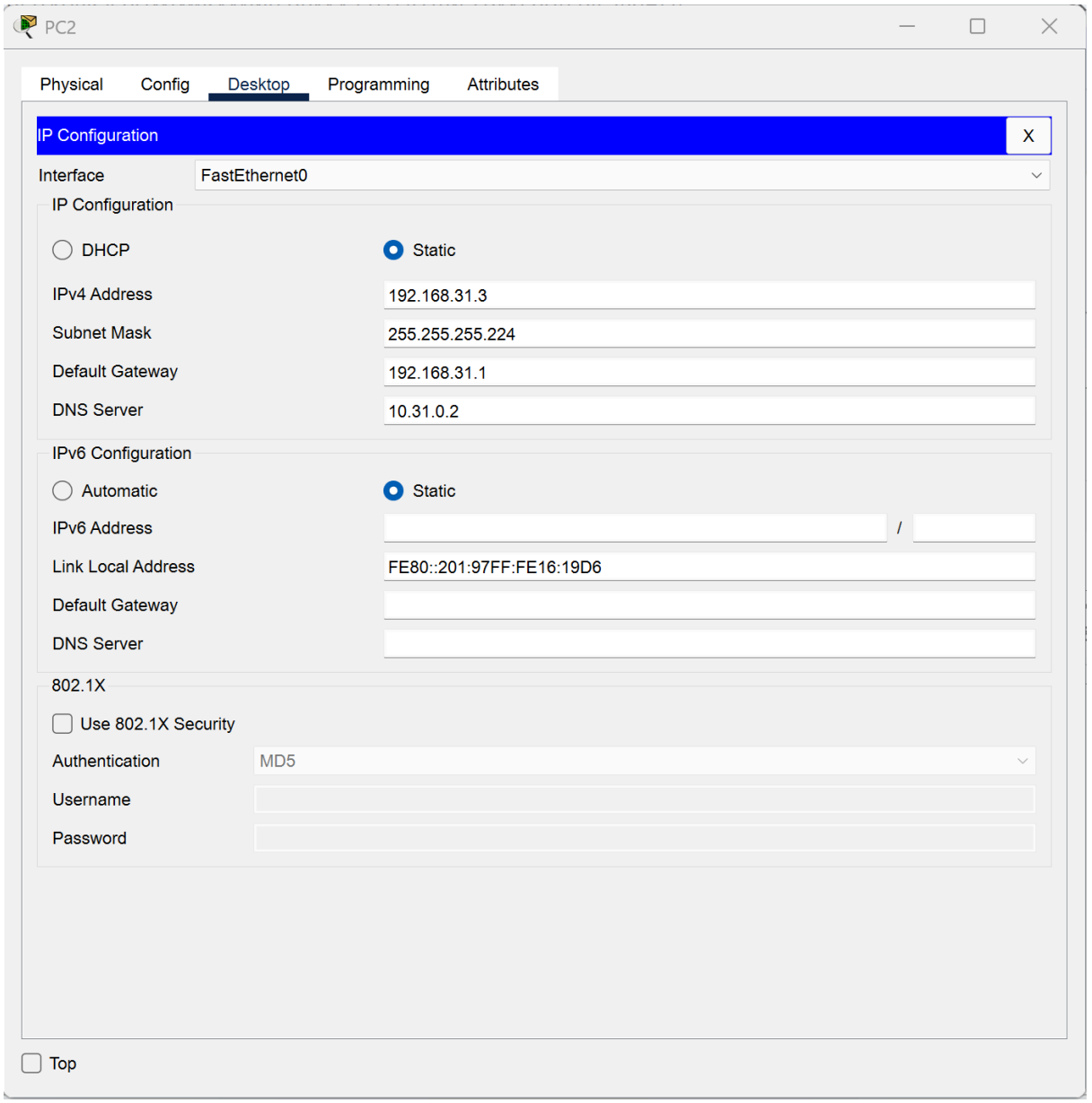


Рис. 6.7. Вікно налаштування ПК мережі B

Налаштовуємо поштові скриньки на всіх ПК. Для цього заходимо на вкладку *Desktop і* вибираємо елемент *Email.* З'явиться вікно для настроювання поштової скриньки. У полі *Your Name* вказуємо довільне ім'я поштової скриньки, яке зберігатиметься тільки на локальному ПК. В полі *Email Address* потрібно вказати повне ім'я поштової скриньки:

email = ім'я облікового запису на сервері + @ + доменне ім'я сервера

Для PC0 це Mumbai@india.com, а для PC1 це Delhi@india.com. В розділі *Server Information* вкажемо IP-адресу для серверів вхідної і вихідної пошти – в нашому випадку *Incoming Mail Server* и *Outgoing Mail Server* адреса буде однакова

для обох ПК з мережі A – 10.31.0.2. У розділі *Logon Information* вказуємо ім'я та пароль облікового запису, раніше записаного на сервері (для PC0 – Mumbai з паролем 123, а для PC1 – Delhi з паролем 123). Щоб зберегти конфігурацію, натискаємо кнопку *Save* (рис 6.8).

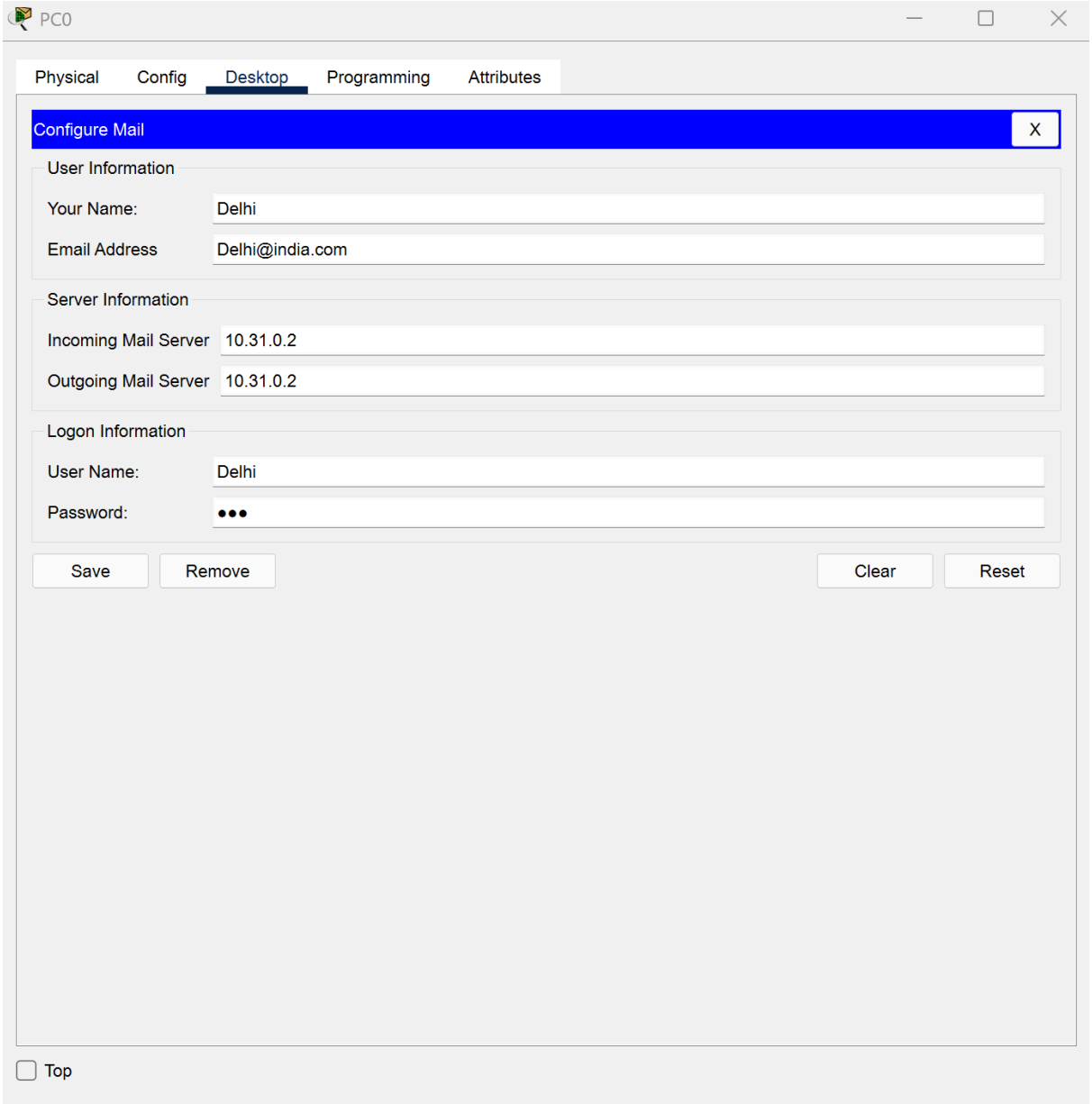


Рис. 6.8. Налаштування облікового запису на ПК мережі A

Аналогічні дії проводимо для двох інших ПК з мережі B (рис 6.9).

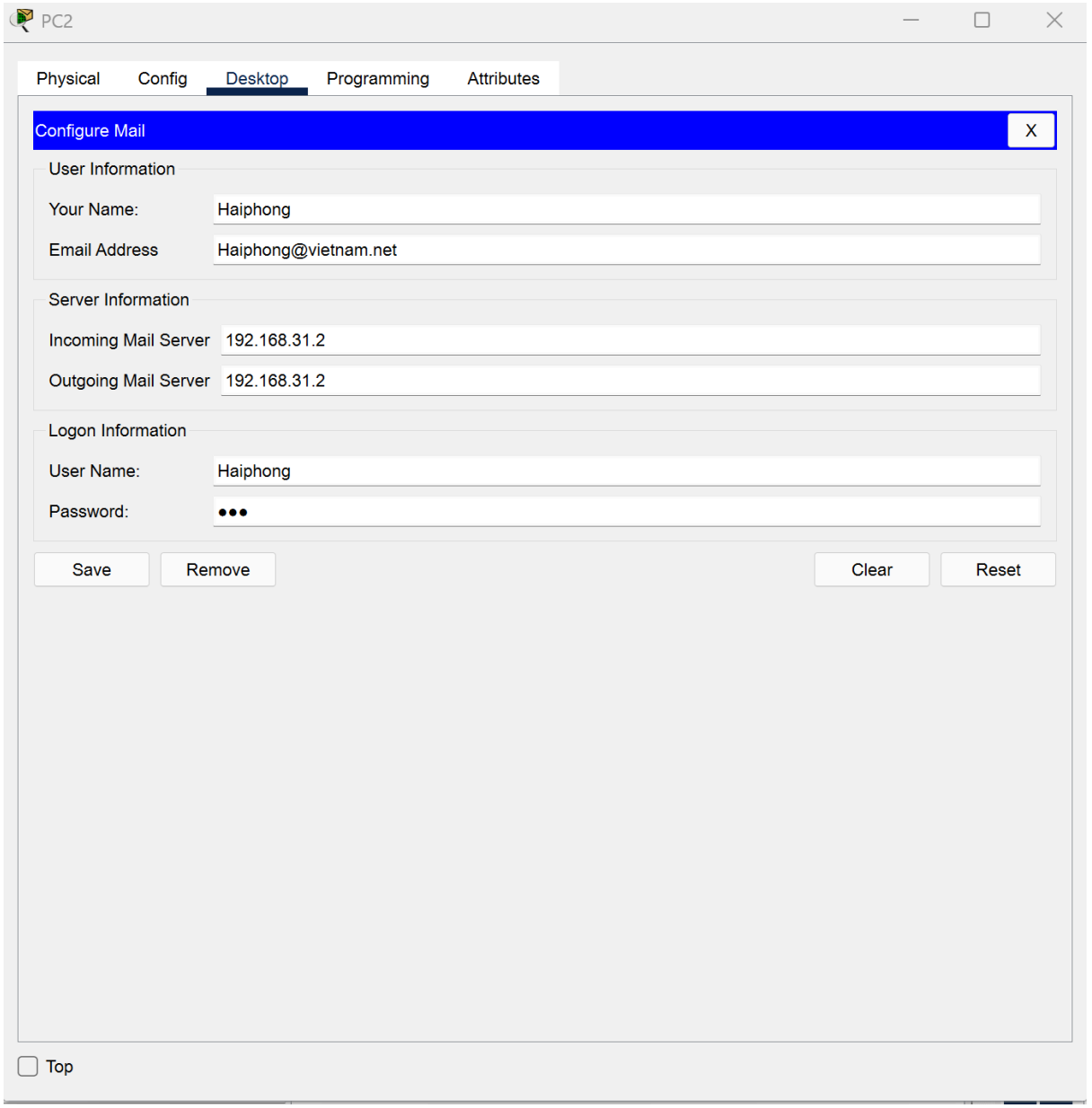


Рис. 6.9. Налаштування облікового запису на ПК мережі B

3. Перевіряємо працездатність поштових скриньок. Наприклад, заходимо на компютер PC0 до розділу *Desktop / Email*. Відкриється вікно *Mail Browser*. Для відправки листа необхідно натиснути кнопку *Compose*. У полі *To* вказуємо e-mail адресу отримувача – `Mumbai@india.com`, в поле *Subject* вводимо тему листа (наприклад, «тест»), а в нижнє поле – текст листа (наприклад, «Мій перший лист!!!»). Щоб надіслати повідомлення, натискаємо кнопку *Send (рис 6.10)*. Після відправки листа в нижній частині вікна з'явиться запис про те, що повідомлення було відправлено (рис. 6.11).

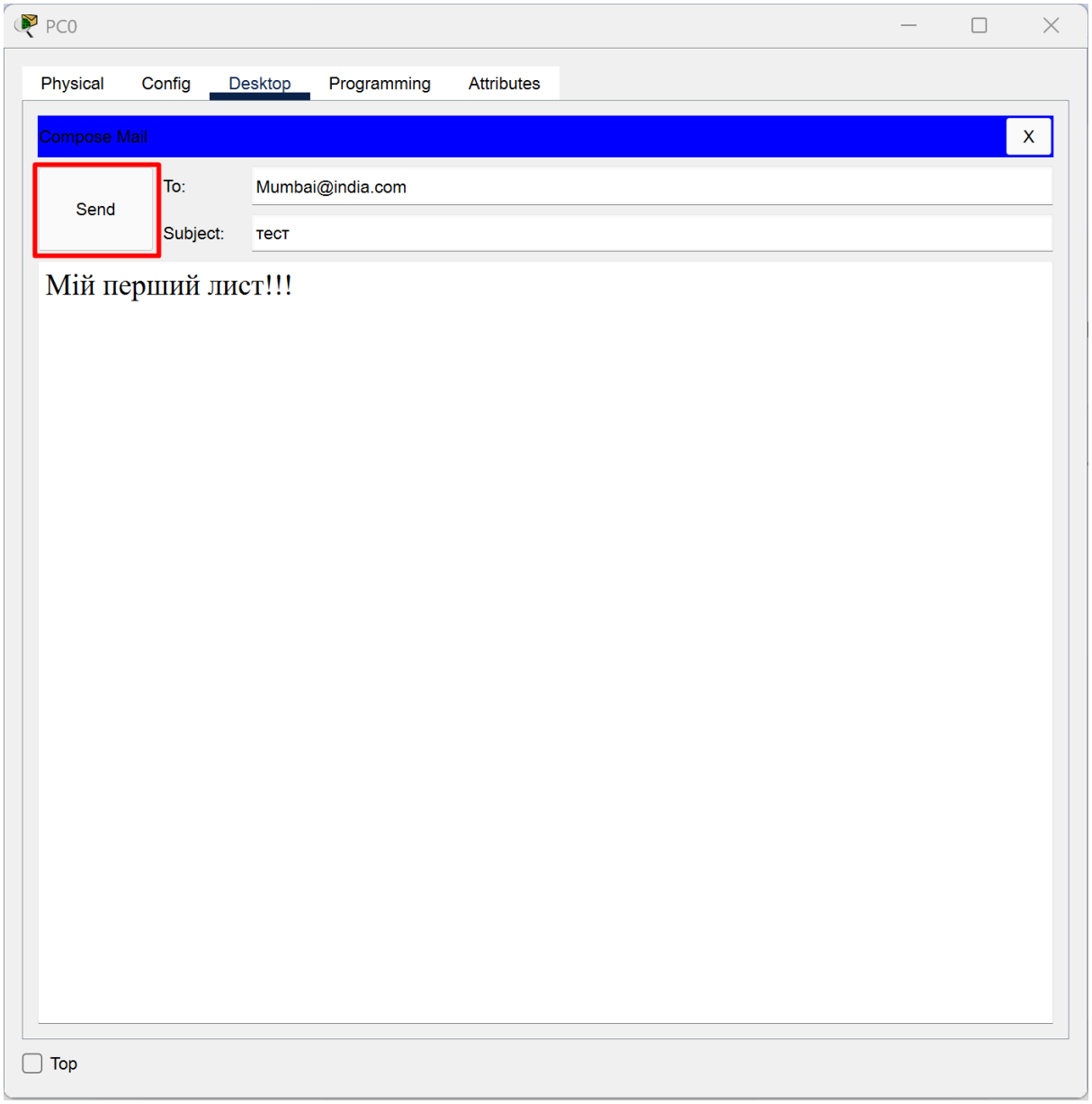


Рис. 6.10. Вікно написання листа

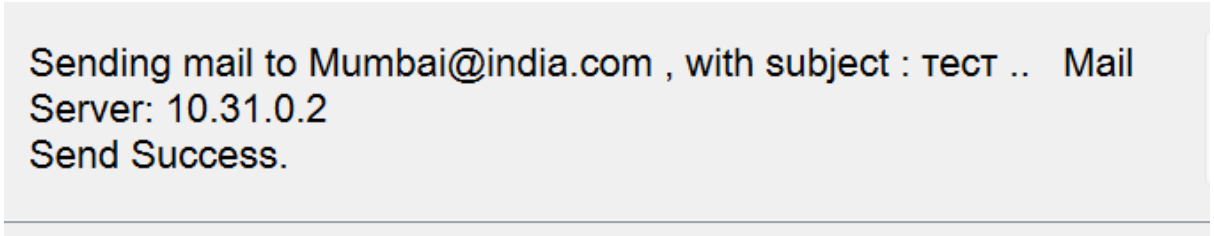


Рис 6.11. Повідомлення про успішне відправлення листа

4. Щоб прочитати отриманий лист, перейдемо до розділу *Desktop / Email* на комп'ютері PC1 та натиснемо кнопку *Receive*. Відобразиться список усіх отриманих листів (рис. 6.12). Відкрити лист можна подвійним натисканням лівої кнопки миші.

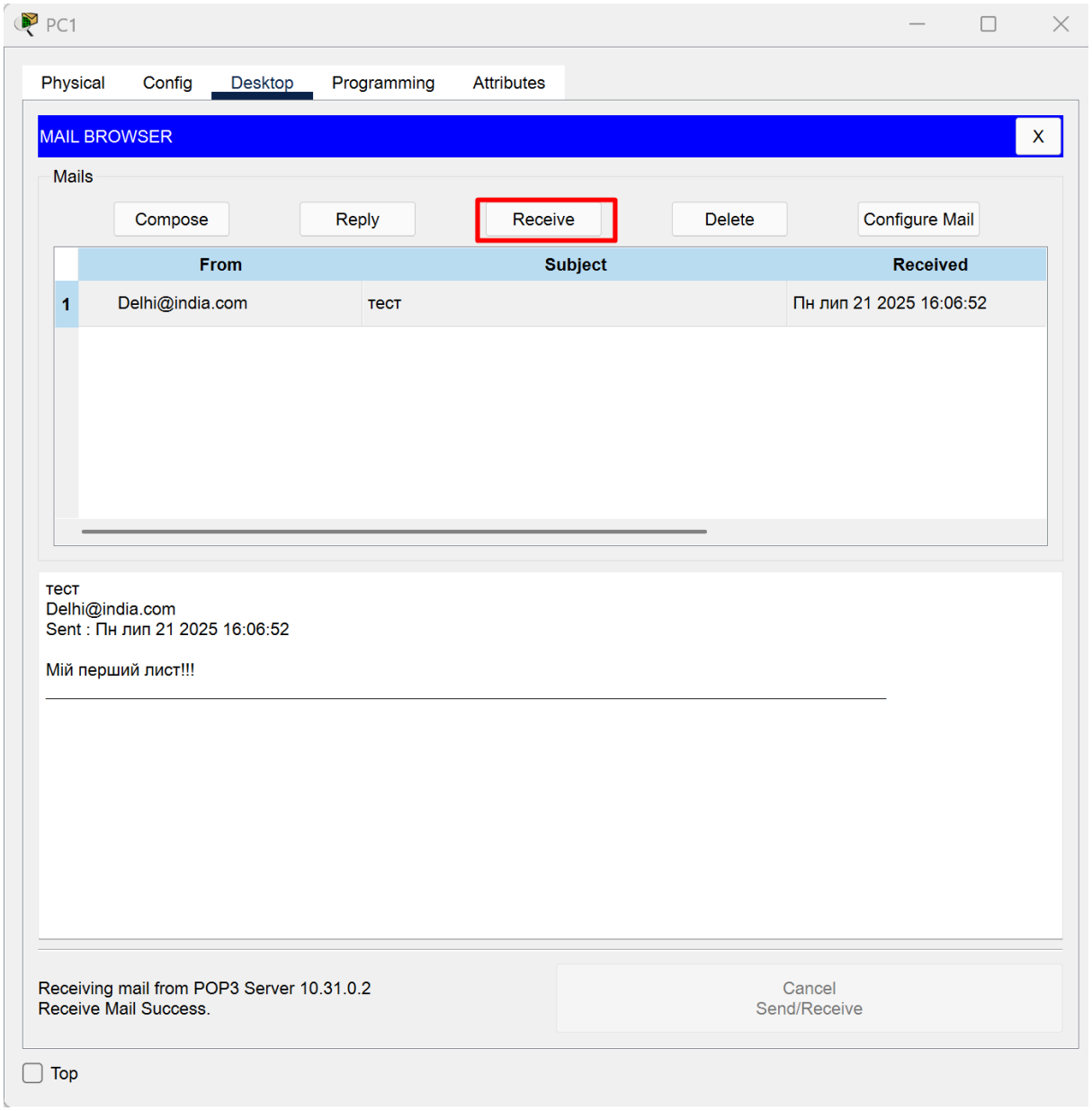


Рис 6.12. Перелік отриманих повідомлень на ПК1

5. Далі надсилаємо листи між усіма комп'ютерами і перевіряємо їх доставлення (рис 6.13).

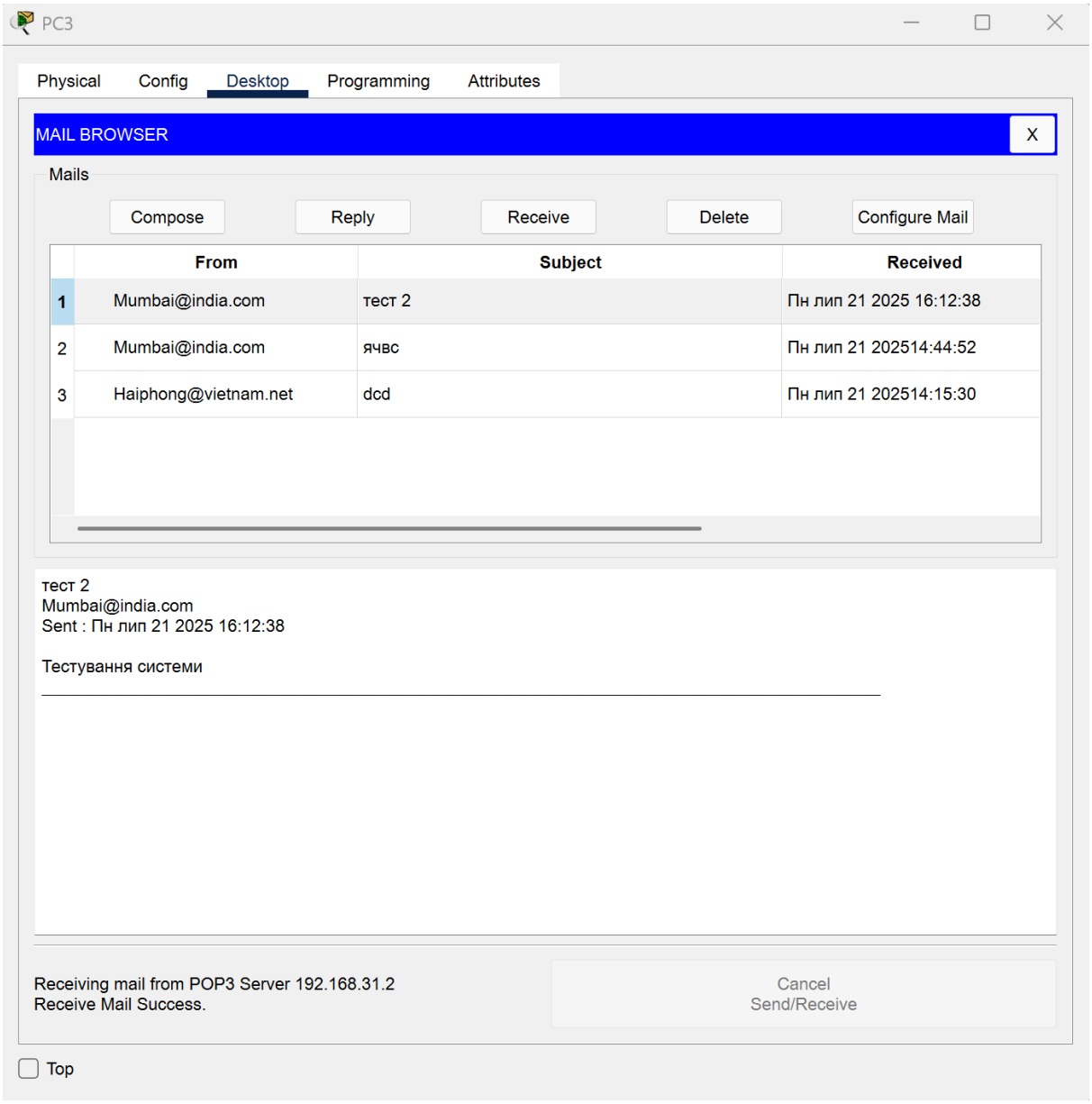


Рис 6.13. Перелік отриманих повідомлень на ПК4

6. Зберігаємо проєкт мережі.

Завдання для індивідуальної роботи

1. Створіть новий проєкт. Назвіть його.

2. Додайте до робочого поля програми Packet Tracer два стаціонарні комп'ютери (PC0, PC1), два ноутбуки (Laptop0, Laptop1), два комутатори (2960), роутер (1941) та два сервери Generic Server-PT (email_A, email_Б).

3. Об’єднайте всі пристрої за допомогою витої пари. Порти підключення роутера та комутаторів – GigabitEthernet, решти пристроїв з комутаторами – FastEthernet. Топологія мережевої моделі показана на рис. 6.14.

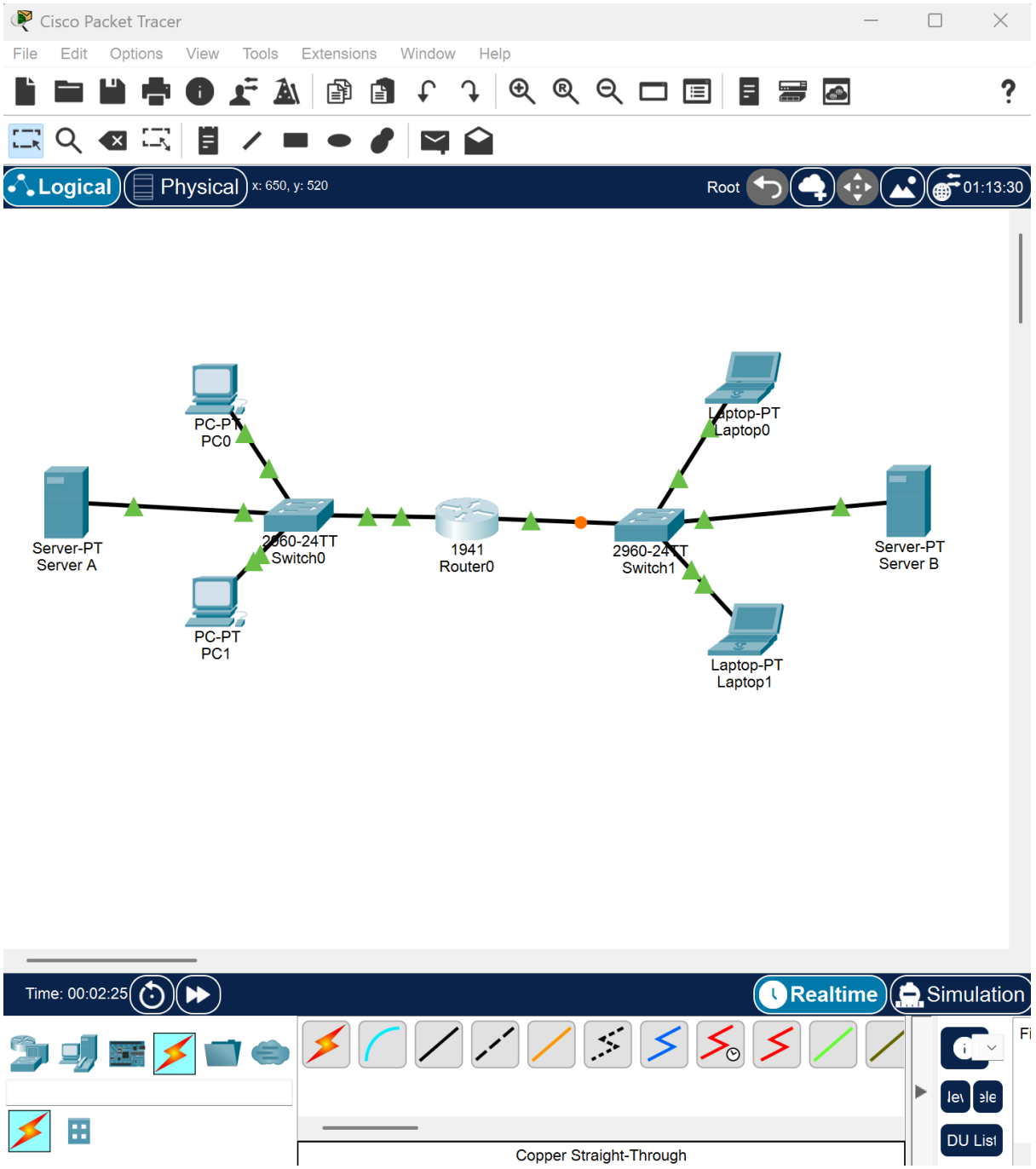


Рис 6.14. Проєкт мережі для індивідуальної роботи

4. Призначте статичні IP-адреси цільовим вузлам у мережах А та Б відповідно до зазначеного варіанту (табл. 6.1):

   - призначте першу доступну адресу інтерфейсу роутера в мережах А і Б.
   - призначте останні доступні адреси серверам у мережах А та Б.
   - призначте другу доступну адресу в мережі А.
   - комп'ютеру PC1 призначте третю доступну адресу в мережі А.
   - призначте другу доступну адресу в мережі В для Laptop0.
   - призначте третю доступну адресу в мережі В для Laptop1.

Таблиця 6.1.

№	Мережа А	Маска А	Мережа Б	Маска Б	Домен А	Домен Б	Користувачі (по 2)
1	10.1.0.0	255.255.255.192	192.168.1.0	255.255.255.224	orion.edu	apollo.edu	Luna, Zoe / Milo, Kai
2	10.2.0.0	255.255.255.192	192.168.2.0	255.255.255.224	terra.org	quantum.org	Nova, Ivy / Leo, Nina
3	10.3.0.0	255.255.255.192	192.168.3.0	255.255.255.224	aether.dev	neuron.dev	Aria, Jude / Ezra, Mira
4	10.4.0.0	255.255.255.192	192.168.4.0	255.255.255.224	nova.co	cosmos.co	Nico, Skye / Remy, Juno
5	10.5.0.0	255.255.255.192	192.168.5.0	255.255.255.224	aurora.tech	titan.tech	Orin, Lia / Axel, Elle
6	10.6.0.0	255.255.255.192	192.168.6.0	255.255.255.224	helix.net	nebula.net	Cleo, Theo / Elio, Sage
7	10.7.0.0	255.255.255.192	192.168.7.0	255.255.255.224	orion.edu	apollo.edu	Luna, Zoe / Milo, Kai
8	10.8.0.0	255.255.255.192	192.168.8.0	255.255.255.224	terra.org	quantum.org	Nova, Ivy / Leo, Nina
9	10.9.0.0	255.255.255.192	192.168.9.0	255.255.255.224	aether.dev	neuron.dev	Aria, Jude / Ezra, Mira
10	10.10.0.0	255.255.255.192	192.168.10.0	255.255.255.224	nova.co	cosmos.co	Nico, Skye / Remy, Juno
11	10.11.0.0	255.255.255.192	192.168.11.0	255.255.255.224	aurora.tech	titan.tech	Orin, Lia / Axel, Elle
12	10.12.0.0	255.255.255.192	192.168.12.0	255.255.255.224	helix.net	nebula.net	Cleo, Theo / Elio, Sage
13	10.13.0.0	255.255.255.192	192.168.13.0	255.255.255.224	orion.edu	apollo.edu	Luna, Zoe / Milo, Kai
14	10.14.0.0	255.255.255.192	192.168.14.0	255.255.255.224	terra.org	quantum.org	Nova, Ivy / Leo, Nina
15	10.15.0.0	255.255.255.192	192.168.15.0	255.255.255.224	aether.dev	neuron.dev	Aria, Jude / Ezra, Mira
16	10.16.0.0	255.255.255.192	192.168.16.0	255.255.255.224	nova.co	cosmos.co	Nico, Skye / Remy, Juno
17	10.17.0.0	255.255.255.192	192.168.17.0	255.255.255.224	aurora.tech	titan.tech	Orin, Lia / Axel, Elle
18	10.18.0.0	255.255.255.192	192.168.18.0	255.255.255.224	helix.net	nebula.net	Cleo, Theo / Elio, Sage
19	10.19.0.0	255.255.255.192	192.168.19.0	255.255.255.224	orion.edu	apollo.edu	Luna, Zoe / Milo, Kai
20	10.20.0.0	255.255.255.192	192.168.20.0	255.255.255.224	terra.org	quantum.org	Nova, Ivy / Leo, Nina
21	10.21.0.0	255.255.255.192	192.168.21.0	255.255.255.224	aether.dev	neuron.dev	Aria, Jude / Ezra, Mira
22	10.22.0.0	255.255.255.192	192.168.22.0	255.255.255.224	nova.co	cosmos.co	Nico, Skye / Remy, Juno
23	10.23.0.0	255.255.255.192	192.168.23.0	255.255.255.224	aurora.tech	titan.tech	Orin, Lia / Axel, Elle
24	10.24.0.0	255.255.255.192	192.168.24.0	255.255.255.224	helix.net	nebula.net	Cleo, Theo / Elio, Sage
25	10.25.0.0	255.255.255.192	192.168.25.0	255.255.255.224	orion.edu	apollo.edu	Luna, Zoe / Milo, Kai
26	10.26.0.0	255.255.255.192	192.168.26.0	255.255.255.224	terra.org	quantum.org	Nova, Ivy / Leo, Nina
27	10.27.0.0	255.255.255.192	192.168.27.0	255.255.255.224	aether.dev	neuron.dev	Aria, Jude / Ezra, Mira
28	10.28.0.0	255.255.255.192	192.168.28.0	255.255.255.224	nova.co	cosmos.co	Nico, Skye / Remy, Juno

№	Мережа А	Маска А	Мережа Б	Маска Б	Домен А	Домен Б	Користувачі (по 2)
29	10.29.0.0	255.255.255.192	192.168.29.0	255.255.255.224	aurora.tech	titan.tech	Orin, Lia / Axel, Elle
30	10.30.0.0	255.255.255.192	192.168.30.0	255.255.255.224	helix.net	nebula.net	Cleo, Theo / Elio, Sage

5. Перевірте працездатність мережі – пропінгуйте з PC0 решту вузлів мережі.
6. Згідно з таблицею 1 створіть на серверах email_A та email_B поштові сервери з доменними іменами і додайте до них по два облікові записи. Для кожного запису придумайте свій пароль.
7. Налаштуйте поштові скриньки на всіх цільових вузлах відповідно до таблиці 1.
8. Перевірте відправку пошти:
   - відправте тестові листи з PC0 на всі інші поштові скриньки;
   - відправте тестові листи з Laptop0 на всі інші поштові скриньки.
9. Перевірте прийом листів на всіх пристроях.
10. Збережіть проєкт мережі.

Звіт має містити:

1. Мета роботи
2. Скріншот схеми мережі
3. Таблиця IP-адрес пристроїв
4. Скріншот налаштування сервера
5. Скріншот налаштування роутера
6. Скріншот налаштування всіх ПК (IP та поштові скриньки)
7. Скріншот результатів перевірки ехо-пакетами між усіма ПК
8. Скріншот надсилання листів
9. Скріншот отримання листів
8. Висновки

Контрольні запитання:

1. Що таке електронна пошта і які її основні функції в комп’ютерних мережах?

2. Які протоколи використовуються для надсилання та отримання електронної пошти? У чому їх різниця?
3. Яку роль відіграє SMTP-сервер у передачі електронних листів?
4. Чим відрізняються протоколи POP3 та IMAP у процесі отримання повідомлень?
5. Які типи серверів необхідні для повноцінної роботи електронної пошти в мережі?
6. Що таке DNS і як він використовується при надсиланні електронних листів?
7. Як додати DNS-запис на сервері у Cisco Packet Tracer?
8. Які параметри необхідно вказати у поштовому клієнті для правильної роботи з email-сервером?
9. Які дії слід виконати, щоб забезпечити успішне надсилання листа з однієї мережі до іншої?
10. Чому пінг між пристроями не гарантує успішну доставку електронної пошти?
11. Як перевірити працездатність DNS-сервера у Cisco Packet Tracer?
12. Яка інформація вказується в полі “Email address” поштового клієнта і що вона означає?
13. Чому важливо вказувати коректні IP-адреси SMTP, POP3 і DNS у налаштуваннях клієнта?
14. Які помилки можуть виникнути під час надсилання листа і як їх виправити?
15. Як забезпечити безпеку при налаштуванні поштових серверів у навчальному середовищі?

ЛАБОРАТОРНА РОБОТА №7
ПІДКЛЮЧЕННЯ ПРИНТЕРІВ ТА ІНШИХ ПРИСТРОЇВ У ЛОКАЛЬНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ CISCO PACKET TRACER

Мета роботи: Закріпити навички підключення принтерів до комп'ютерної мережі, навчитися налаштовувати доступ до мережевого принтера з декількох ПК, створити сервер друку як окрему роль у мережі.

Теоретичні відомості:

У локальних комп'ютерних мережах, окрім комп'ютерів, часто використовуються й інші пристрої — зокрема, мережеві принтери. Такий принтер підключається до комутатора як звичайний вузол і має власну IP-адресу. Щоб забезпечити стабільний доступ, йому зазвичай призначають статичну адресу, а комп'ютери в мережі можуть отримувати свої адреси динамічно за допомогою DHCP-сервера. Для зручності взаємодії із принтером також можна використовувати DNS, щоб звертатися до нього не за IP-адресою, а за простим іменем, наприклад `printer.local`.

У Cisco Packet Tracer симулюється базова робота принтера в мережі. Такий пристрій може мати IP-адресу, відповідати на ping-запити та бути об'єктом DNS-іменування, однак він не має реального веб-інтерфейсу або друкарських функцій. Програми, як-от Text Editor, іноді містять кнопку Print, але вона лише імітує успішну відправку завдання — без реального зв'язку з принтером. Через це Web Browser не зможе завантажити сторінку з принтера, і при спробі звернення до нього буде повідомлення про скидання з'єднання.

Перевірка доступності принтера в Packet Tracer виконується через ping або DNS-запит, що підтверджує правильне підключення до мережі. У навчальних сценаріях зручно використовувати ці методи для симуляції доступу до принтера, а сам пристрій можна розглядати як пасивний вузол, що виконує роль точки доступу до ресурсу. Це дозволяє студентам на практиці освоїти принципи підключення мережевих пристроїв, навіть якщо віртуальне середовище не повністю відтворює реальну функціональність.

Хід роботи

Створюємо новий проєкт в Cisco Packet Tracer. У робочу область переносимо 1 сервер, 1 коммутатор (Switch 2960), 1 маршрутизатор (Router), 1 принтер, 3 ПК. З'єднуємо сервер, принтер і комп'ютери з комутатором через FastEthernet, а роутер через GigabitEthernet з комутатором, використовуючи скручену пару (рис 7.1).

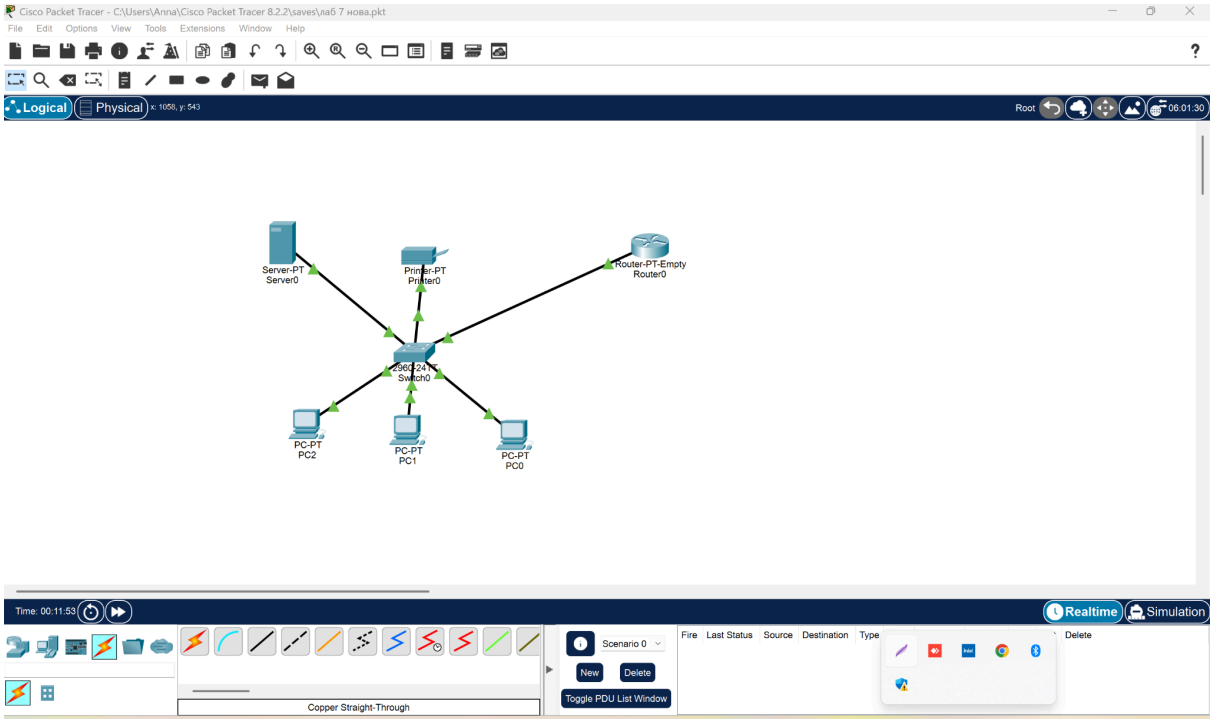


Рис. 7.1 Схема мережі

Налаштовуємо сервер:

Заходим на вкладку *Config* → FastEthernet0: в поле IP пишемо IP-адресу сервера `192.168.50.1` та маску: `255.255.255.0`

Далі вкладка *Services* → DHCP: в поле Default Gateway пишемо Gateway IP `192.168.50.254`, в поле DNS Server пишемо IP-адресу сервера `192.168.50.1`, в поле Start IP Address пишемо IP з якого розпочнеться роздача `192.168.50.100` та в полі Maximum Number of Users пишемо максимальну кількість користувачів, тут 100. Все це змінюємо у створеному пулі serverPool і зберігаємо зміни кнопкою Save, потім ON (рис. 7.2).

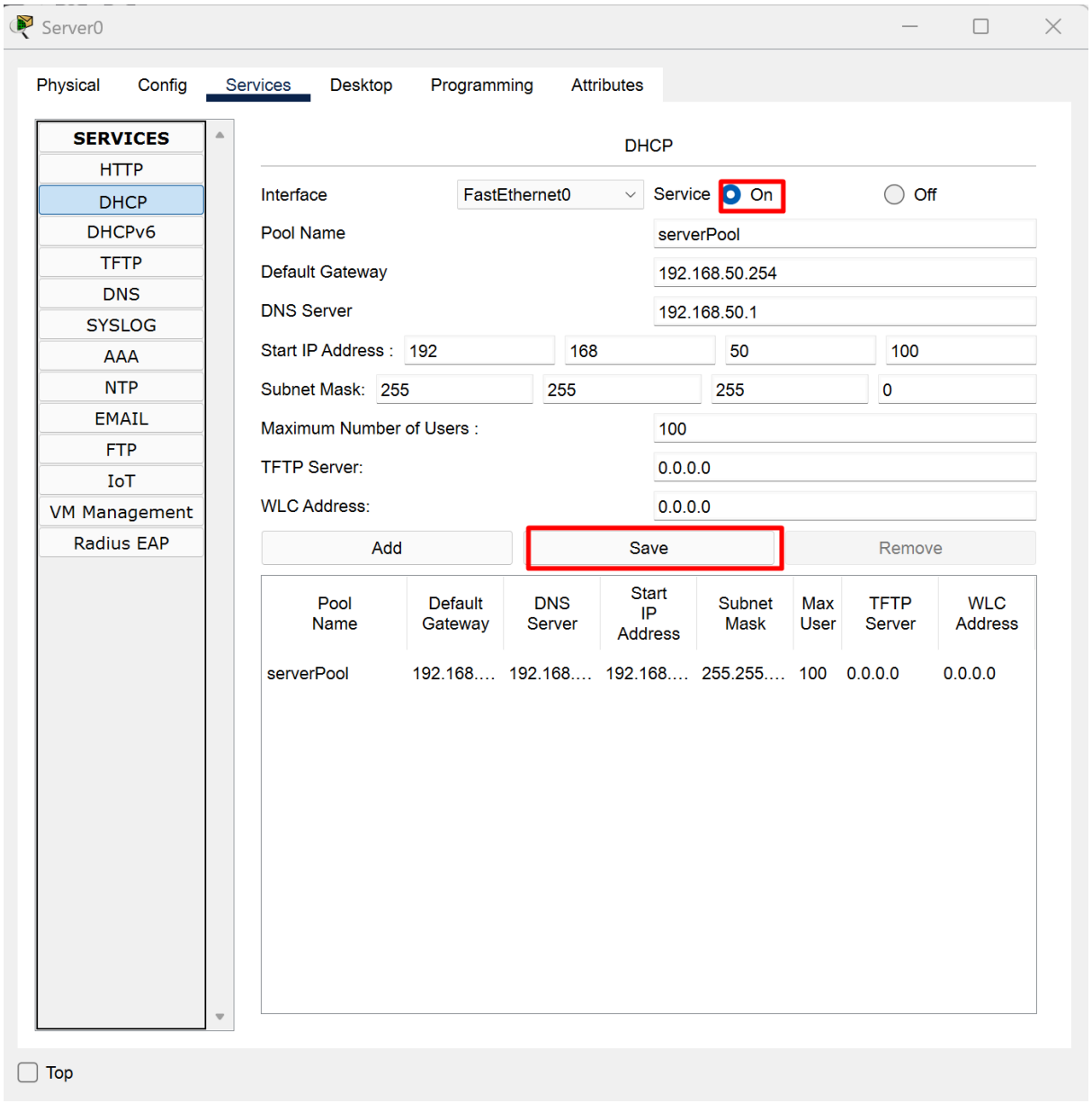


Рис. 7.2 Налаштування DHCP на сервері

Наступною обираємо вкладку *Services* → HTTP та ставимо перемикач на перемикач ON.

Після цього обираємо вкладку *Services* → DNS. У полі Name записуємо ім'я DNS server.local, а в полі Address пишемо IP-адресу сервера `192.168.50.1` та натискаємо натискаємо кнопку ADD. Далі створюємо ще один запис: ім'я DNS `printer.local`, а в полі Address пишемо IP-адресу `192.168.50.10.` Тоді натискаємо перемикач ON (рис. 7.3).

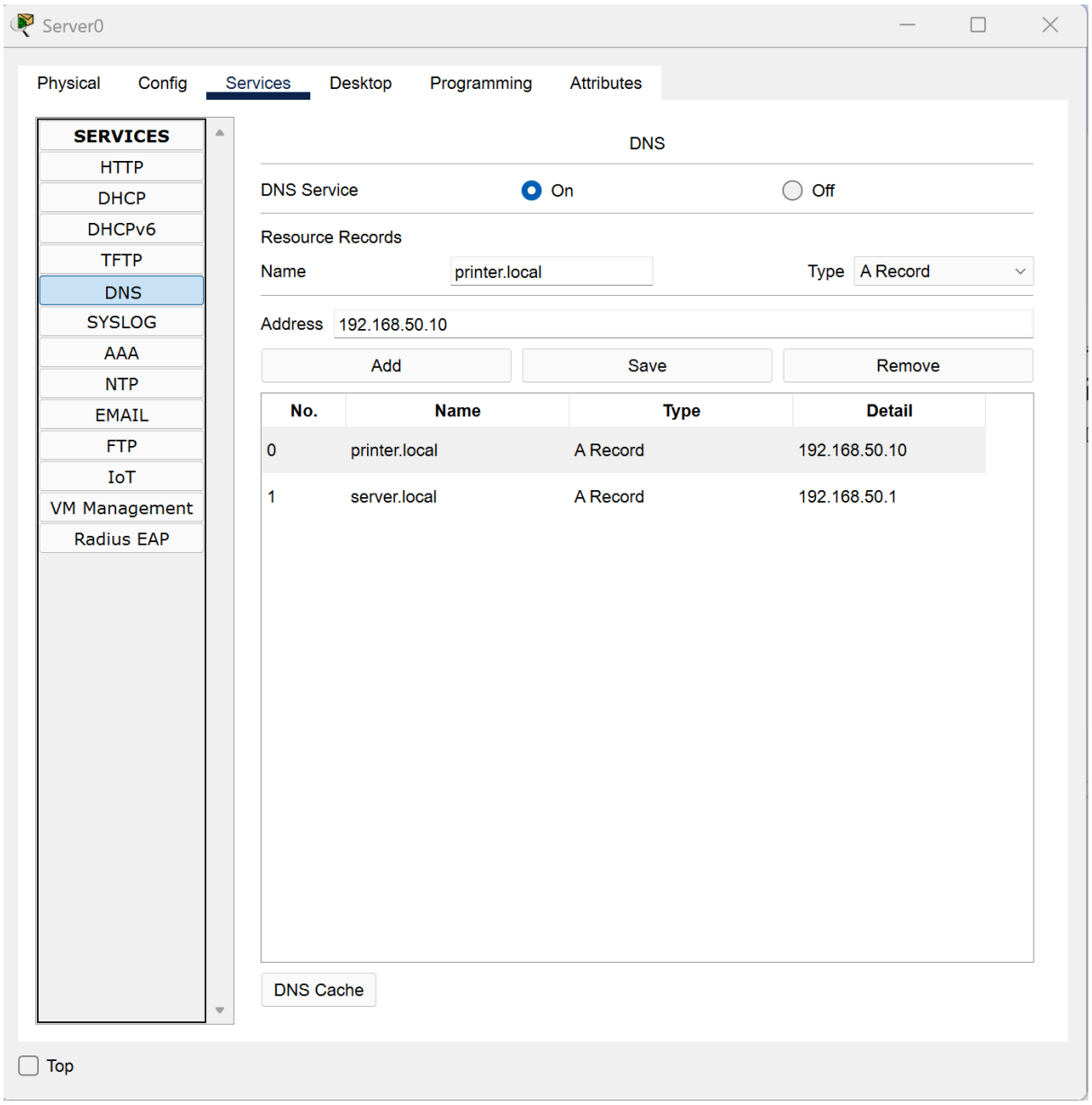


Рис. 7.3 Налаштування DNS на сервері

Наступною обираємо вкладку *Services* → HTTP та ставимо перемикач на перемикач ON.

Налаштовуємо роутер:

Заходимо у вкладку *Config* → GigabitEthernet0/0 та в полі IPv4 Address записуємо Gateway IP `192.168.50.254`, в поле Subnet Mask: `255.255.255.0`. Не забудьте увімкнути порт On.

Налаштовуємо принтер:

Заходимо у вкладку *Config* → FastEthernet0 та в полі IPv4 Address записуємо IP `192.168.50.10`, в поле Subnet Mask: `255.255.255.0` (рис. 7.4).

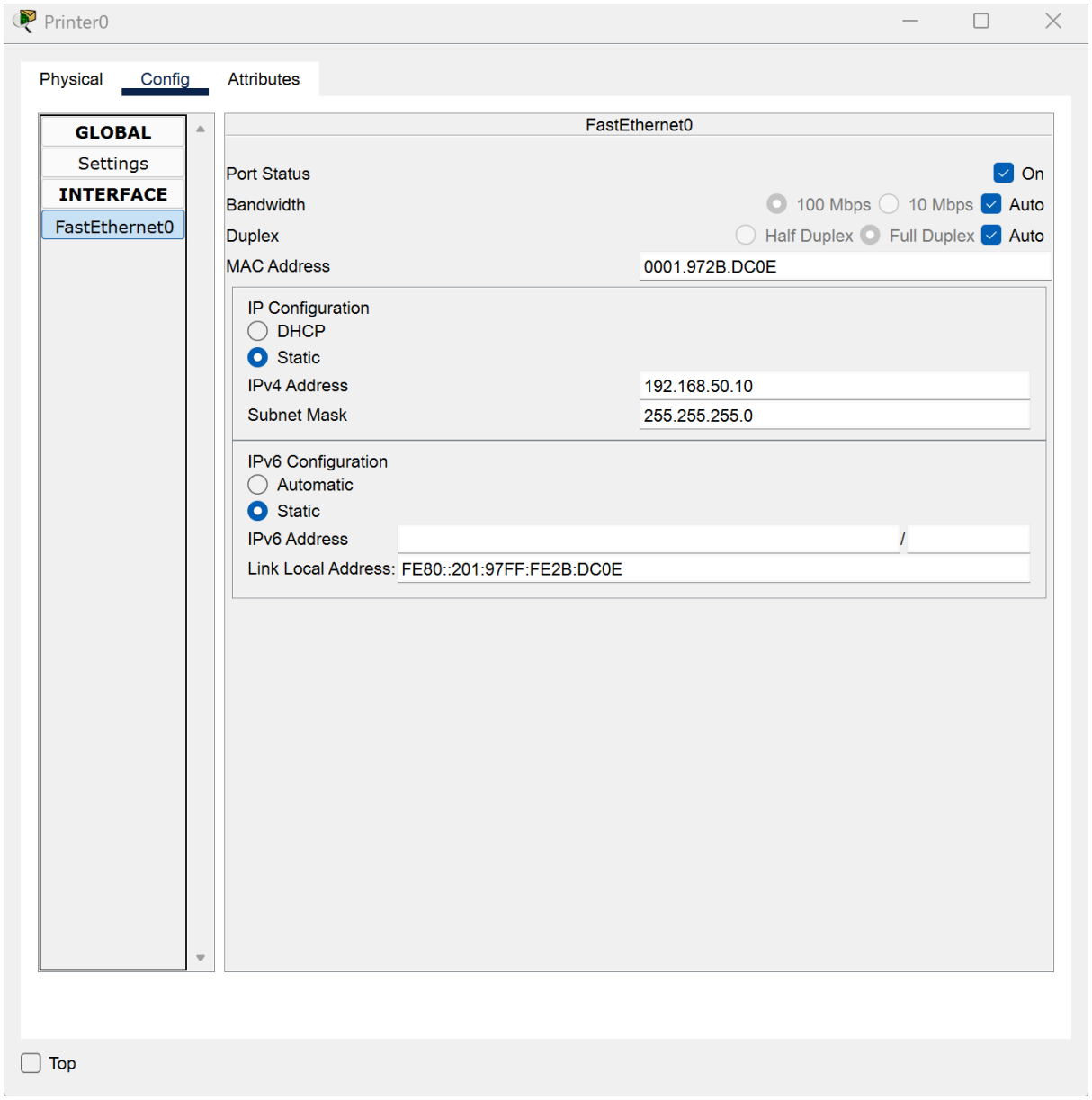


Рис. 7.4 Налаштування IP на принтері

Після цього заходимо у вкладку *Config* → Global → Setting та в полі Default Gateway записуємо IP `192.168.50.254` (рис 7.5).

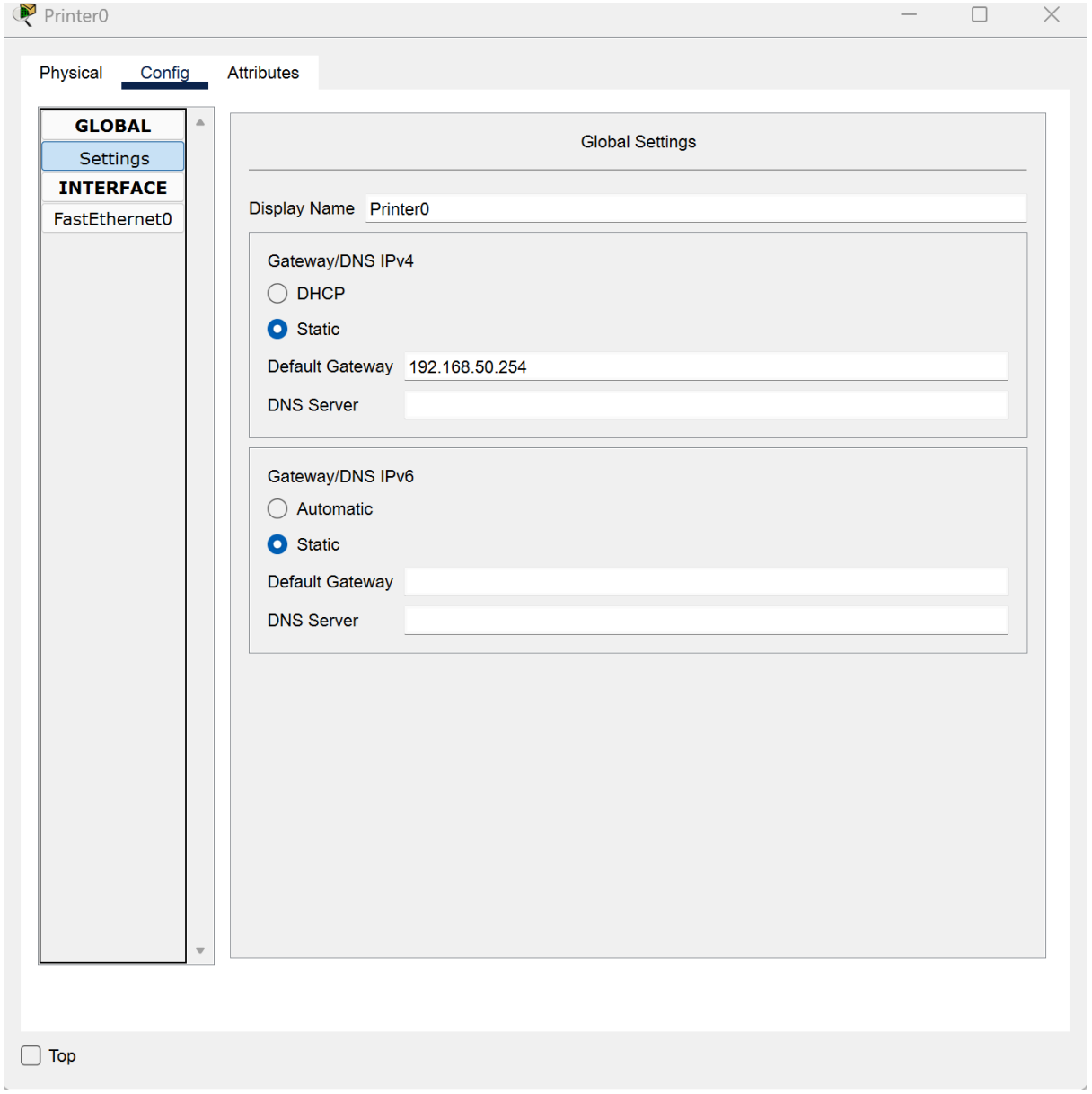


Рис. 7.5 Налаштування Default Gateway на принтері

Наступні налаштування робимо для всіх ПК. Заходим на вкладку *Desktop* → IP Configuration → DHCP. Перевіряємо отримання адреси (рис. 7.6).

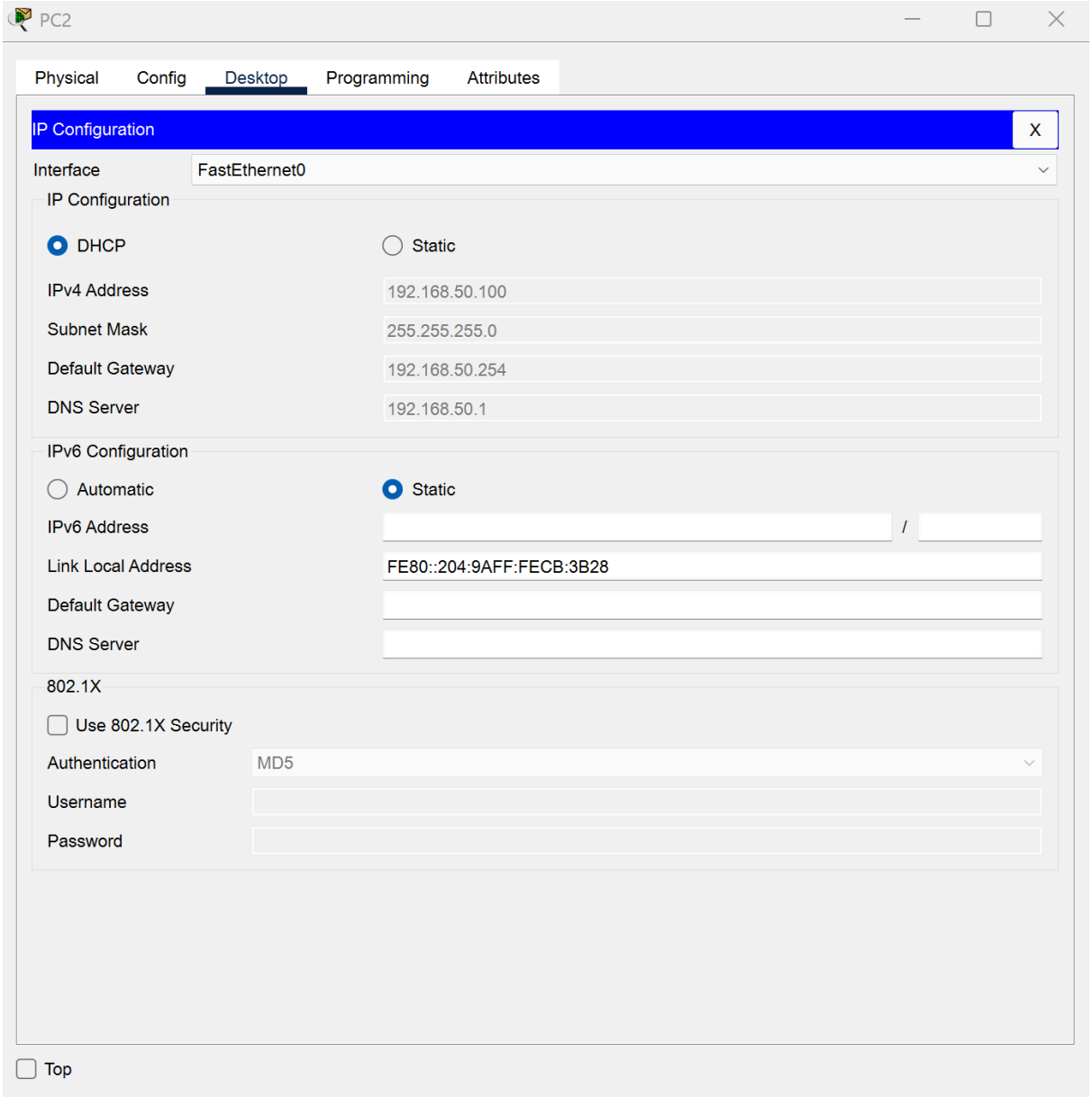


Рис. 7.6 Отримана IP адреса на комп'ютері

Перевірка роботи.

Оскільки Cisco Packet Tracer не підтримує реальний вибір принтера для друку, процес друку імітується:

1. Відкрийте Text Editor на ПК
2. Введіть тестовий текст
3. Натисніть Print (якщо кнопка доступна)

Якщо використовується новіша версія Cisco Packet Tracer, то для того щоб перевірити коректність роботи необхідно з кожного ПК зробити PING - запит до принтера. Це можна зробити двома способами

1. Відкрийте **Command Prompt** та введіть запит

ping `printer.local`

2. Відкрийте **Command Prompt** та введіть запит

   ping `192.168.50.10` (рис. 7.7)

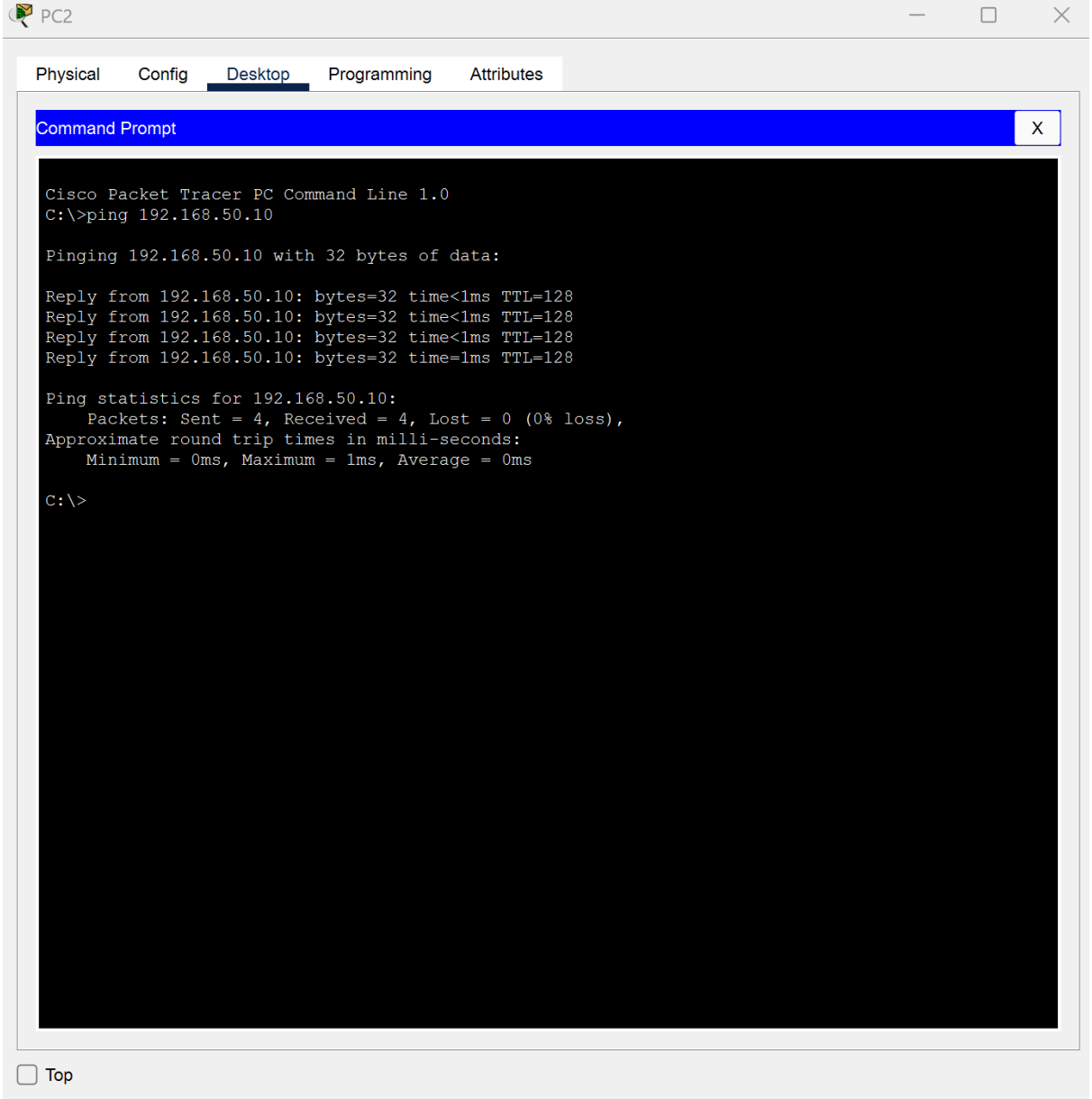


Рис. 7.7 Виконання PING - запиту до принтера з ПК

Також робимо перевірку через **DNS.** Заходимо на ПК, обираємо вкладку *Desktop* → Web Browser і у полі URL пишемо DNS-ім'я, в цьому випадку `server.local` та натиснути кнопку Go. Стартова сторінка має бути доступна. Якщо ж ввести `printer.local`, то отримаємо повідомлення про те, що принтер не відповідає (рис 7.8).

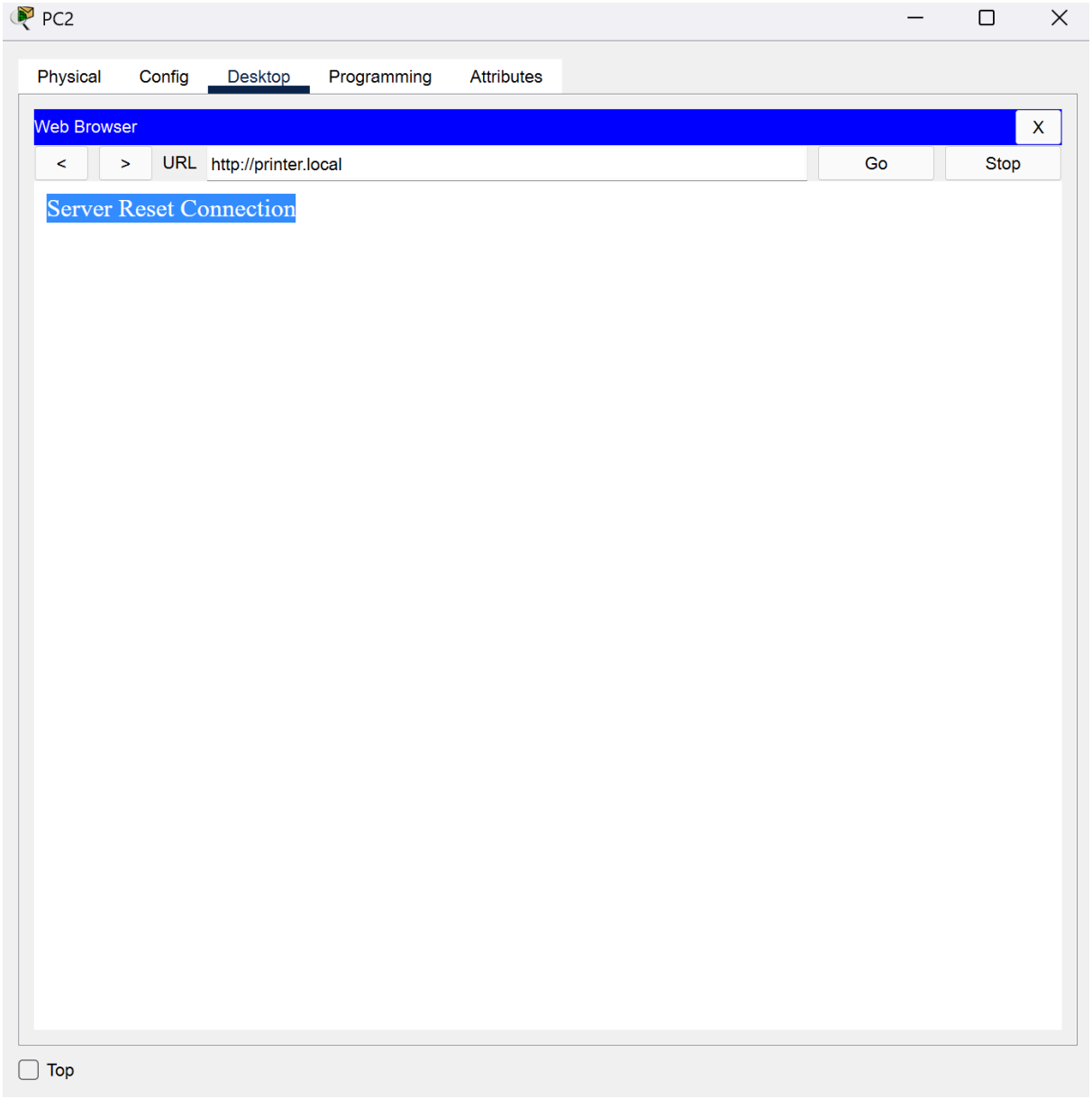


Рис. 7.8 Доступ до HTTP-сервера

Це означає, що DNS-запит до printer.local відпрацював успішно, але HTTP-з'єднання не було встановлено, бо принтер не відповідає як вебсервер.

Завдання для індивідуальної роботи

1. Створіть новий проєкт та назвіть його.
2. Додайте в робочу область Cisco Packet Tracer 1 сервер, 1 комутатор (Switch 2960), 1 маршрутизатор (Router), 1 принтер, 2 ПК, 2 ноутбуки.
3. Об’єднайте всі пристрої за допомогою витої пари. Порти підключення роутера та комутатора – GigabitEthernet, решти пристроїв з комутатором - FastEthernet.

4. Зробіть налаштування сервера, роутера, принтера та комп’ютерів відповідно до свого варіанту з таблиці 7.1.

Таблиця 7.1

Варіант	IP-адреса принтера	DNS-ім’я	Gateway IP	DHCP Start IP
1	192.168.60.10	print01.local	192.168.60.254	192.168.60.100
2	192.168.70.10	print02.local	192.168.70.254	192.168.70.100
3	192.168.80.10	print03.local	192.168.80.254	192.168.80.100
4	192.168.90.10	print04.local	192.168.90.254	192.168.90.100
5	192.168.100.10	print05.local	192.168.100.254	192.168.100.100
6	10.1.1.10	printerA.local	10.1.1.254	10.1.1.100
7	10.2.2.10	printerB.local	10.2.2.254	10.2.2.100
8	10.3.3.10	printerC.local	10.3.3.254	10.3.3.100
9	172.16.1.10	laser1.local	172.16.1.254	172.16.1.100
10	172.16.2.10	laser2.local	172.16.2.254	172.16.2.100
11	192.168.110.10	office1.local	192.168.110.254	192.168.110.100
12	192.168.120.10	office2.local	192.168.120.254	192.168.120.100
13	192.168.130.10	hpdesk.local	192.168.130.254	192.168.130.100
14	192.168.140.10	xerox.local	192.168.140.254	192.168.140.100
15	192.168.150.10	canon.local	192.168.150.254	192.168.150.100
16	172.20.10.10	brother.local	172.20.10.254	172.20.10.100
17	172.21.0.10	colorjet.local	172.21.0.254	172.21.0.100
18	172.22.1.10	officejet.local	172.22.1.254	172.22.1.100
19	10.4.4.10	mono1.local	10.4.4.254	10.4.4.100
20	10.5.5.10	mono2.local	10.5.5.254	10.5.5.100
21	192.168.160.10	branch1.local	192.168.160.254	192.168.160.100
22	192.168.170.10	branch2.local	192.168.170.254	192.168.170.100
23	192.168.180.10	branch3.local	192.168.180.254	192.168.180.100
24	192.168.190.10	color1.local	192.168.190.254	192.168.190.100
25	192.168.200.10	bwprinter.local	192.168.200.254	192.168.200.100
26	10.6.6.10	fastprint.local	10.6.6.254	10.6.6.100
27	10.7.7.10	printcloud.local	10.7.7.254	10.7.7.100
28	172.30.1.10	laserpro.local	172.30.1.254	172.30.1.100

Варіант	IP-адреса принтера	DNS-ім’я	Gateway IP	DHCP Start IP
29	192.168.210.10	officedoc.local	192.168.210.254	192.168.210.100
30	192.168.220.10	sharedprint.local	192.168.220.254	192.168.220.100

5. Отримайте динамічні адреси для своїх ПК.
6. Зробіть пінгування з кожного ПК до принтера обома способами.
7. Перевірте доступ до HTTP-сервера.
8. Збережіть проєкт мережі.

Звіт має містити:

1. Мета роботи
2. Скріншот схеми мережі
3. Таблиця IP-адрес (включно з DHCP)
4. Скріншоти налаштувань сервера, роутера, принтера та отриманих динамічних IP кожного ПК.
5. Результати ping і доступ до HTTP-сервера
6. Висновки

Контрольні запитання:

1. Яка роль DHCP у підключенні мережевого принтера?
2. Як DNS полегшує роботу з принтерами у мережі?
3. Яка різниця між локальним і мережевим принтером?
4. Що станеться, якщо у принтера і ПК буде однакова IP-адреса?
5. Як перевірити підключення до принтера на рівні мережі?

ЗВІТ

Про виконання лабораторної роботи №2

“Проєктування комп’ютерної мережі в Cisco Packet Tracer”

з дисципліни “Комп’ютерні мережі”

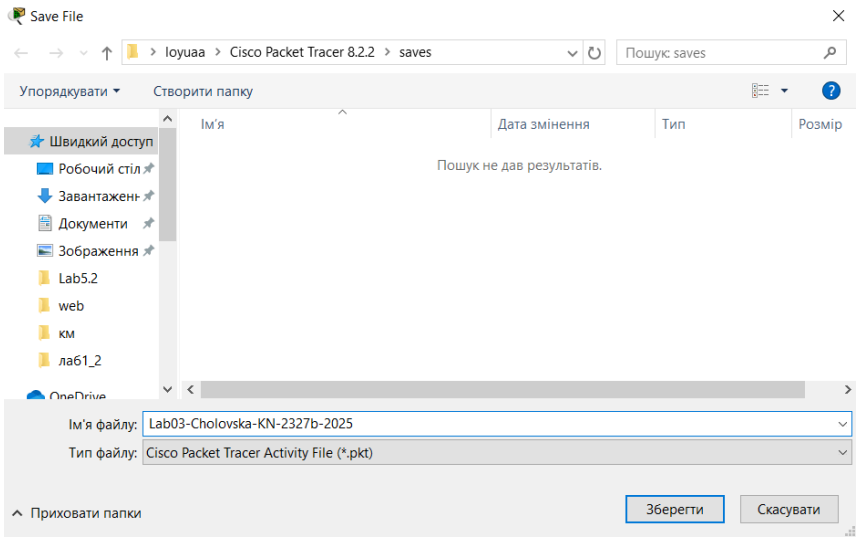
студентки групи КН-2327Б Марушко Оксани

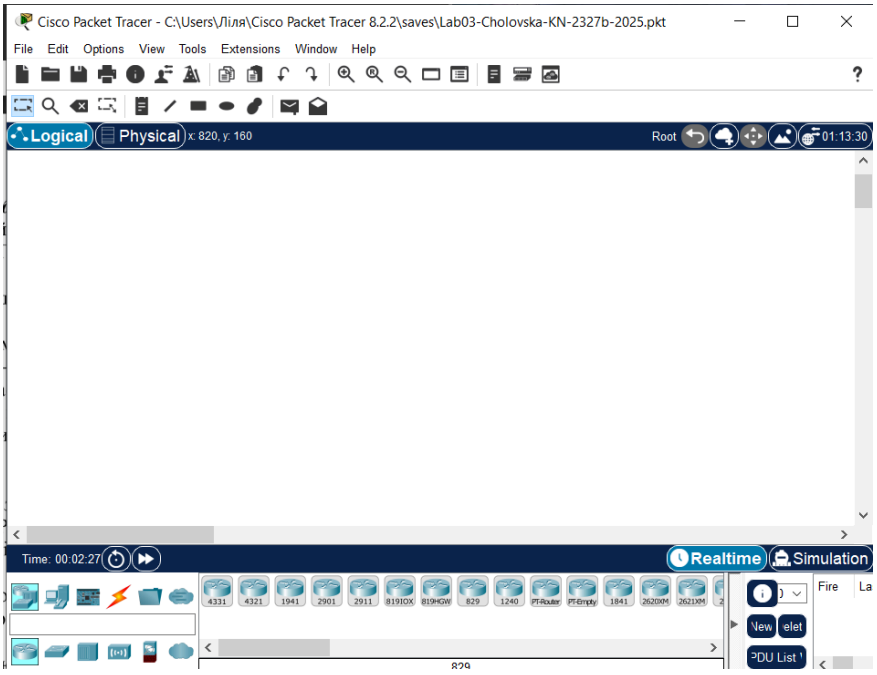
Мета роботи: ознайомитися з графічним інтерфейсом Cisco Packet Tracer, навчитись моделювати комп’ютерну мережу, а також здійснювати її моніторинг.

Хід роботи:

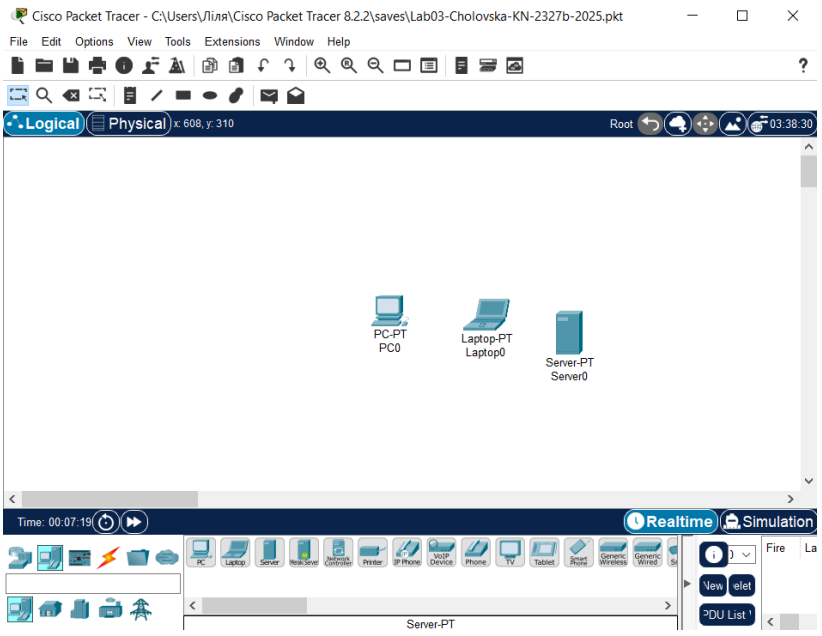
Варіант 3

1. Запустити програму і створити новий проєкт мережі. Назвати проєкт.



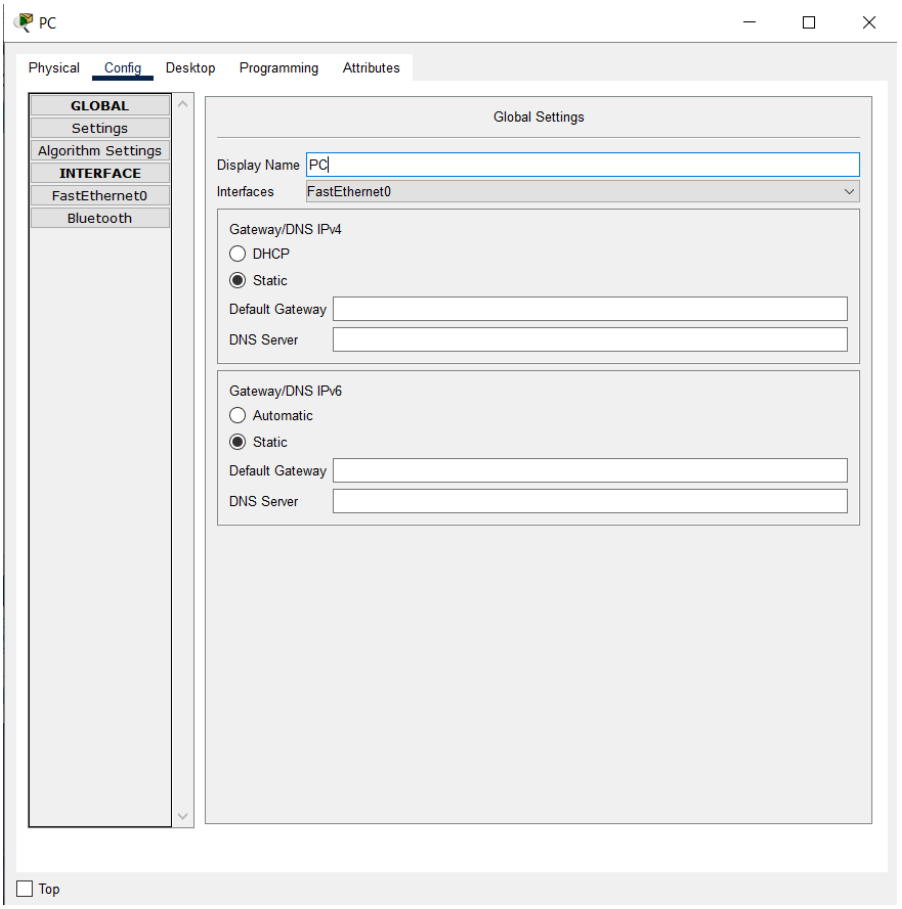


2. Додати у проєкт кінцеві пристрої – декілька робочих станцій, ноутбуків та сервер.

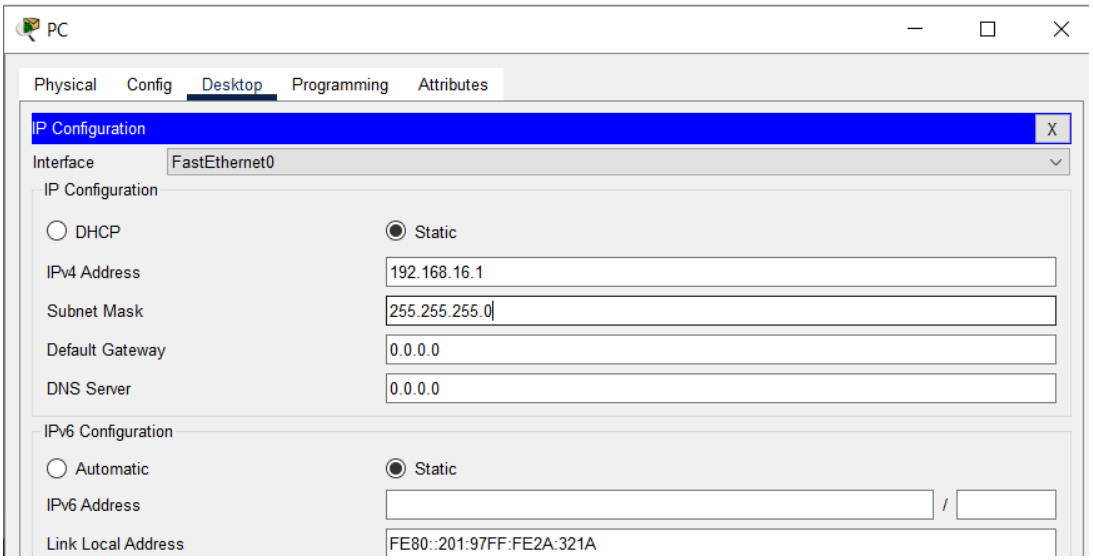


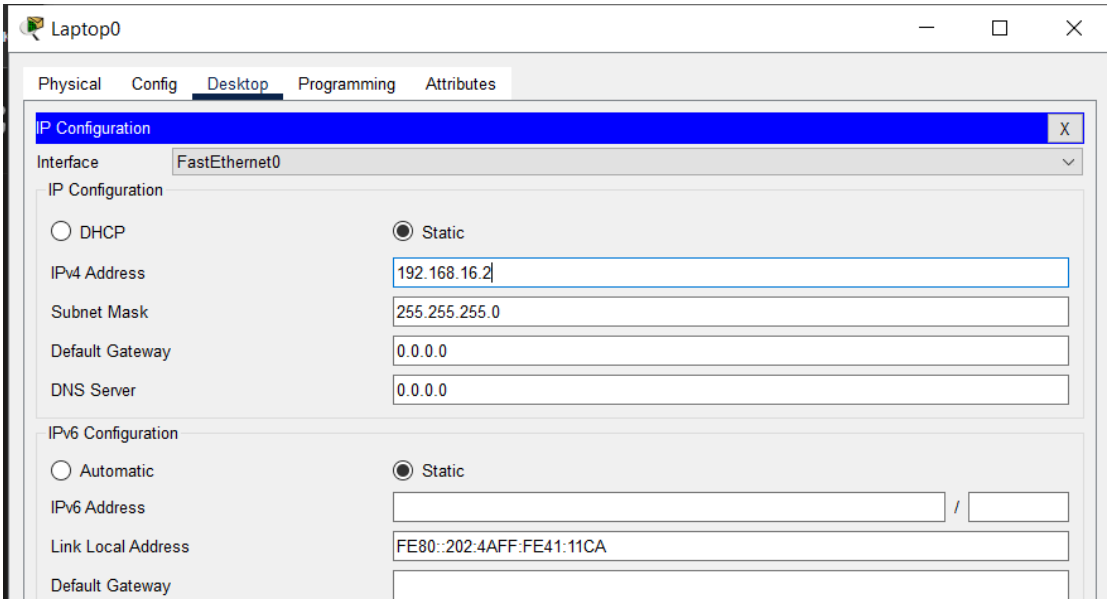
3. Змінити кінцевим пристроям, доданим у п.2, стандартні імена і налаштувати IP-адреси.

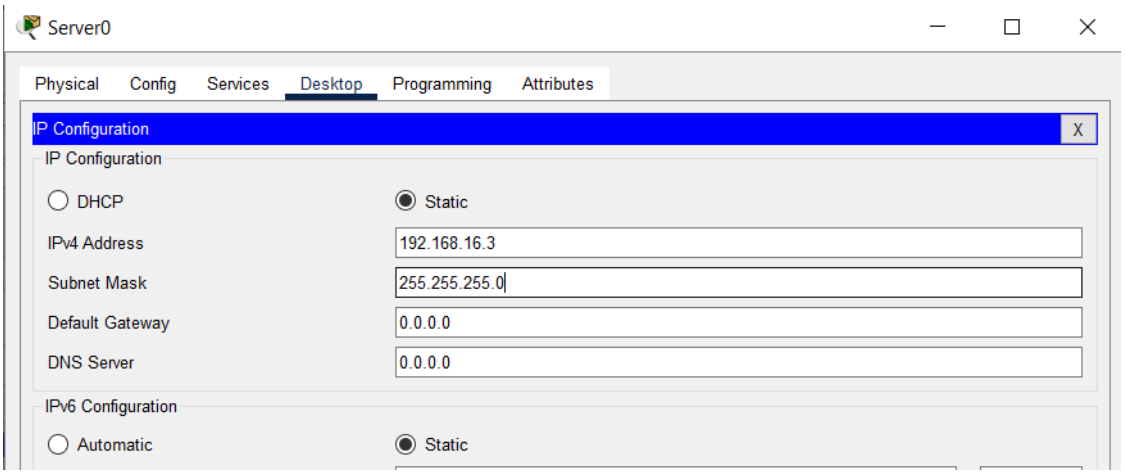
- Додати стандартні імена:



- Налаштувати IP-адреси і маску:

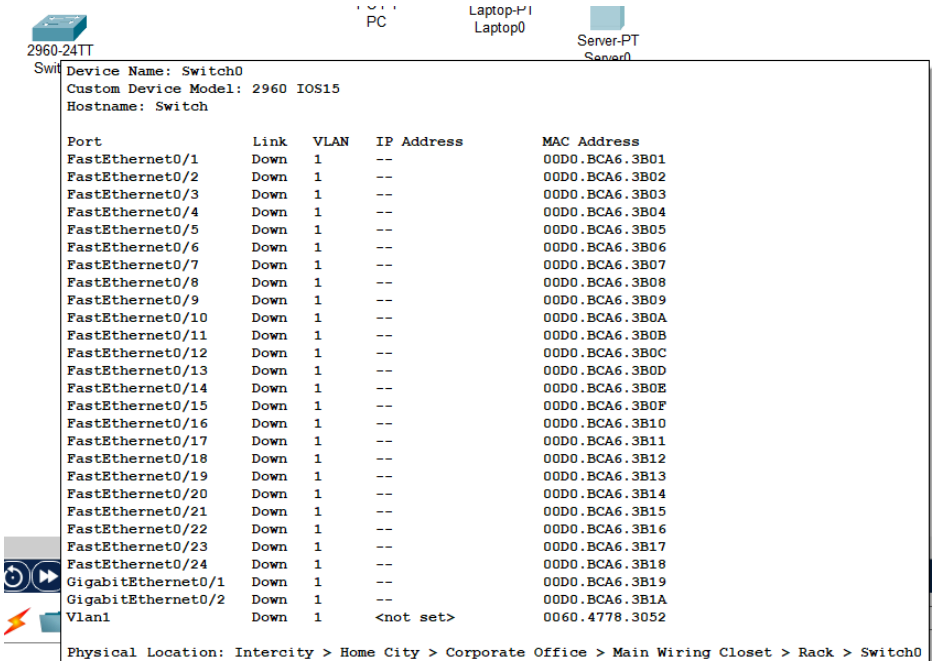



Laptop0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.16.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::202:4AFF:FE41:11CA
Default Gateway

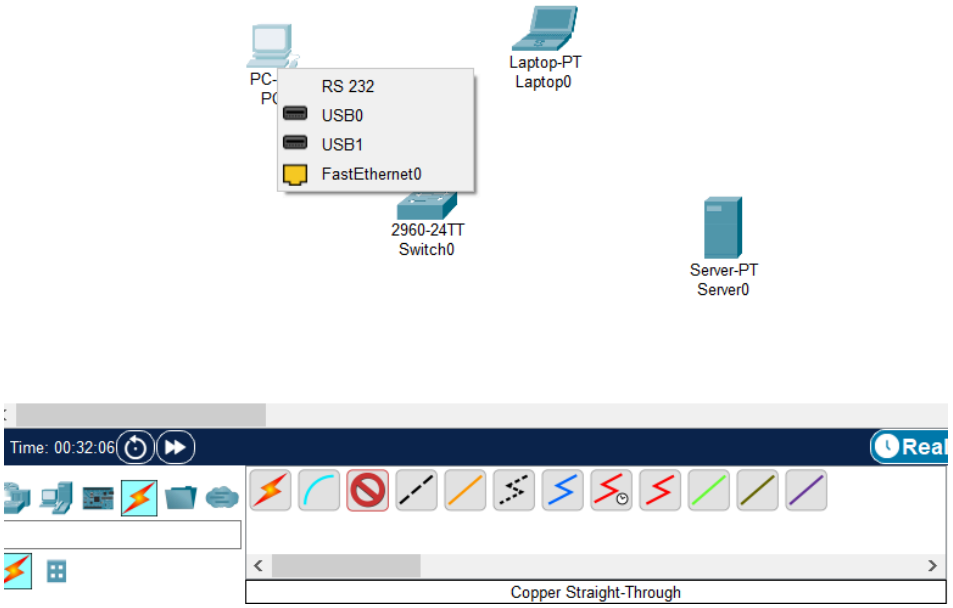

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.16.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static

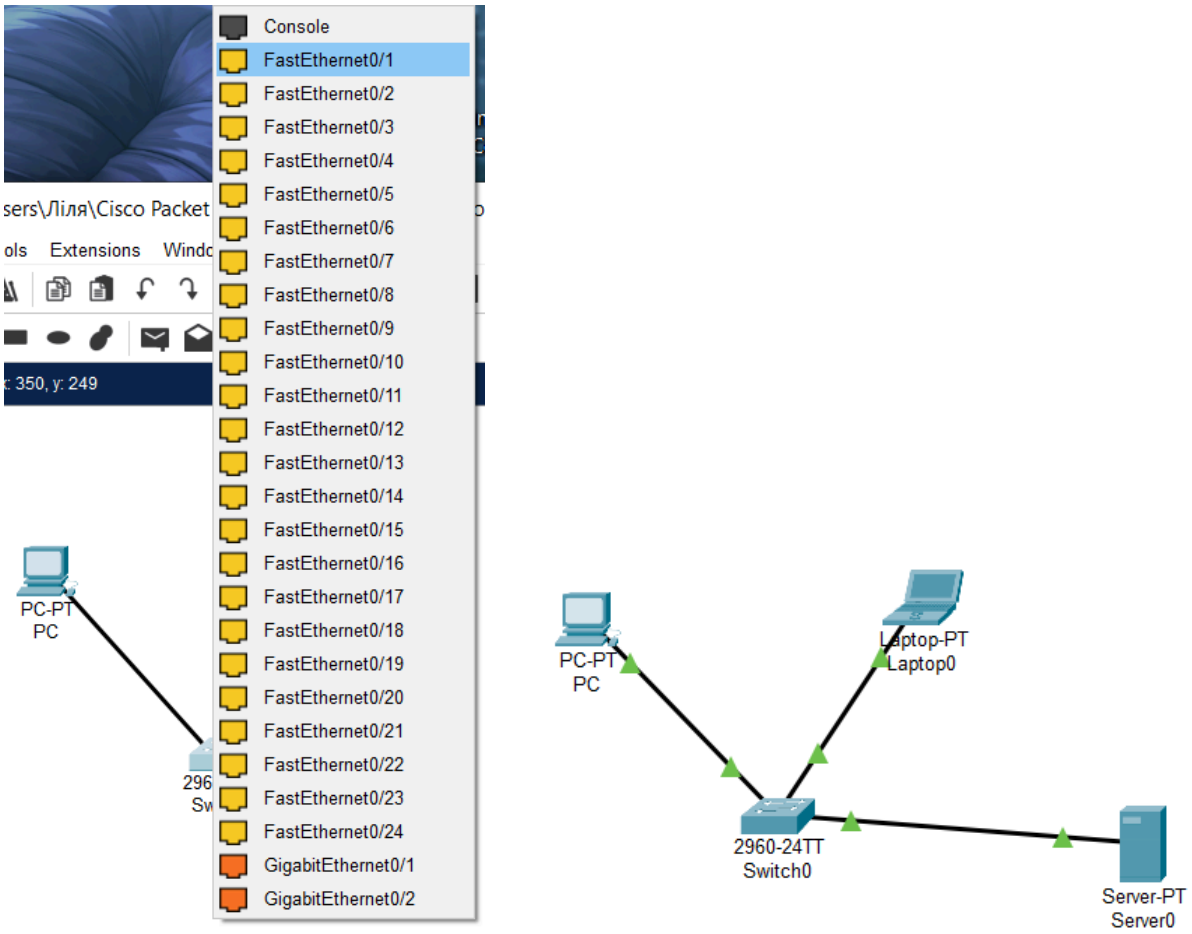
4. Додати у проєкт комутатор і з’єднати всі пристрої за топологією “зірка”.

- Додати комутатор:

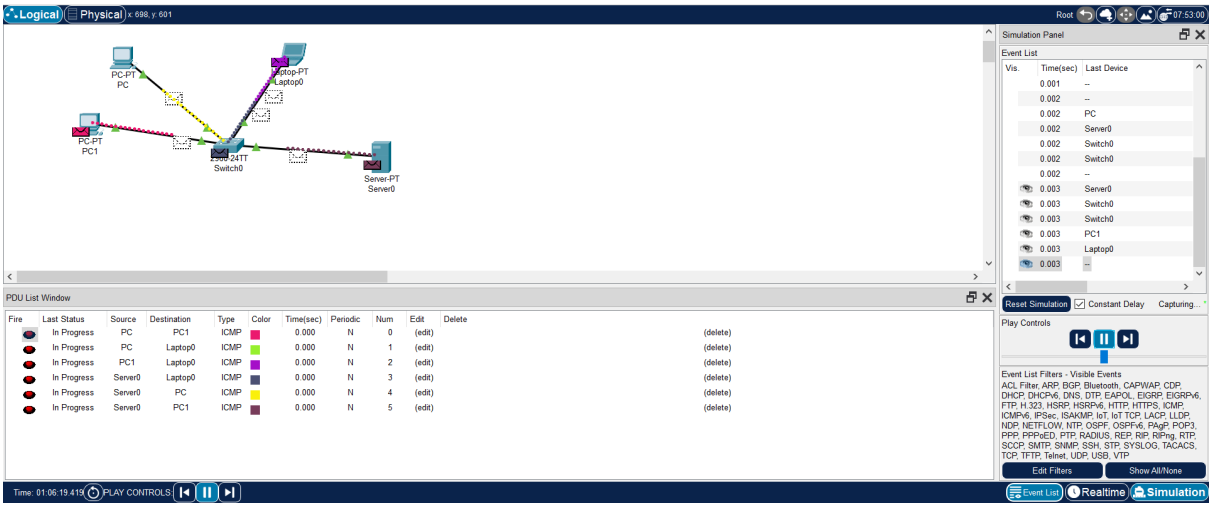


- з’єднати всі пристрої за топологією “зірка”:





5. Використовуючи ехо-пакети, перевірити доступність різних вузлів мережі.



Висновок: на даній лабораторній роботі я ознайомилась з графічним інтерфейсом Cisco Packet Tracer, навчилась моделювати комп'ютерну мережу, а також здійснювати її моніторинг.

Бібліографічний список

Основні джерела

1. Задерейко О. В., Багнюк Н. В., Толокнов А. А. Комп’ютерні мережі: навчально-методичний посібник. Одеса: Фенікс, 2023. 210 с.
2. Макогон С. В., Мінухін С. В. Комп’ютерні мережі. Харків: ХНУМГ ім. О. М. Бекетова, 2023. 99 с.
3. Лунтовський А., Мельник І. Проектування та дослідження комп’ютерних мереж. Львів: Університет «Україна», 2020. 362 с.
4. Отрох С. І., Аушева Н. М., Гусєва І. І., Кузьміних В. О. Комп’ютерні мережі. Комп’ютерний практикум: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020. 127 с.
5. Городецька О. С., Гикавий В. А., Онищук О. В. Комп’ютерні мережі: навчальний посібник. Вінниця: ВНТУ, 2018. 129 с.
6. Кравченко Ю. В., Труш О. В., Герасименко О. Ю., Лещенко О. О. Комп’ютерні мережі: навчальний посібник. Київ: КНУ ім. Т. Шевченка, 2021. 156 с.
7. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 2: навчальний посібник. Львів: Магнолія-2006, 2013. 328 с.
8. Dordal P. L. An Introduction to Computer Networks. Version 2.0.11. 2023. 684 p.
9. Introduction to Computer Networks – Second Edition. Open Textbook. 2022. 512 p.
10. Benabderrezak Y. Introduction to Computer Networks. 2023. 274 p.

Додаткові джерела

1. Tyagi P., Nishant R., Priyadarshi P. Understanding Computer Networks: A Comprehensive Overview of Types, Configurations, and the OSI Model. 2024. 152 p.
2. Velychko O., et al. New Information Technologies, Simulation and Automation. 2023. 228 p.
3. Gamal A., Kim Y. H. Lecture Notes on Network Information Theory. 2010. 648 p.

4. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 7th ed. 2017. 864 p.
5. Комп’ютерні мережі – частина 2. Київ: ЦП «Компринт», 2018. 682 с.
6. Introduction to Networks Companion Guide (CCNAv7). Cisco Networking Academy. 2021. 720 p.
7. An Introduction to Computer Networks. 2019. 680 p.
8. Методичні матеріали: «Комп’ютерні системи та мережі». Харків: НТУ «ХПІ», 2023. 95 с.
9. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. 6th ed. 2021. 848 p.
10. Кравченко Ю. В., та ін. Навчальні матеріали з комп’ютерних мереж. Київ: КНУ ім. Т. Шевченка, 2021. 140 с.

Електронне навчально-методичне видання

Анна Карпин, Дмитро Карпин, Олег Наум

КОМП'ЮТЕРНІ МЕРЕЖІ:
методичні рекомендації до виконання лабораторних робіт

**Дрогобицький державний педагогічний університет
імені Івана Франка**