ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет інформаційних технологій
Кафедра телекомунікацій, медійних та інтелектуальних технологій

КВАЛІФІКАЦІЙНИЙ ПРОЄКТ

Бакалавр
Освітній рівень

Телекомунікаційна мережа сучасного офісу
Назва теми

Галузь знань 17 «*Електроніка та телекомунікації*»
Шифр і назва спеціальності

Спеціальність 172 «*Телекомунікації та радіотехніка*»
Шифр і назва спеціальності

Освітня програма «Телекомунікації, медійні технології та інтелектуальні мережі»

Шифр КПТР. 210140.01.04 ПЗ

Виконав: здобувач 4 курсу, група ТР2-21-1 _____ Д.Ю. Кланцатий
Підпис Ініціали, прізвище

Керівник: д-р техн. наук, проф. 6.06.2025 Ю.М. БОЙКО
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. Кафедри телекомунікацій,
медійних та інтелектуальних
технологій _____ С.К. ПІДЧЕНКО
підпис Ініціали, прізвище

9 06 2025 р.

Хмельницький 2025

Хмельницький національний університет

Факультет *інформаційних технологій*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій*
Освітній рівень *бакалавр*
Галузь знань *17 Електроніка та телекомунікації*
Спеціальність *172 Телекомунікації та радіотехніка*
Освітня програма *«Телекомунікації, медійні технології та інтелектуальні мережі»*

ЗАТВЕРДЖУЮ
Завідувач кафедри ТМІТ
10.02.25р.
Підпис, дата

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНИЙ ПРОЄКТ

КЛАНЦАТОМУ Дмитру Юрійовичу

1 Тема проєкту: Телекомунікаційна мережа сучасного офісу
керівник проєкту БОЙКО Юлій Миколайович, д.т.н, професор.
Затверджено наказом по університету від «07» 02. 2025р. № 20
2 Строк подання здобувачем роботи на кафедру: 02.06.2025р.
3 Вихідні дані до проєкту
Розробити телекомунікаційну мережу за технологією розумного будинку.
В ході виконання кваліфікаційного проєкту потрібно:
- розглянути особливості побудови телекомунікаційної мережі сучасного офісу;
- виконати розподіл адресного простору мережі;
- виконати базове налаштування пристроїв у середовищі Cisco Packet Tracer;
- виконати налаштування статичних маршрутів і маршрутів за замовчуванням.

4 Зміст пояснювальної записки (перелік питань, що їх належить розробити):
1) Аналітичний огляд літературних джерел по темі кваліфікаційного проєкту 2) Вибір і техніко-економічне обгрунтування структури телекомунікаційної мережі сучасного офісу 3) Налаштування статичних марштурів і маршрутів за замовчуванням.
5 Перелік графічного матеріалу. 1) Телекомунікаційна мережа сучасного офісу. Схема логічної структуризації мережи; 2) Телекомунікаційна мережа сучасного офісу. Схема електрична структурна; 3) Налаштування інтерфейсів комутаторів і маршрутизаторів; 4) Налаштування статичних маршрутів і маршрутів за замовчуванням.

6 Консультанти розділів кваліфікаційного проєкту

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7 Дата видачі завдання 07.02.2025

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) кваліфікаційного проєкту	Термін виконання етапів проєкту	Примітка
1	Вступ. Аналітичний огляд літературних джерел по темі кваліфікаційного проекту	20.03.24	Вик.
2	Вибір і техніко-економічне обгрунтування структури телекомунікаційної мережі сучасного офісу	15.04.24	Вик.
3	Налаштування статичних маршрутів і маршрутів за замовчуванням	15.05.24	Вик.
4	Висновки. Підготовка презентаційних матеріалів за результатами виконання кваліфікаційного проєкту.	02.06.2025	Вик.

Здобувач _____ Д.Ю. Кланцатий
Підпис Ініціали, прізвище

Керівник проєкту _____ Ю.М. Бойко
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційного проєкту:

«Телекомунікаційна мережа сучасного офісу».

Автор роботи: Кланцатий Дмитро Юрійович

Керівник роботи: доктор техн., проф. Бойко Юлій Миколайович.

Пояснювальна записка: 87 сторінок, 50 рисунків, 6 таблиці, 32 джерел.

Графічна частина: 4 креслення, 24 презентаційних слайдів.

КЛЮЧОВІ СЛОВА: КОМУТАТОР, МАРШРУТИЗАТОР, ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, ТАБЛИЦЯ МАРШРУТИЗАЦІЯ, СТАТИЧНИЙ МАРШРУТ, МАРШРУТ ЗА ЗАМОВЧУВАННЯМ

Метою кваліфікаційного проєкту є розробка телекомунікаційної мережі сучасного офісу. Виконати базове налаштування пристроїв, налаштування статичних маршрутів і маршрутів за замовчуванням.

Зроблений аналітичний огляд літературних джерел по особливостям проектування телекомунікаційної мережі сучасного офісу. Найчастіше мережі будують на основі комутаторів і маршрутизаторів. Виконано розбиття адресного простору телекомунікаційної мережі. Визначено схему поділу на підмережі, враховуючи кількість комп'ютерів в кожній підмережі. При цьому IP-адреси назначені для кожного інтерфейсу локальної мережі кожного маршрутизатора. Для побудови мережі використані комутатори Cisco Catalyst 2960 і маршрутизатори 2911. Побудована телекомунікаційна мережа в середовищі в Cisco Packet Tracer і проведено базове налаштування пристроїв. Налаштовані інтерфейси комутаторів і маршрутизаторів. Налаштовані персональні комп'ютери та проведена перевірка підключень до мережі. Проведено налаштування статичних марштурів і маршрутів за замовчуванням. Проведена симуляція відправки пакетів між вузлами в різних підмережах. Підтверджена вірність введених налаштувань. Проведена діагностика мережі, яка показала високу пропускну здатність мережі і швидкість передачі.

Д.Ю. Кланцатий

Ініціали, прізвище здобувача

Підпис, дата

Поз.	Формат	Позначення	Найменування	Кіл.	Примітка
			Документація загальна		
1	А4	КПТР.210140.01.04 ПЗ	Пояснювальна записка	1	87 арк.
			Документація графічна		
2	А2	КПТР.210140.01.04 Е3	Телекомунікаційна мережа		
			сучасного офісу		
			Схема логічної структуризації мережи	1	
3	А2	КПТР.210140.01.04 Е1	Телекомунікаційна мережа		
			сучасного офісу		
			Схема електрична структурна	1	
4	А2	Плакат	Налаштування інтерфейсів	1	
			комутаторів і маршрутизаторів		
5	А2	Плакат	Налаштування статичних маршрутів		
			і маршрутів за замовчуванням	1	

				КПТР.210140.01.04 ВП	
Зм.	*Арк.*	*№ докум.*	*Підп.*	*Дата*	
Розроб.		Кланцатий Д. Ю.		Телекомунікаційна мережа сучасного офісу Відомість проекту	*Літ.* / *Аркуш* / *Аркушів*: 1 / 1
Перевір.		Бойко Ю. М.			
Н. контр.		Стецюк В.І.			ХНУ, гр. ТР2-21-1
Затв.		Підченко С.К.			

ЗМІСТ

ВСТУП

Сучасна офісна телекомунікаційна мережа — це комплексна система, яка забезпечує високошвидкісну, надійну і безпечну передачу даних, голосу та відео між пристроями всередині офісу та із зовнішнім світом (Інтернет, VPN, хмари тощо).

Основні характеристики такої мережі можна окреслити наступним чином: використовується топологія зірка або ієрархічна (core-distribution-access). Використовуються наступні мережеві пристрої: Комутатори (switches) — для з'єднання ПК, принтерів, IP-телефонів; маршрутизатори (routers) — для підключення до зовнішньої мережі; для забезпечення безпеки потрібне використання межових міжмережевих екранів (firewalls), ACL, VLAN, VPN; використовується бездротовий доступ: Access Points (APs) для мобільних пристроїв. Використовуються наступні протоколи: Ethernet, VLAN, STP, DHCP, DNS, NAT, RIP/OSPF, ACL, SSH, HTTPS, VPN. Надаються наступні послуги: IP-телефонія (VoIP); відеоконференції (Zoom, Webex); Обмін файлами, хмарні сервіси, принтери. Можуть бути використані наступні сервери: DHCP, DNS, Email, File, Web; вони можуть бути фізичні або віртуальні (локальні чи в хмарі). Якість обслуговування (QoS) — для пріоритезації трафіку (наприклад, для VoIP). Можуть бути забезпечені такі заходи безпека: сегментація через VLAN; використання VPN для віддаленого доступу, ACL для контролю трафіку, IDS/IPS використовується для захисту від атак.

Комп'ютерна мережа, побудована на комутаторах (switches) та маршрутизаторах (routers), є типовим рішенням для сучасних офісів, підприємств і організацій. Розглянемо її переваги та недоліки.

Переваги мережі на комутаторах і маршрутизаторах: висока продуктивність; Комутатори працюють на канальному рівні (2 рівень OSI) і забезпечують швидку передачу даних між пристроями з мінімальною затримкою;

підтримка full-duplex та gigabit/10G Ethernet дає змогу уникати колізій і зменшити затори.

Сегментація мережі (через VLAN) дає змогу логічно поділити мережу на ізольовані зони (наприклад, бухгалтерія, адміністрація), підвищуючи безпеку і керованість.

Масштабованість дозволяє легко додавати нові пристрої або розширювати мережу без збоїв у роботі.

Покращена безпека складається у наступному: маршрутизатори можуть фільтрувати трафік за допомогою ACL, NAT, VPN, Firewall; VLAN дозволяє обмежити трафік між різними підрозділами.

Можливість маршрутизації між підмережами здійснюється через router-on-a-stick або L3 switch, забезпечується зв'язок між VLAN або окремими мережами.

Централізоване адміністрування може бути реалізовано через наявність управлінських комутаторів, що дозволяє віддалено керувати мережею через SSH, SNMP, Telnet, Web GUI.

Недоліки мережі на комутаторах і маршрутизаторах наступні: вартість - керовані комутатори та маршрутизатори можуть бути дорогими, особливо L3-комутатори та пристрої з підтримкою QoS, PoE, VPN; складність налаштування - вимагає знань у сфері мереж (VLAN, ACL, маршрутизація, NAT, STP, QoS); помилки конфігурації можуть спричинити втрату зв’язку; центральні точки відмови - якщо вийде з ладу центральний комутатор або маршрутизатор — велика частина мережі може стати недоступною; відбувається обмеження за кількістю портів - звичайні комутатори мають 24 або 48 портів — при перевищенні доведеться використовувати стекування або каскадування; складність в усуненні несправностей.

Велика мережа з VLAN та маршрутизацією вимагає систем моніторингу (наприклад, NetFlow, Wireshark), інакше діагностика проблем стає складною.

Поділ комп’ютерної мережі на відділи за допомогою VLAN (Virtual Local Area Network) — це ефективний спосіб організації, безпеки та масштабованості сучасної мережі.

Переваги поділу мережі на відділи за допомогою VLAN: підвищення безпеки - кожен відділ (наприклад, бухгалтерія, HR, технічний відділ) розміщується в окремій VLAN; пристрої з різних VLAN не можуть напряму обмінюватися даними без маршрутизатора або правил ACL, що унеможливлює несанкціонований доступ.

Відбувається зменшення широкомовного трафіку (broadcast) - broadcast-пакети обмежуються межами VLAN, що зменшує навантаження на мережу.

Логічна організація мережі - VLAN дозволяє групувати пристрої за функціональністю, а не фізичним розташуванням? що зручно при гнучкому офісному плануванні або для віддалених працівників.

Відбувається централізоване управління - просте керування доступом до ресурсів між VLAN через ACL, маршрутизацію або Firewall.

Забезпечується краща масштабованість - додати новий відділ — просто створити нову VLAN, не змінюючи фізичну структуру мережі.

Для підтримка якості обслуговування (QoS) необхідно для окремих VLAN пріоритезувати трафік — наприклад, для VoIP або відеоконференцій.

Економія коштів при використанні VLAN дозволяє уникати потреби в окремих фізичних мережах для кожного відділу, що економить на обладнанні.

Таким чином, побудова розробка телекомунікаційної мережі сучасного офісу є актуальним завданням.

Метою кваліфікаційного проєкту є розробка телекомунікаційної мережі сучасного офісу. Для досягнення мети було поставлено такі завдання:

- розглянути особливості побудови телекомунікаційної мережі сучасного офісу;

- виконати розподіл адресного простору мережі;

- виконати базове налаштування пристроїв у середовищі Cisco Packet Tracer;

- виконати налаштування статичних маршрутів і маршрутів за замовчуванням.

1 АНАЛІТИЧНИЙ ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ ПО ТЕМІ КВАЛІФІКАЦІЙНОГО ПРОЄКТУ

1.1 Сучасні комп'ютерні мережі і мережеві технології

Технології, які забезпечили розвиток комп'ютерних мереж:

− програмно-конфігуровані мережі (SDN);

− хмарні сервіси (CCS);

− інтернет речей (IoT);

− віртуалізація мережевих функцій (NFV);

− якість взаємодії компонентів мережі (QoE).

У загальному вигляді мережева екосистема – це з'єднання між користувачами, підприємствами та речами, які використовують цифрову платформу. Сучасна мережева екосистема у загальному вигляді наведена на рисунку 1.1.

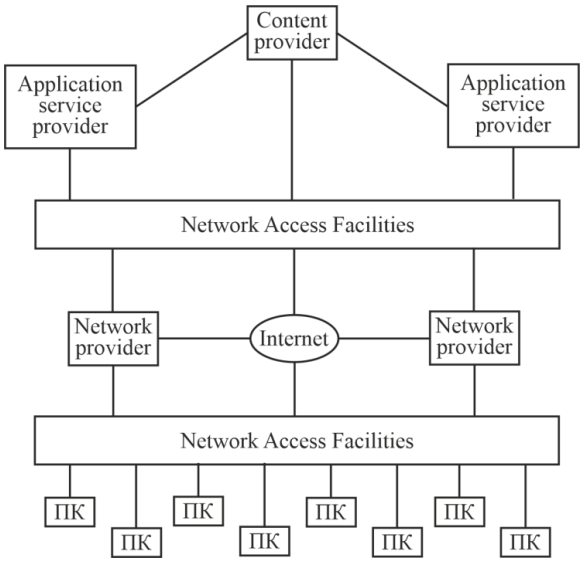


Рисунок 1.1 – Сучасна мережева екосистема

Одним з напрямків розвитку цифрових технологій стають мережеві (цифрові) екосистеми (СЕС). Головний елемент будь-якої цифрової екосистеми – технологія єдиного входу (Single Sign-On), тобто робота під єдиним обліковим записом для багатьох цифрових сервісів.

Вся екосистема існує для надання послуг кінцевим користувачам.

Платформа користувача (Network Access Facilities, NAF) може бути стаціонарною, портативною (ноутбук) або мобільною (планшет, смартфон).

Розглянемо сервісні служби, необхідні користувачам мереж (рис.1.1).

Постачальники програм (Application Providers, AP), які надають програми, що працюють на платформі користувача. Концепція магазину додатків стає доступнішою для стаціонарних та мобільних платформ.

Окремою категорією провайдерів є провайдер прикладних послуг (Application Service Provider, ASP). Він діє як сервер, прикладне програмне забезпечення якого працює на платформах провайдера. Це веб-сервери, електронна пошта, сервери баз даних та інше.

Постачальник контенту (content provider) надає дані, які використовуватимуться користувачем (електронна пошта, музика, відео).

Мережна структура підприємства складається з наступних компонентів:

− канали зв'язку;

− локальні та глобальні мережі;

− підключення до Інтернету, доступні підприємству.

Інфраструктура корпоративної мережі все частіше включає приватні/загальнодоступні хмарні підключення до центрів обробки даних (ЦОД), де розміщуються сховища великих обсягів даних та веб-сервіси.

Ключовим аспектом конвергенції на цьому рівні є можливість передачі голосу, зображення та відео мережами, які спочатку були розроблені для передачі трафіку даних. Конвергенція інфраструктури також відбулася щодо мереж, розроблених для голосового трафіку.

виділяють два основні елементи сучасних мереж:

− мережа центрів обробки даних: як центри обробки даних великих підприємств, так і центри обробки даних хмарних провайдерів складаються з дуже великої кількості взаємозалежних серверів;

− IoT (Internet of Things – інтернет речей), або хмарна мережа: інтернет речей, розгорнутий на підприємстві, може складатися із сотень, тисяч і навіть мільйонів сучасних пристроїв.

На рисунку 1.2 показано деякі типові елементи зв'язку та мережі, що використовуються в контексті архітектури, яка може представляти корпоративну мережу національного або глобального масштабу або частину Інтернету з деякими з її мережами.

Рисунок 1.2 – Елементи зв'язку та мережі, що використовуються у телекомунікаційній мережі

У центрі малюнка знаходиться магістраль IP, або ядро, – мережа, яка може бути частиною Інтернету або корпоративною IP-мережею. Зазвичай магістраль складається з високопродуктивних маршрутизаторів, які називають базовими маршрутизаторами, з'єднаних між собою оптичними каналами з високою пропускною здатністю.

В оптичних каналах часто використовується так зване мультиплексування з поділом по довжині хвилі (WDM), так що кожен канал має кілька логічних каналів, що займають різні частини смуги пропускання в оптичному діапазоні.

На периферії магістралі IP знаходяться маршрутизатори, що забезпечують підключення до зовнішніх мереж та користувачів. Ці маршрутизатори іноді називають граничними маршрутизаторами.

Граничні маршрутизатори також використовуються в корпоративній мережі для підключення кількох маршрутизаторів та комутаторів до зовнішніх ресурсів, таких як магістраль IP або високошвидкісна глобальна мережа. Аналіз показує, що вимоги до маршрутизаторів агрегації зараз у діапазоні від 200 до 400 Гбіт/с на оптичний канал і від 400 Гбіт/с до 1 Тбіт/с на оптичний канал – для базових маршрутизаторів.

Верхня частина рисунку 1.2 є частиною того, що може бути великою корпоративною мережею. Вона може мати декілька ділянок мережі, які підключені через приватну високошвидкісну глобальну мережу з комутаторами, з'єднаними оптичними лініями.

Багатопротокольна комутація за мітками (MPLS) з використанням IP є поширеним протоколом комутації для глобальних мереж. Корпоративні активи підключаються до магістральної IP-мережі або Інтернету та захищаються від них через маршрутизатори з міжмережевим екраном. Підключення до Інтернету через маршрутизатор може здійснюватися через DSL, кабельне з'єднання або виділений високошвидкісний канал.

Підприємства проектують мережеві об'єкти у вигляді трирівневої ієрархії:

− мережа доступу (Access Network);

− розподільча мережа (Distribution Network);

− базова мережа (Core Network).

Найближче до кінцевого користувача знаходиться мережа доступу (Access Network). Як правило, мережа доступу є локальною мережею (LAN), що складається з комутаторів Ethernet, IP-маршрутизаторів, що забезпечують зв'язок між комутаторами. Мережа доступу підтримує обладнання кінцевих користувачів, такі як настільні та портативні комп'ютери та мобільні пристрої. Мережа доступу також підтримує локальні сервери.

Один або кілька маршрутизаторів доступу з'єднують мережі доступу з наступним вищим рівнем ієрархії – розподільчою мережею (Distribution Network). Маршрутизатори доступу функціонують як граничні маршрутизатори, які перенаправляють трафік в мережу доступу і з неї. Для локальної мережи можуть використовуватись додаткові маршрутизатори доступу, для забезпечення внутрішньої маршрутизацію.

Розподільча мережа з'єднує мережі доступу між собою та базовою мережею. Граничний маршрутизатор у розподільчій мережі підключається до граничного маршрутизатора у мережі доступу для підключення користувачів.

Два маршрутизатори налаштовані для розпізнавання один одного і зазвичай обмінюються інформацією про маршрутизацію та підключення, а також деякою інформацією, пов'язаною з трафіком. Ця взаємодія між маршрутизаторами називається пірінгом.

Розподільча мережа також служить для агрегування трафіку, призначеного для основного маршрутизатора, який захищає ядро від пірингу з високою густиною. Це означає, що використання розподільчої мережі обмежує кількість маршрутизаторів, які встановлюють однорангові відносини з граничними маршрутизаторами в ядрі, заощаджуючи пам'ять, обробку та пропускну здатність. Мережа розповсюдження може безпосередньо з'єднувати сервери, які використовуються в мережах з множинним доступом: сервери баз даних і сервери управління мережею.

Базова мережа (Core Network), яка також називається магістральною мережею (Backbone Network), з'єднує географічно рознесені розподільчі мережі, а також забезпечує доступ до інших мереж у глобальному просторі.

Як правило, базова мережа використовує високопродуктивні маршрутизатори, лінії передачі з великою пропускною здатністю для збільшення пропускної спроможності. Базова мережа може також підключатися до високопродуктивних серверів з великою ємністю, таких як великі сервери баз даних та об'єкти приватної хмари.

Ієрархічна мережева архітектура – приклад гарної модульної конструкції. Завдяки такій конструкції ємність, характеристики та функціональність мережевого обладнання (маршрутизаторів, комутаторів, серверів управління мережею) можуть бути оптимізовані відповідно до їх положення в ієрархії та вимог на даному ієрархічному рівні.

1.2 Ethernet, Wi-Fi та стільникові мережі 4G/5G

Технології Ethernet, Wi-Fi, стільникові мережі 4G/5G, в сучасному суспільстві еволюціонують для забезпечення високих швидкостей передачі даних, що підтримують багато мультимедійних додатків для підприємств і споживачів.

Ethernet використовується в домашніх умовах для створення локальної мережі комп'ютерів з доступом до Інтернету через широкосмуговий модем/маршрутизатор. Зі збільшенням доступності високошвидкісного та недорогого Wi-Fi на комп'ютерах, планшетах, смартфонах, модемах/маршрутизаторах та інших пристроях залежність таких мереж від Ethernet знизилася. На рисунку 1.3 подано спрощений приклад архітектури корпоративної локальної мережі.

Рисунок 1.3 – Приклад архітектури корпоративної локальної мережі

LAN підключається до Інтернету/WAN через брандмауер. Ієрархічне розташування маршрутизаторів і комутаторів забезпечує взаємозв'язок серверів, користувацьких та бездротових пристроїв. Зазвичай, бездротові пристрої підключаються тільки на краю або внизу ієрархічної архітектури; решта інфраструктури організації – це мережа Ethernet. Також може використовуватися сервер IP-телефонії, що забезпечує функції керування викликами (комутація голосу) для телефонних операцій у корпоративній мережі з можливістю підключення до телефонної мережі загального користування (Public Switched Telephone Network, PTSN).

Підприємство може легко реалізувати мережу Ethernet між кількома будинками, що знаходяться на певній відстані один від одного, використовуючи канали від 10 Мбіт/с до 100 Гбіт/с, різні типи кабелів та обладнання Ethernet. Оскільки все обладнання та комунікаційне програмне забезпечення відповідають одному стандарту, можна легко комбінувати обладнання від різних постачальників.

Останнім часом почали говорити про особливості застосування Ethernet у різних галузях, у зв'язку з чим виділяють стандартний та промисловий Ethernet.

Стандартний Ethernet більше підходить для офісних застосувань, ніж для використання у промисловості. Він призначений для повсякденного використання, у той час як промисловий Ethernet передбачає різні рівні і може застосовуватися у складніших умовах експлуатації (у тому числі у зашумлених виробничих приміщеннях).

Як і в інших областях, Ethernet став домінувати в центрах обробки даних, ЦОД (Data Center, DC), де потрібна дуже висока швидкість передачі даних для обробки величезних обсягів даних між мережними серверами та пристроями зберігання.

Історично склалося так, що ЦОД використовували різні технології передачі великих обсягів даних на короткі відстані, включаючи Infini Band і Fibre Channel. Але тепер, коли Ethernet може масштабуватися до 100 Гбіт/с, а перспективі – до

400 Гбіт/с, аргументи на користь єдиного протоколу для підприємства стають більш вагомими.

Використовується термін міської Ethernet або Ethernet міської мережі (MAN). Тут перевага Ethernet полягає в тому, що він легко вбудовується в корпоративну мережу, яка забезпечує глобальний доступ.

Операторський Ethernet (Carrier Ethernet, CE – розширений Ethernet для постачальників послуг зв'язку) – одна з найшвидше зростаючих технологій Ethernet, якою судилося стати домінуючим засобом, за допомогою якого підприємства отримують доступ до великих мереж та засобів Інтернету.

Але більш важливою перевагою є те, що операторський Ethernet забезпечує набагато більшу гнучкість з точки зору швидкості передачі даних.

Слід зазначити дві інші особливості нового підходу до Ethernet. По-перше, для розташованих рядом серверів та пристроїв зберігання необхідну мережеву інфраструктуру забезпечують високошвидкісні оптоволоконні канали та комутатори Ethernet.

Друга особливість пов'язана з використанням так званої об'єднувальної плати Ethernet (Backplane Ethernet) – друкованої плати, яка забезпечує паралельне з'єднання кількох контактів один з одним, формуючи комп'ютерну шину.

Об'єднувальна плата Ethernet забезпечує швидкість до 100 Гбіт/с на дуже коротких відстанях. Ця технологія ідеально підходить для блейд-серверів (Blade Server), що є модульною електронною платою, що містить один, два або більше мікропроцесорів і пам'ять, яка призначена для одного спеціального додатка і може бути легко вставлена в блейд-шасі.

1.3 Еволюція Wi-Fi

Подібно до того, як Ethernet став домінуючою технологією для провідних локальних мереж, Wi-Fi домінує в бездротових мережах.

Wi-Fi –технологія бездротового доступу до Інтернету, яка використовується у будинках, офісах, громадських місцях.

Wi-Fi у будинку тепер з'єднує комп'ютери, планшети, смартфони та багато електронних пристроїв, таких як відеокамери, телевізори та термостати. Wi-Fi на підприємстві став важливим засобом підвищення продуктивності праці та ефективності мережі.

А громадські точки доступу Wi-Fi значно розширилися, щоб забезпечити безкоштовний доступ до Інтернету.

Сьогодні важливість Wi-Fi у будинку значно зросла. Wi-Fi залишається стандартною схемою для з'єднання домашньої комп'ютерної мережі. Перше важливе застосування Wi-Fi у домашніх умовах пов'язане з можливістю прибрати кабелі Ethernet для з'єднання комп'ютерів один з одним та з Інтернетом. Типова структура домашньої мережі зазвичай є настільним комп'ютером з підключеним маршрутизатором/модемом, який забезпечує інтерфейс з Інтернетом. Інші настільні та портативні комп'ютери підключаються до центрального маршрутизатора через Ethernet або Wi-Fi.

Основна якість бездротових з'єднань полягає в тому, що вони значно спростили підключення. Немає потреби у фізичному використанні кабелю. Wi-Fi значно спростило підключення.

Дедалі все більше об'єктів надають точку доступу Wi-Fi: кафе, рестора-ни, громадський транспорт, вокзали, аеропорти, бібліотеки, готелі тощо.

Завдяки гігабітним швидкостям передачі даних, доступним в офісній локальній мережі, необхідний гігабітний Wi-Fi, щоб мобільні користувачі могли ефективно використовувати офісні ресурси. Стандарт IEEE 802.11ac спрямований на вирішення даної задачі. У міру вдосконалення антенного обладнання, методів бездротової передачі комітет IEEE 802.11 зміг ввести стандарти для нових версій Wi-Fi на більш високих швидкостях.

Стандарт 802.11ac використовує передові технології в конструкції антен та обробці сигналів для досягнення високої швидкості передачі даних при меншій витраті енергії батареї.

Стандарт IEEE 802.11ax відрізняється збільшеною швидкістю передачі даних – до 9,6 Гбіт/с. Крім того, новий стандарт передбачає досконалішу систему шифрування WPA3 (Wi-Fi Protected Access III). Технологія працює в діапазонах частот 2,4 та 5 ГГц, що забезпечує більшу пропускну здатність.

Wi-Fi 6 додає режим OFDMA (Orthogonal Frequency Division Multiple Access – множинний доступ з ортогональним частотним поділом каналів) для покращення спектральної ефективності. Технологія OFDMA була запозичена із стільникової індустрії 4G LTE і схожа на розраховану на багато користувачів версію OFDM, яка застосовується в мережі Wi-Fi 5.

OFDMA забезпечує можливість встановлення з'єднань між точкою доступу і кількома клієнтами одночасно за рахунок розподілу сигналу на підносійні і поділу їх на групи для обробки окремих потоків даних, званих ресурсними одиницями (Resource Units, RU). Вона дозволить одночасно транслювати дані одразу кільком клієнтам Wi-Fi 6 з усередненою швидкістю і використовувати один і той же канал без очікування.

Wi-Fi 6 забезпечує для технології MU-MIMO (Multi-User Multiple-Input, Multiple-Output – багатокористувацький багатоканальний вхід/вихід) підтримку висхідного напрямку (UL MU-MIMO).

1.4 Технології 4G/5G

Мережі 4G підтримують мобільний доступ до Інтернету та програми з високою пропускною здатністю, такі як мобільне телебачення високої чіткості, мобільні відеоконференції та ігрові сервіси.

Найбільш значущі характеристики систем 4G наступні:

− функціонують на базі мережі з комутацією пакетів, засновані на IP;

− підтримубть швидкості передачі даних до 100 Мбіт/с для мобільного доступу та приблизно до 1 Гбіт/с – для локального бездротового доступу;

− надають можливість динамічного поділу та використання мережевих ресурсів для підтримки великої кількості одночасних користувачів;

− забезпечують підтримку високої якості обслуговування для мультимедійних програм наступного покоління.

Технологія телекомунікацій 5G – це технологічний стандарт п'ятого покоління для широкосмугових стільникових мереж, який стільникові компанії почали розгортати в усьому світі у 2019 р.

Основна перевага мереж 5G полягає в тому, що вони матимуть більшу пропускну здатність – до 10 Гбіт/с.

Основні послуги в мережах 5G:

− надширокосмуговий мобільний зв'язок (Extreme Mobile Broadband, eMBB) – реалізація ультраширокосмугового зв'язку;

− масовий міжмашинний зв'язок (Massive Machine-Type Communications, mMTC) – підтримка інтернету речей;

− наднадійний міжмашинний зв'язок із низькими затримками (Ultra-Reliable Low Latency Communication, URLLC) – забезпечення особливого класу послуг із дуже низькими затримками.

Основні вимоги до мереж 5G:

− пропускна спроможність мережі до 20 Гбіт/с по лінії «вниз» (тобто до абонента); та до 10 Гбіт/с у зворотному напрямку;

− підтримка одночасного підключення до 1 млн пристроїв на 1 км^2;

− скорочення часової затримки на радіоінтерфейсі до 0,5 мс – для сервісів наднадійного міжмашинного зв'язку URLLC та до 4 мс – для сервісів надширокосмугового мобільного зв'язку eMBB.

Очікується, що через збільшення пропускної спроможності нові мережі будуть не тільки обслуговувати мобільні телефони, але й самі будуть використовуватися як спільні інтернет-провайдери для ноутбуків і настільних комп'ютерів, конкуруючи з існуючими інтернет-провайдерами, а також будуть використовуваим нові програми в Інтернеті речей.

Підвищена швидкість досягається за рахунок використання міліметрових радіохвиль. Для забезпечення широкого спектру послуг мережі 5G будуть працювати у трьох діапазонах частот: низькому, середньому та високому. Мережа 5G складатиметься з мереж, що містять до 3 різних типів комірок, які потребує різних антен, причому кожен тип дає різний компроміс між швидкістю завантаження, відстанню та зоною обслуговування.

Вузькосмуговий 5G використовує той же частотний діапазон, що і стільникові мережі 4G, 600-700 МГц, що дає швидкість завантаження 30-250 Мбіт/с. Середньочастотний 5G використовує мікрохвилі 2,5-3,7 ГГц, що забезпечує швидкість 100-900 Мбіт/с. При цьому кожна вежа стільникового зв'язку забезпечує обслуговування в радіусі до кількох кілометрів.

У високочастотному діапазоні 5G в даний час використовуються частоти 25-39 ГГц, близькі до нижньої межі діапазону міліметрових хвиль, хоча в майбутньому можуть використовуватися вищі частоти. При підвищенні частоти, на якій передається інформація, зменшується дальність зв'язку – збільшити яку можна лише підвищуючи потужність передавача, обмежену санітарними нормами. Однак вважається, що базові станції мереж п'ятого покоління будуть розташовуватися щільніше, ніж зараз, що викликано необхідністю створити набагато більшу ємність мережі.

Є ще одна особливість. Швидкість завантаження гігабіта за секунду можна порівняти з кабельним Інтернетом. Однак міліметрові хвилі мають більш обмежений діапазон, що вимагає багато маленьких комірок. Тут є проблеми з проходженням деяких типів стін та вікон. Через їх більш високу вартість поточні плани полягають у розгортанні цих комірок лише у щільному міському середовищі та в місцях скупчення людей, таких як спортивні стадіони та конференц-центри.

1.5. Мережеві технології та хмарні обчислення

Загальні концепції хмарних обчислень (ОВ) сягають 1950-х років. Проте реальні послуги ОВ вперше стали доступні на початку 2000-х років. Evernote, хмарний сервіс для створення нотаток та архівування, запущений у 2008 р., охопив 100 млн користувачів менш ніж за 6 років. Хмара від Apple iCloud було запущено у 2012 р. Наприкінці 2014 р. Google оголосив, що хмарний сервіс Google Drive має майже чверть мільярда користувачів.

Хмарна мережа (Cloud-Based Network, CBN) – це корпоративна мережа, яку можна розширити до хмари, показаної на рисунку 1.4. Хмара значно полегшує розробку мережевої системи підприємства. У хмарі базова мережа створюється постачальником хмарних послуг. Все, що потрібно зробити підприємству – це підключити свою локальну мережу до мережі, побудованої у хмарі, щоб сформувати глобальну мережеву систему.

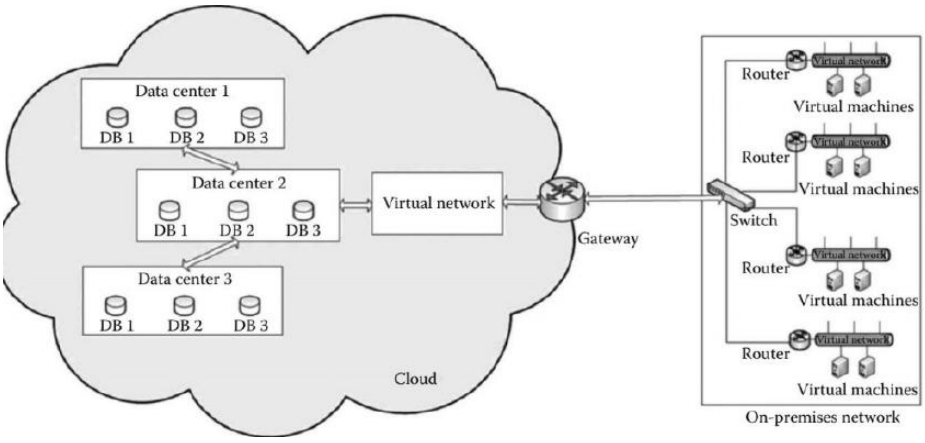


Рисунок 1.4 – Мережа, що базується на хмарній технології

Хмарна мережа має на меті організацію взаємодії з багатьма сайтами по всьому світу.

На кількох об'єктах, таких як філії, школи, клініки, виробничі підприємства або магазини роздрібної торгівлі можуть працювати від кількох сотень до десятків тисяч співробітників. За допомогою інструментів управління, розгорнутих у хмарі, мережні адміністратори можуть керувати розподіленими

корпоративними мережами у будь-якому місці та у будь-який час. Інструменти керування можна використовувати для керування віртуальними машинами та мобільними службами, розміщеними у хмарі. Вони застосовуються для виконання таких завдань, як централізоване керування, віддалений моніторинг, віддалена установка програмного забезпечення та програм, віддалене очищення та аудит безпеки.

Хмарні обчислення є найбільш гнучкими у своїй пропозиції і можуть використовуватися для різних цілей; це залежить від програми, до якої користувач хоче отримати доступ.

Хмарні програми часто позбавляють необхідності встановлювати та запускати програму на власному комп'ютері клієнта, тим самим полегшуючи завдання обслуговування програмного забезпечення.

Національний інститут стандартів та технологій США (NIST) визначає основні характеристики хмарних обчислень таким чином:

− широкий мережевий доступ (Broad Network Access): можливості доступні через мережу та через стандартні механізми, що використовуються різнорідними платформами «тонких» або «товстих» клієнтів (наприклад, мобільні телефони, ноутбуки та персональні цифрові помічники) та інші традиційні або хмарні програмні послуги;

− швидка (миттєва) еластичність (Rapid Elasticity): хмарні обчислення дозволяють розширювати та скорочувати ресурси відповідно до конкретних вимог до послуг; наприклад, якщо потрібно багато ресурсів сервера на час виконання певної задачі, можна звільнити ці ресурси після її завершення;

− вимірність сервісу (Measured Service): хмарні системи автоматично контролюють та оптимізують використання ресурсів, реалізуючи можливість вимірювання або оцінки на певному рівні абстракції, що відповідає типу сервісу (наприклад, зберігання, обробка, пропускна спроможність та активні облікові записи користувачів); використання ресурсів можна відстежувати, контролювати та складати звіти, забезпечуючи прозорість як для постачальника, так і для споживача послуги, що використовується;

− самообслуговування на запит (On-Demand Self-Service): споживач може в односторонньому порядку автоматично надавати обчислювальні можливості, такі як час сервера та мережеве сховище, без необхідності взаємодії людини з кожним постачальником послуг; оскільки послуга надається на запит, ресурси не є постійними частинами IT-інфраструктури;

− об'єднання ресурсів (Resource Pooling): обчислювальні ресурси провайдера об'єднуються для обслуговування кількох споживачів з використанням розрахованої на багато користувачів моделі; при цьому різні фізичні та віртуальні ресурси динамічно призначаються та перепризначаються відповідно до споживчого попиту.

Інтернет речей (Internet of Things, IoT) – одне з останніх досягнень революції у сфері обчислень та комунікацій.

Повсюдне поширення IoT та його вплив на повсякденне життя людей, бізнес та діяльність урядових структур багатьох країн перевершують попередні досягнення у галузі інформаційних технологій.

Інтернет речей - це термін, який відноситься до розширеної взаємодії інтелектуальних пристроїв від побутової техніки до крихітних датчиків.

Інтернет тепер підтримує поєднання мільярдів промислових та особистих об'єктів, зазвичай через хмарні системи. Об'єкти надають сенсорну інформацію, впливають на навколишнє середовище і в деяких випадках змінюють себе, щоб створити загальне управління більшою системою, такою як фабрика або місто, забезпечуючи необхідний рівень захисту даних. Вбудовані пристрої, такі, як камери відеоспостереження вимагають забезпечення потокової передачі з високою пропускною здатністю.

Інтернет речей зазвичай поділяють на групи з галузей: у медицині, телекомунікаціях, ЖКГ, армії, електроенергетиці, будівництві, логістиці, сільському господарстві (IoTAg) тощо.

Промисловий інтернет речей (Industrial Internet of Things) – багаторівнева система, що включає датчики і контролери, встановлені на вузлах і агрегатах

промислового об'єкта, засоби передачі даних і їх візуалізації, потужні аналітичні інструменти інтерпретації одержуваної інформації та багато інших компонентів.

Обсяги накопичуваних даних продовжують зростати, оскільки їх все більше збирають віддалені датчики, мобільні пристрої, камери, мікрофони, зчитувачі радіочастотної ідентифікації (Radio Frequency Identification, RFID).

"Великі дані" - це дані, які не поміщаються в оперативну пам'ять комп'ютера. Це означає, що властивість великих для певного обсягу даних залежить, перш за все, від структури та характеристики системи, що застосовується для обробки цих даних.

Технології Big Data корисні при вирішенні наступних завдань:

− прогнозування ринкової ситуації;

− маркетинг та оптимізація продажів;

− удосконалення продукції;

− прийняття управлінських рішень;

− підвищення продуктивності праці;

− ефективна логістика;

− моніторинг стану основних фондів та середовища;

− криптовалютні операції та ін.

Для роботи з Великими даними використовуються складні системи, в яких можна виділити кілька компонентів або шарів (Layers). Зазвичай виділяють чотири рівні компонентів таких систем:

− прийом даних (Data Ingestion);

− збір даних (Data Staging);

− аналіз даних (Data Analysis; Analysis Layer);

− подання результатів (Consumption Layer).

Цей поділ є значною мірою умовним оскільки, з одного боку, кожен компонент, своєю чергою, може бути розділений на підкомпоненти, з другого – деякі функції компонентів можуть перерозподілятися залежно від розв'язуваного завдання й програмного забезпечення.

Прийом даних від джерел полягає у їхній початковій підготовці з метою приведення цих даних до загального формату подання. Цей єдиний формат вибирається відповідно до прийнятої моделі даних. Виконуються перетворення систем виміру, типів (типізація), верифікація. Обробка даних змістовно не зачіпає наявну в даних інформацію, але може змінювати її подання (наприклад, наводити координати до єдиної системи координат, а значення – до єдиної розмірності).

Етап збору даних характеризується безпосереднім взаємодією із системами їх зберігання. Встановлюється точка збору, в якій зібрані дані забезпечуються локальними метаданими і поміщаються в сховище або передаються подальшої обробки.

Аналіз даних, на відміну від збору, використовує інформацію, що міститься у даних. Аналіз може проводитися як реальному часі, і у пакетному режимі. Аналіз даних - основне трудомістке завдання для роботи з Великими даними.

Системи обробки Великих даних є фреймворками (каркасами), для використання яких необхідно з'єднувати їх з іншими фреймворками, прикладним програмним забезпеченням та системою зберігання даних.

Ключові елементи мережі Великі даних підприємства включають:

− сховище даних (Data Warehouse, DW): містить інтегровані дані з кількох джерел даних, які використовуються для звітності та аналізу;

− сервери управління даними (Data Management Servers, DMS): великі групи серверів виконують кілька функцій щодо великих даних: на серверах працюють програми для аналізу даних: інструменти інтеграції даних, інструменти аналітики;

− робочі станції/системи обробки даних (Workstations/Data Processing Systems, DPS) – системи, що беруть участь у використанні додатків для Великих даних та у створенні вхідних даних для сховищ Великих даних;

− сервер управління мережею (Network Management Server, NMS): один або кілька серверів, які відповідають за керування та моніторинг мережі.

Корпоративна мережа може містити декілька сайтів, розподілених на регіональному, національному або глобальному рівнях. Вплив великих даних на мережну інфраструктуру визначається наступними параметрами:

− обсяг (Volume, зростаючий обсяг даних);

− швидкість (Velocity, збільшення швидкості запису та читання даних);

− мінливість (Variability, зростаючі обсяги даних).

Устаткування для обробки даних розміщується в центрі обробки даних ЦОД або в дата-центрах ДЦ (Data Center, DC). Крім локальної обчислювальної мережі (ЛВС), основними компонентами ЦОД є система управління, обчислювальні ресурси, система зберігання даних.

Основна вимога до локальної мережі – низькі затримки.

При великій кількості вузлів використовуються мережеві комутатори, що починають передачу пакета даних відразу після обробки заголовка пакета даних. Традиційні технології зберігання та управління даними включають:

− системи управління реляційними базами даних (Relational Database Management Systems, RDBMS);

− мережевий накопичувач (Network-Attached Storage, NAS);

− мережу зберігання даних (Storage-Area Networks, SAN);

− сховища даних (Data Warehouses, DW);

− систему бізнес-аналітики (Business Intelligence, BI).

Висновки до першого розділу

1. Мережева екосистема – це веб-з'єднання між користувачами, підприємствами та речами, які спільно використовують цифрову платформу.

2. Інфраструктура корпоративної мережі включає приватні або загальнодоступні хмарні підключення до центрів обробки даних, в яких розміщуються сховища великих обсягів даних та веб-сервіси.

3. Підприємства проектують свої мережеві об'єкти як трирівневі ієрархії: мережа доступу ; мережа розподілу, чи розподільна мережа; базова мережа.

4. Wi-Fi – це технологія бездротового доступу до Інтернету, яка використовується в будинках, офісах та громадських місцях.

5. Мережі 4G підтримують мобільний доступ до Інтернету та програми з високою пропускною здатністю, такі як мобільне телебачення високої чіткості, мобільні відеоконференції та ігрові сервіси. Основна перевага мереж 5G полягає в тому, що вони матимуть більшу пропускну здатність, забезпечуючи більш високу швидкість завантаження, зрештою до 10 Гбіт/с.

6. IoT-системи працюють у режимі реального часу та зазвичай складаються з мережі smart-пристроїв та хмарної платформи, до якої вони підключені за допомогою Wi-Fi, Bluetooth або інших видів зв'язку.

7. Цифрові трансформації зазвичай визначаються терміном програмно-визначена мережа або програмно-конфігурована мережа (Software-Defined Networking, SDN) і є однією з форм віртуалізації мережевих функцій.

2 ВИБІР І ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ СТРУКТУРИ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ СУЧАСНОГО ОФІСУ

2.1 Розробка і аналіз структурної схеми телекомунікаційної мережі

Для побудови телекомунікаційної мережі задана деяка організація, що має 4 приміщення. Необхідно реалізувати можливість зв'язуватися з будь-яким із цих приміщень, але приміщення (відділи) мають бути ізольованими. Таким чином, для кожного приміщення має бути реалізована окрема підмережа. Нехай адміністратором надана адреса організації 10.160.0.0. Задані мінімально необхідні кількості вузлів у кожній з підмереж приведені у таблиці 2.1.

Таблиця 2.1 – Мінімально необхідні кількості вузлів підмереж

Префікс	LAN1	LAN2	LAN3	LAN4	Загалом
/20	20	24	200	150	392

Структурна схема телекомунікаційної мережі приведена на рисунку 2.1.

Префікс мережі /20 вказує, яка кількість біт IP-адреси зарезервована для мережевої частини. Загалом, IP-адреса містить 32 біти (IPv4), які поділюються на мережеву частина та хостову частину. Тобто, 20 біт використовується для адресації мережі, а 12 біт – для хостів. Мінімальна кількість адрес: $2^{12} = 4096$, серед яких перша адреса – це мережева адреса (всі нулі в хостовій частині); остання адреса – це широкомовна адреса (всі одиниці в хостовій частині).

Якщо є мережа 10.160.0.0/20, то:

Діапазон адрес: 10.160.0.0 – 10.160.19.255

Мережева адреса: 10.160.0.0

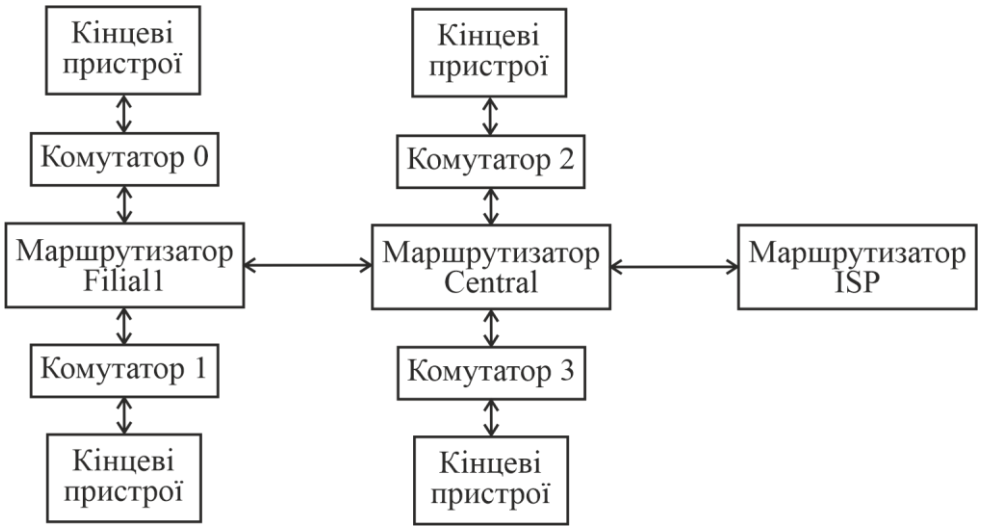


Рисунок 2.1 – Структурна схема телекомунікаційної мережі

Широкомовна адреса: 10.160.19.255

Доступні хост-адреси: 10.160.0.1 – 10.160.19.254

У двійковому вигляді: біти мережі позначаються 1, а біти хоста – 0.

Префікс /20 має 20 біт для адресації мережі (20 одиниць) і 12 біт для адресації хостів (12 нулів):

11111111.11111111.11110000.00000000

Що відповідає масці мережі: 255.255.240.0

2.2 Розрахунок підмереж за допомогою маски постійної довжини

Постає задача розбити мережу на підмережі за допомогою маски постійної довжини, визначати адреси підмереж, а також діапазон IP-адрес вузлів для підмереж. За номером мережі ми можемо визначити першу допустиму адресу в цій підмережі. Перша допустима адреса у двійковій системі числення: 0000.00000001. Ми можемо визначити останню допустиму адресу 1111.11111110.

$2^{12} – 2 = 4096 – 2 = 4094$ - мінімальна кількість IP-адрес для вузлів мережі.

Недолік такої мережі - це те, що трафік об'єднаний і при генерації широкомовної адреси - всі 392 комп'ютери отримували би ці пакети - і це не дуже

добре: у нас є різні користувачі, різний рівень доступу до мережі. Цих користувачів нам би хотілося розділити на окремі підмережі. Тому задамося, що всіх користувачів ми ділимо на чотири окремі підмережі. У кожної групи користувачів буде окремий номер мережі зі своєю розрахованою маскою. Пристрої, які можуть об'єднувати мережі - це маршрутизатори. У нас є відокремлені філіал і офіс. На філіалі є дві окремі підмережі - це бухгалтерія і адміністрація, а в центральному офісі - програмісти і тестувальники.

Необхідно задати схему поділу на підмережі в заданому сценарії, враховуючи кількість комп'ютерів в кожній підмережі. При цьому IP-адреси будуть потрібні для кожного інтерфейсу локальної мережі кожного маршрутизатора. Кожний інтерфейс маршрутизатора - це окрема мережа.

200 вузлів - 8 біт на мережеву адресу, тому маска у двійковому вигляді така: 255.255.11110000.00000000. На звільнившихся чотирьох бітах ми можемо створити 16 підмереж по 254 вузла в кожній.

Для маски 255.255.255.0 ми отримаємо 16 підмереж з максимальною кількістю вузлів 254. З маскою 255.255.254.0 ми отримаємо меншу кількість підмереж з більшою кількістю вузлів. Приймаємо маску 255.255.254.0 - тобто плануємо збільшення кількості вузлів в кожній підмережі.

З'ясувавши яка маска підмережі відповідає всім зазначеним вимогам, необхідно заповнити таблицю 2.2

Таблиця 2.2. – Маски підмережі в організації

Вихідна адреса мережі	Вихідна маска мережі в десятковому вигляді	Розрахована маска підмережі в десятковому вигляді	Кількість зарезервованих біт для адреси підмереж	Кількість комбінацій підмереж для визначеної маски
10.160.0.0/20	255.255.240.0	255.255.240.0	3	$2^3 = 8$

Оскільки ми зарезервували на підмережі 3 біти, 9 біт у нас залишається на вузли, тобто ми отримуємо 8 підмереж по 510 вузлів в кожній. З 8 підмереж ми використовуємо п'ять для нашої організації. Розписуємо всі комбінації, які ми можемо мати у таблицю

Розрахувати підмережі з новою маскою і занести інформацію в табл. 2.3

Таблиця 2.3 - Відомості про підмережі

Назва підмережі	Необхідн. розмір підмережі	Виділений розмір підмер.	Десятков. формат адреси	Двійков. формат адреси	Перший використов. адрес вузла	Останній використов. адрес вузла	Широкомов. адреса
LAN1	20	1022	10.160.0.0/23	10.160.00000000.00000000	10.160.0.1	10.160.3.254	10.160.3.255
LAN2	24	1022	10.160.4.0/23	10.160.00000100.00000000	10.160.4.1	10.160.7.254	10.160.7.255
LAN3	200	1022	10.160.8.0/23	10.160.00001000.00000000	10.160.8.1	10.160.11.254	10.160.11.255
LAN4	150	1022	10.160.12.0/23	10.160.00001100.00000000	10.160.12.1	10.160.15.254	10.160.15.255
LAN5	2	1022	10.160.16.0/23	10.160.00010000.00000000	10.160.16.1	10.160.19.254	10.160.19.255
Загал	396	5110					

Для мережі LAN1 десять біт ми не змінюємо. Це задано завданням. Далі три біти ми зарезервували. Для LAN1 – це три нулі 000. І далі – дев’ять біт на вузли. Перша допустима адреса – в кінці одиниця. Остання допустима адреса – це вісім біт і в кінці нуль. Це адреса 1.254.

2.3 Побудова мережі в Cisco Packet Tracer і базове налаштування пристроїв

Будемо використовувати Cisco Catalyst комутатори 2960. Для мереж - маршрутизатор 2911.Кожну підмережу представляємо трьома комп'ютерами. Використовуємо маршрутизатори 2911. Для з'єднання комп'ютерів з мережевими пристроями використовуємо потрібні інтерфейси. Підключаємо комп'ютери до комутаторів за допомогою прямого з'єднання за допомогою порту Fast Ethernet.

Для з'єднання двох маршрутизаторів router2 і router3 треба поставити додатковий модуль. Відкриваємо вікно налаштувань router2, вимикаємо пристрій, під'єднуємо модуль для роботи з оптичним кабелем HWIC-1GE-SFP.

І так само додаємо цей модуль до інтернет сервіс провайдера - router3. Після цього вибираємо оптичний кабель і з'єднуємо два роутера. Використовуємо гігабітний порт 0/3/0.

При розробці IP-адресації ми притримуємись таких вимог:

- перші допустимі IP-адреси призначаються інтерфейсам маршрутизаторів в вказаних мережах

- другі з допустимих IP-адрес призначаються комутаторам

- останні з використовуваних IP-адрес призначаються ПК;

- на каналі підключення граничного маршрутизатора організації Central до інтернет провайдера ISP назначити першу допустиму адресу мережі 209.165.201.224/28, а маршрутизатору організації - наступну. Адресація і маски у підмережах приведено у таблиці 2.4

Таблиця 2.4 – Адресація і маски у підмережах

Назва підмережі	Необх. розмір	Адреса підмережі	Маска	Діапазон адрес	Широкомов. адреса	Необх. розмір підмереж
LAN1	20	10.160.0.0/22	255.255.252.0	10.160.0.1 - 10.160.3.254	10.160.3.255	1022
LAN2	24	10.160.4.0/22	255.255.252.0	10.160.4.1 - 10.160.7.254	10.160.7.255	1022
LAN3	200	10.160.8.0/22	255.255.252.0	10.160.8.1 - 10.160.11.254	10.160.11.255	1022
LAN4	150	10.160.12.0/22	255.255.252.0	10.160.12.1 - 10.160.15.254	10.160.15.255	1022
LAN5	2	10.160.16.0/22	255.255.252.0	10.160.16.1 - 10.160.19.254	10.160.19.255	1022

Підключення інтернет провайдера до інтернету змодельовано loopback-адресою маршрутизатора ISP. loopback-інтерфейс — це віртуальний інтерфейс, який завжди залишається активним (в UP-стані), якщо його явно не вимкнути. Він не прив'язаний до фізичного інтерфейсу пристрою (маршрутизатора чи комутатора), і використовується для різних цілей в налаштуванні мереж.

Основні характеристики loopback-інтерфейсу: віртуальний – не залежить від фізичного стану портів; надійний – завжди «вгору» (UP/UP), якщо не відключено вручну. Використовується для: ідентифікації маршрутизатора (наприклад, у протоколах OSPF, EIGRP); налаштування тестових адрес; моніторингу та

керування (наприклад, для SNMP або SSH доступу); резервної адресації, оскільки loopback IP не змінюється при зміні фізичних інтерфейсів. Адресація пристроїв і їх підключення приведена ц таблиці 2.5.

Таблиця 2.5 - Адресація пристроїв і їх підключення

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Префікс
Filial1	Gig0/0	10.160.0.1	255.255.252.0	/22
	Gig0/1	10.160.16.1	255.255.252.0	/22
	Gig0/2	10.160.4.1	255.255.252.0	/22
Central	Gig0/0	10.160.12.1	255.255.252.0	/22
	Gig0/1	10.160.16.2	255.255.252.0	/22
	Gig0/2	10.160.8.1	255.255.252.0	/22
	Gig0/3/0	209.165.201.226	255.255.255.224	/27
ISP	Gig0/3/0	209.165.201.225	255.255.255.224	/27
	Io0	8.8.8.8	255.255.255.0	/24
Switch-LAN1	VLAN1	10.160.0.2	255.255.252.0	/22
Switch-LAN2	VLAN1	10.160.4.2	255.255.252.0	/22
Switch-LAN3	VLAN1	10.160.8.2	255.255.252.0	/22
Switch-LAN4	VLAN1	10.160.12.2	255.255.252.0	/22

Кожному ПК задається статична IP адреса, маска і шлюз за замовчуванням. Зведемо в таблицю 2.6 відповідні дані для кожної робочої станції.

Таблиця 2.6 – IP-адреса, маска і шлюз за замовчуванням для PC

Мережа	IP-адреса PC1	IP-адреса PC2	IP-адреса PC3	Маска	Шлюз
LAN1	10.160.0.3	10.160.0.4	10.160.0.5	255.255.252.0	10.160.0.1
LAN2	10.160.4.3	10.160.4.4	10.160.4.5	255.255.252.0	10.160.4.1
LAN3	10.160.8.3	10.160.8.4	10.160.8.5	255.255.252.0	10.160.8.1
LAN4	10.160.12.3	10.160.12.4	10.160.12.5	255.255.252.0	10.160.12.1

Встановимо консольне підключення до комутатора в LAN1. Для цього у групі Connections виберемо світло-блакитний консольний кабель (Console); клацнемо будь-який ПК у LAN1. Виберемо варіант підключення RS-232.

Для встановлення сеансу термінального зв'язку з комутатором Switch LAN1 необхідно виконати наступні дії: клацнути на ПК з консольним підключенням і відкрити вкладку Desktop, як показано на рисунку2.2.

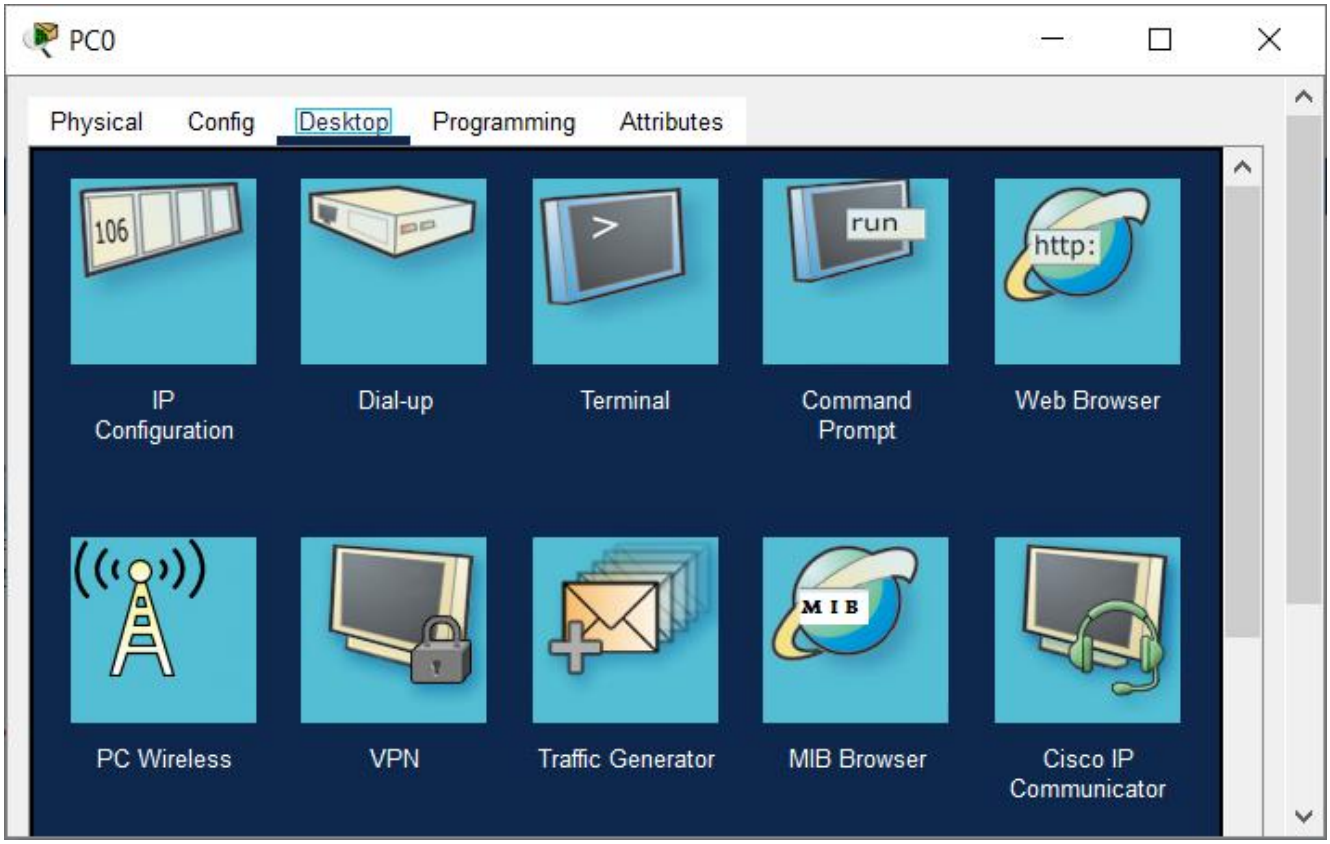


Рисунок 2.2 – Вкладка Desktop персонального комп’ютера PC0

Далі необхідно клацнути значок програми Terminal і перевірити параметри за замовчуванням, що задаються для термінального підключення як показано на рисунку 2.3. Тут вказується кількість бітів за секунду, біти даних та інше. Це налаштування, які керують тим, як користувач взаємодіє з пристроєм через командний рядок (CLI): консольний порт, Telnet або SSH. Їх налаштовують для забезпечення безпеки, контролю доступу, зручності адміністрування. Основні режими зв’язку та інтерфейси CLI: Console – фізичне з'єднання через консольний порт (для початкового налаштування); VTY (Virtual Terminal Lines) – логічні лінії для Telnet або SSH-доступу; AUX (Auxiliary port) – додатковий порт, який може рідко використовуватися, але іноді потрібний.

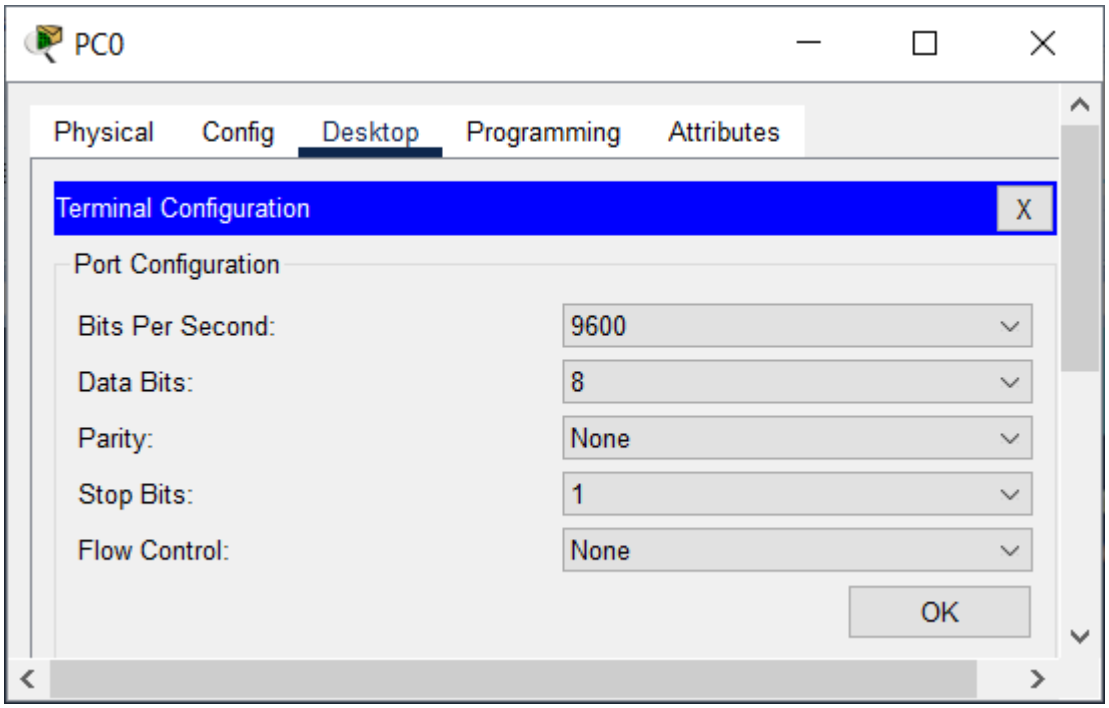


Рисунок 2.3 – Параметри конфігурації Desktop

2.4 Налаштування інтерфейсів комутаторів

Комутатори Cisco мають власну операційну систему для налаштування параметрів. Операційна система називається Cisco IOS (Internetwork Operating System). Основні характеристики Cisco IOS:нтеріфейс командного рядка (CLI) – основний спосіб керування пристроями; доступна підтримка різноманітних мережевих протоколів, наприклад, OSPF, EIGRP, BGP, VLAN, STP; доступна можливість налаштування безпеки, QoS, NAT, ACL тощо. Є також інші варіанти ОС Cisco: NX-OS – використовується в комутаторах серії Nexus; IOS XE – модульна версія IOS, використовується в нових маршрутизаторах і комутаторах. В IOS доступна довідка по командам. В даний момент відображається запрошення, зване режимом користувача, і пристрій очкує введення команд. Найпростіший спосіб викликати довідку, це ввести знак питання(?) в будь-якому місці командного рядка. Вікно комутатора Switch0 в режимі налаштування зображено на рисунку 2.4.

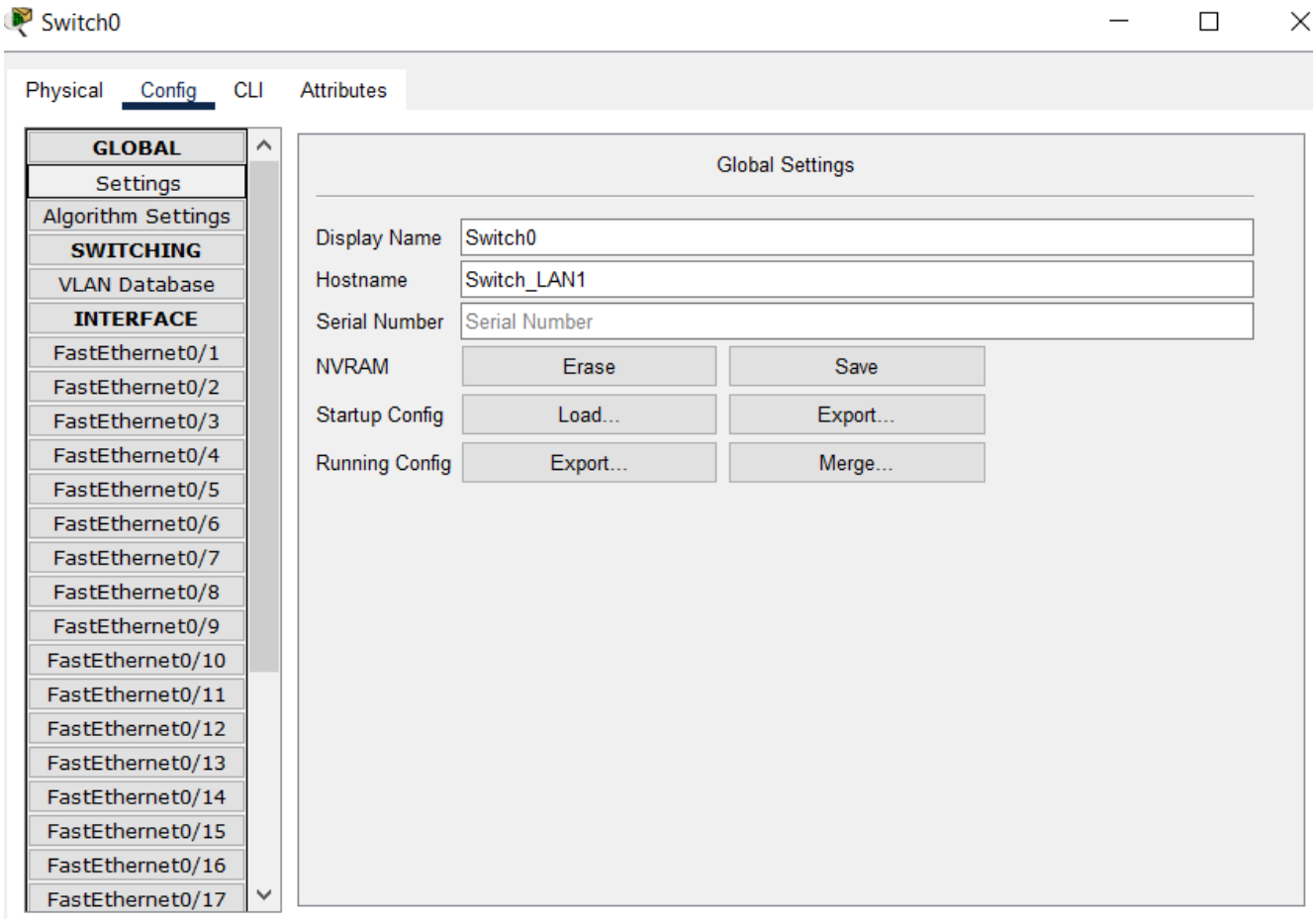


Рисунок 2.4 – Вікно налаштувань комутатора Switch_LAN1

У роботі налаштування пристроїв буде відбуватись через інтерфейс CLI, відкрити список допустимих команд якого можна так, як показано на рис. 2.5.

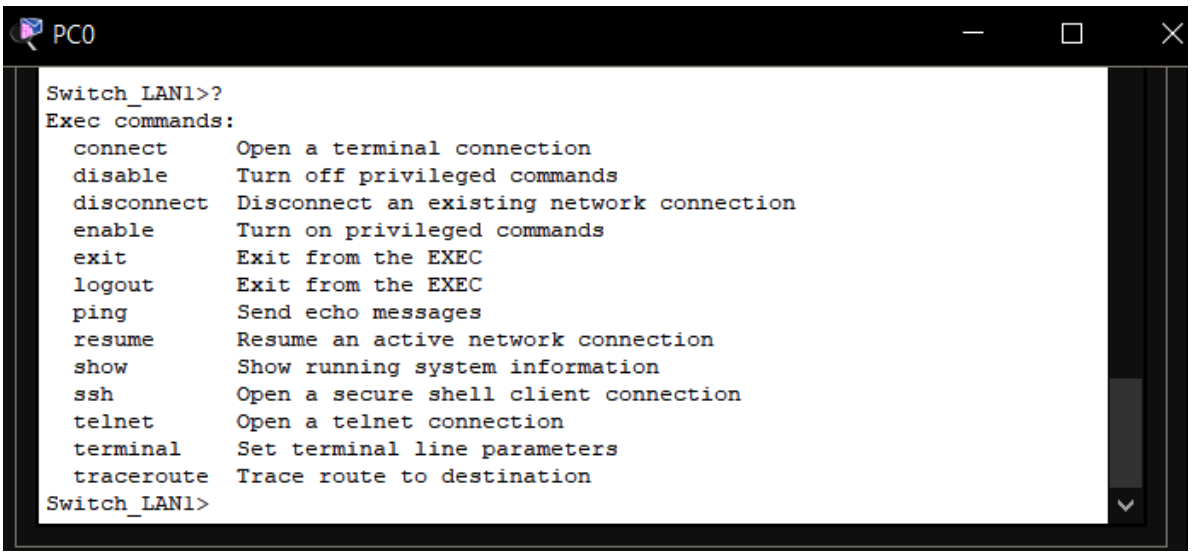


Рисунок 2.5 - Список допустимих команд комутатора Switch_LAN1

Далі треба виконати вхід в привілейований режим командою

Switch>en <Tab>

Встановимо поточні дату і час на комутаторі за командами:

```
Switch#clock ?
Switch#clock set ?
Switch#clock set 10:30:30 ?
Switch#clock set 10:30:30 17 March ?
```

Проведені дії показані на рисунку 2.6

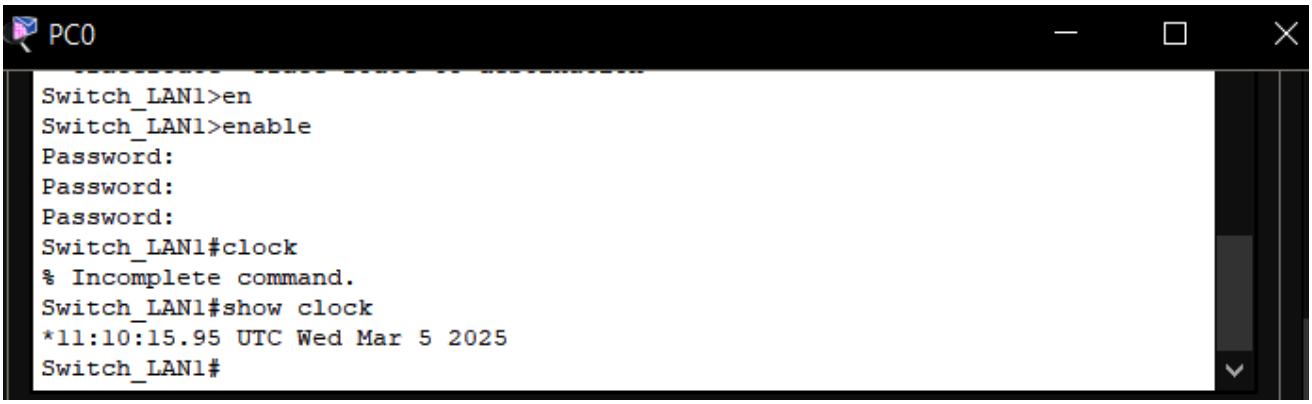


Рисунок 2.6 – Встановлення дати і часу комутатора Switch_LAN1

Переглянемо поточну конфігурацію коммутатора за командою "show running config", як приведено на рисунку 2.7

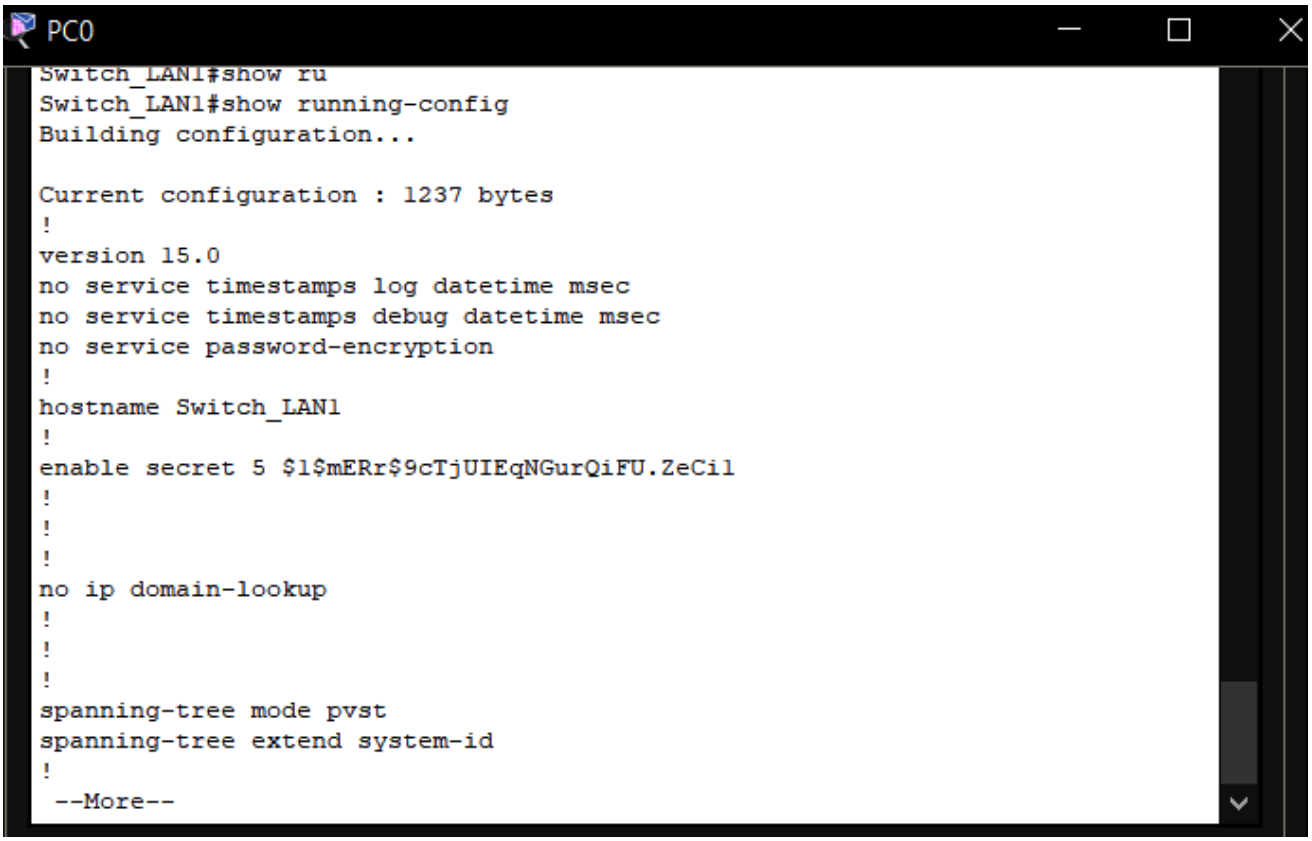


Рисунок 2.7 - Поточна конфігурація коммутатора Switch_LAN1

Комутатор має 24 інтерфейси Fast Ethernet, 2 інтерфейси Gigabit Ethernet

До пристрою ми можемо робити підключення по 16 віртуальним лініям vty.

Для входу в режим конфігурації необхідно набрати "config" і вибрати режим конфігурації "terminal". Для перевірки поточної конфігурації комутатора необхідно у привілейованому режимі набрати команду: "show running-config". Приставка do дозволяє виконати команду "show" в будь-якому режимі, не входячи в привілейований.

Далі необхідно налаштувати інтерфейс керування комутатором. Через віртуальний інтерфейс комутатора (SVI) можна отримати віддалений доступ по telnet або ssh з метою відображення і налаштування його параметрів. За замовчуванням через VLAN 1 забезпечується керування комутатором по мережі. Щоб налаштувати IP-адресу на комутаторі Switch_LAN1, необхідно використовувати команди:

```
Switch_LAN1(config)#interface vlan 1
Switch_LAN1(config-if)#ip address 192.168.1.254 255.255.255.0
Switch_LAN1(config-if)#no  shutdown
Switch_LAN1(config)#ip default-gateway IP-gateway
```

Для доступу до комутатора з віддалених мереж необхідно вказати IP-адресу шлюзу. Команда "show ip interface brief" в привілейованому режимі інформує про IP-адресу, а також про стан всіх портів і інтерфейсів комутатора. Для цього можна також використовувати команду "show running-config". Стан інтерфейсу VLAN 1 повинен бути up/up, а інтерфейсу призначена IP-адреса. Стан портів комутатора F0/1 та F0/2 також up, оскільки до них підключені ПК.

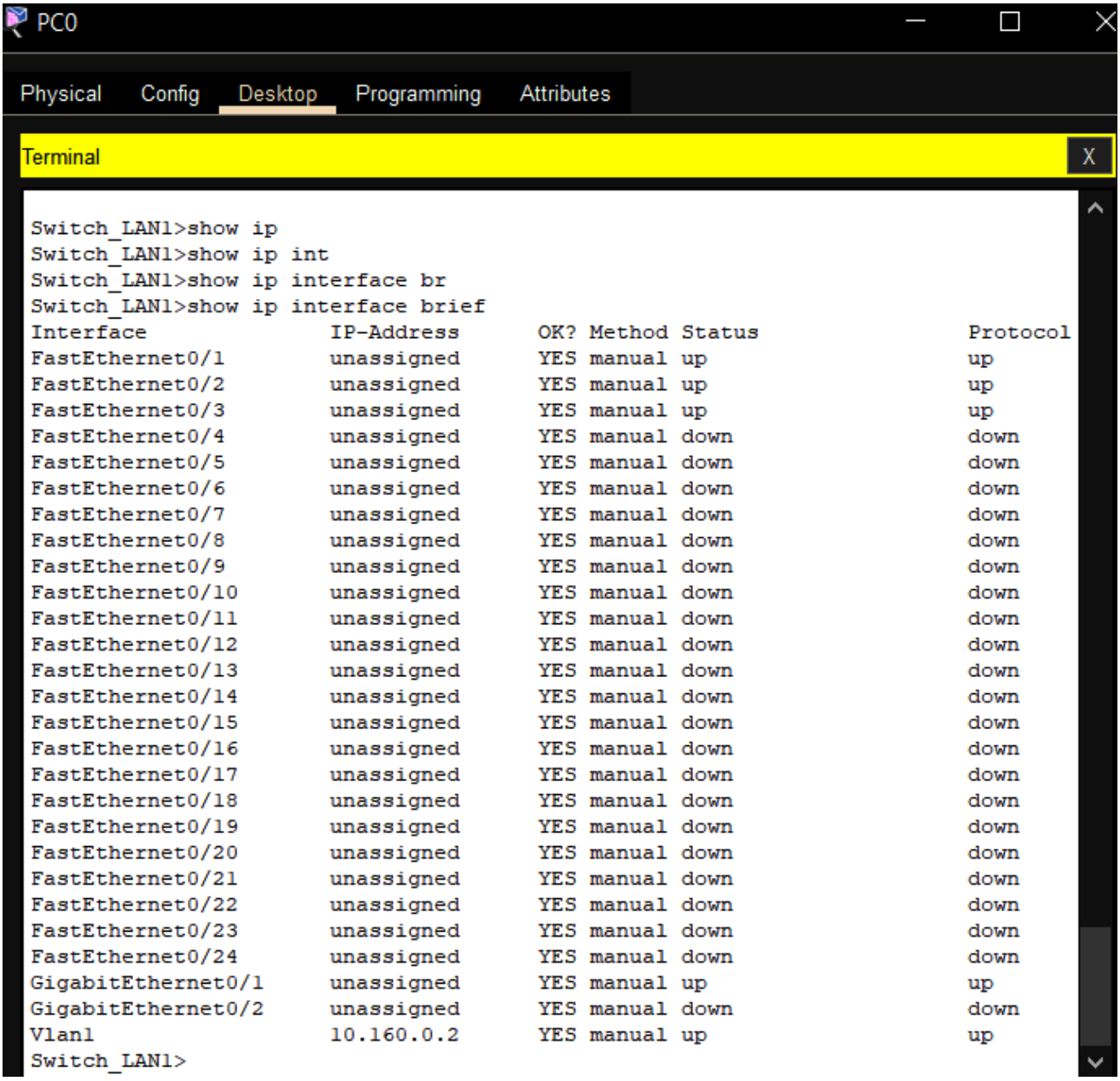


Рисунок 2.8 – Інформація про стан портів комутатора Switch_LAN1

Збереження конфігурації комутатора в NVRAM.

Налаштування комутаторів здійснюється через термінальну програму (PuTTY, Tera Term, HyperTerminal), яка підключена до консольного порту комутатора. Доступна аєрархічна структура режимів. CLI Cisco має кілька рівнів доступу: User EXEC mode: обмежений доступ для базових переглядів; Privileged EXEC mode: доступ до діагностики та конфігурації; Global Configuration mode: дозволяє змінювати налаштування пристрою.

2.5. Налаштування інтерфейсів маршрутизаторів

Cisco Packet Tracer дозволяє побудувати мережу з маршрутизаторами, комутаторами, ПК, IoT-пристроями тощо. Існує два режими налаштування маршрутизаторів: графічний режим, що дозволяє налаштування через форми, випадаючі списки (інтерфейси, IP-адреси, маршрути). Режим CLI дозволяє: повноцінне конфігурування; підтримує більшість базових команд Cisco IOS. Можна моделювати й налаштовувати: статичну маршрутизацію; динамічну маршрутизацію; NAT, DHCP, ACL, VLAN; налаштовувати інтеграцію з комутаторами, ПК, серверами тощо. Router має наступні параметри: Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB; CISCO2911/K9 platform with 524288 Kbytes of main memory

Для налаштування необхідно встановити унікальне ім'я за допомогою команди "hostname"; використовувати відомості з таблиці адресації та активувати задіяні інтерфейси (рис. 2.9). Приклад налаштування:

```
R1(config)#interface  gigabitethernet 0/0
R1(config-if)#ip address 10.160.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#description Connection to LAN1 bookkeeping
```

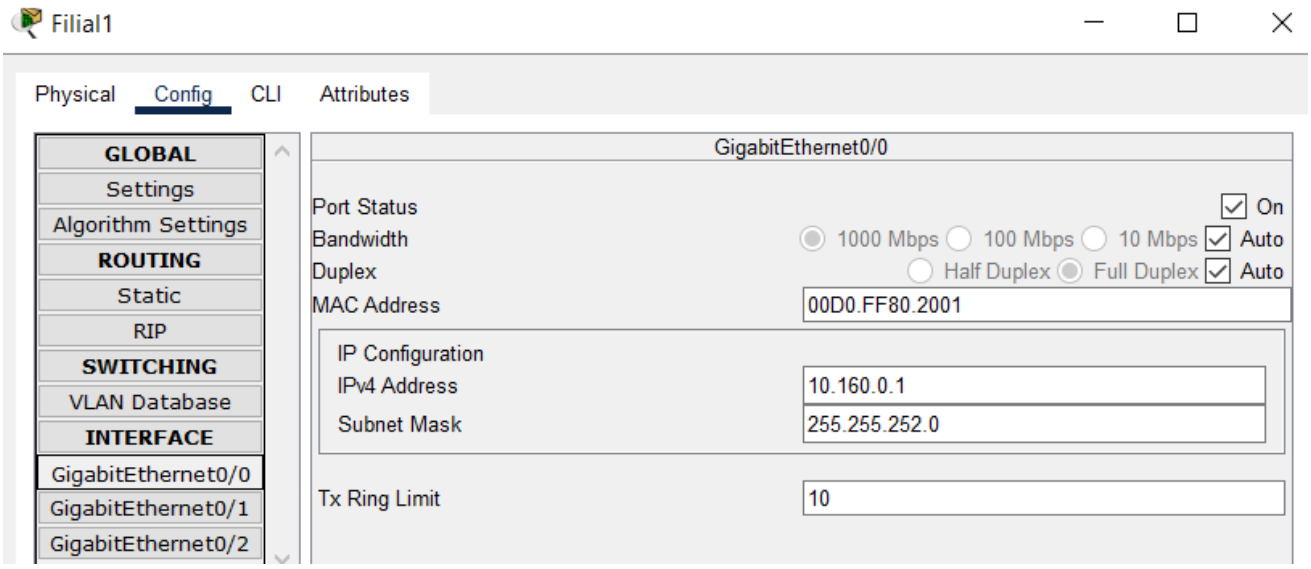


Рисунок 2.9 – Конфігурація інтерфейса GigabitEthernet0/0

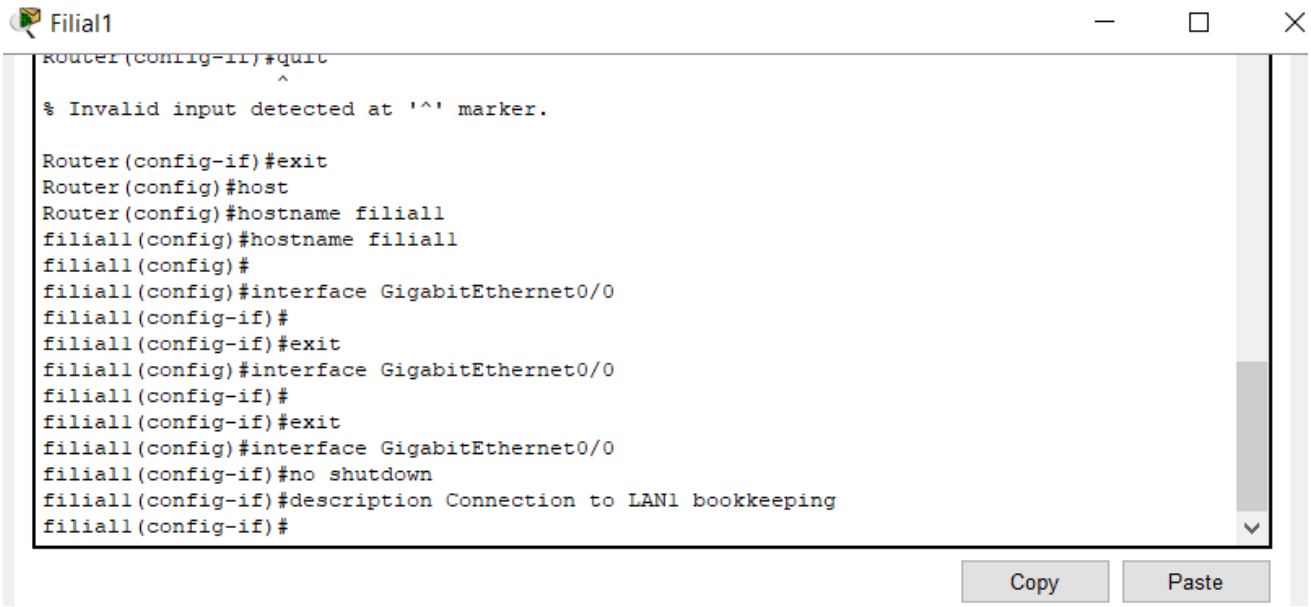


Рисунок 2.10 – Конфігурація маршрутизатора Filial1

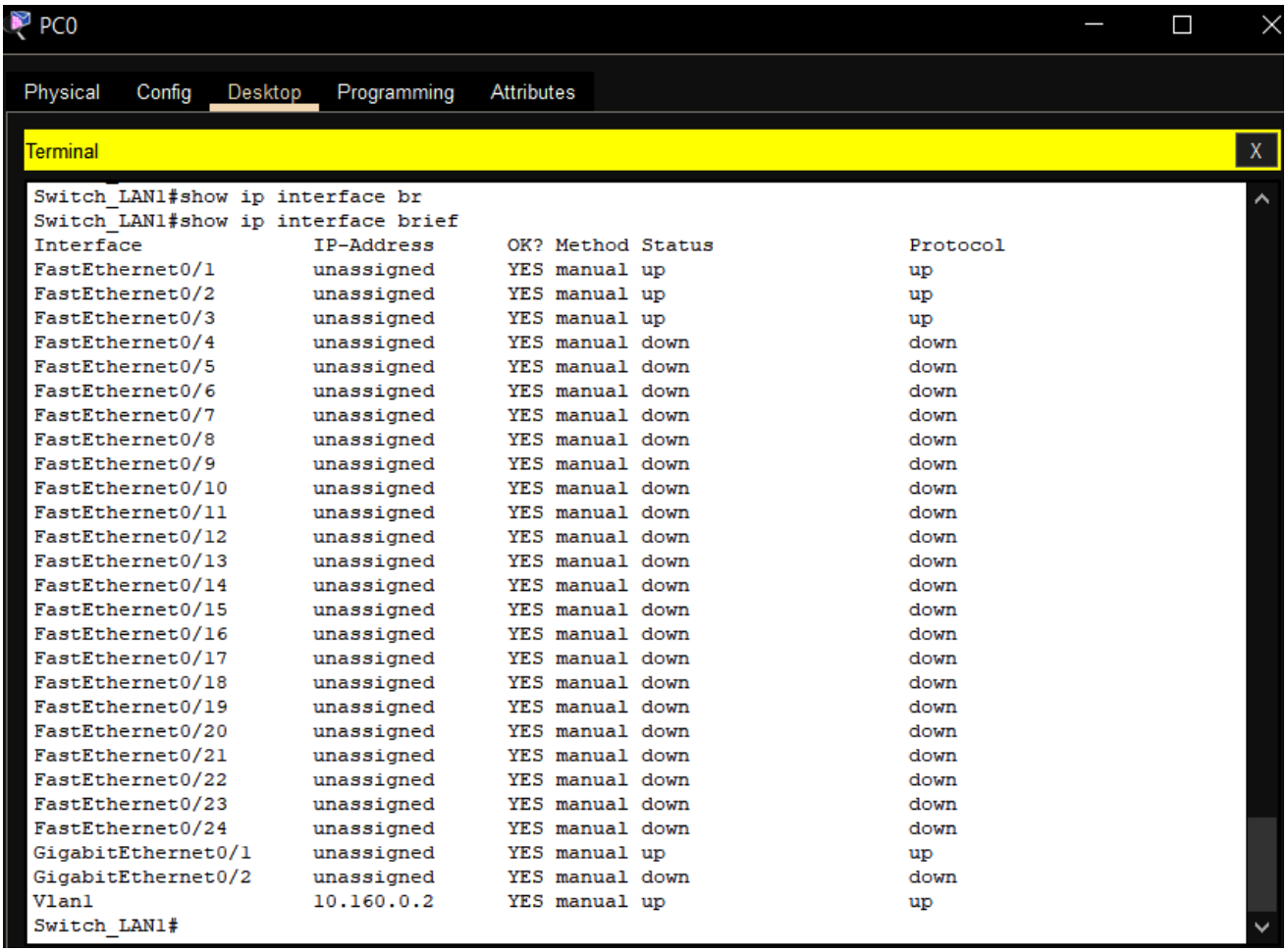


Рисунок 2.11 – Налаштування маршрутизатора

Налаштування підключення до LAN2

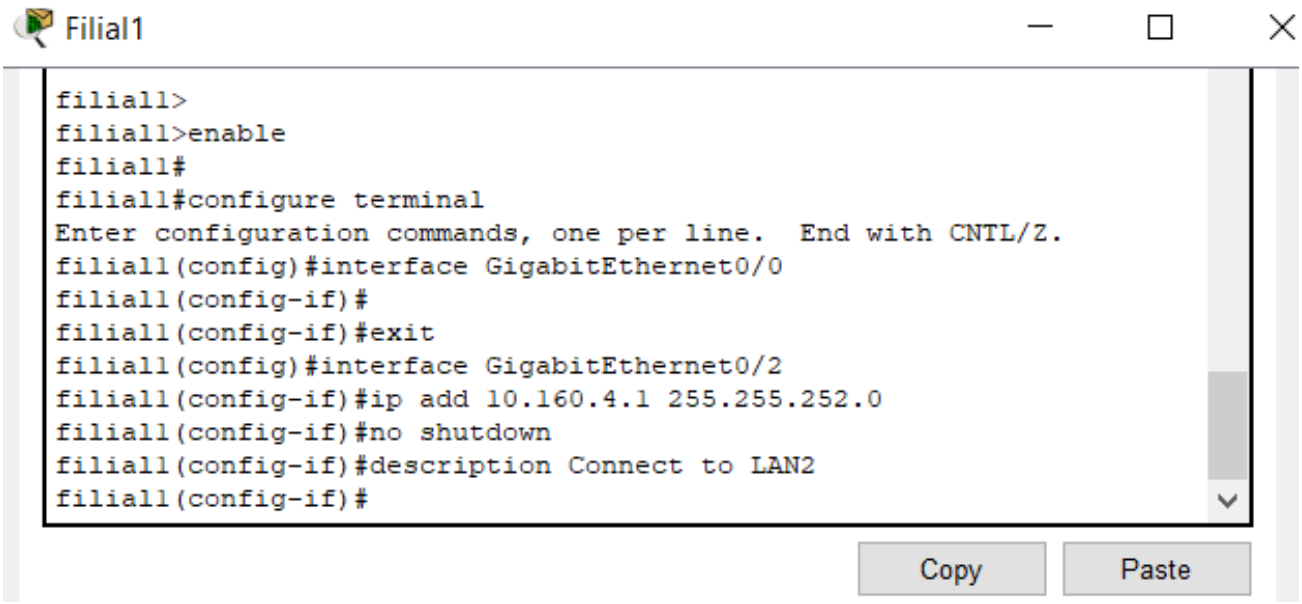


Рисунок 2.12 – Налаштування маршрутизатора

Налаштування підключення до LAN5

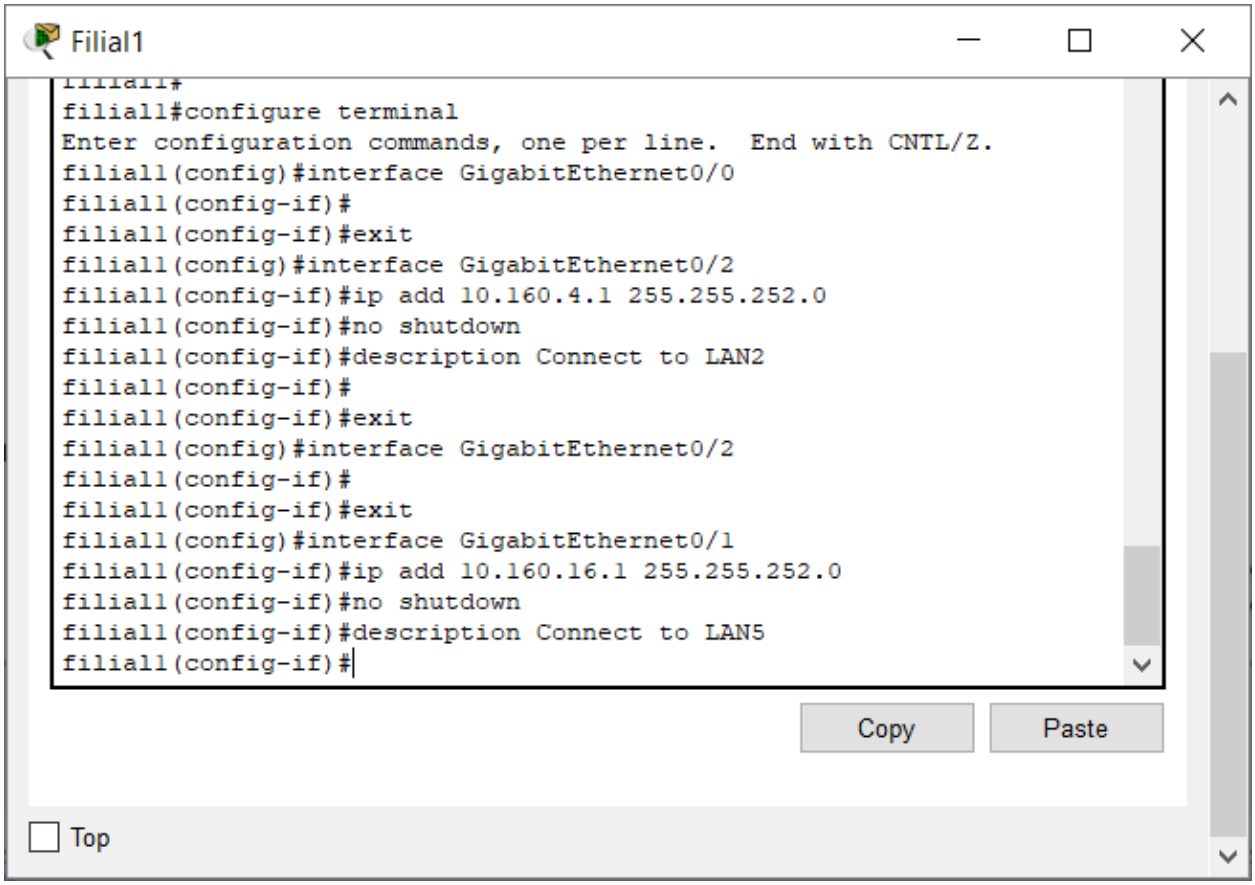


Рисунок 2.13 – Налаштування інтерфейсів маршрутизатора

Підключення інтернет-провайдера до інтернету змодельоване loopback-адресом (lo0) маршрутизатора ISP. Інтерфейс loopback - це логічний інтерфейс, що емулює роботу фізичного, тому його не можна підключити до іншого пристрою. Він вважається програмним інтерфейсом, який автоматично переводиться в стан up (активний) під час роботи маршрутизатора

loopback-інтерфейс – це віртуальний інтерфейс, який завжди залишається активним (в UP-стані), якщо його явно не вимкнути. Він не прив'язаний до фізичного інтерфейсу пристрою (маршрутизатора чи комутатора), і використовується для різних цілей в налаштуванні мереж. Основні характеристики loopback-інтерфейсу: віртуальний — не залежить від фізичного стану портів; надійний — завжди ввімкнений (UP/UP). Використовується для виконання дій: ідентифікації маршрутизатора; налаштування тестових адрес; моніторингу та керування; резервної адресації. Приклад налаштування:

```
Router> enable
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 8.8.8.8 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# show ip interface brief
```

2.6 Налаштування ПК та перевірка підключень до мережі

Проведемо налаштування IP-адрес на ПК у наступному порядку: послідовно клацаємо на кожному ПК та у вікні управління відкриваємо вкладку Desktop; обираємо додаток IP Configuration, як показано на рисунку 2.14.

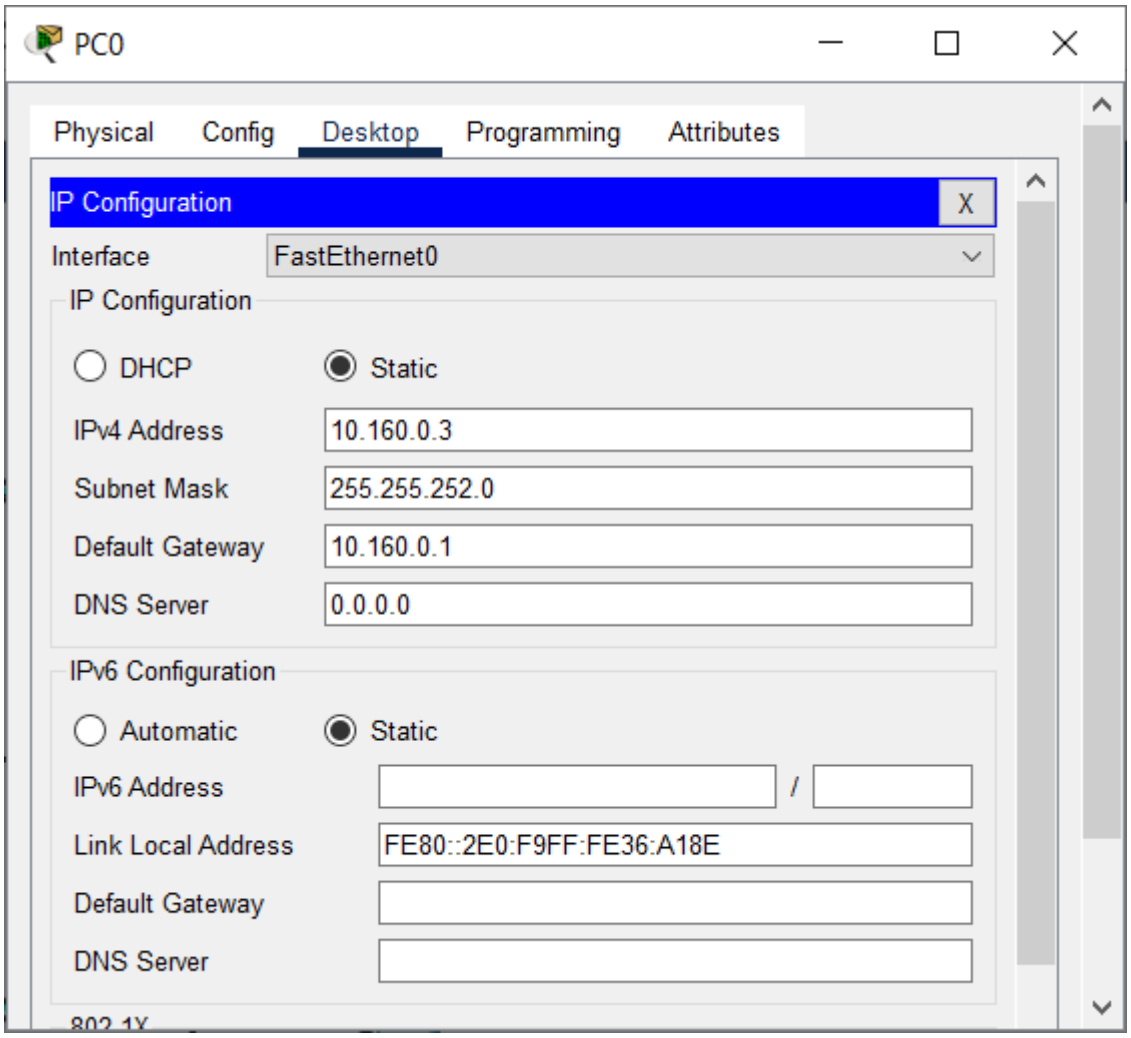


Рисунок 2.14 – Конфігурація персонального комп’ютера PC0

Далі необхідно перевірити підключення до мережі: виконуємо команду "ping" з командного рядка кожного ПК на його шлюз. Перевірка зв’язку вузла PC0 з шлюзом за замовчуванням показано на рисунку

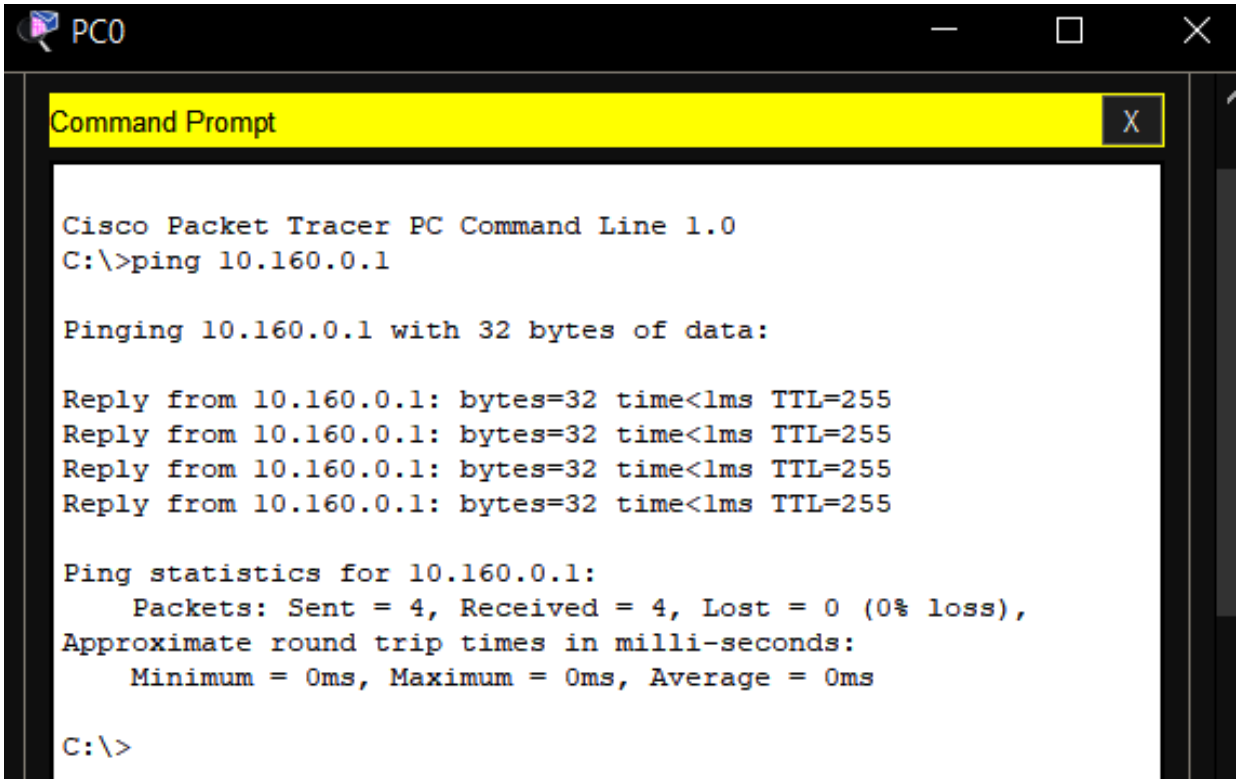


Рисунок 2.15 – Перевірка зв’язку з вузлом 10.160.0.1

Зв’язок є

ПК в віддалених мережах не можуть відправляти один одному ехо-запити

Для перевірки віддаленого підключення до комутатора через адресу управління SVI в командному рядку вводимо команду "telnet ip-адреса". Конфігулація IP протокола для комп’ютера PC5 приведена на рисунку 2.16

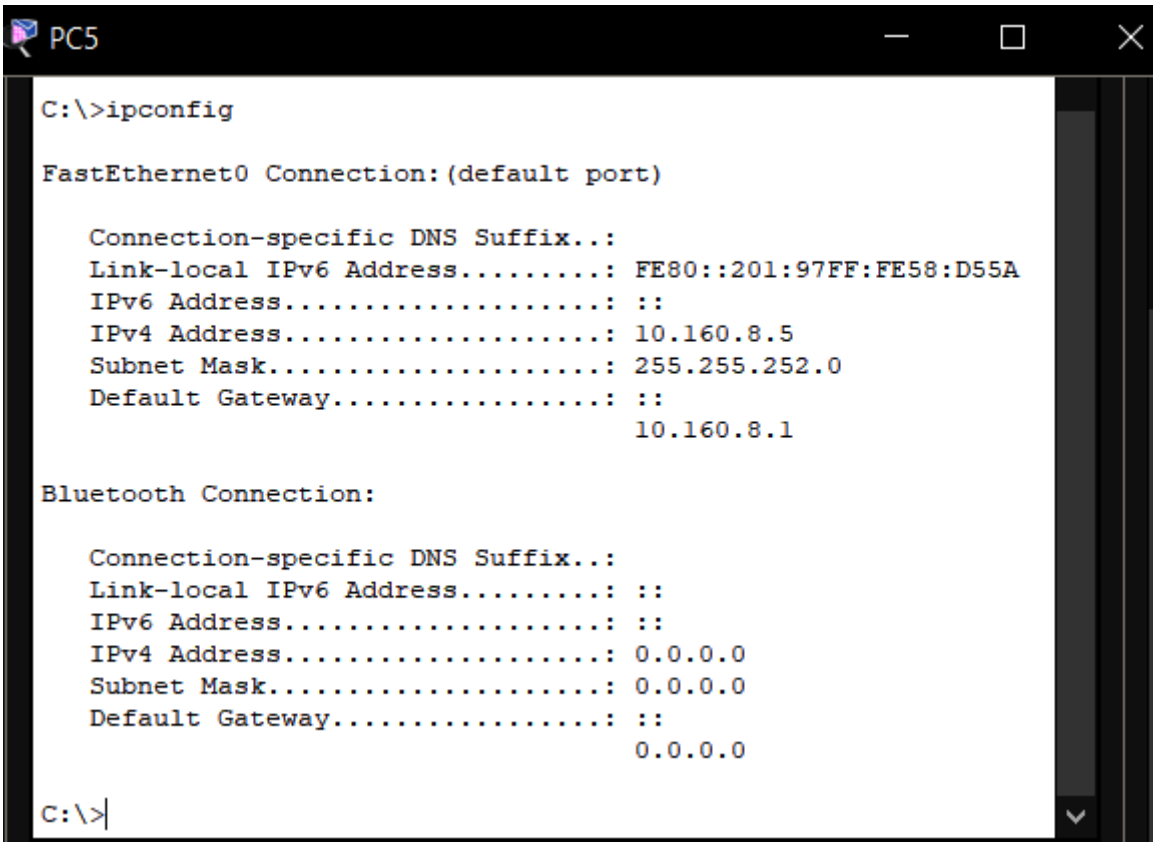


Рисунок 2.16 – Перевірка налаштувань IP протокола вузла PC5

Команда ping з PC11 на PC0 приведена на рисунку 2.17

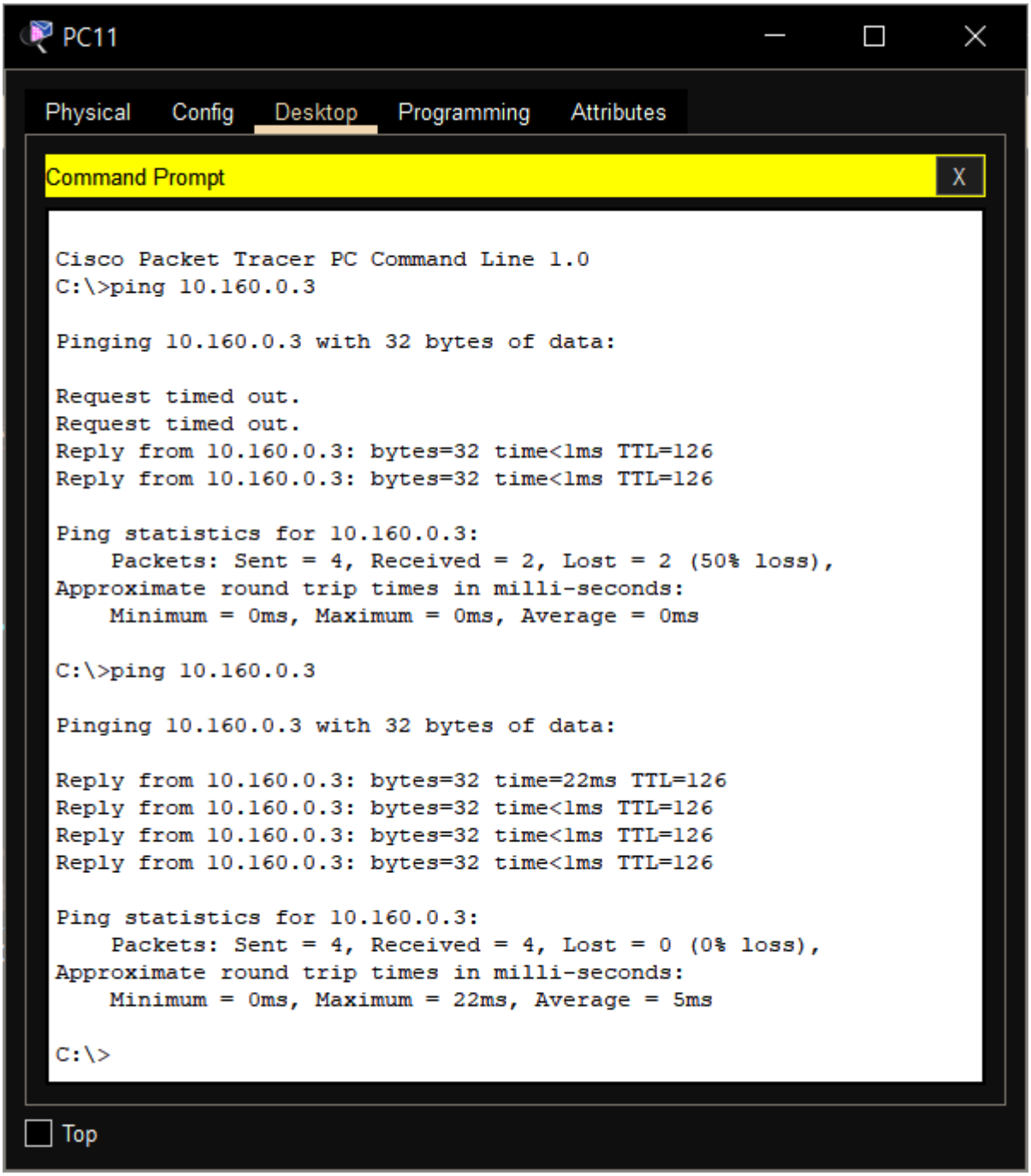


Рисунок 2.17 – Результат виконання команди ping з PC11 на PC0

Тест перехресних команд ping з PC11 на PC0 і з PC5 на PC6 приведена на рисунках 2.18-2.19

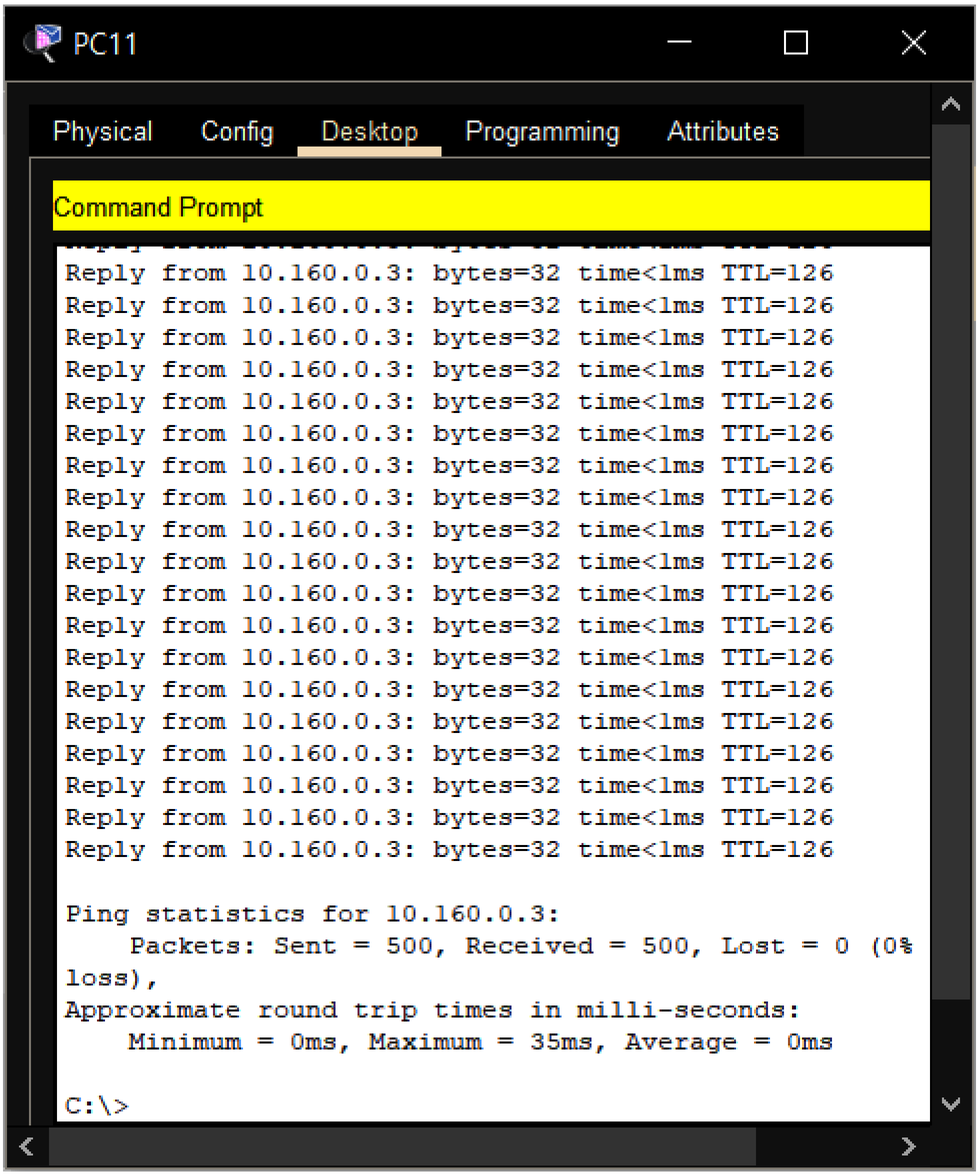


Рисунок 2.18 – Тест перехресних команд ping з PC11 на PC0

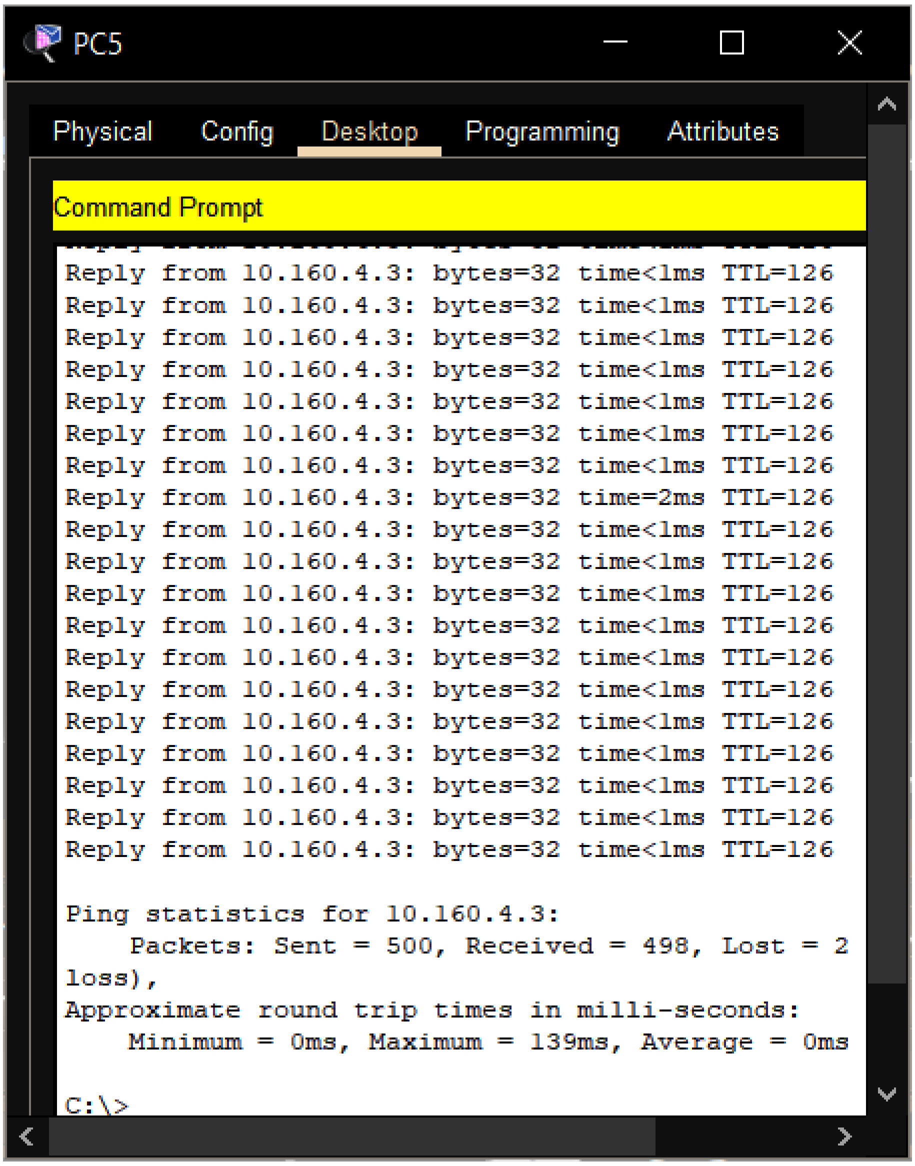


Рисунок 2.19 - Тест перехресних команд ping з PC5 на PC6

Вузол PC11, з якого команда ping була запущена першою, продемонстрував передачу 500 пакетів без втрат з максимальною затримкою 35 мс. Вузол PC5 продемонстрував гірші результати: з 500 пакетів було втрачено 2, максимальна затримка була 139 мс з розміром пакетів 32 байти.

Створену мережу можна охарактеризувати як локальну керовану мережу з повним ручним контролем над IP-адресацією та маршрутизацією. Статично адресована LAN характеризується тим, що: IP-адреси призначаються вручну кожному пристрою; маршрути також прописуються вручну в таблиці маршрутизації на маршрутизаторах; використовується без DHCP - відсутня

автоматична IP адресація. Така мережа добре підходить для початкового вивчення мережевих технологій, логіки IP-адресації та статичної маршрутизації.

2.7 Виникнення широкомовного шторм у LAN

Широкомовний (broadcast) трафік – це мережеві пакети, адресовані всім хостам у певному домені широкомовлення (наприклад, IPv4-адреса 255.255.255.255 або ARP-запит). Широкомовний шторм виникає, коли в мережі циркулює надзвичайно велика кількість широкомовних пакетів за короткий час, і комутатори з хостами не справляються з їх обробкою. Через відсутність таймера життя (TTL) в рівні L2 такі пакети можуть безперервно повторюватися (наприклад, ARP- чи DHCP-запити), що «затоплює» мережу та призводить до деградації її роботи. Типові причини широкомовних штормів:

- Шлюзові петлі (loop): коли в мережі є декілька активних шляхів між комутаторами (наприклад, два чи більше з’єднання між тими ж комутаторами), один і той же широкомовний кадр може нескінченно циркулювати. Наприклад, якщо з’єднати два комутатори двома кабелями і вимкнути STP, пакети почнуть знову і знову передаватися по колу.

- Занадто великий домен широкомовлення: чим більше пристроїв у VLAN (секундній мережі чи L3-підмережі), тим більше вони генерують широкомовних повідомлень (ARP-відповіді, вітальні запити тощо). Великий домен (наприклад, /16 або масивна VLAN) природно генерує значно більше широкомовного трафіку.

- DHCP-шторм: за замовчуванням DHCP Discovery та інші етапи можуть бути широкомовними. Якщо багато пристроїв одночасно запитують IP-адреси (наприклад, після перезавантаження мережі), це створює хвилю DHCP-запитів. Для мережі зі статичною адресацією великих DHCP-штормів зазвичай немає, але слід враховувати, що будь-яка масова ARP-активність схожа за ефектом.

- Помилкове чи несправне обладнання: наприклад, недоречно налаштовані комутатори, підключені незнайдені конвертери, випадково роз’єднані порти тощо,

можуть самостійно генерувати широкомовні пакети (через запит всіх, хто тут є). Аварія устаткування може призвести до того, що порт комутатора починає безупинно надсилати широкомовні пакети – і тоді спостерігається «шторм».

Розглянемо роль VLAN у поширенні широкомовного трафіку. Кожен VLAN на комутаторі створює окремий домен широкомовлення. Це означає, що широкомовний кадр, переданий в межах одного VLAN, досягне лише пристроїв цього VLAN і не буде переданий в інші VLAN без маршрутизації. Наприклад, якщо ПК у VLAN10 відправив широкомовний ARP-запит, його побачать лише хости теж у VLAN10 (як і передбачається у лабораторії Cisco Packet Tracer). Таким чином, сегментація мережі на VLAN суттєво обмежує зону розповсюдження широкомовного трафіку: кожен VLAN розглядається комутаторами як «віртуальний окремий комутатор», а широкомовні пакети поширюються через всі порти, які належать цьому VLAN.

Водночас слід зазначити, що якщо всі комутатори в мережі беруть участь у одному VLAN, цей VLAN утворює один суцільний домен широкомовлення. У такому разі навіть одна неуторована петля призведе до неконтрольованого розповсюдження широкомовних пакетів у цьому VLAN (тобто «дуже великий шторм»). Тому найкраща практика – обмежувати обсяг кожного VLAN: не прокладати всі VLAN по всіх сегментах, а розмежовувати пристрої на невеликі VLAN/субмережі, де це доцільно.

Розглянемо запобігання широкомовним штормам. Щоб уникнути широкомовних штормів у мережі з VLAN, використовують такі заходи:

- Сплячі протоколи захисту від петель (STP/RSTP/MST). На комутаторах Cisco за замовчуванням увімкнено Spanning Tree Protocol. Він блокує надлишкові шляхи в топології, запобігаючи петлям. При коректній роботі STP один з дублікатних каналів перейде в заблокований стан, і широкомовні кадри більше не зможуть нескінченно циркулювати. На прикладі: після вибору корневого комутатора інтерфейс одного з дублікатних зв’язків стає заблокованим, і відправлений клієнтом широкомовний кадр не обходить мережу по колу. У практиці в Packet Tracer можна вимкнути STP командою `no spanning-tree vlan

<ID>` на комутаторі – тоді всі порти переходять у пересилальний стан, і шторм виникає (наочно видно “мигання” індикації портів і флаппінг MAC-адрес). Зауважимо, що наявність помилкових фізичних проблем (так званих «уніджирекціональних» лінків) може змусити STP некоректно працювати, тому добре продуманий дизайн мережі (ревізія кабелів, надійні канали зв’язку) – важливий фактор профілактики петлей.

- Storm Control (контроль шторму). На деяких комутаторах Cisco існує можливість налаштувати обмеження на інтерфейсі – наприклад, команда `storm-control broadcast level X` задає максимальну частоту широкомовних кадрів. Якщо трафік перевищує поріг, пакети починають відсікатися. Це не вирішує причину петлі, але локально обмежує шкоду. Cisco рекомендує активувати Storm Control або подібні механізми, якщо вони є на вашому обладнанні. Зокрема, конфігурований поріг дозволяє «урізати» надлишкові широкомовні сигнали раніше, ніж вони заповнять порт. (В Packet Tracer така детальна конфігурація зазвичай недоступна, але принципово в докувентації Cisco описано функцію Storm Control.)

- Адекватна сегментація мережі (правильна побудова VLAN). Як зазначено вище, зменшення розміру доменів широкомовлення знижує загальне навантаження. Групуйте пристрої за VLAN за призначенням: наприклад, комп’ютери користувачів, сервери, IP-телефони, відеокамери – кожен клас в окремому VLAN, якщо це доцільно. При інтеграції нових сегментів спроектуйте VLAN так, щоб не було масивних непотрібних широкомовних доменів. Використовуйте окремі підмережі (L3) для VLAN і, за потреби, маршрутизатор з VLAN-інтерфейсами (SVI) або маршрутизатор-on-a-stick для зв’язку між VLAN. Таким чином, широкомовні повідомлення (наприклад, ARP, DHCP) розповсюджуються тільки всередині свого підмережевого VLAN. Наприклад, при розбивці великої /24-мережі на дві підмережі /25 в різних VLAN ви автоматично зменшуєте потенційний «радіус дії» ARP-запитів і DHCP Discover. Проективні документи Cisco підтверджують, що масштабний broadcast-домен прямо залежить

від кількості хостів у VLAN, тож сегментація і балансування навантаження між VLAN суттєво зменшують широту шторму.

- Вимкнення направлених широкомовних пакетів (Directed Broadcast). Якщо в мережі є маршрутизатори, варто заборонити надходження широкомовних пакетів ззовні (конфігурація `no ip directed-broadcast` на роутерах Cisco). Це убезпечить від можливих DoS-атак на базі спрямованих широкомовних пінгів, що можуть спровокувати шторм всередині VLAN. Для внутрішньої мережі Packet Tracer така опція зазвичай за замовчуванням вимкнена або не моделюється, але у реальних мережах це важливий захід.

- Додаткові заходи безпеки і налаштування портів. На інтерфейсах комутаторів часто вмикають функції BPDU Guard (автоматичне відключення порту, якщо він приймає STP BPDU, корисне на кінцевих портах, щоб запобігти підключенню інших комутаторів до клієнтських портів) і PortFast (швидкий перехід порту в режим Forwarding при підключенні від кінцевої станції, що прискорює підняття порту без ризику петлі). Крім того, обмеження числа MAC-адрес на порті (port security) може перервати спробу підключити до мережі нелегальний концентратор із багатьма пристроями (що могло б створити петлю). Хоча це скоріше налаштунки безпеки/доступу, вони ускладнюють виникнення петель на кінцевих портах.

Усі ці заходи сумісно дозволяють мінімізувати ризик широкомовного шторму: STP розриває петлі, Storm Control гальмує надлишкові пакети, а VLAN і добрий дизайн мережі обмежують масштаб потенційного шторму. Cisco також рекомендує налаштовувати лише необхідні VLAN на транках, обмежувати транкові VLAN (команда `switchport trunk allowed vlan`), і взагалі не об’єднувати різні рівні доступу одним транком, щоб локалізувати проблеми.

Розглянемо моделювання широкомовних штормів у Cisco Packet Tracer, який добре показує базові механізми VLAN та STP, але не гарантує автентичну поведінку реального обладнання. За замовчуванням в Packet Tracer комутатори імітують STP (зазвичай PVST+ на VLAN 1) – і через це в звичайному сценарії петлі не утворяться. Наприклад, у NetAcad Packet Tracer-промоції прямо

навчають, що VLAN є доменом широкомовлення: симулюючи ping на широкомовну адресу, бачимо, що сигнал доходить тільки до пристроїв свого VLAN.

Якщо ж бажати проілюструвати ефект шторму в симуляторі, потрібно навмисне створити умови: з'єднати комутатори зайвими лінками і відключити STP. Дослідники відмітили, що в Packet Tracer навіть для простих хабів програма іноді «автоматично вимикає» надлишковий канал (що неначе є петлею) – імітуючи власний захист від петель. Проте на Cisco IOS-комутаторах PT дійсно можна видати no spanning-tree vlan 1, щоб вимкнути STP на VLAN 1. Потім, наприклад, команда ping 255.255.255.255 з ПК в мережі спричинить справжній шторм: комутатори почнуть відсилати широкомовний кадр по петлі до нескінченності. У моделі Packet Tracer це візуалізується як постійне мерехтіння індикації портів і флаппінг MAC-адрес між інтерфейсами. Зафіксовано, що після вимкнення STP результати пінгу (давання broadcast) показали багаторазові відповіді: комутатор у відповідь отримував копії власного пакету десятки разів. Це демонструє типовий прояв широкомовного шторму в симуляторі.

Водночас слід пам'ятати, що Packet Tracer – спрощений симулятор. Як зауважено в критичних оглядах, PT відтворює мережеві протоколи в наближеному середовищі з обмеженими параметрами: він дає практичну уяву про маршрутизацію, VLAN, STP тощо, але не імітує всіх нюансів "живої" мережі. Наприклад, реальні Catalyst-комутатори можуть мати апаратні механізми ARP-чи DAG-таймерів, додаткові статистики або особливу поведінку на помилках, які Packet Tracer не показує. Тому будь-який експеримент із широкомовними штормами в PT слід сприймати як навчальну демо-версію: вона добре ілюструє основні принципи (що в один VLAN широкомовлення досягає всіх вузлів, що петлі призводять до флаппінгу, що STP їх зупиняє), але може опускати деталі (наприклад, PT може «підказувати» про петлі навіть на хабах, чого не було б у реальному середовищі).

Висновок: широкомовні шторми можливі й у мережі, змодельованій у Packet Tracer з VLAN і статичними адресами, якщо виникають петлі або інші аномалії. В той же час, правильно спроектована мережа з увімкненим STP та розбиттям на VLAN/підмережі практично виключає реальні широкомовні шторми. У лабораторії Packet Tracer ці явища демонструються на базовому рівні (STP, VLAN, ARP), але слід враховувати обмеження симуляції та перевіряти ключові налаштування (й STP не відключено) при аналізі проблем.

Висновки до другого розділу

1. Відповідно до заданих вимог виконано розбиття адресного простору телекомунікаційної мережі, виділений адресний простір з врахуванням можливого розширення кількості вузлів в кожній підмережі.

2. Побудована модель мережі у середовищі Cisco Packet Tracer, виконано базове налаштування пристроїв: комутаторів, маршрутизаторів, ПК.

3. Налаштований віртуальний інтерфейс VLAN 1 для керування комутатором по мережі, перевірений стан активованих портів.

4. Налаштовані всі активні інтерфейси маршрутизаторів, задані IP-адреси, маски підмереж, налаштований loopback-інтерфейс маршрутизатора ISP.

5. Виконаний тест перехресних команд ping з PC11 на PC0 і з PC5 на PC6, який показав хорошу навантажувальну здатність мережі.

6. Проаналізовані можливості виникнення широкомовних штормів у мережі

3 НАЛАШТУВАННЯ СТАТИЧНИХ МАРШРУТІВ І МАРШРУТІВ ЗА ЗАМОВЧУВАННЯМ

3.1 Перевірка налаштувань і досяжність вузлів мережі

Розглянемо мережу, представлену на рисунку 3.1

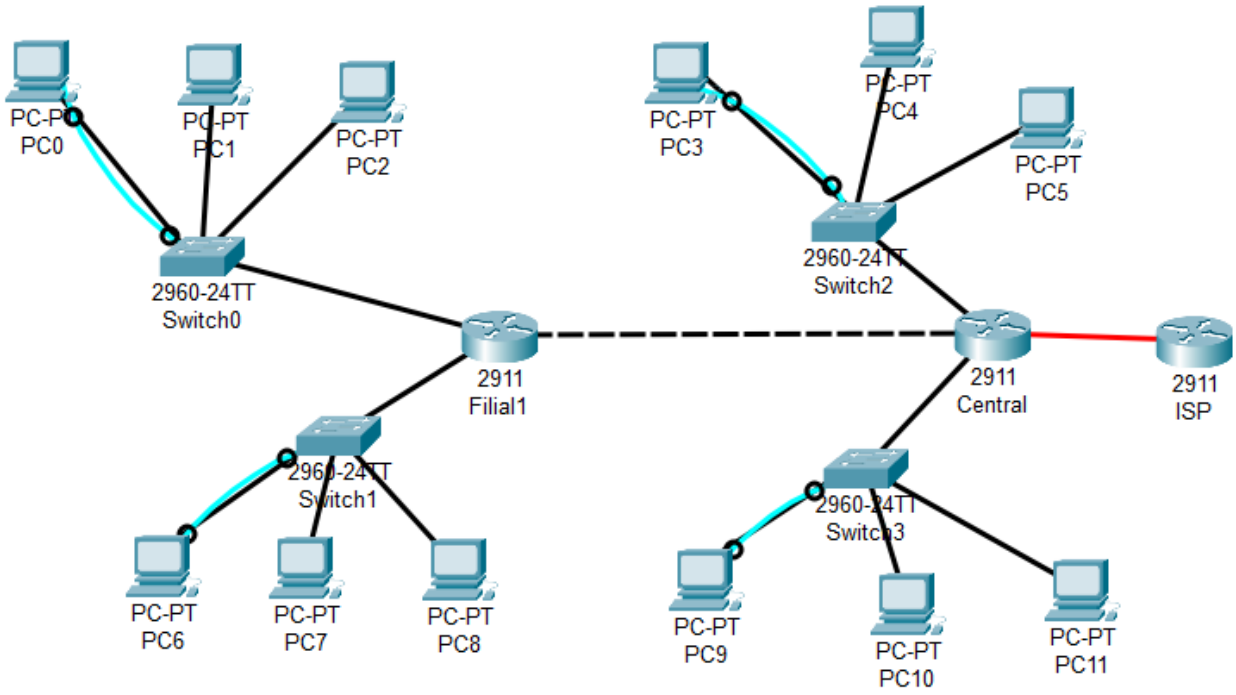


Рисунок 3.1 – Схема телекомунікаційної мережі сучасного офісу

Необхідність налаштування різних видів маршрутів виходить з того, що різні вузли в різних підмережах повинні взаємодіяти між собою (пересилати і отримувати деяку інформацію), а також вузли повинні мати доступ до інтернету шляхом підключення до маршрутизатора ISP. Глобальна мережа моделюється за допомогою loopback інтерфейсу з адресою 8.8.8.8.

Спочатку перевіримо досяжність мереж. З комп’ютера в першій підмережі необхідно направити ехо-запит до комп’ютера в третій під мережі (рис. 3.2)

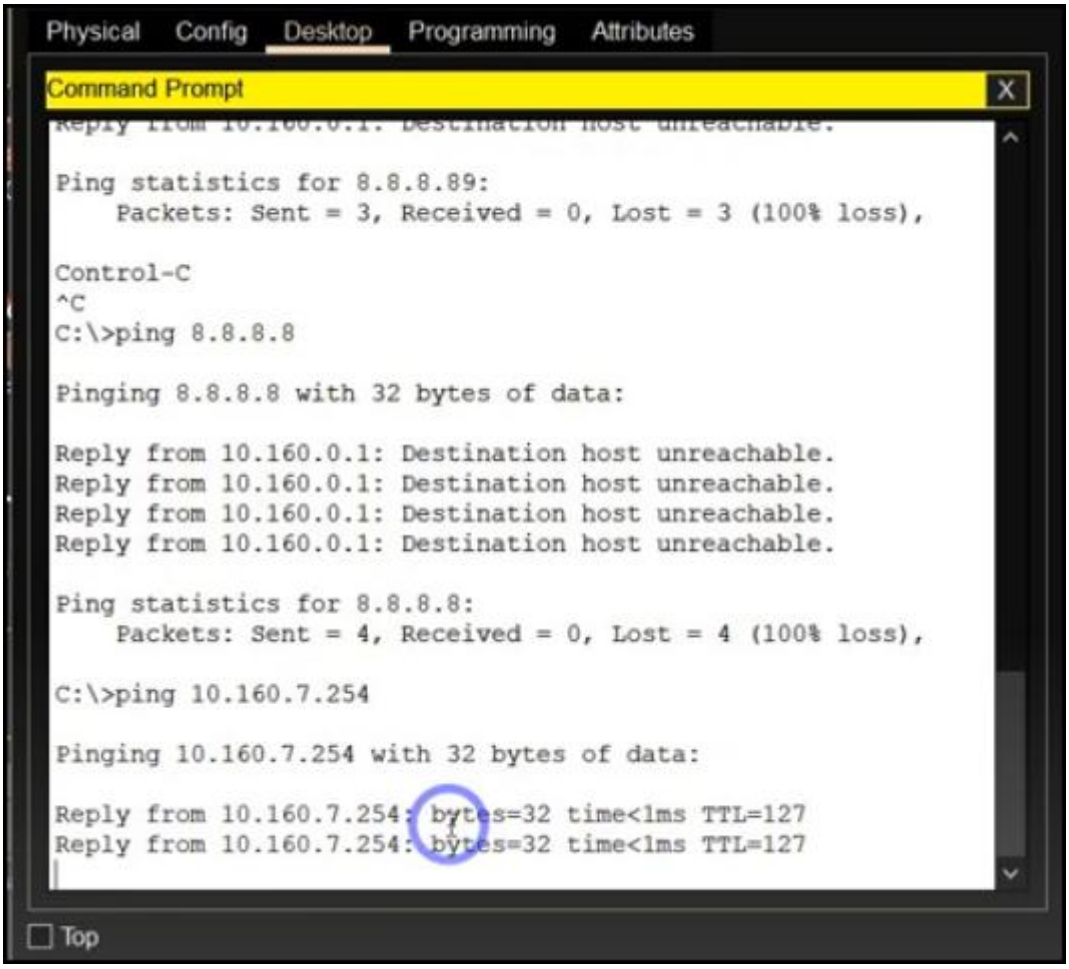


Рисунок 3.2 – Ехо-запит з першої підмережі до третьої підмережі

Відправляємо пакет в другу підмережу– нема, зв’язку з ISP – нема. Маршрутизатори не знають про існування підмереж нашої організації. Інформацію про них треба написати явно в таблиці маршрутизації, що дозволить роутерам правильно відсилати пакети і підтримувати комп’ютерну мережу у працездатному стані. Переглянемо таблиці маршрутизації на кожному роутері. Входимо у вкладку CLI роутера filial1. Таблиці маршрутизації у роутерах — це основний інструмент, за допомогою якого роутер приймає рішення: куди і через який інтерфейс переслати IP-пакет, щоб він досяг свого призначення.

Таблиця маршрутизації — це список маршрутів до різних мереж, де кожен запис описує: до якої мережі належить IP-пакет; через який інтерфейс або шлюз

його потрібно надсилати; яка це була інформація (динамічна, статична, за умовчанням).

Роутер обирає маршрут за такими правилами: найточніше співпадіння маски – перевага надається маршрутам із найбільш специфічною маскою (наприклад, /30 кращий за /24); менша адміністративна відстань (AD) – чим менше, тим пріоритетніший маршрут; краща метрика – залежить від протоколу (OSPF – кількість стрибків, EIGRP – пропускна здатність і затримка). Адміністративна відстань вказує пріоритет маршруту. У командному рядку набираємо команди, як показано на рисунку 3.3.

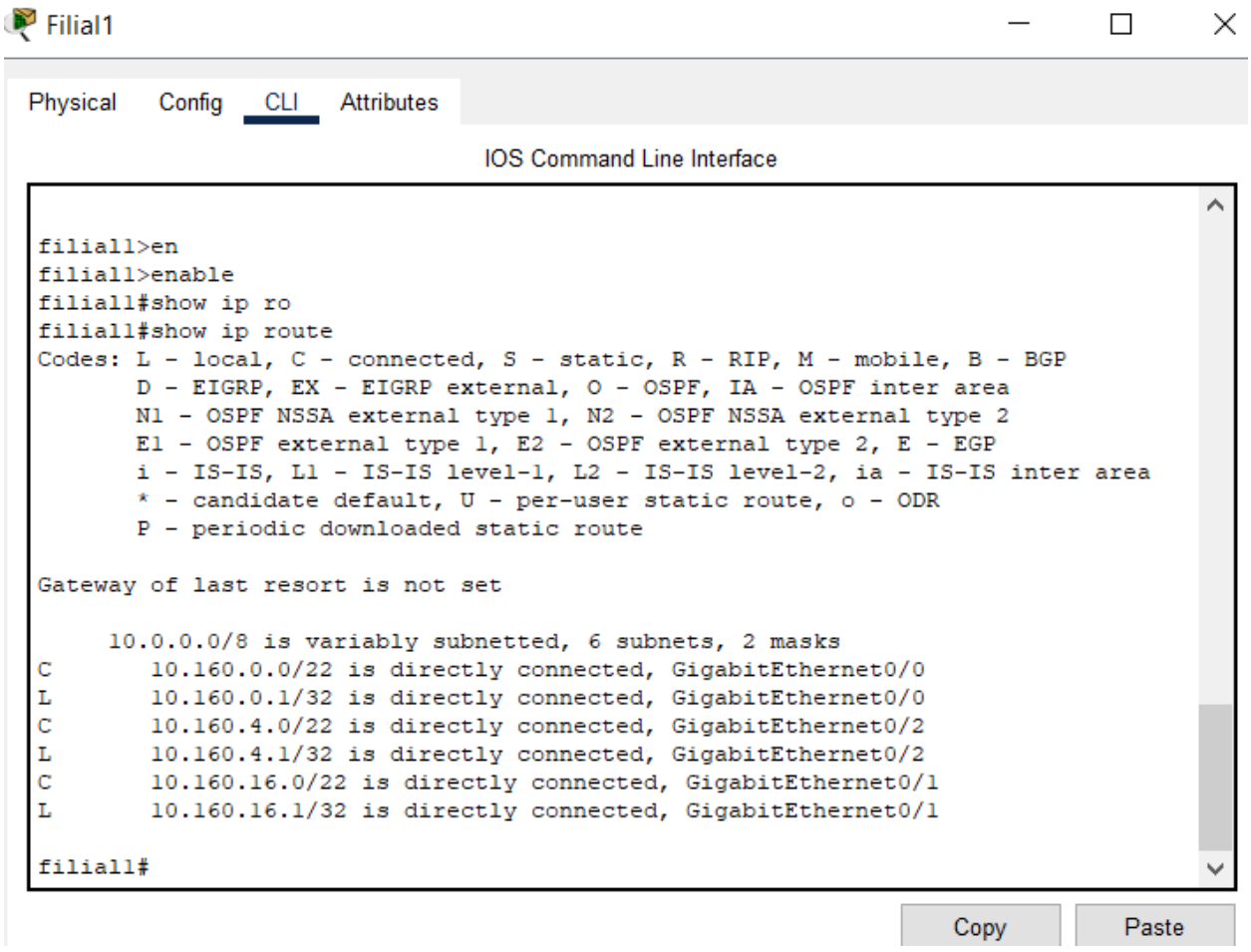


Рисунок 3.3 – Таблиця маршрутизації роутера Filial1

У таблиці маршрутизації є відомості про відомі даному маршрутизатору мережі. Є мітки, які говорять про те, яким чином записи у цю таблицю були додані: C – Connect – це напряму під’єднана мережа – і ми бачимо, що до роутера

під’єднана мережа 10.160.0.0/22. На маршрутизаторі під’єднані напряму три мережі. Маршрутизатор не знає про існування інших підмереж і ISP.

3.2 Налаштування статичних маршрутів

Налаштування статичних маршрутів та маршрутів за умовчанням (default routes) є базовою необхідністю для забезпечення правильного руху даних між різними мережами, особливо якщо вони мають кілька підмереж або вихід в Інтернет.

Маршрутизація — це процес вибору шляху, яким пакет передається до місця призначення.

У маршрутизаторах зберігається маршрутна таблиця, що вказує, куди надсилати пакети залежно від IP-адреси призначення.

Статичні маршрути потрібні, коли: у мережі немає динамічного маршрутизатора (OSPF, EIGRP); є кілька підмереж, і потрібно явно вказати, як до них дістатися; ми хочемо контролювати трафік і мати максимальну передбачуваність маршрутизації.

Маршрут за замовчуванням (Default Route) потрібний, коли немає точного маршруту в таблиці, а пакети все одно потрібно кудись надсилати (наприклад, в Інтернет).

У невеликих мережах або на крайових маршрутизаторах — це основний шлях для всіх маршрутів. Переваги ручного налаштування маршрутів(табл. 3.1).

Таблиця 3.1 – Переваги статичних маршрутів

Перевага	Пояснення
Контроль	Повна передбачуваність шляху трафіку
Безпека	Тільки визначені шляхи, немає ризику «динамічних атак»
Продуктивність	Менше навантаження на CPU маршрутизатора
Простота для малих мереж	Не потрібно впроваджувати складні протоколи

Встановлення статичних маршрутів має такі недоліки: такі маршрути не масштабуються: у великих мережах важко керувати великою кількістю маршрутів; при зміні топології маршрути потрібно вручну оновлювати; відсутнє автоматичне резервування шляхів.

Коли доцільно використовувати різні типи маршрутів: Мала офісна мережа з кількома під мережами – Статичні маршрути; доступ до Інтернету через один шлюз – маршрут за умовчанням; DMZ або специфічні сегменти – статичні маршрути; немає підтримки динамічної маршрутизації – обидва типи.

Проведем налаштування та перевірку статичних маршрутів. На маршрутизаторі Filial1 налаштуємо рекурсивні статичні маршрути до всіх віддалених мереж організації та мереж провайдера (LAN2, LAN4, ISP), вказавши в якості наступного переходу IP-адресу на протилежному кінці інтерфейсу маршрутизатора Central.

Тобто необхідно оголосити маршрутизатор Filial1 і сказати, що у нас існує в нашій топології ще один маршрутизатор (для цього необхідно перейти в режим конфігурації термінал).

Необхідно оголосити, що існує мережа, у якій IP адреса 10.160.8.0. Наступний параметр – вказати маску 255.255.252.0 і далі треба або вказати IP адресу наступного маршрутизатора, або свій вихідний інтерфейс – куди треба відправляти пакети. Вказуємо IP-адресу 10.160.16.2 (рис. 3.4). Це називається рекурсивним статичним маршрутом. Додаємо запис про існування мережі LAN4.

Переваги таблиці маршрутизації: автоматичний вибір маршруту - роутер сам визначає найкращий шлях до мережі; безпека - дозволяє контролювати, які мережі доступні; масштабованість - у великих мережах використовуються динамічні маршрути (OSPF, EIGRP); гнучкість - можна поєднувати статичні і динамічні маршрути.

```
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up


Router>en
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 10.160.8.0 255.255.252.0 10.160.16.2
Router(config)#Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#exit
Router(config)#ip route 10.160.12.0 255.255.252.0 10.160.16.2
Router(config)#ip route 209.165.201.224 255.255.255.240 10.160.16.2
Router(config)#
```

Рисунок 3.4 – Додавання нових маршрутів роутера Filial1

Далі треба вказати, що існує маршрутизатор ISP з адресою 209.165.201.224 з маскою 255.255.255.240. Всі ці маршрути проходять по одному інтерфейсу Gig0/3/0, яким з'єднані обидва маршрутизатори. Продовження налаштування маршрутизатора Filial1 приведено на рис. 3.5.

Filial1

```
filial1>enable
filial1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
filial1(config)#ip route 10.160.8.0 255.255.252.0 ?
  A.B.C.D          Forwarding router's address
  Dialer           Dialer interface
  Ethernet         IEEE 802.3
  FastEthernet     FastEthernet IEEE 802.3
  GigabitEthernet  GigabitEthernet IEEE 802.3z
  Loopback         Loopback interface
  Null             Null interface
  Serial           Serial
  Vlan             Catalyst Vlans
filial1(config)#ip route 10.160.8.0 255.255.252.0 10.160.16.2
filial1(config)#ip route 10.160.12.0 255.255.252.0 10.160.16.2
filial1(config)#ip route 209.165.201.224 255.255.255.240 10.160.16.2
filial1(config)#
```

Copy Paste

Рисунок 3.5 – Довідка при налаштуванні маршрутизатора Filial1

І далі треба вказати IP адресу наступного переходу. Як змінилась таблиця маршрутизації можна дізнатись за командою show IP route (рисунок 3.6).

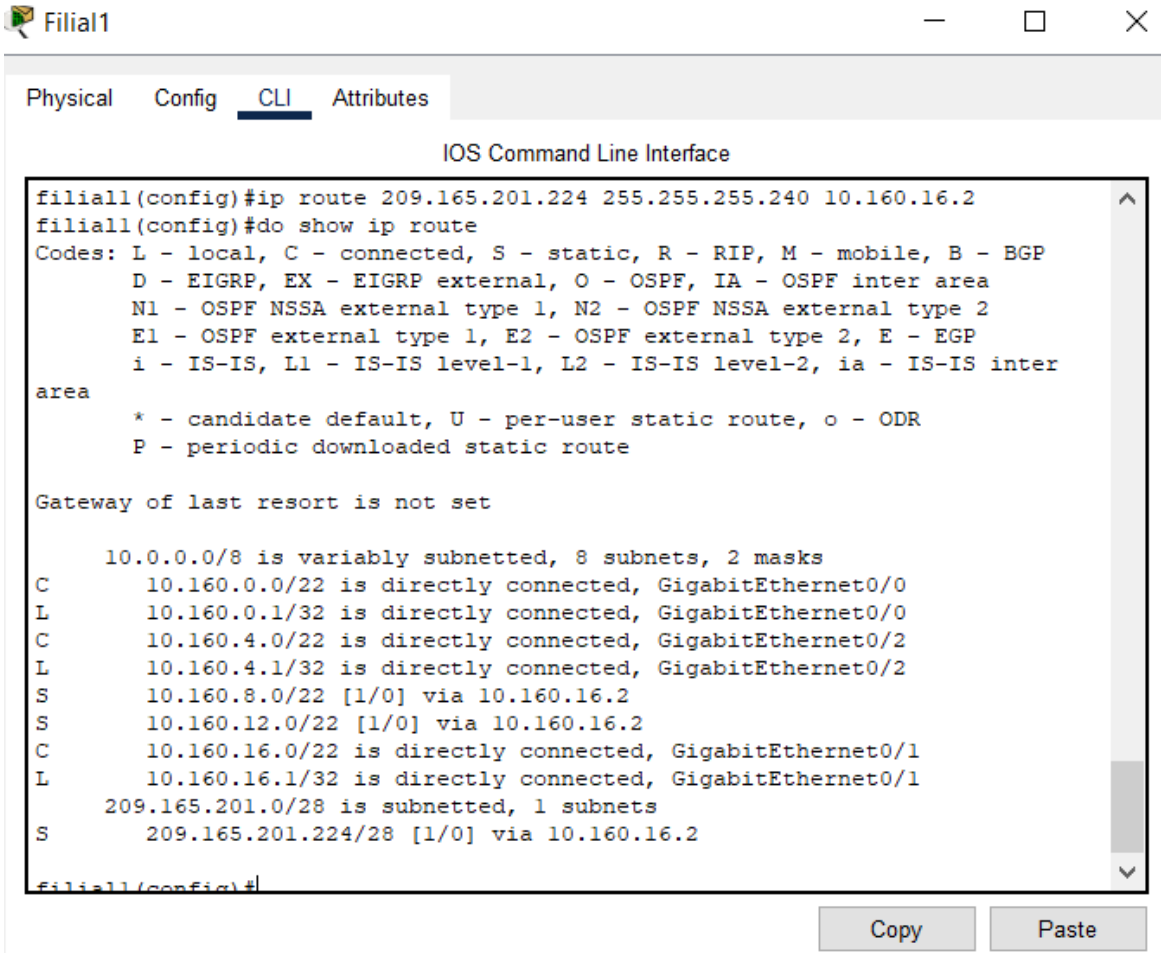


Рисунок 3.6 – Таблиця маршрутизації роутера Filial1

Появились три нових записи з поміткою S – це означає, що вони додані статично.

Після оголошення мережі та префікса в квадратних дужках вказується адміністративна відстань. Для статичних маршрутів вона дорівнює одиниці. Чим менше значення адміністративної відстані – тим більш надійний цей маршрут. Після слеша вказується метрика – оскільки це статичний маршрут (не враховується пропускна здатність), то метрика дорівнює нулю. Далі вказується наступна IP адреса.

Ці записи називаються рекурсивними тому, що коли маршрутизатор отримує пакети, мережна частина яких відповідає LAN2, маршрутизатору треба

знати – через який свій інтерфейс треба відправляти ці пакети. Тому, коли пакет надійде до роутера – він подивиться по таблиці маршрутизації і визначить, що його треба відправити на адресу 10.160.16.2. Але до якого інтерфейсу ця адреса належить – визначається ще одним переглядом таблиці маршрутизації, де буде визначатись, що ця адреса належить інтерфейсу GigabitEthernet0/2.

При симуляції відправки пакетів і перевірці роботи таблиці маршрутизації від PC1 до PC9 ми маємо такі результати (рисунок 3.7):

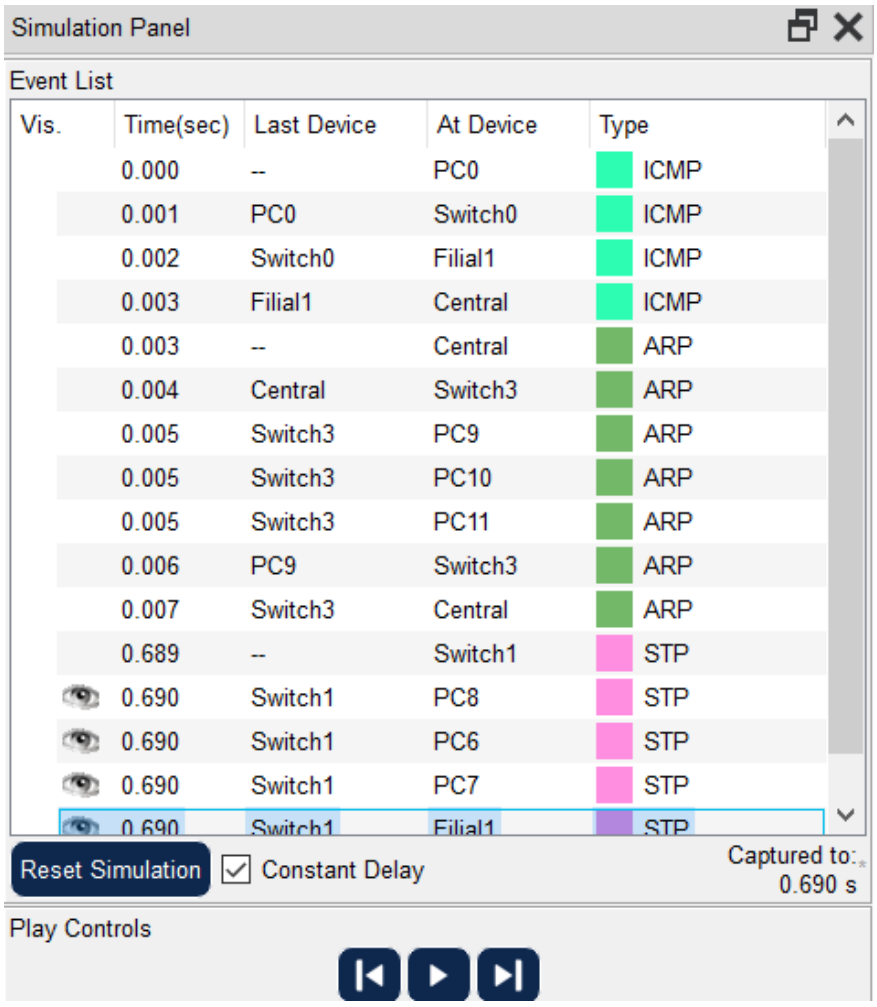


Рисунок 3.7 – Перевірка роботи таблиці маршрутизації від PC1 до PC9

Налаштуємо маршрутизатор Central. Він не знає про існування мереж LAN1 і LAN2. На маршрутизаторі Central необхідно налаштувати безпосередньо підключені статичні маршрути до віддалених мереж (LAN1, LAN2) і вказати відповідний інтерфейс. Введення статичних маршрутів до вказаних мереж у вікні налаштування маршрутизатора Central має вигляд (рис. 3.8):

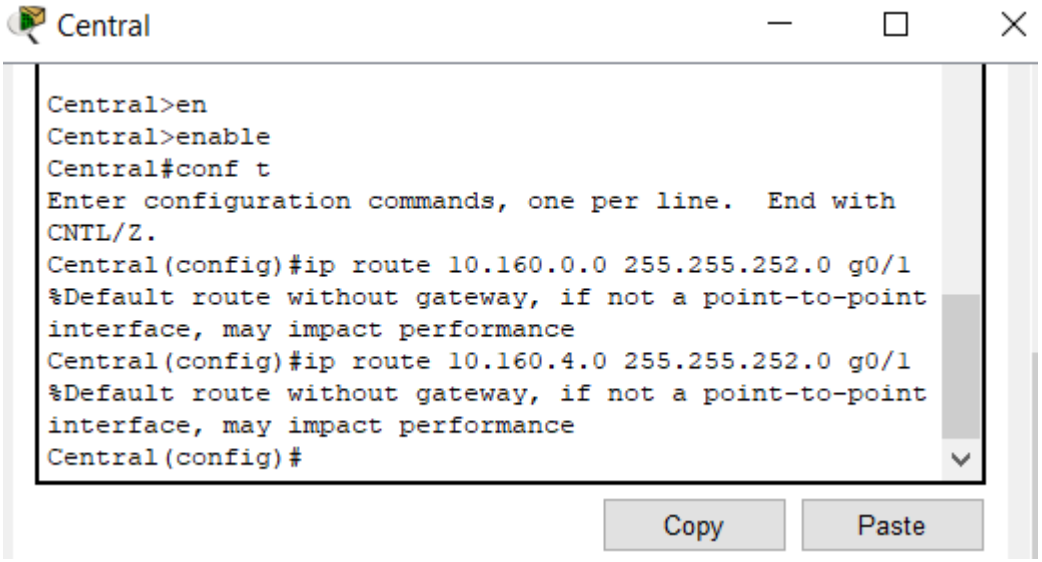


Рисунок 3.8 – Вікно налаштування маршрутизатора Central

Налаштування таблиці маршрутизації маршрутизатора Central (рис. 3.9).

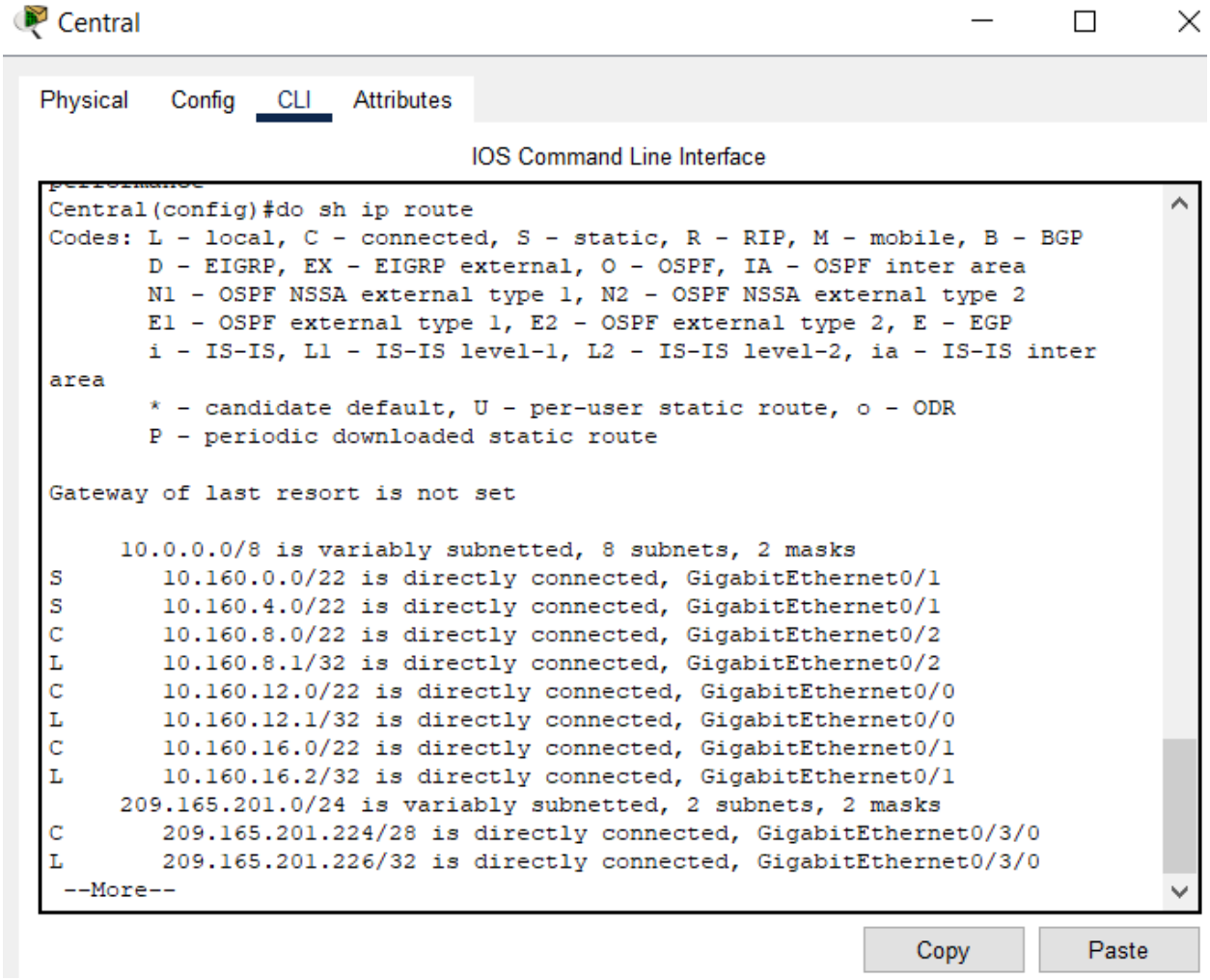


Рисунок 3.9 – Таблиця маршрутизації маршрутизатора Central

Ми бачимо відомості про існування двох введених статичних маршрутів.

Далі необхідно налаштувати маршрутизатор ISP. На даний момент таблиця маршрутизації приведена на рисунку 3.10.

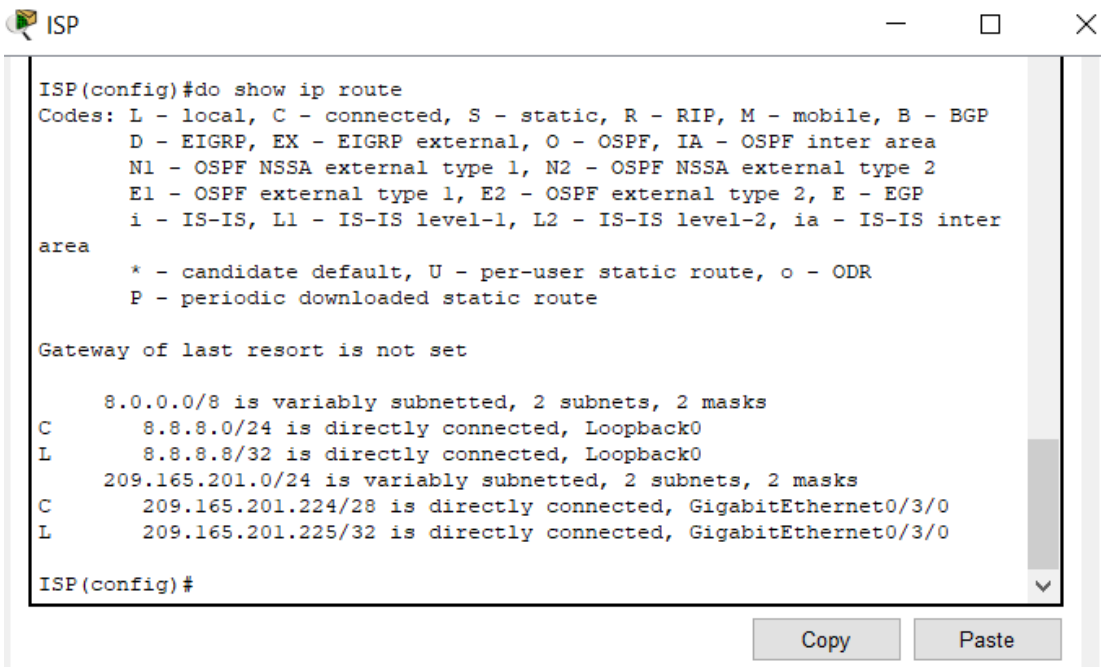


Рисунок 3.10 – Таблиця маршрутизації маршрутизатора ISP

Ми бачимо локальні маршрути і пряме з’єднання пристроїв. Про існування мережи 10.160.0.0 провайдер не знає, тому треба додати відповідні налаштування.

На рисунку 3.11 приведена таблиця маршрутизації роутера ISP. У таблиці маршрутизації кожен запис вказує на те, як і куди може бути направлений IP-трафік. Записи мають маркування (букви), які позначають тип маршруту. Найбільш базові з них:Connected – безпосередньо підключена мережа (інтерфейс маршрутизатора має IP з цієї мережі); Local – IP-адреса самого інтерфейсу маршрутизатора; Static – Статично заданий маршрут вручну. Connected означає, що маршрутизатор має фізичний або логічний інтерфейс, який підключений безпосередньо до цієї мережі. Local – це IP-адреса інтерфейсу самого маршрутизатора, яка належить до підключеної мережі. Static – маршрут, який вручну налаштовується адміністратором. Він використовується для направлення трафіку до мереж, які не є безпосередньо підключеними.

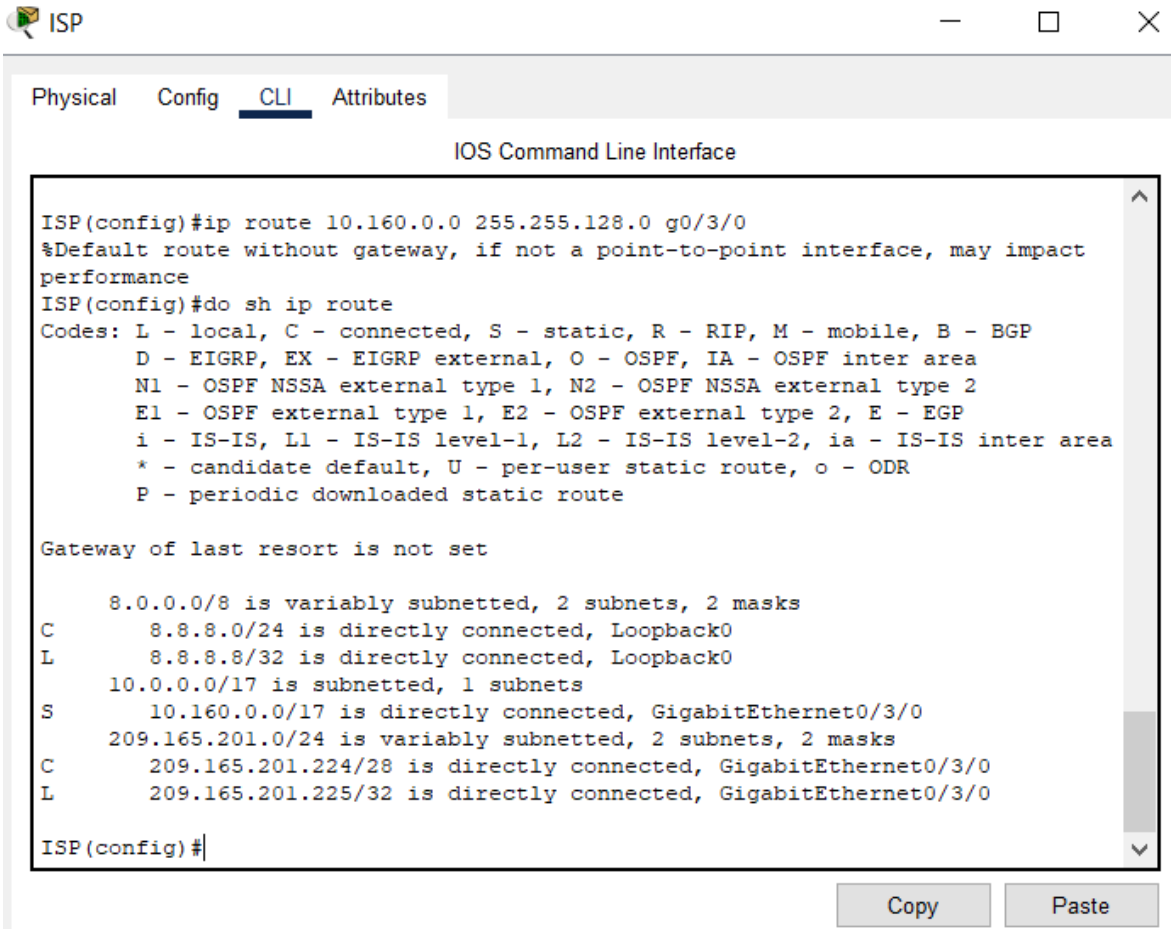


Рисунок 3.11 – Оновлена таблиця маршрутизації маршрутизатора ISP

Далі необхідно перевірити досяжність мереж, відправивши ехо-запити на пристрої в різних підмережах. Перевірка досяжності мереж після складання таблиці маршрутизації – це критично важливий крок у налаштуванні комп'ютерної мережі, оскільки навіть правильно записані маршрути не гарантують, що трафік дійсно досягне призначення. Перевірка досяжності необхідна: для виявлення помилок - у таблиці маршрутизації можуть бути неправильно вказані IP-адреси шлюзів, маски або інтерфейси; для перевірка активності маршруту - випадку, якщо шлюз може бути недоступним або інтерфейс вимкнений; для перевірка фізичної доступності - кабель, порт, або пристрій на іншому кінці можуть бути несправні; для перевірки наявності зворотного маршруту - пакет може дійти до кінцевої точки, але відповідь не повернеться без правильного зворотного маршруту; для визначення

продуктивності і затримки - визначення, наскільки стабільне і швидке з’єднання. Встановлення зв’язку між мережами LAN1 і LAN3 показано на рисунку 3.12.

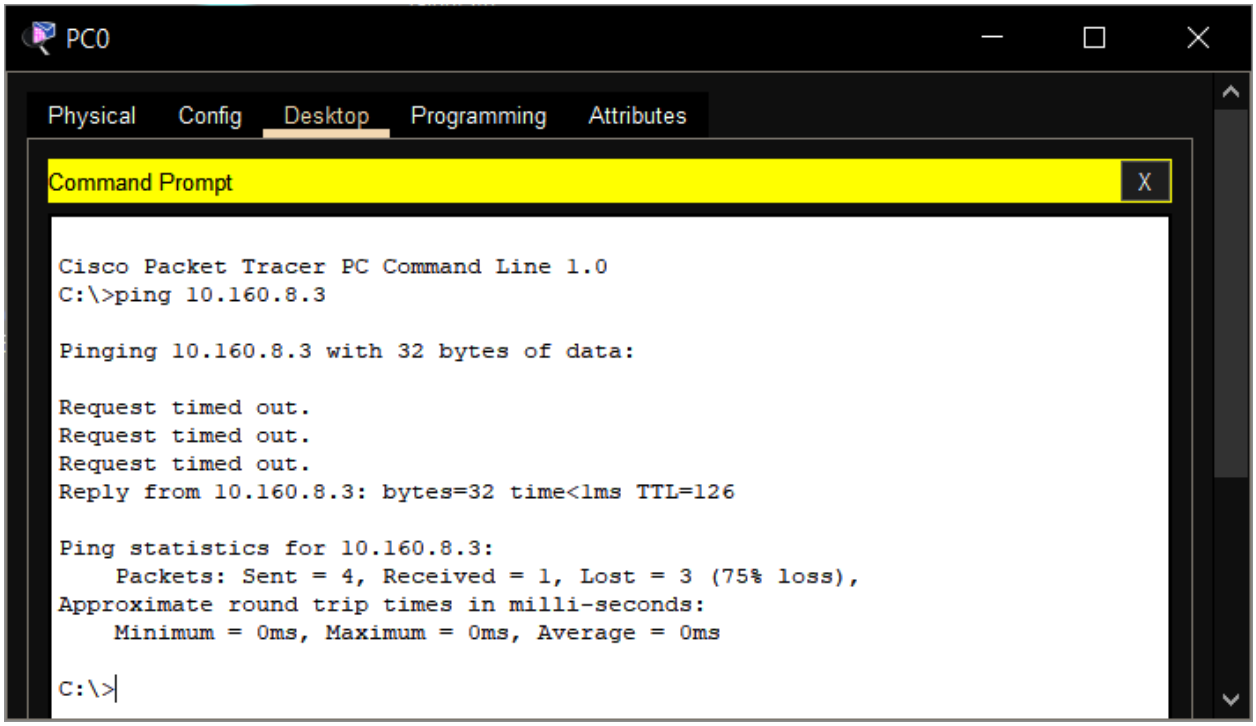


Рисунок 3.12 – Встановлення зв’язку між мережами LAN1 і LAN3

Видно, що перші три ехо-запити залишились без відповіді через прописування таблиць маршрутизації. Всі подальші запити проходять без збоїв. Перевірка дозволяє визначити: чи відповідає IP-адреса шлюзу реальній адресі; чи активні інтерфейси на обох пристроях; чи можна пропінгувати задану адресу; чи є зворотний маршрут з тієї мережі. Навіть правильно побудована таблиця маршрутизації не гарантує зв’язку, якщо не перевірена фактична доступність хостів, інтерфейсів і шлюзів. Тестування — це обов’язковий етап для пошуку проблем і впевненості у працездатності мережі.

Встановлення зв’язку між мережами LAN1 і LAN4 показано на рисунку 3.13. Тут залишився без відповіді тільки перший ехо-запит. І затримка відповідає надійному і якісному зв’язку.

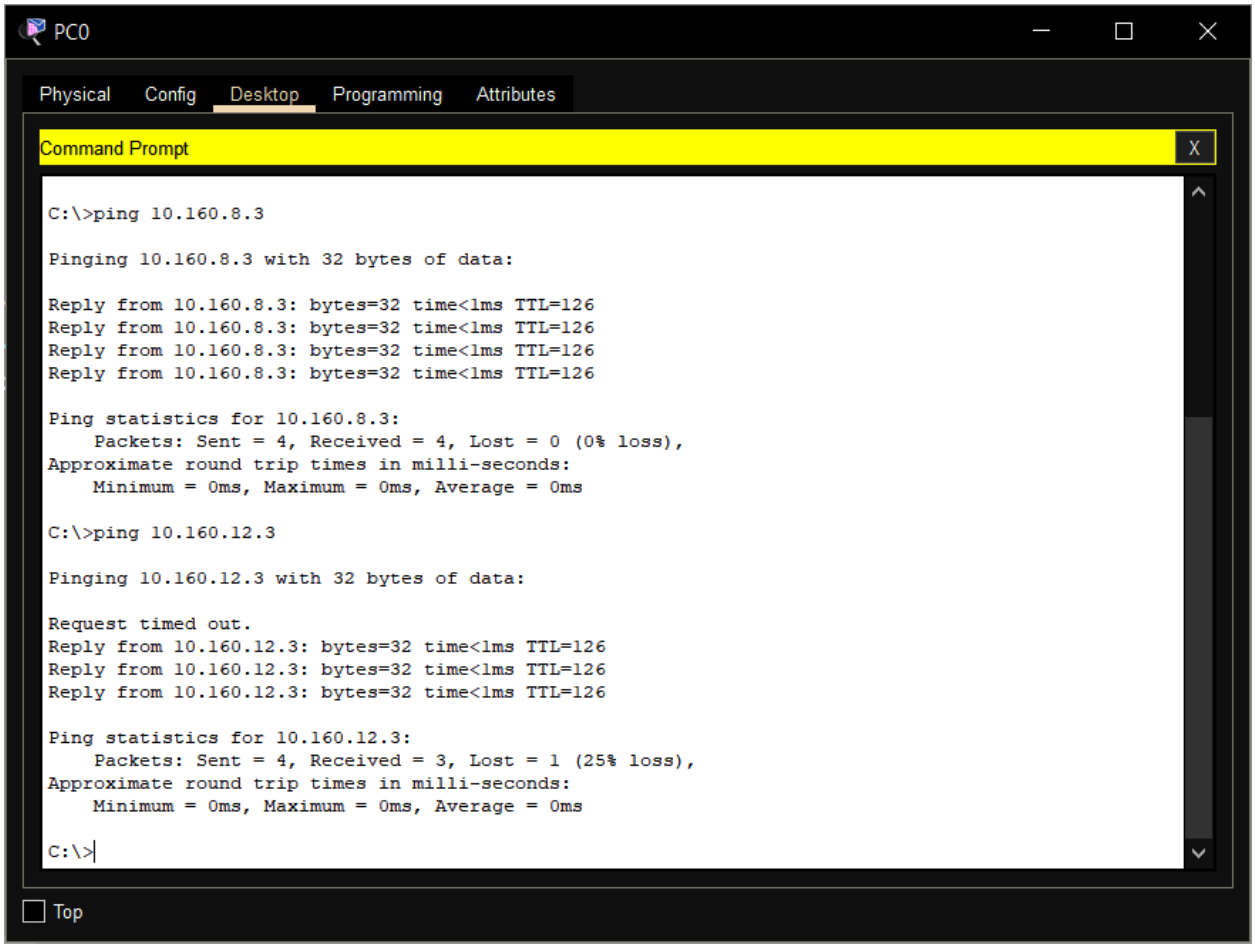


Рисунок 3.13 – Встановлення зв’язку між мережами LAN1 і LAN4

Пропінгуємо мережу провайдера. Доступність мережі провайдера — це здатність інфраструктури інтернет-провайдера забезпечувати стабільний, безперервний і якісний зв'язок для клієнтів у будь-який час. Це ключовий показник надійності послуг зв'язку. Основні характеристики доступності мережі провайдера наступні: безперервність - наскільки довго мережа працює без збоїв; наявність резервування - чи є резервні канали і обладнання, які автоматично замінюють основні у разі збою; моніторинг і керування - провайдер постійно слідкує за станом мережі за допомогою NMS-систем, що дозволяє швидко виявити та усунути проблеми; пропускна здатність - чи може мережа витримувати великі обсяги трафіку без втрат і затримок; захищеність мережі - наявність захисту від атак (DDoS, фільтрація, IDS/IPS) впливає на стабільність зв'язку; якість обладнання - надійні маршрутизатори, комутатори, сервери — основа стабільної роботи мережі. Доступність мережі провайдера показана на рис. 3.14.

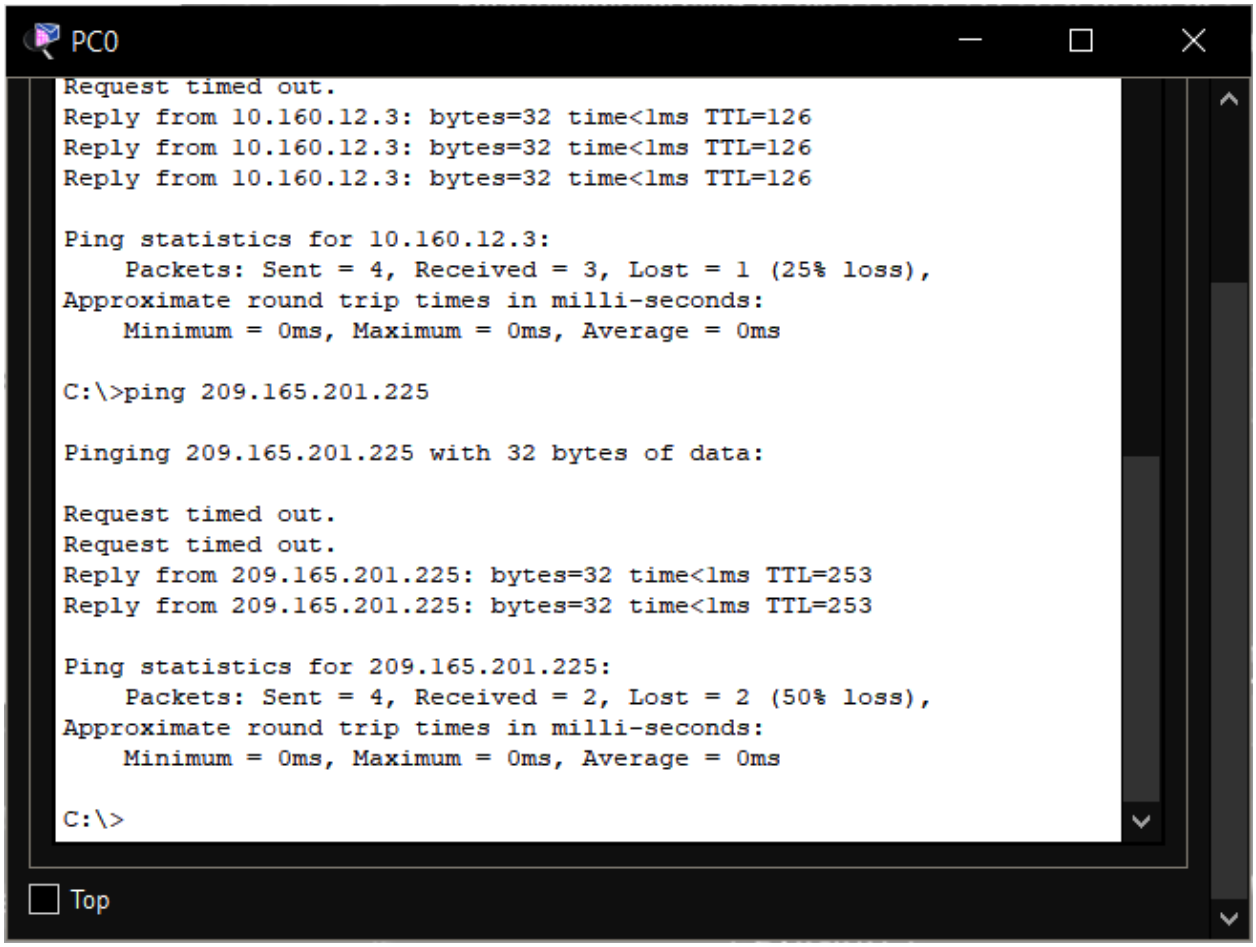


Рисунок 3.14 – Результат перевірки доступності мережі провайдера

Доступність мережі провайдера - це відповідь на запитання: чи працює інтернет, коли він потрібен, і наскільки добре. Якщо мережа провайдера: часто «падає» свідчить про низьку доступність; не має резервування свідчить про підвищений ризик відключень; не моніториться - свідчить про те, що мережа довго відновлюється після збоїв.

Видно, що через встановлення таблиці маршрутизації загубились тільки перші два ехо-запити. Зв’язок встановлено В панелі симуляції виводиться така інформація: Time - час події в симуляції (не реальний час, а покроковий таймер); Last Device - вузол, який відправив або обробив пакет на цьому етапі; At Device - вузол, який зараз обробляє пакет; Type - тип протоколу пакету (ICMP, ARP, IP, TCP, DNS, HTTP тощо); Event - опис дії — надсилання, прийом, передача, помилка; Info - Деталі пакета: 'ICMP Echo Request'. Панель симуляції для перевірки зв’язку між вузлами PC0 і PC11 показана на рисунку 3.15.

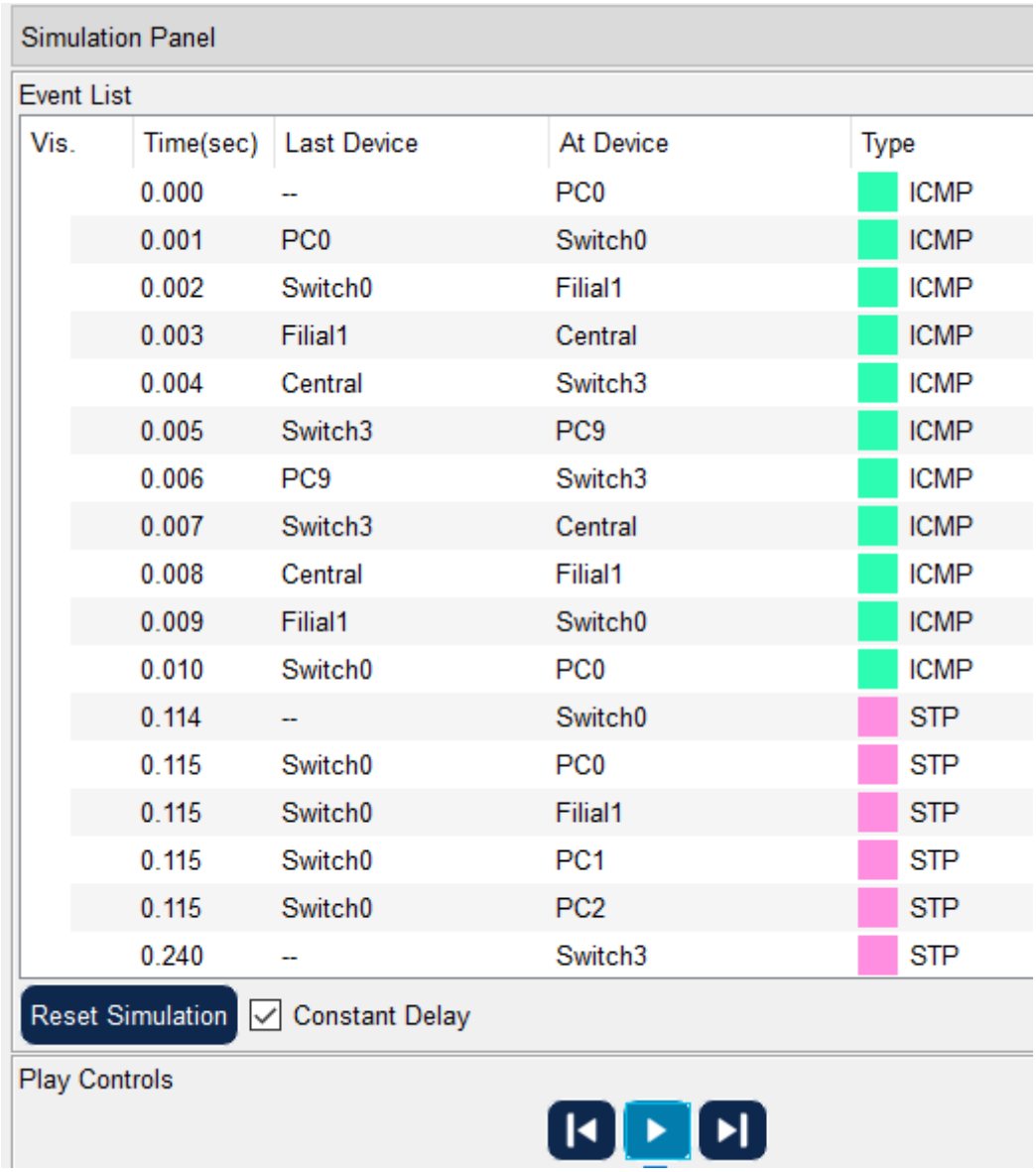


Рисунок 3.15 – Панель симуляції для перевірки зв’язку між PC0 і PC11

Далі необхідно прописати маршрути за замовчуванням таким чином, щоб пакети доходили до вузла призначення. Для цього спочатку виберемо маршрутизатор Filial1 і налаштуємо маршрут за замовчуванням з відповідною IP-адресою наступного переходу. Маршрутизатори такого типу, як Filial1 називають тупіковими тому, що від нього маршрути далі не ідуть. В якості вузла призначення є тільки єдиний шлях. Іншого шляху нема (нема інших шляхів з іншими маршрутизаторами). Тому можна вказати єдиний статичний маршрут. Всі раніше зроблені статичні маршрути можна видалити і зробити єдиний статичний маршрут.

Зо командою do show running config ми виведемо налаштування маршрутизатора:

```
ip classless
ip route 10.160.8.0 255.255.252.0 10.160.16.2
ip route 10.160.12.0 255.255.252.0 10.160.16.2
ip route 209.165.201.224 255.255.255.240 10.160.16.2
```

І перед кожною командою налаштування маршрута напишемо приставку No. Всі маршрути можна скопіювати в текстовий документ і додати no, а потім ці команди виконати в режимі конфігурування термінала.

```
no ip route 10.160.8.0 255.255.252.0 10.160.16.2
no ip route 10.160.12.0 255.255.252.0 10.160.16.2
no ip route 209.165.201.224 255.255.255.240 10.160.16.2
```

І додати нову команду:

```
Filial1(config)#ip route 0.0.0.0 0.0.0.0 10.160.16.2
Filial1(config)#
```

Далі треба вибрати маршрутизатор Central і оголосити маршрут за замовчуванням до постачальника послуг інтернету. Маршрутизатор Central не тупіковий – у нього є зв’язки з іншими маршрутизаторами і записані раніше статичні маршрути треба залишити.

У режимі конфігурації терміналу треба створити новий статичний маршрут: всі пакети з IP-адресами, що не належать нашій організації – направляти на маршрутизатор постачальника послуг інтернету (рис. 3.16).

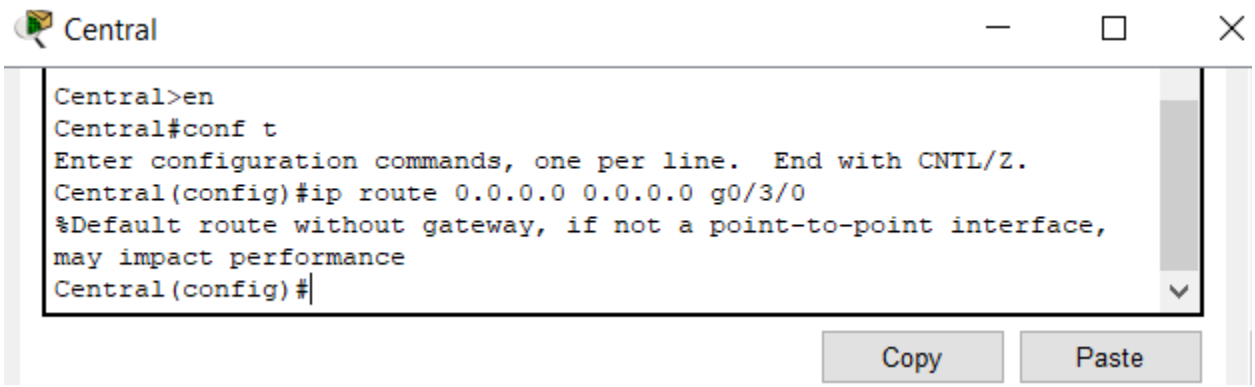


Рисунок 3.16 – Введення нового статичного маршруту

Далі за командою : do sh ip route ми виводимо оновлену таблицю маршрутизації, яка приведена на рисунку 3.17.

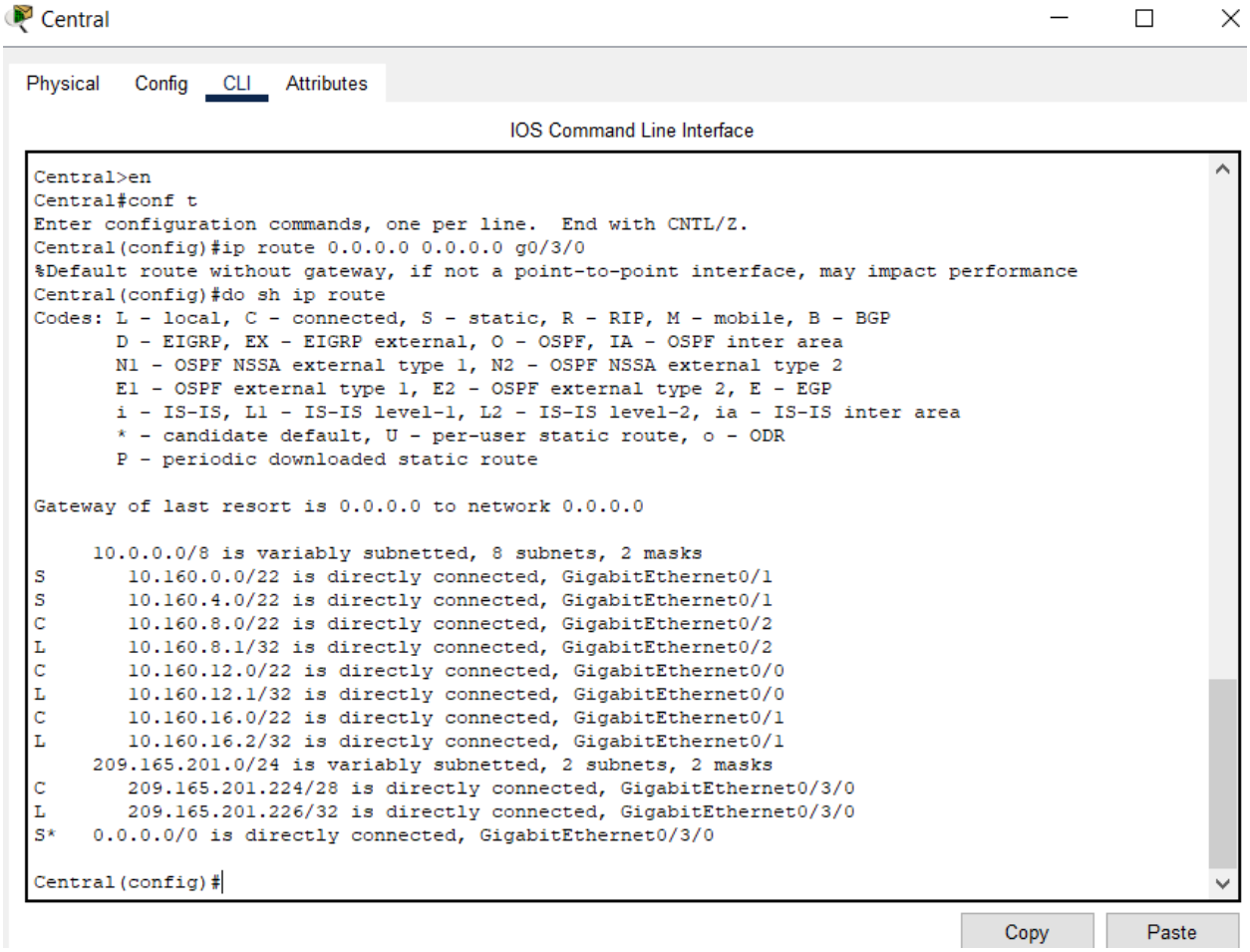


Рисунок 3.17 – Оновлена таблиця маршрутизації маршрутизатора Central

Панель Simulation – це потужний інструмент для: навчання мережевих протоколів, налагодження зв’язку, виявлення помилок маршрутизації, VLAN, ACL, NAT, розуміння, що саме і де виходить з ладу.

Останній запис таблиці маршрутизації – статичний маршрут з зірочкою означає, що це статичний маршрут за замовчуванням.

Далі перевіримо досяжність мереж, як показано на рисунку 3.18.

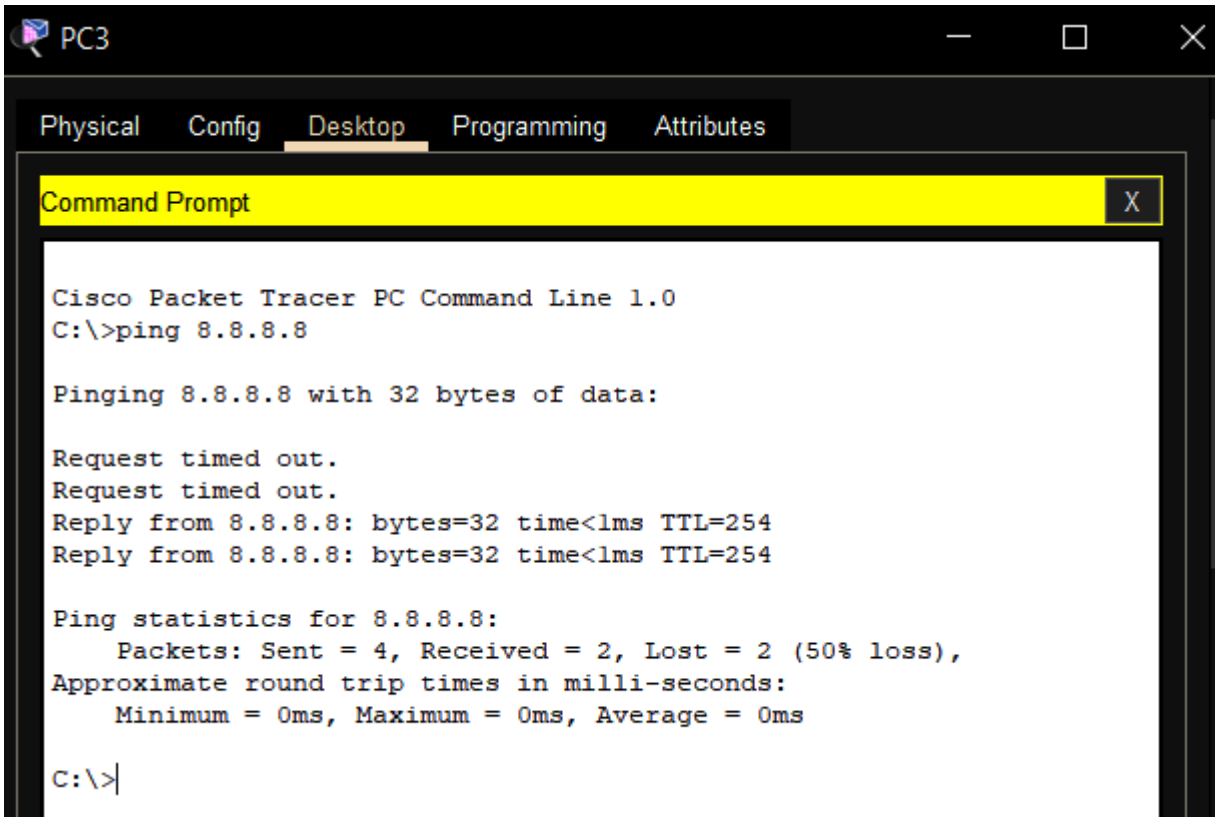


Рисунок 3.18 – Перевірка досяжності мережі провайдера

З рисунку видно, що цей маршрут доступний, а перші два ехо-запити без відповіді свідчать про прокладання таблиці маршрутизації.

Дослідження передачі пакетів між PC0 і PC11 з використанням Traffic Generator. Налаштування вікна Traffic Generator вузла PC0 показано на рис. 3.19.

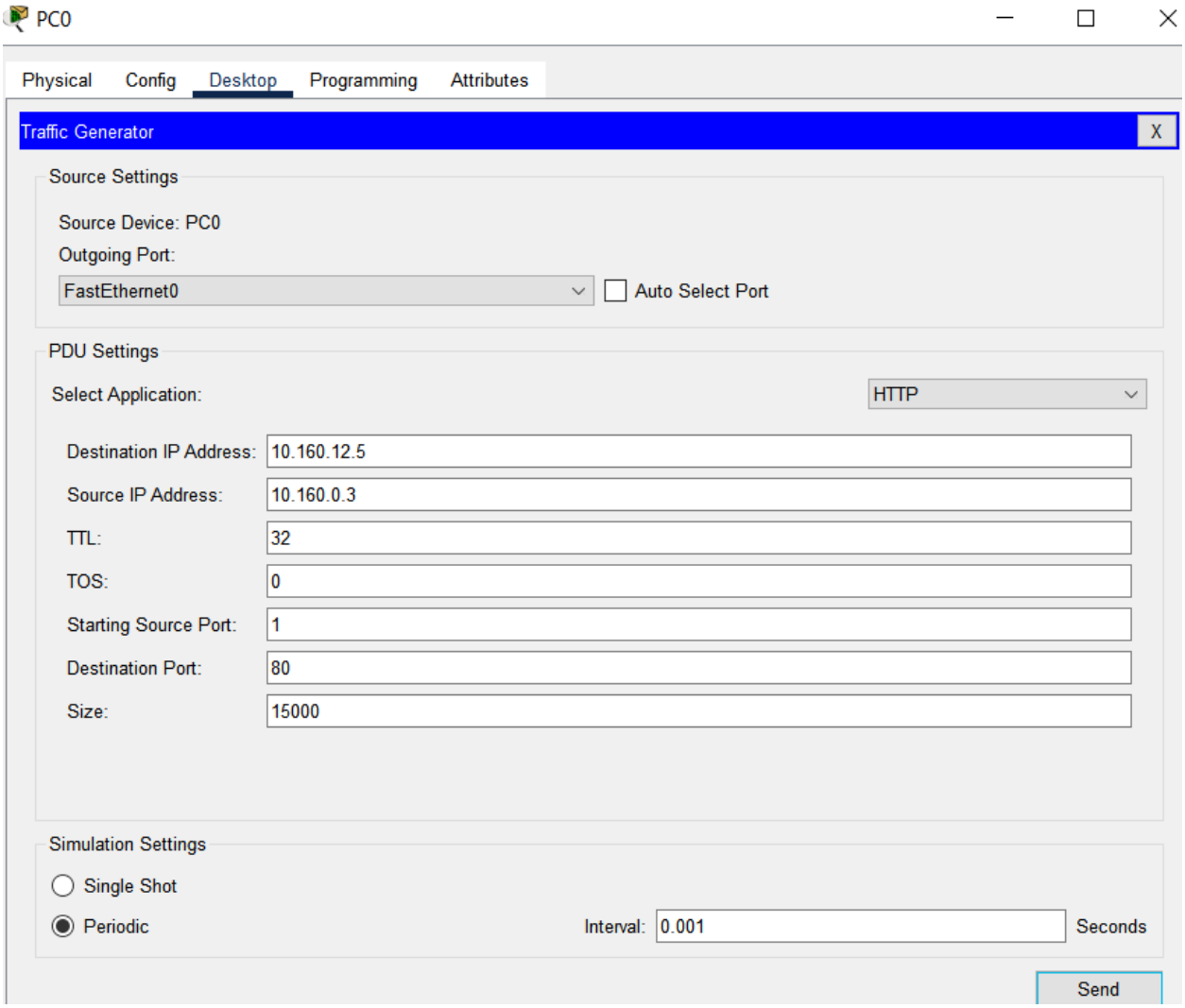


Рисунок 3.19 – Налаштування вікна Traffic Generator вузла PC0

Симуляція режиму передачі пакетів мережею показано на рисунку 3.20.

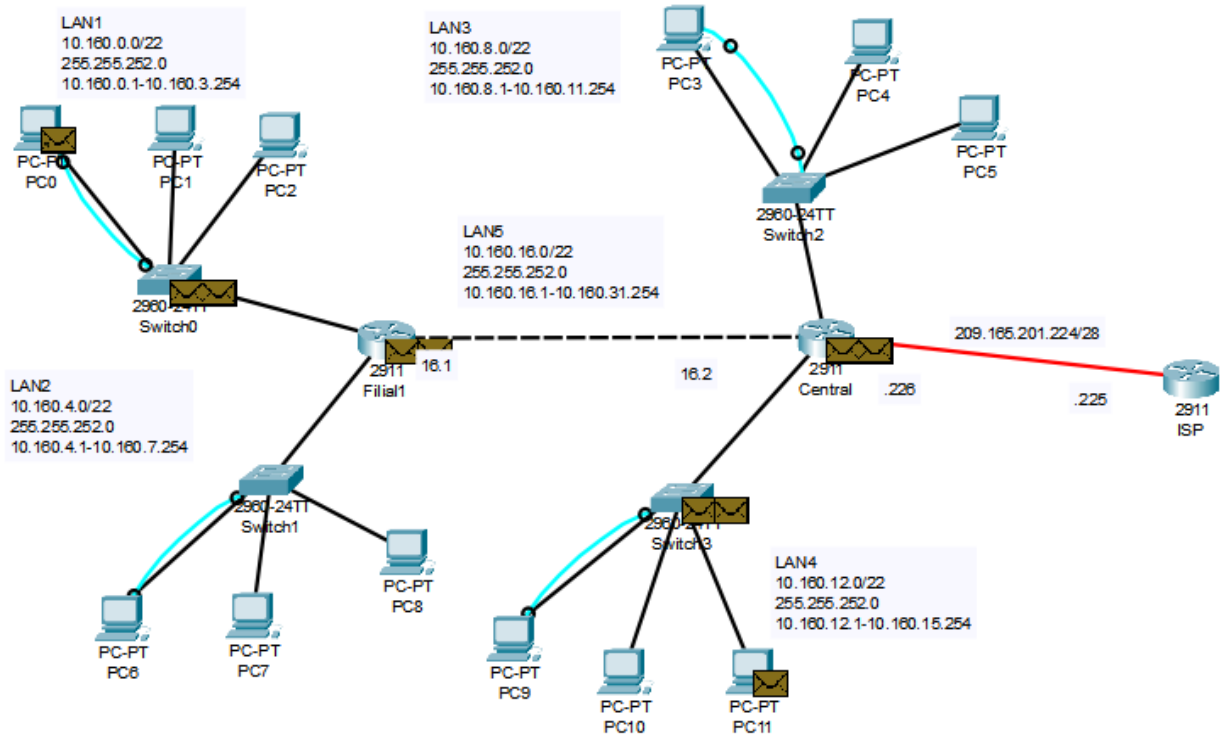


Рисунок 3.20 – Симуляція режиму передачі пакетів мережею

Вікно режиму симуляції показано на рисунку 3.21.

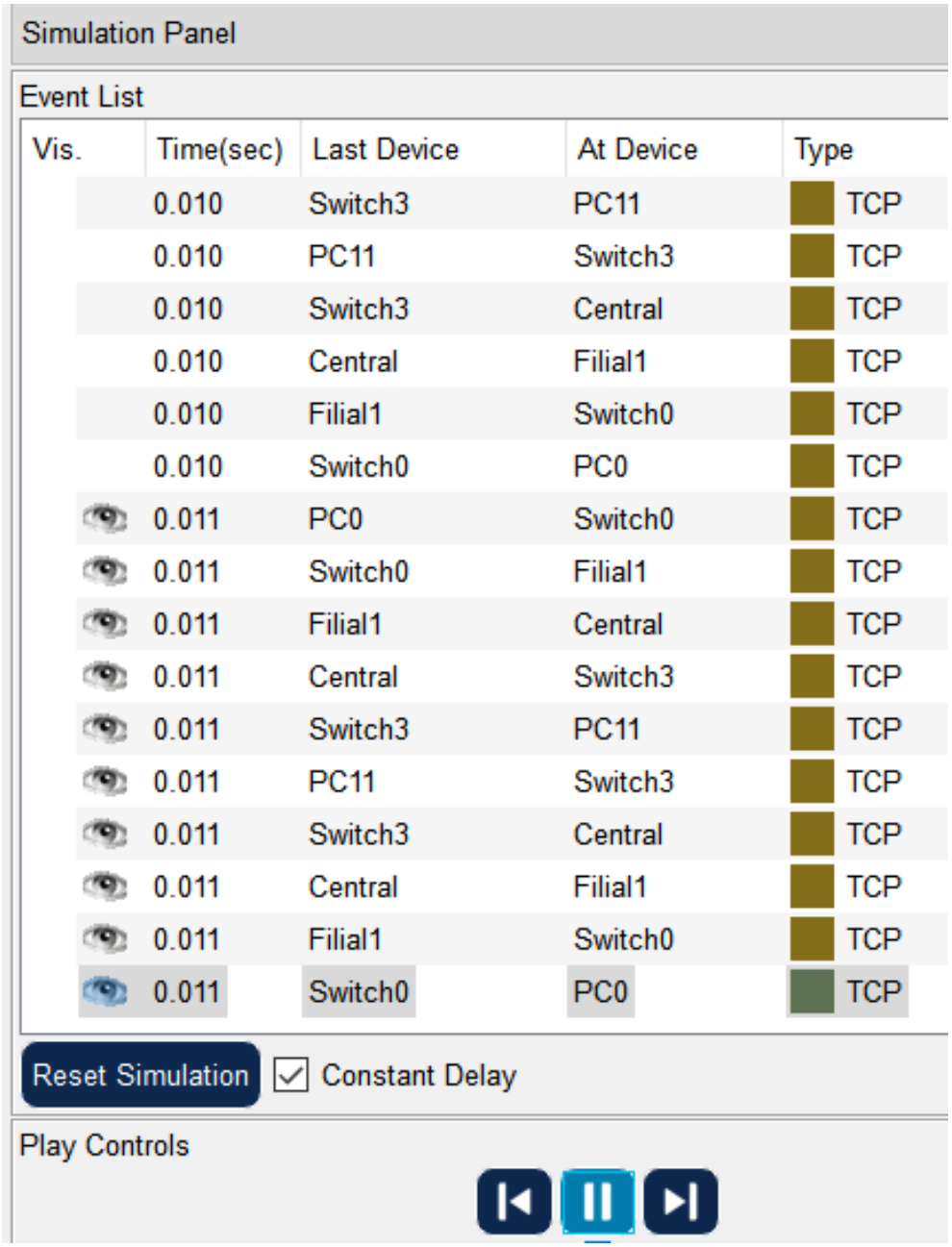


Рисунок 3.21 – Вікно режиму симуляції

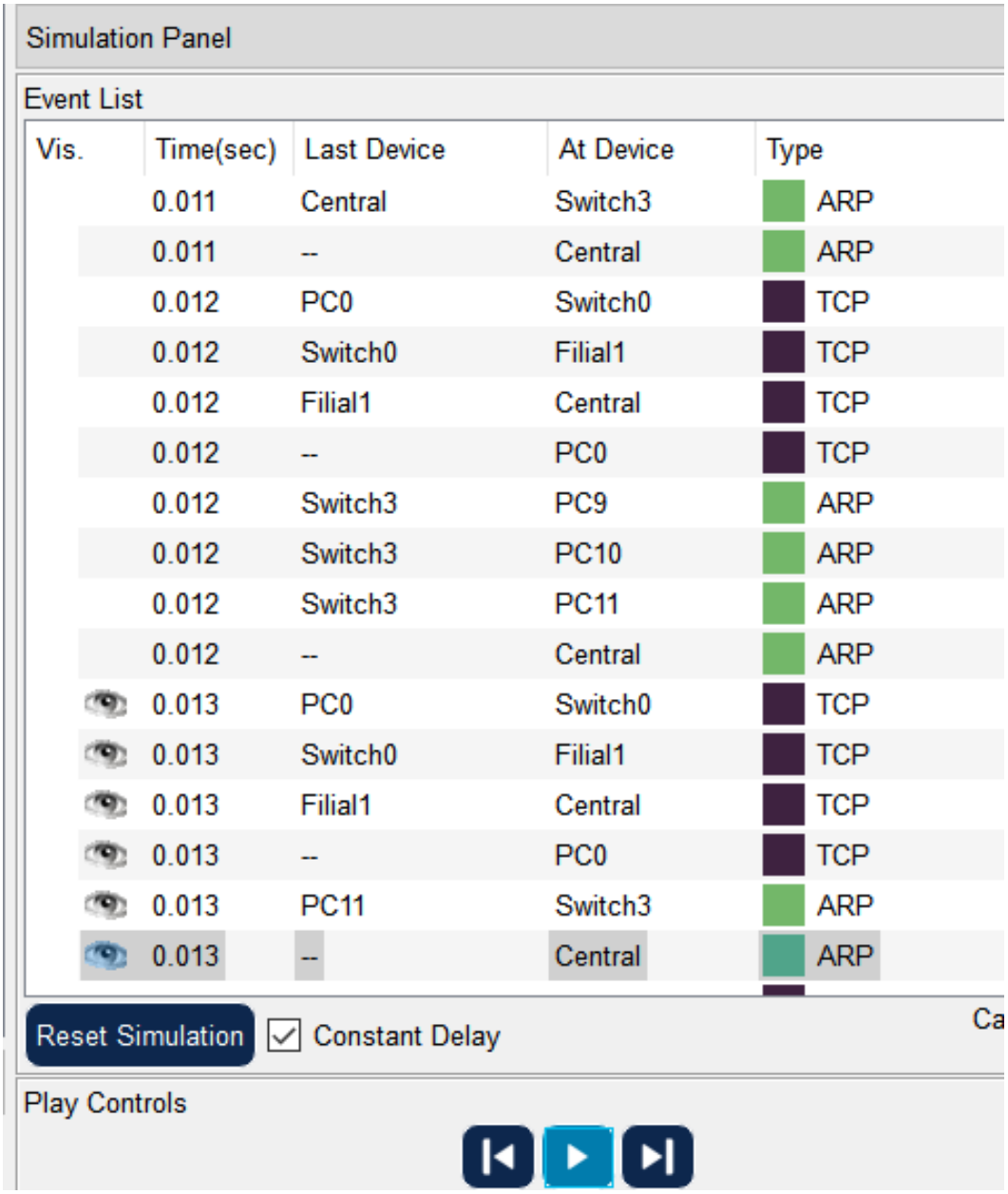


Рисунок 3.22 – Вікно режиму симуляції

Пінгування комп’ютера 10.160.12.5 приведено на рисунку 3.23.

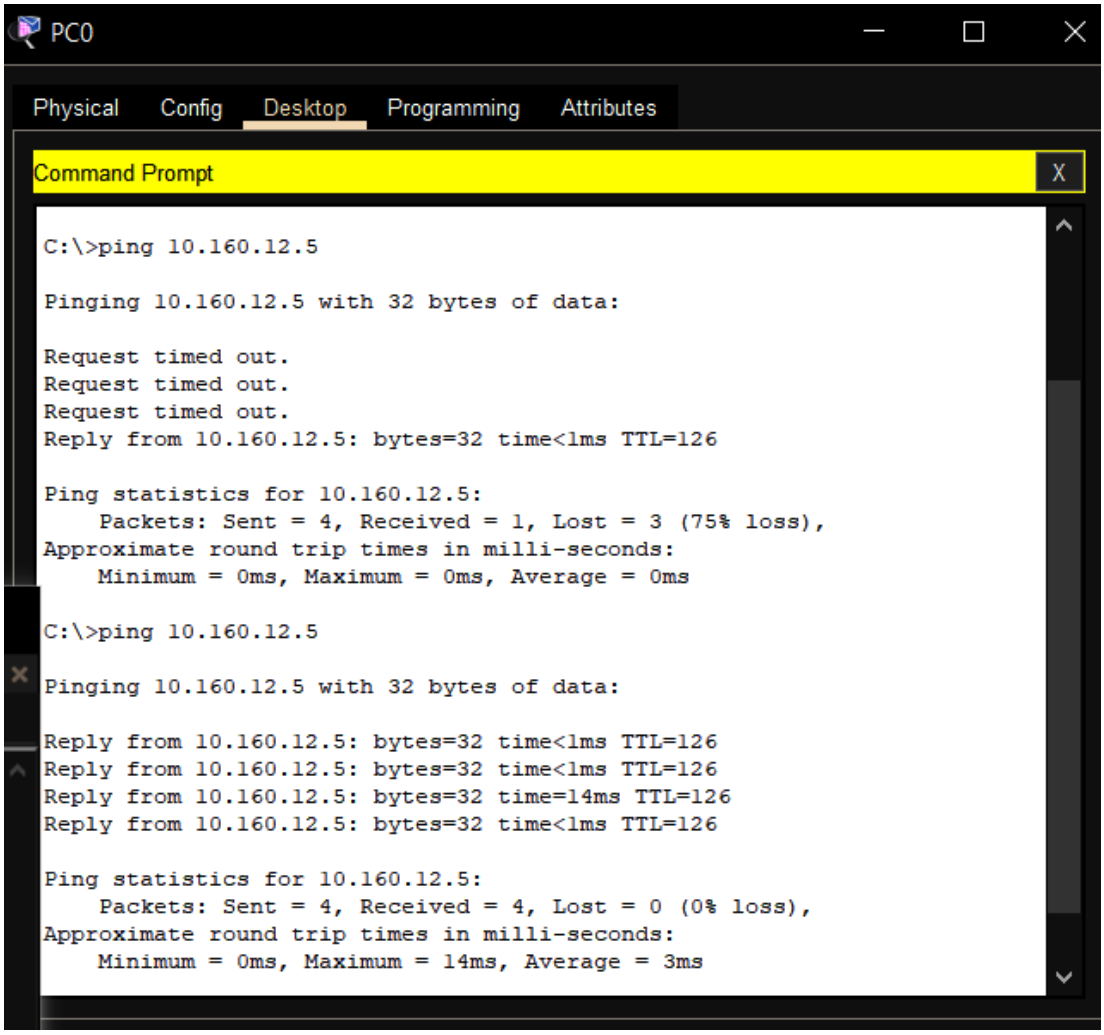


Рисунок 3.23 – Пінгування вузла 10.160.12.5

Трасування шляху проходження пакетів від PC0 до PC11 приведено на рисунку 3.24.

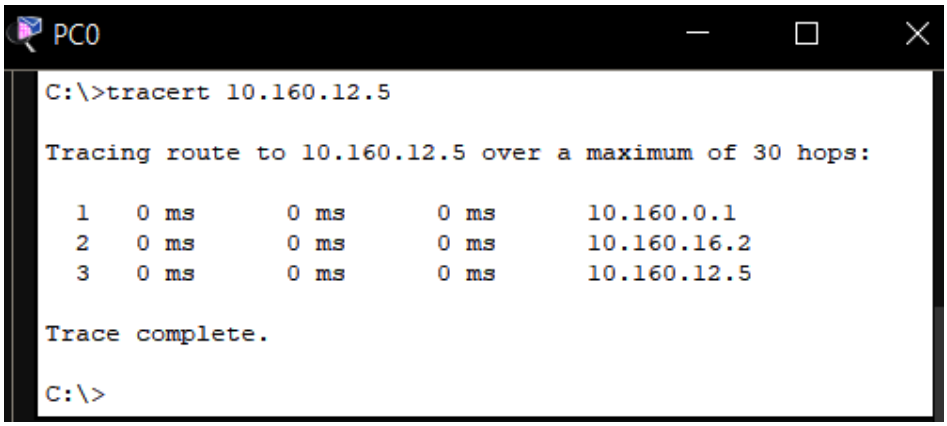


Рисунок 3.24 – Трасування шляху проходження пакетів від PC0 до PC11

Проведемо симуляцію передачі пакетів між PC5 і PC6. Для цього налаштуємо генератор трафіку з параметрами, як показаний на рисунку 3.25

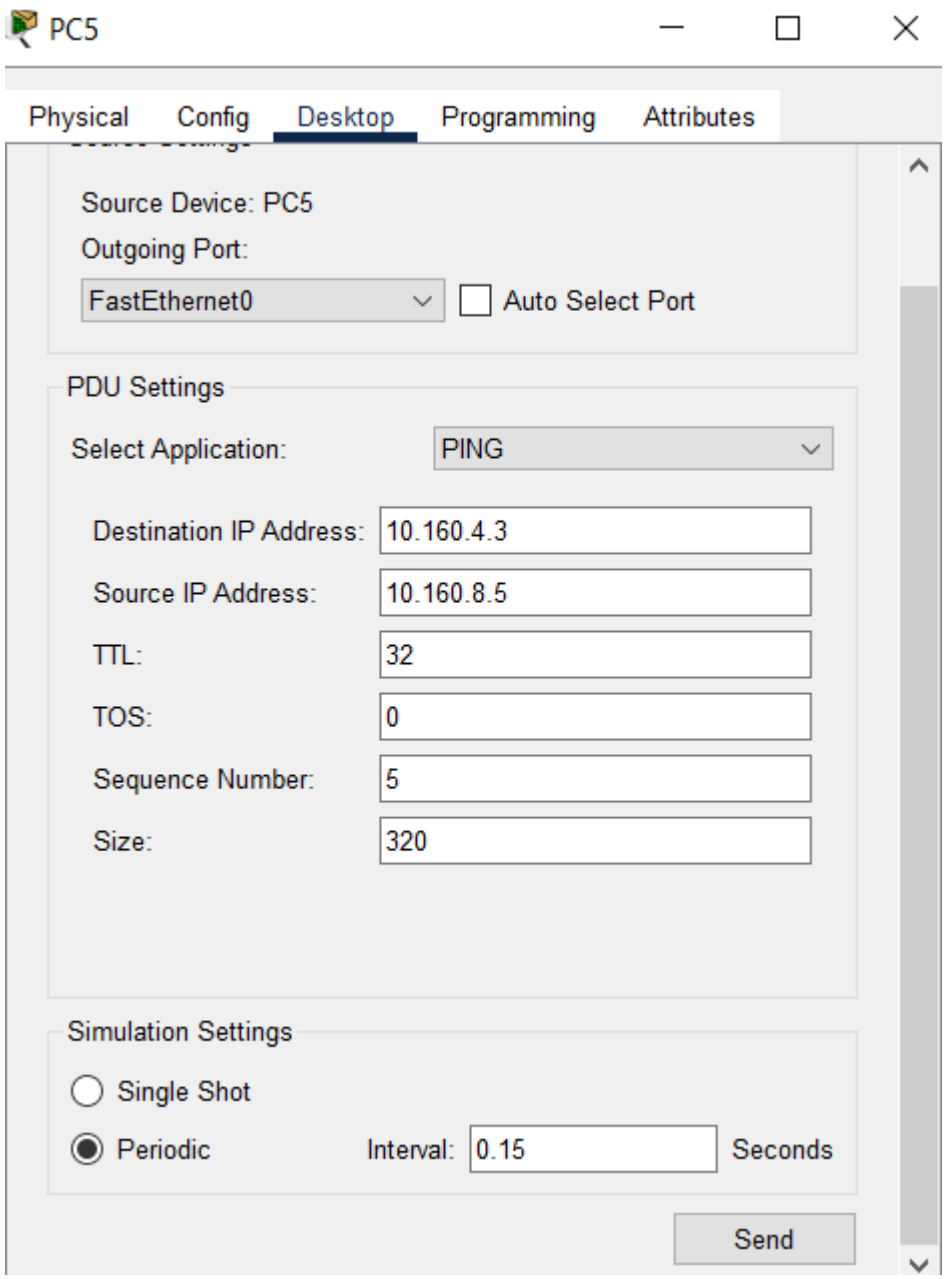


Рисунок 3.25 – Генератор трафіку для симуляції передачі пакетів

Тобто генеруються пакети розміром 320 байт через кожні 150 мс.

Панель симуляції має вигляд (рис. 3.27):

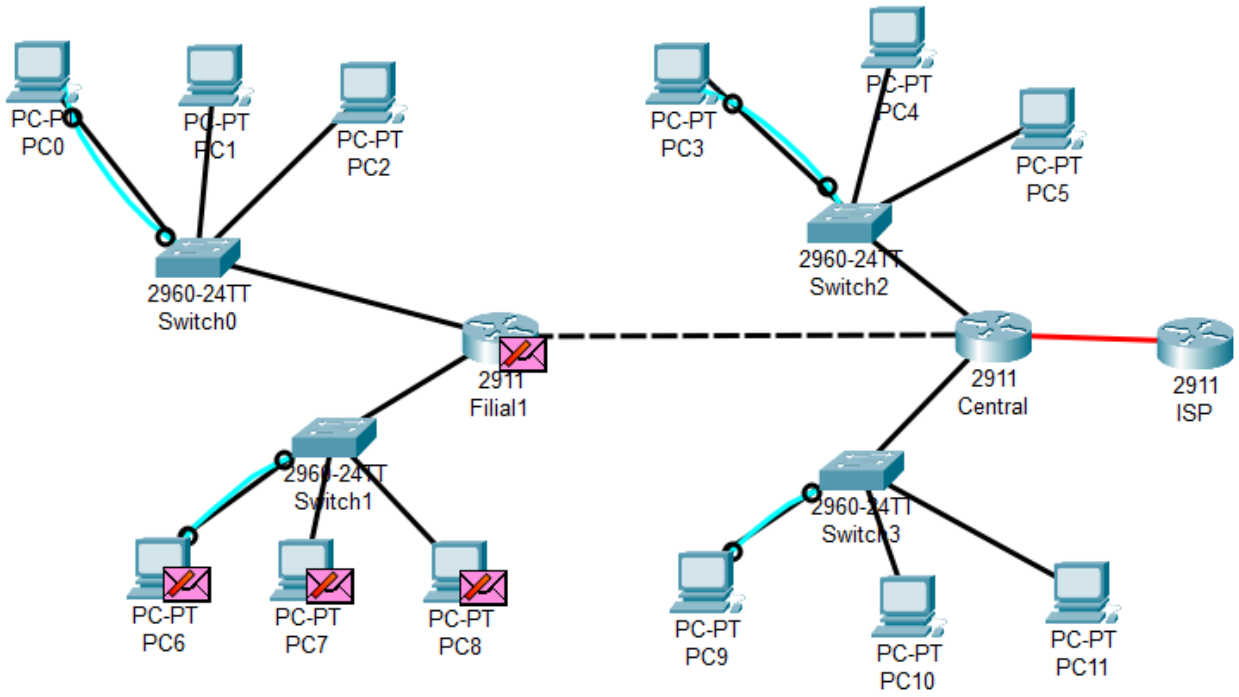


Рисунок 3.26 – Симуляція режиму передачі пакетів

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC5	ICMP
	0.001	PC5	Switch2	ICMP
	0.002	Switch2	Central	ICMP
	0.003	Central	Filial1	ICMP
	0.004	Filial1	Switch1	ICMP
	0.005	Switch1	PC6	ICMP
	0.006	PC6	Switch1	ICMP
	0.007	Switch1	Filial1	ICMP
	0.008	Filial1	Central	ICMP
	0.009	Central	Switch2	ICMP
	0.010	Switch2	PC5	ICMP
	0.150	--	PC5	ICMP
	0.151	PC5	Switch2	ICMP
	0.152	Switch2	Central	ICMP
	0.153	Central	Filial1	ICMP
	0.154	Filial1	Switch1	ICMP

Reset Simulation Constant Delay

Play Controls

Рисунок 3.27 – Панель симуляції

З панелі симуляції можна зробити висновок, що від PC5 до PC6 передача пакетів відбувається за 5 кроків, що складає 5 мс. У Cisco Packet Tracer у режимі симуляції кожен крок у списку подій (Event List) представляє окрему дію, яку виконує пакет під час проходження через мережу — наприклад, надсилання, приймання або обробку на пристрої. Ці кроки не відповідають реальному часу, а є логічними подіями, які дозволяють детально відстежувати маршрут пакета.

Якщо симуляція показує, що пакет від ПК5 до ПК6 проходить за 5 кроків, це означає, що він проходить через п’ять логічних етапів у мережі. Однак ці кроки не відображають реальну затримку в 5 мілісекунд. У Packet Tracer затримки не моделюються точно в реальному часі, тому час, вказаний у симуляції, є умовним і слугує для аналізу маршруту пакета, а не для точного вимірювання затримок.

Висновки до третього розділу

1. Проєкт демонструє ефективне впровадження логічної сегментації мережі за допомогою VLAN, що дозволило створити ізольовані широкомовні домени, підвищити безпеку та керованість мережі. Статична IP-адресація забезпечила чіткий контроль над адресним простором, що спростило налаштування та діагностику.

2. Базове налаштування комутаторів і маршрутизаторів, а також конфігурація таблиць статичної маршрутизації, забезпечили надійну маршрутизацію між VLAN. Тестування підтвердило стабільну роботу мережі, відсутність широкомовних штормів та повну зв'язність між пристроями відповідно до заданої топології.

3. Загалом, проєкт відповідає вимогам щодо побудови масштабованої та безпечної локальної мережі з розмежуванням трафіку, що є важливою практикою для реальних корпоративних інфраструктур.

ВИСНОВКИ

1. В результаті виконання кваліфікаційного проекту на тему «Телекомунікаційна мережа сучасного офісу» побудована модель мережі в середовищі Cisco Packet Tracer, виконано розбиття адресного простору, проведено налаштування мережевих пристроїв, прописані таблиці маршрутизації для маршрутизаторів.

2. Проведена симуляція відправки пакетів між вузлами в різних підмережах. Підтверджена вірність введених налаштувань.

3. Проведена діагностика мережі, яка показала високу навантажувальну здатність мережі і швидкість передачі пакетів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Кваліфікаційний проєкт : методичні вказівки щодо його підготовки та виконання здобувачами вищої освіти (ОР «бакалавр») спеціальності 172 «Телекомунікації та радіотехніка» / уклад.: С. К. Підченко, А. А. Таранчук, В. І. Стецюк, О. С. Пивовар. Хмельницький: ХНУ, 2021. – 71 с.

2. Бойко Ю.М. Текстові документи. Загальні вимоги СОУ 207.01:2017 / Ю.М. Бойко, Г.В. Красильникова, Л.І. Першина, Т.Ф. Косянчук. – Хмельницький : ХНУ, 2017. – 45 с.

3. Городецька, О. С. Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с

4. Комп'ютерні мережі: Навчальний посібник. Частина 1 /Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

5. Комп'ютерні мережі: Навчальний посібник. Частина 2 /Б. Ю. Жураковський, І. О. Зенів ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 372 с.

6. Комп'ютерні мережі.Конспект лекцій /Ю.А. Зав'ялець – Чернівці, 2015. – 183 с.

7. Жураковский, Б. Ю. Комп'ютерні мережі. Навчальний посібник для виконання лабораторних робіт /Б. Ю. Жураковский, І. О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 213 с.

8. «Телемедицина та комп'ютерні мережі: Лабораторний практикум у Cisco Packet Tracer» / В.А. Данілова, В.В. Шликов; КПІ ім. Ігоря Сікорського.– Київ: КПІ ім. Ігоря Сікорського», 2021. – 73 с.

9. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта. Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2021. – 43 с.

10. Наумук І. М. Використання Cisco packet tracer як засобу симуляції мережевої інфраструктури у підготовці інженерів-програмістів /І. М.Наумук, О.

В. Наумук //Вісник Херсонського національного технічного університету №1, 2024. с. 253-257

11. Методичні вказівки до виконання лабораторних робіт «Моделювання комп'ютерних мереж» з курсу «Архітектура комп'ютерних мереж» / уклад. Д. О. Лунін, А. І. Гапон – Х.: НТУ «ХПІ». 2023 – 39 с.

12. Комп'ютерні мережі. Частина 1. Моделювання комп'ютерних мереж: Лабораторний практикум. / Укладачі: О. С. Яценко, О. І. Яценко. – Житомир: Вид-во ЖДУ ім. І. Франка, 2022. – 76 с.

13. Побудова бездротових мереж в Cisco Packet Tracer [Відео]. URL: https://ua5.org/lan/1481-pobudova-bezdrotovyh-merezh-v-cisco-packet-tracer.html (дата звернення: 21.04.2025).

14. Гайдусь А., Галагуз А. Cisco Packet Tracer як складова навчальної дисципліни «Комп'ютерні мережі». Наумовські читання : матеріали XXI Всеукр. наук.-метод. конф. здобувачів вищ. освіти та молод. вчених, присвяч. 100-річчю до дня народж. І. О. Наумова, м. Харків, 23–24 листоп. 2023 р. / Харків. нац. пед. ун-т ім. Г. С. Сковороди ; за заг. ред. О. А. Жерновникової. Харків, 2024. С. 327–328.

15. Побудова мережі в Cisco Packet Tracert і базове налаштування пристроїв [Відео]. URL: https://www.youtube.com/watch?v=nIth_eesQ9s&t=2837s&ab_channel=Інформаційнітехнології такомп'ютернаінженерія (дата звернення: 29.04.2025).

16. Розрахунок підмереж [Відео]. URL: https://www.youtube.com/watch?v=2mILqH37RSs (дата звернення: 30.04.2025).

17. Optimizing Local Area Network Performance: Insight from Riverbed Modelling /Kalu J., Nwauzor J.N., Suleman K.O, Igbo M. E., Igbo N. E //Journal of Engineering Research and Reports, 2024. Volume 26, Issue 6, Page 212-222.

18. N. B. Ltayef, M. Y. Alzogni, A. A. Abu-Gunaydah and E. A. Alhmadi, "Improving Network's Performance by Applying Different Quality of Service Mechanisms," 2022 IEEE 2nd International Maghreb Meeting of the Conference on

Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya, 2022, pp. 345-349

19. G. Ciccarella, G. Paris, I. Tobia and G. Valent, "Performance evaluation of a local area network for real-time applications," Proceedings of the Third IEEE Symposium on Parallel and Distributed Processing, Dallas, TX, USA, 1991, pp. 504-512.

20. Obelovska, K.; Panova, O.; Karovič, V., Jr. Performance Analysis of Wireless Local Area Network for a High-/Low-Priority Traffic Ratio at Different Numbers of Access Categories. Symmetry 2021, 13, 693.

21. Nourildean, S.W.; Mohammed, Y.A.; Attallah, H.A. Virtual Local Area Network Performance Improvement Using Ad Hoc Routing Protocols in a Wireless Network. Computers 2023, 12, 28.

22. Holan Rahmatullah Suhut Nadenggan, Imam Riadi . Analysis of Local Area Network Performance using Quality of Service. International Journal of Computer Applications. 183, 46 (Jan 2022), 43-51.

23. Azamuddin, W.M.H.; Hassan, R.; Aman, A.H.M.; Hasan, M.K.; Al-Khaleefa, A.S. Quality of Service (QoS) Management for Local Area Network (LAN) Using Traffic Policy Technique to Secure Congestion. Computers 2020, 9, 39.

24. Thoyyibah T Analysis of Networking Tools Using Cisco Packet Tracer (CPT) /T. Thoyyibah, Asep Ridwan Hidayat, Imam Satria Hanggara //International Journal Software Engineering and Computer Science (IJSECS) № 4, 2024, p. 721-730.

25. Belzarena, P., Bermolen, P., Casas, P., & Simon, M. Virtual paths networks fast performance analysis /P. Belzarena, P. Bermolen, P. Casas, M. Simon //Virtualization Techniques in Cloud Computing. №2. - 2022, p. 359-385.

26. Md. Anwar Hossain Performance Comparison of EIGRP, OSPF and RIP Routing Protocols using Cisco Packet Tracer and OPNET Simulator /Md. Anwar Hossain, Md. Mohon Ali, Mst. Sharmin Akter, Md.Shahriar Alam Sajib //Global Journal of Computer Science and Technology: Interdisciplinary. Volume 20. Issue 2.

27. Kabir, M.H.; Kabir, M.A.; Islam, M.S.; Mortuza, M.G.; Mohiuddin, M. Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols. Eng. Proc. 2021, 10, 47.

28. Cao, Yang, Zeyu Xu, Pengxiang Qin and Tao Jiang. “Video Processing on the Edge for Multimedia IoT Systems.” ArXiv abs/1805.04837 (2018)

29. Shivani Rajendra Teli, Vicente Matus, Stanislav Zvanovec, Rafael Perez-Jimenez, Stanislav Vitek. Optical Camera Communications for IoT–Rolling-Shutter Based MIMO Scheme with Grouped LED Array Transmitter.Sensors,2020,20(12), p.3361.

30. CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine

31. Onay, A., Ertürk, G., Kıranlı, C., Ateş, H. and Isikdemir, Y. (2023) A Smart Home Energy Monitoring System Based on Internet of Things and Inter Planetary File System for Secure Data Sharing. Journal of Computer and Communications, 11, 64-81.

32. Muliadi, M. Y. Fahrezi, I. S. Areni, E. Palantei and A. Achmad, A Smart Home Energy Consumption Monitoring System Integrated with Internet Connection // 2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), Batam, Indonesia, 2020, pp. 75-80.

Додаток А

Презентаційні матеріали

Хмельницький національний університет

Кафедра телекомунікацій, медійних та інтелектуальних технологій

Телекомунікаційна мережа сучасного офісу

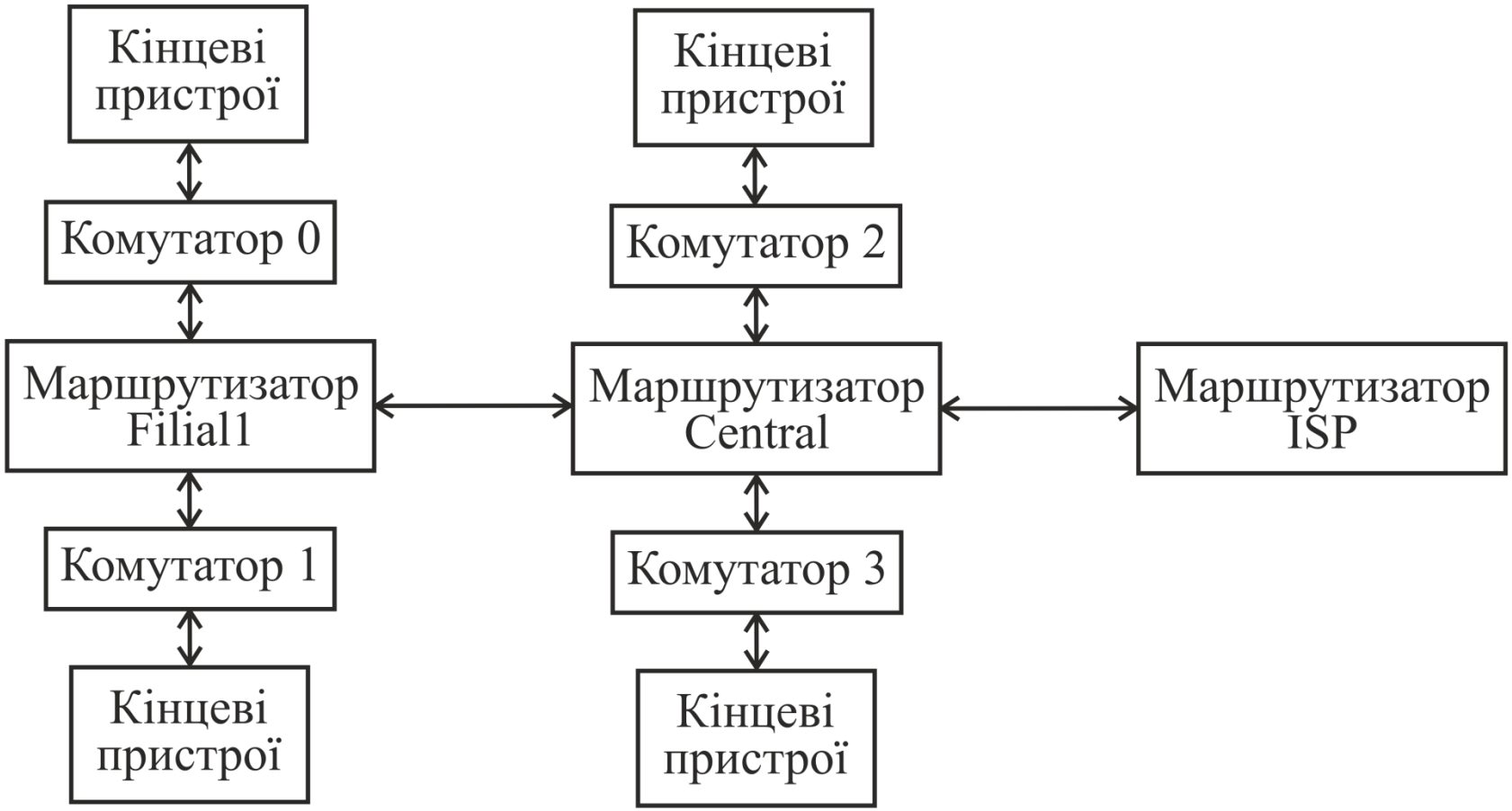
Виконав: студент гр. ТР2-21-1
Кланцатий Дмитро Юрійович

Керівник: д.т.н., професор
Бойко Юлій Миколайович

Метою кваліфікаційного проєкту є розробка телекомунікаційної мережі сучасного офісу. Для досягнення мети було поставлено такі завдання:

- розглянути особливості побудови телекомунікаційної мережі сучасного офісу;
- виконати розподіл адресного простору мережі;
- виконати базове налаштування пристроїв у середовищі Cisco Packet Tracer ;
- виконати налаштування статичних маршрутів і маршрутів за замовчуванням .

Сучасна офісна телекомунікаційна мережа — це комплексна система, яка забезпечує високошвидкісну, надійну і безпечну передачу даних, голосу та відео між пристроями всередині офісу та із зовнішнім світом



					КПТР.210140.01.04 Е1	
Вил	Арк.	№документа	Підпис	Дата	Телекомунікаційна мережа сучасного офісу	Літера: У; Маса; Масштаб
Розробив		Кланцатий Д.Ю.				
Перевірив		Бойко Ю.М.			Схема електрична структурна	Аркуш; Аркушів 1
Т.контр.						
Н.контр.		Стецюк В.І.				ХНУ гр. ТР2-21-1
Затвердив		Підченко С.К.				

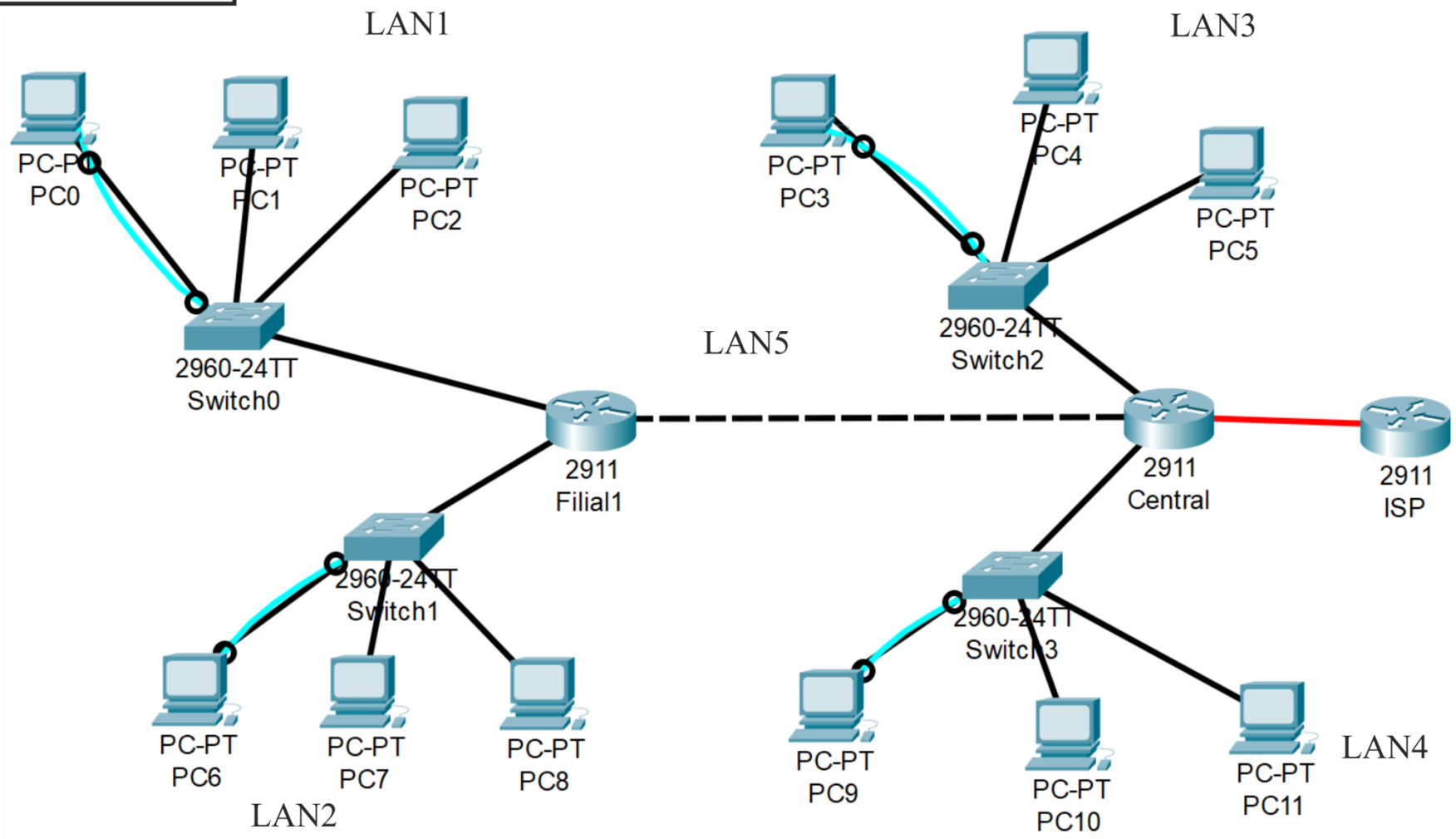
Розподіл адресного простору

Таблиця 4.1 – Відомості про підмережі

Назва підмережі	Необхідний розмір підмережі	Виділений розмір підмережі	Десятковий формат адреси	Двійковий формат адреси	Перший використов адрес вузла	Останній використов адрес вузла	Широкомовна адреса
LAN1	20	1022	10.160.0.0/22	10.160.000000 00.00000000	10.160.0.1	10.160.3.254	10.160.3.255
LAN2	24	1022	10.160.4.0/22	10.160.000001 00.00000000	10.160.4.1	10.160.7.254	10.160.7.255
LAN3	200	1022	10.160.8.0/22	10.160.000010 00.00000000	10.160.8.1	10.160.11.254	10.160.11.255
LAN4	150	1022	10.160.12.0/22	10.160.000011 00.00000000	10.160.12.1	10.160.15.254	10.160.15.255
LAN5	2	1022	10.160.16.0/22	10.160.000100 00.00000000	10.160.16.1	10.160.19.254	10.160.19.255
Загалом	396	5110					

Таблиця 5.1 – Адресація пристроїв і їх підключення

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Префікс
Filial1	Gig0/0	10.160.0.1	255.255.252.0	/22
	Gig0/1	10.160.16.1	255.255.252.0	/22
	Gig0/2	10.160.4.1	255.255.252.0	/22
Central	Gig0/0	10.160.12.1	255.255.252.0	/22
	Gig0/1	10.160.16.2	255.255.252.0	/22
	Gig0/2	10.160.8.1	255.255.252.0	/22
	Gig0/3/0	209.165.201.226	255.255.255.224	/27
ISP	Gig0/3/0	209.165.201.225	255.255.255.224	/27
	Io0	8.8.8.8	255.255.255.0	/24
Switch-LAN1	VLAN1	10.160.0.2	255.255.252.0	/22
Switch-LAN2	VLAN1	10.160.4.2	255.255.252.0	/22
Switch-LAN3	VLAN1	10.160.8.2	255.255.252.0	/22
Switch-LAN4	VLAN1	10.160.12.2	255.255.252.0	/22



					КПТР.210140.01.04 Е3			
					Телекомунікаційна мережа сучасного офісу Схема логічної структуризації мережі	Літера	Маса	Масштаб
Вил	Арк.	№документа	Підпис	Дата		У		
Розробив		Кланцатий Д.Ю.				Аркуш	Аркушів 1	
Перевірив		Бойко Ю.М.						
Т.контр.								
Н.контр.		Стецюк В.І.				ХНУ гр. ТР2-21-1		
Затвердив		Підченко С.К.						

Конфігурація комутаторів

PC0

Physical Config Desktop Programming Attributes

Terminal X

```
Switch_LAN1>show ip
Switch_LAN1>show ip int
Switch_LAN1>show ip interface br
Switch_LAN1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  10.160.0.2      YES manual up                    up
Switch_LAN1>
```

Рисунок 7.1 –Вікно конфігурації комутатора

Налаштування маршрутизаторів

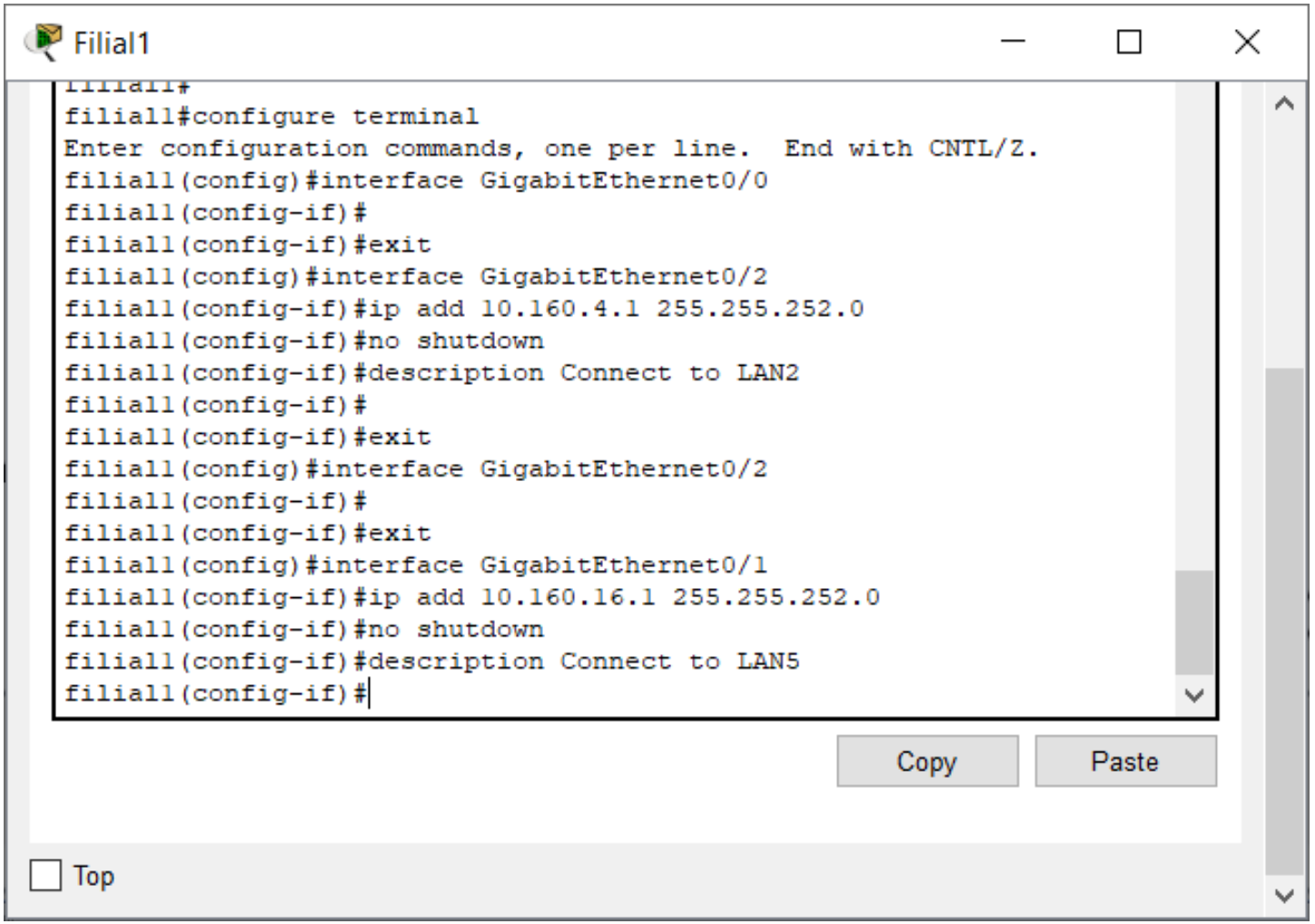


Рисунок 8.1 – Налаштування інтерфейсів маршрутизатора

Налаштування персональних комп’ютерів

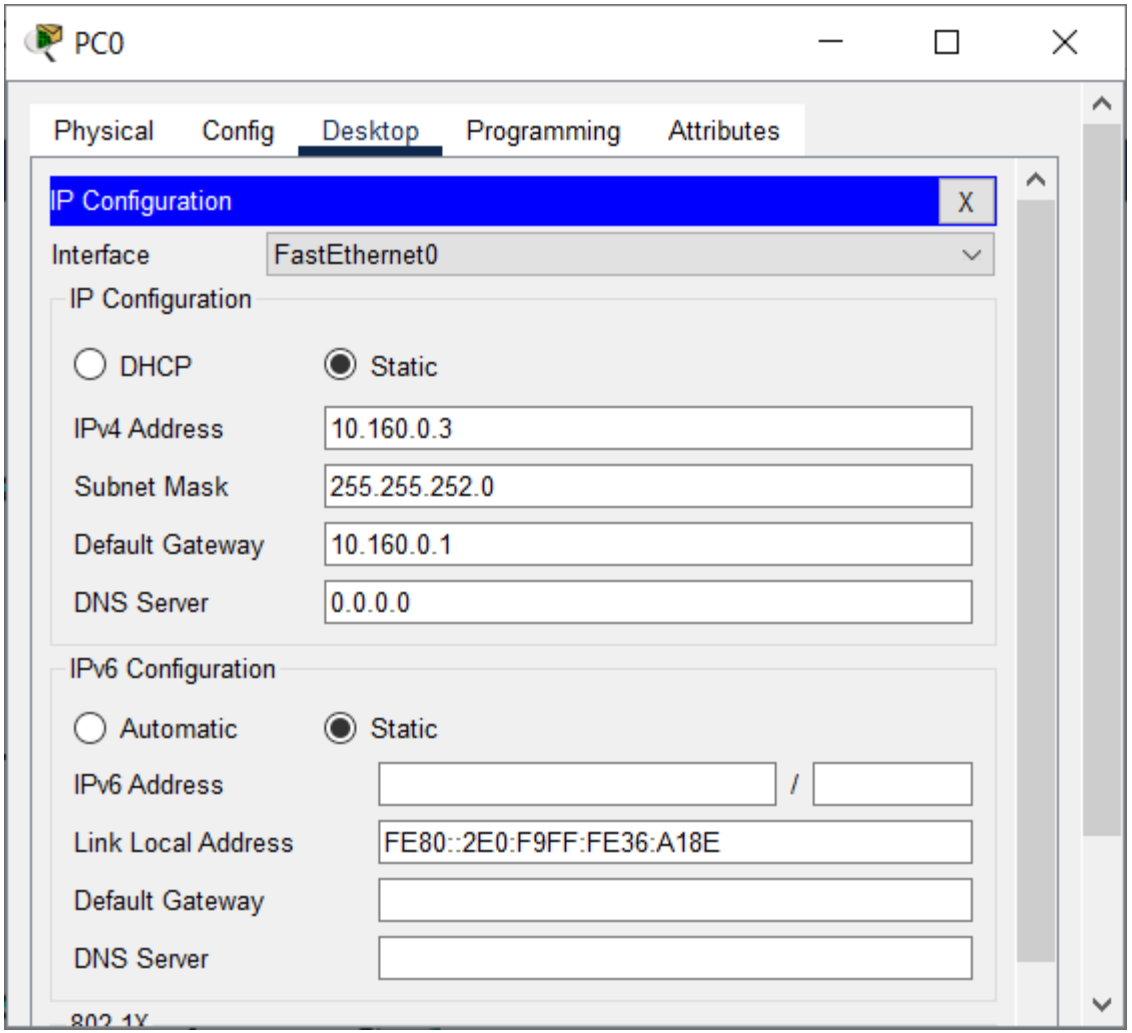


Рисунок 9.1 – Конфігурація персонального комп’ютера PC0

Перевірка налаштувань ПК

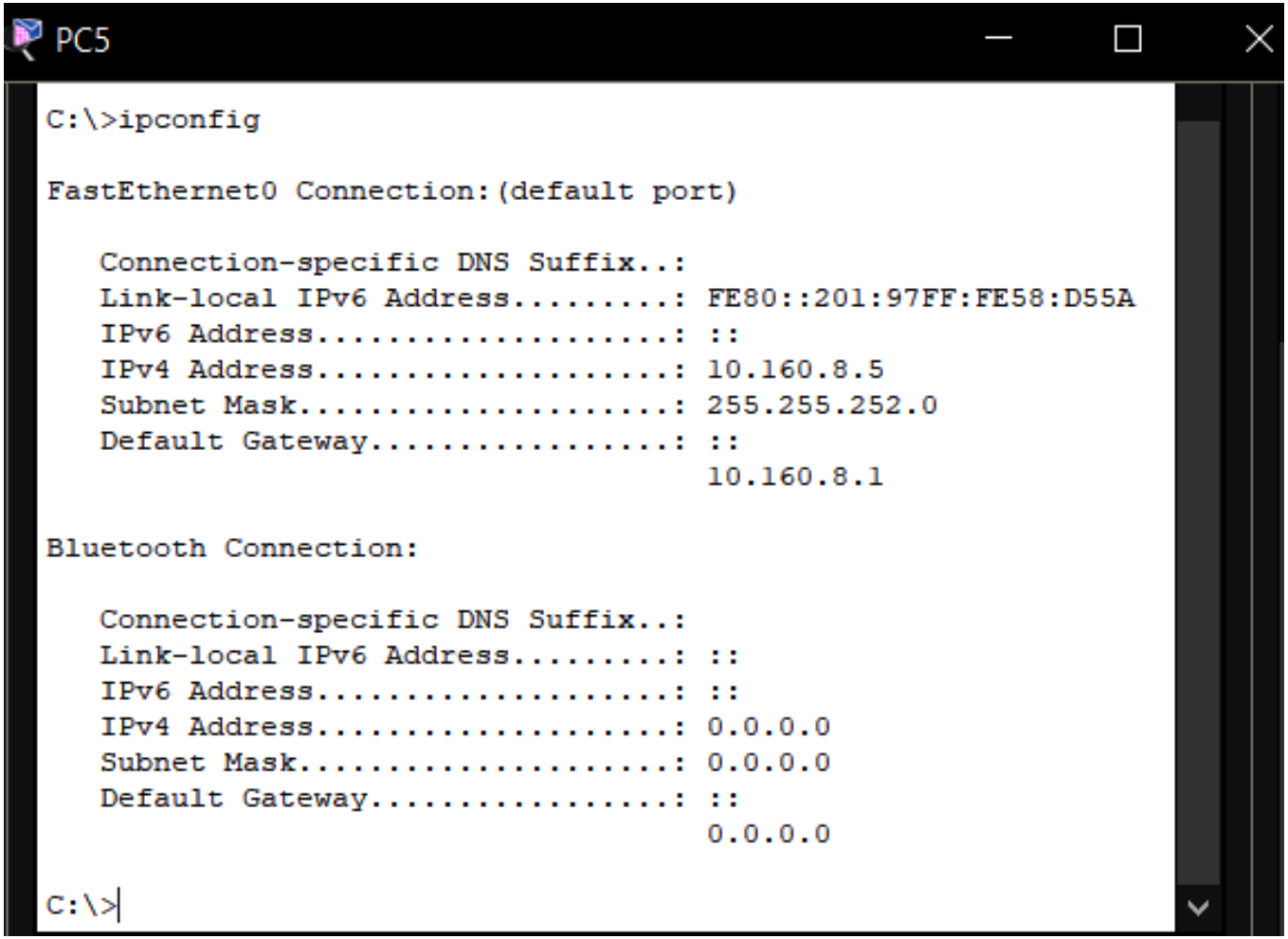


Рисунок 10.1 – – Перевірка налаштувань IP протокола вузла PC5

Перевірка зв’язку з ПК

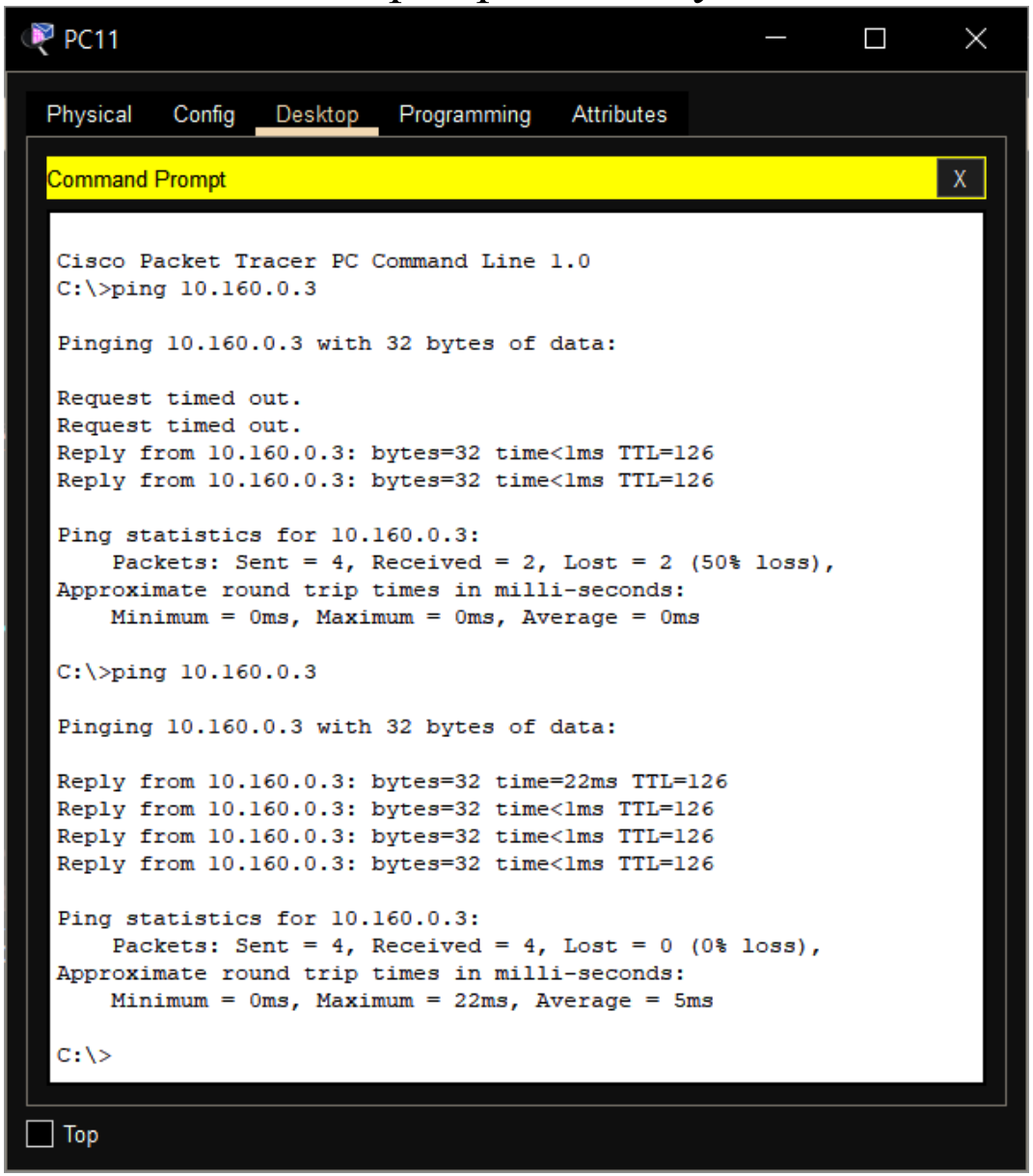


Рисунок 11.1 – Результат виконання команди ping з PC11 на PC0

Тест перехресних команд ping з PC11 на PC0 і з PC5 на PC6

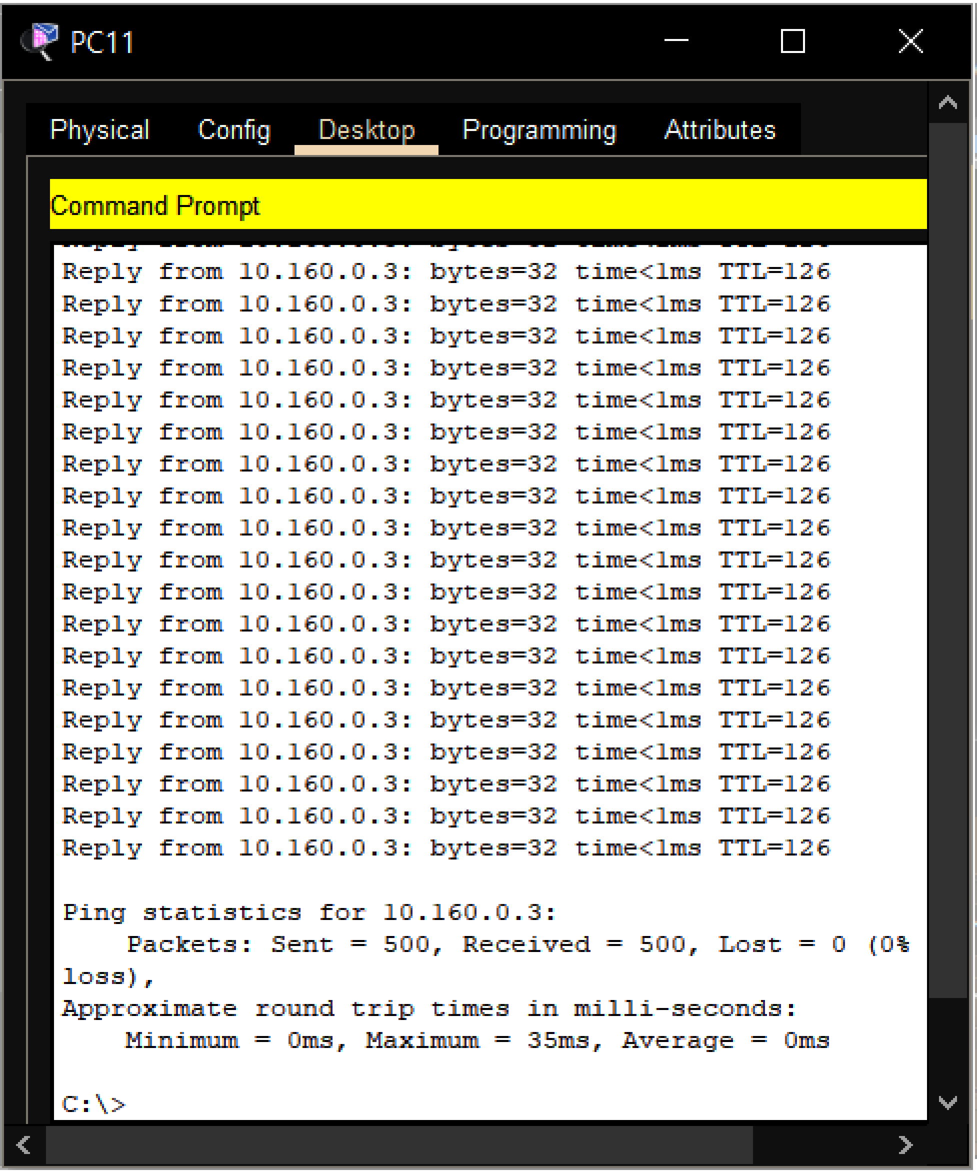


Рисунок 12.1 – Тест перехресних команд ping з PC11 на PC0

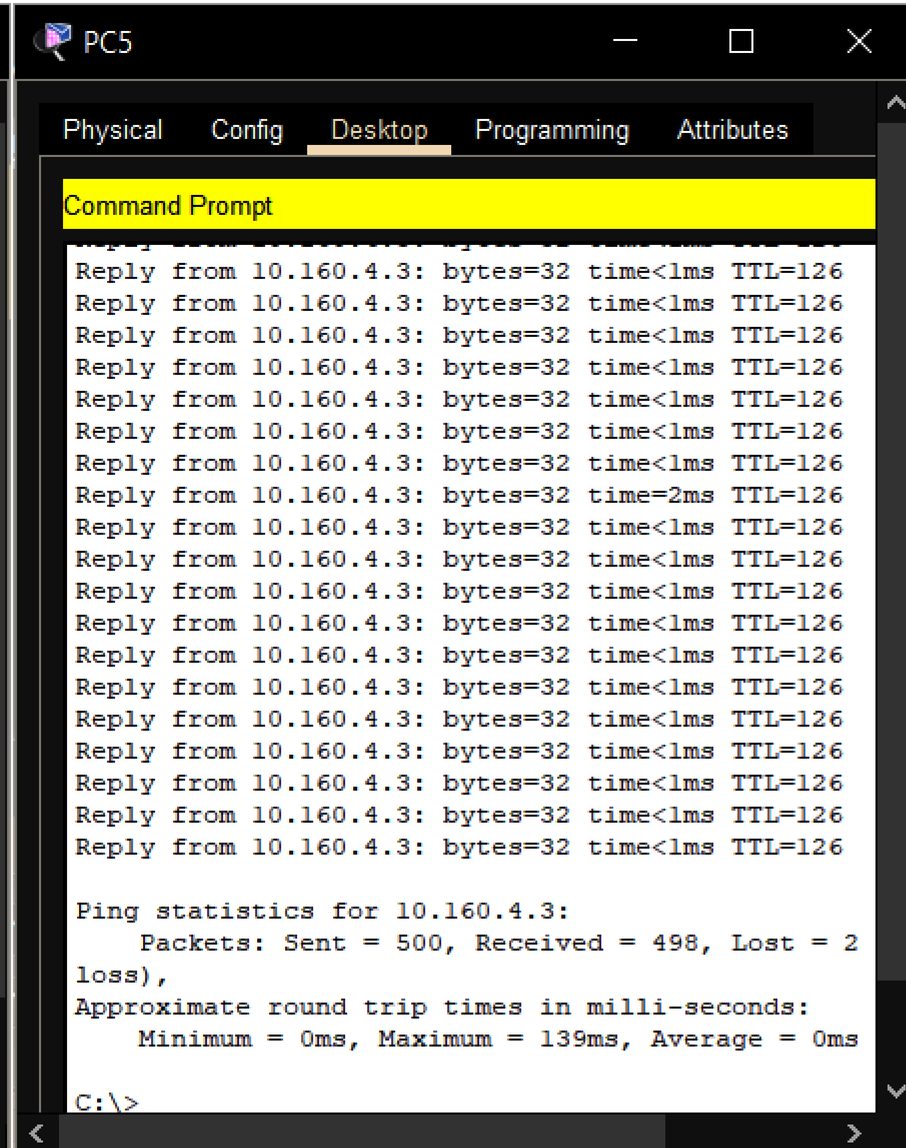


Рисунок 12.2 - Тест перехресних команд ping з PC5 на PC6

Вкладка CLI роутера filial1

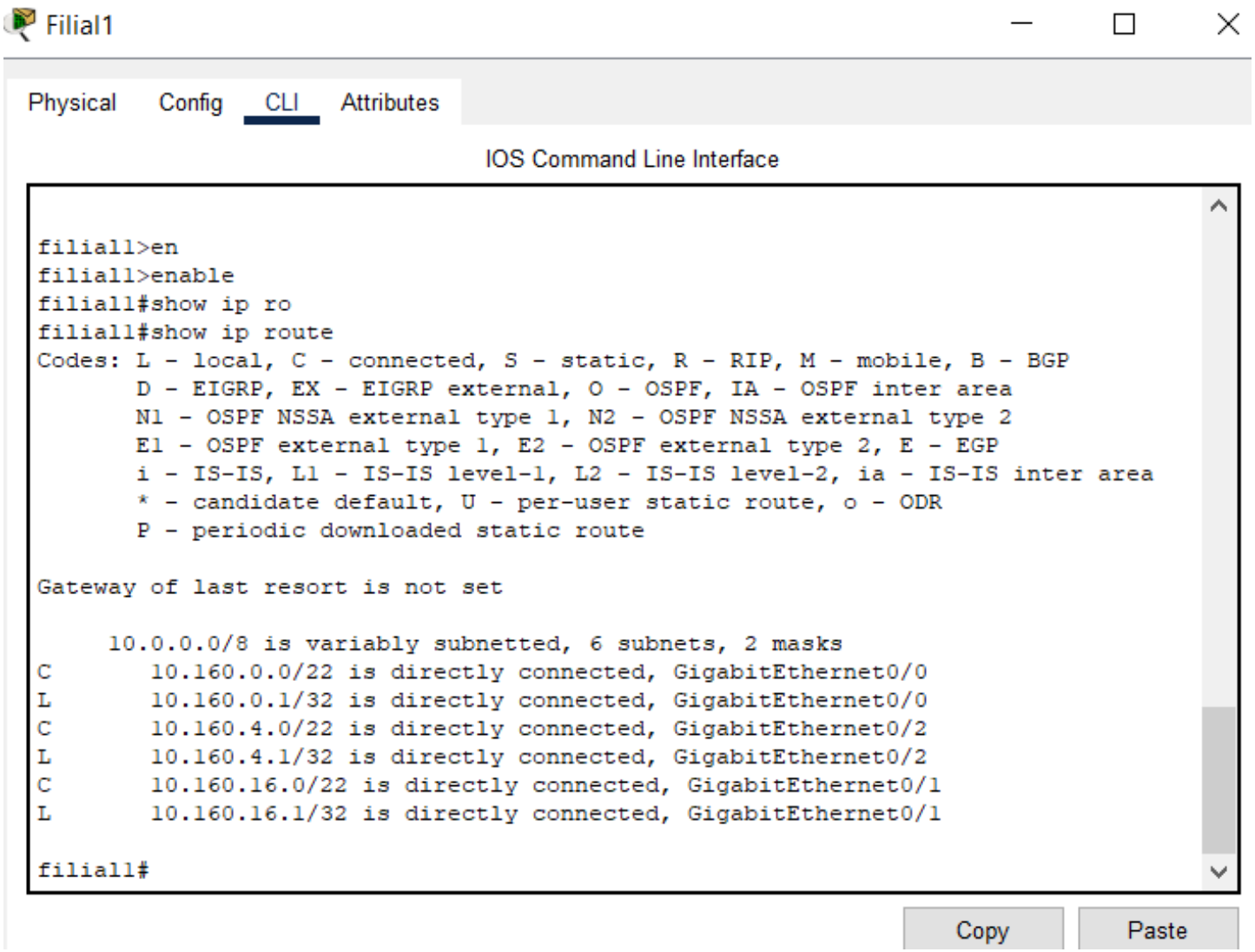


Рисунок 13.1 – Таблиця маршрутизації роутера filial1

```
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up


Router>en
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 10.160.8.0 255.255.252.0 10.160.16.2
Router(config)#Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#exit
Router(config)#ip route 10.160.12.0 255.255.252.0 10.160.16.2
Router(config)#ip route 209.165.201.224 255.255.255.240 10.160.16.2
Router(config)#
```

Рисунок 14.1 – Додавання нових маршрутів роутера Filial1

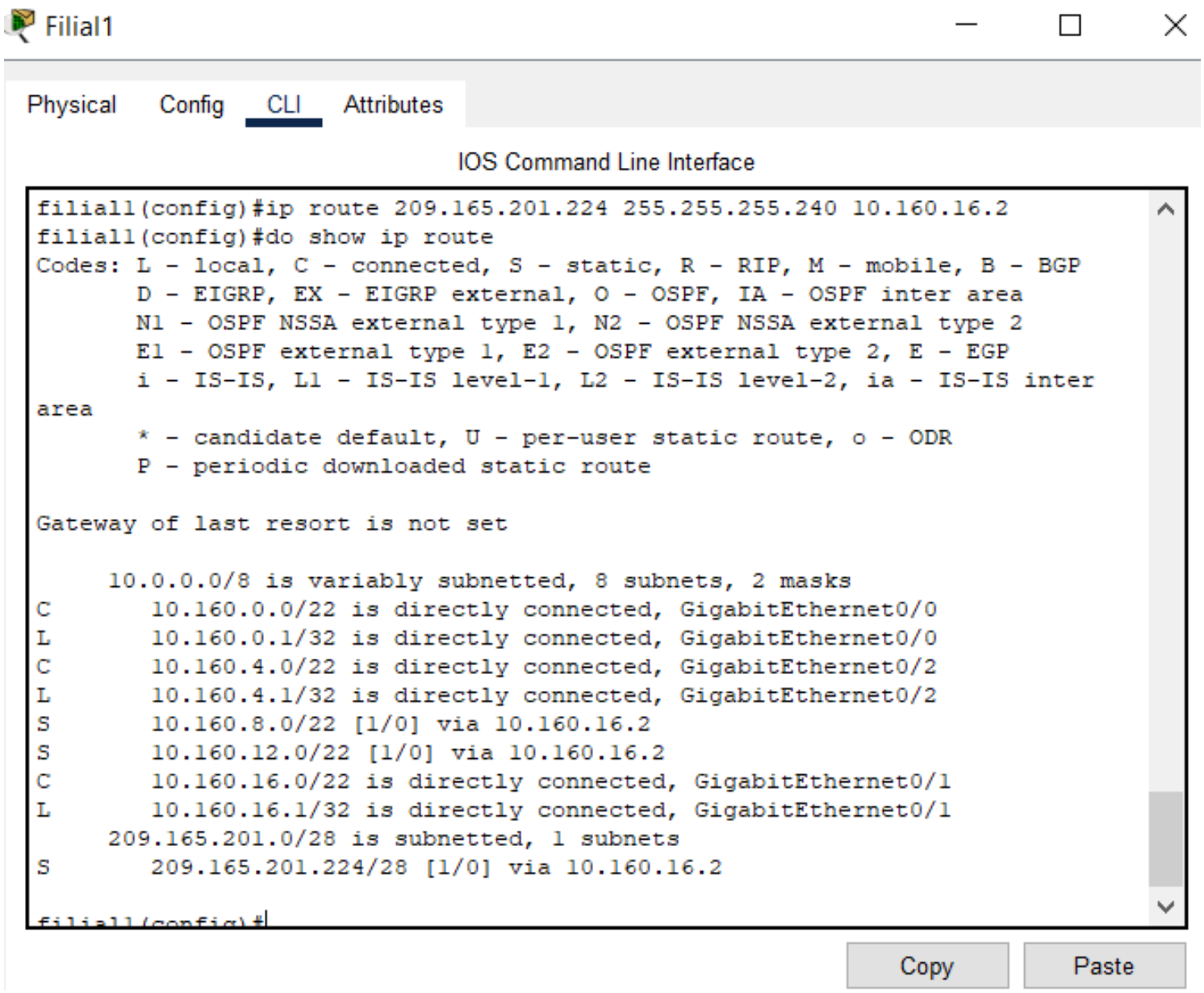


Рисунок 15.1 – Оновлена таблиця маршрутизації роутера Filial1

Симуляція відправки пакетів

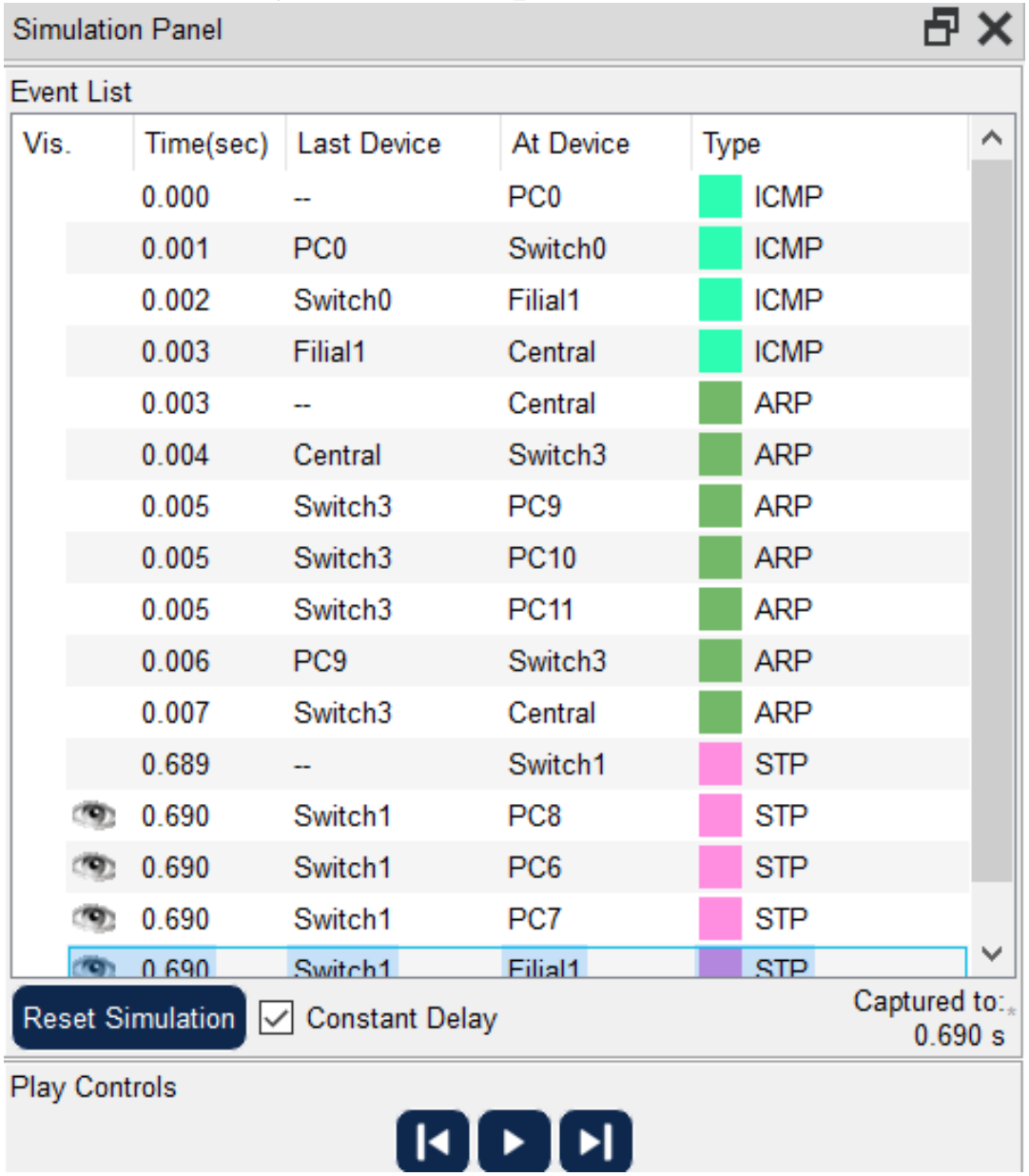


Рисунок 16.1 – Перевірка роботи таблиці маршрутизації від PC1 до PC9

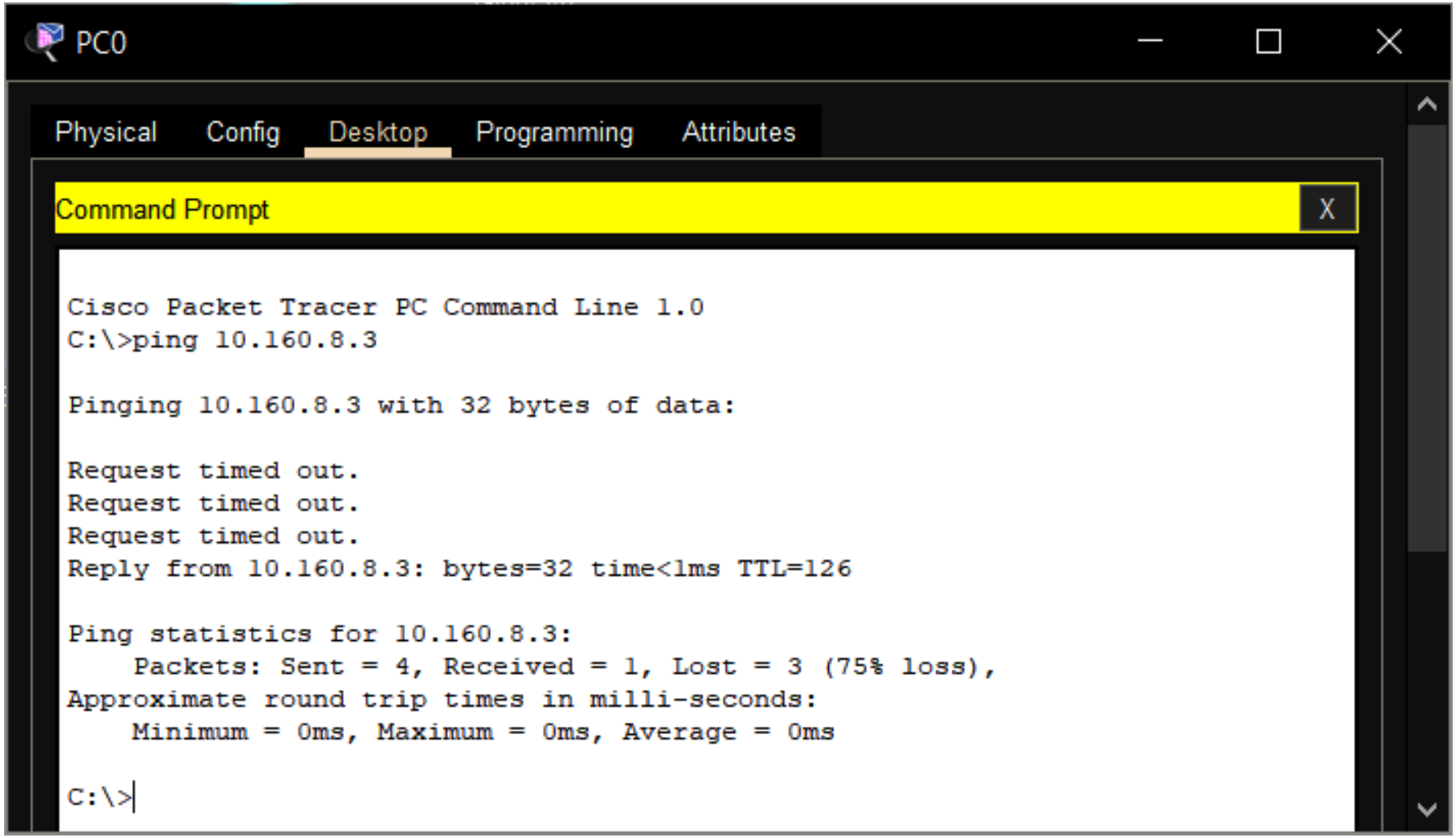


Рисунок 17.1 – Встановлення зв’язку між мережами LAN1 і LAN3

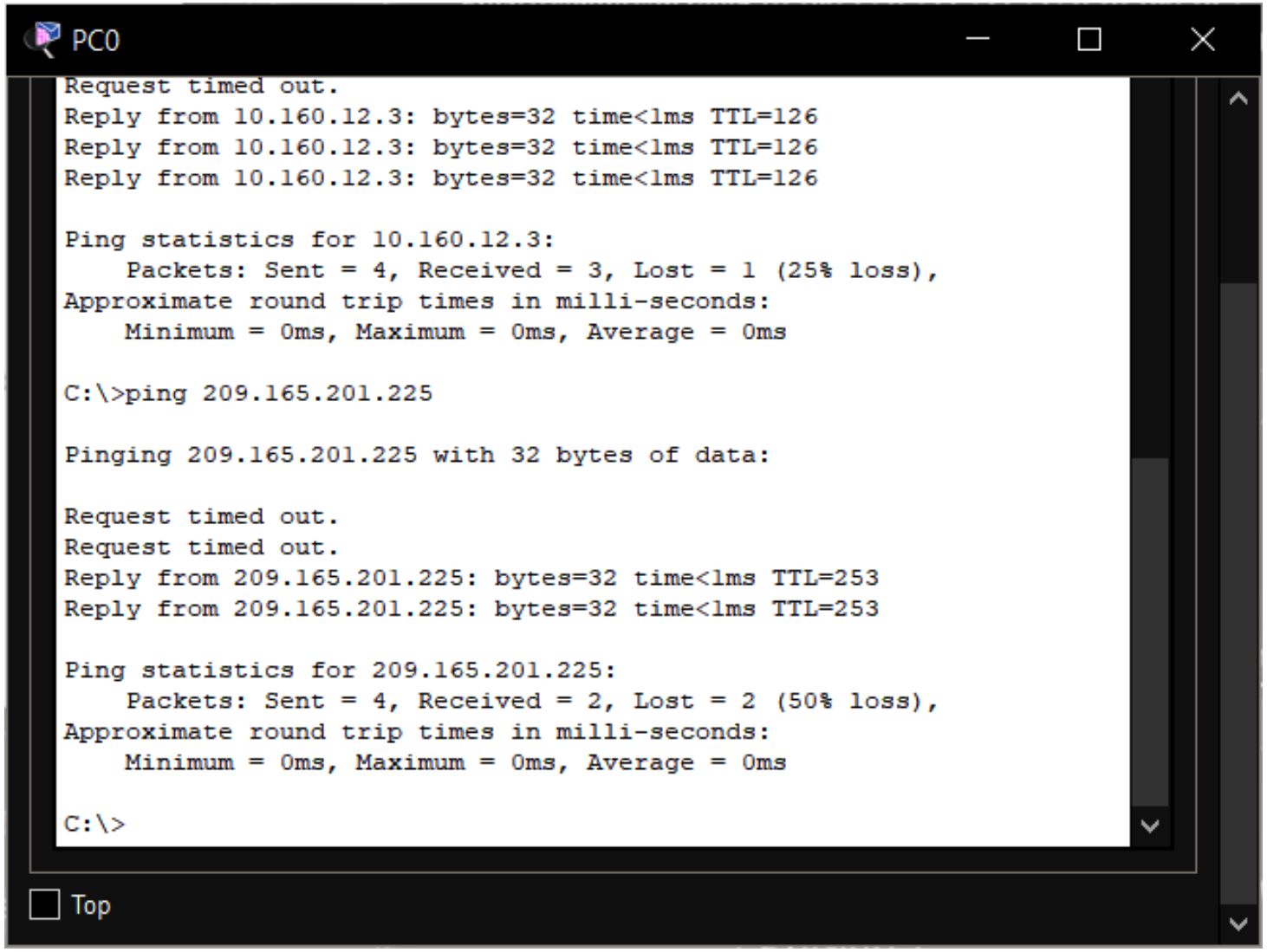


Рисунок 18.1 – Результат перевірки доступності мережі провайдера

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	Filial1	ICMP
	0.003	Filial1	Central	ICMP
	0.004	Central	Switch3	ICMP
	0.005	Switch3	PC9	ICMP
	0.006	PC9	Switch3	ICMP
	0.007	Switch3	Central	ICMP
	0.008	Central	Filial1	ICMP
	0.009	Filial1	Switch0	ICMP
	0.010	Switch0	PC0	ICMP
	0.114	--	Switch0	STP
	0.115	Switch0	PC0	STP
	0.115	Switch0	Filial1	STP
	0.115	Switch0	PC1	STP
	0.115	Switch0	PC2	STP
	0.240	--	Switch3	STP

Reset Simulation Constant Delay

Play Controls

Рисунок 19.1 – Панель симуляції для перевірки зв’язку між PC0 і PC11

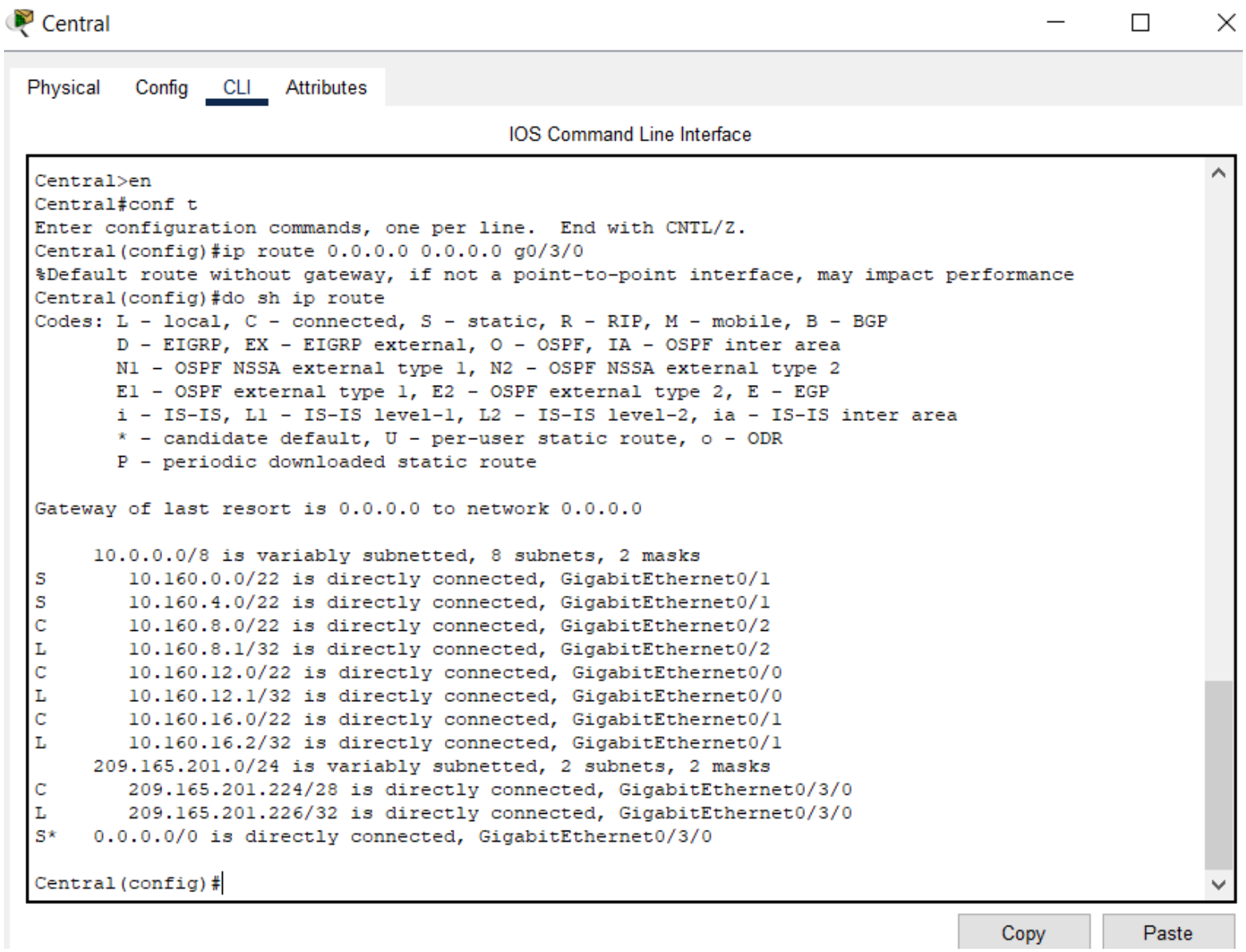


Рисунок 20.1 – Оновлена таблиця маршрутизації маршрутизатора Central

Симуляція роботи телекомунікаційної мережі

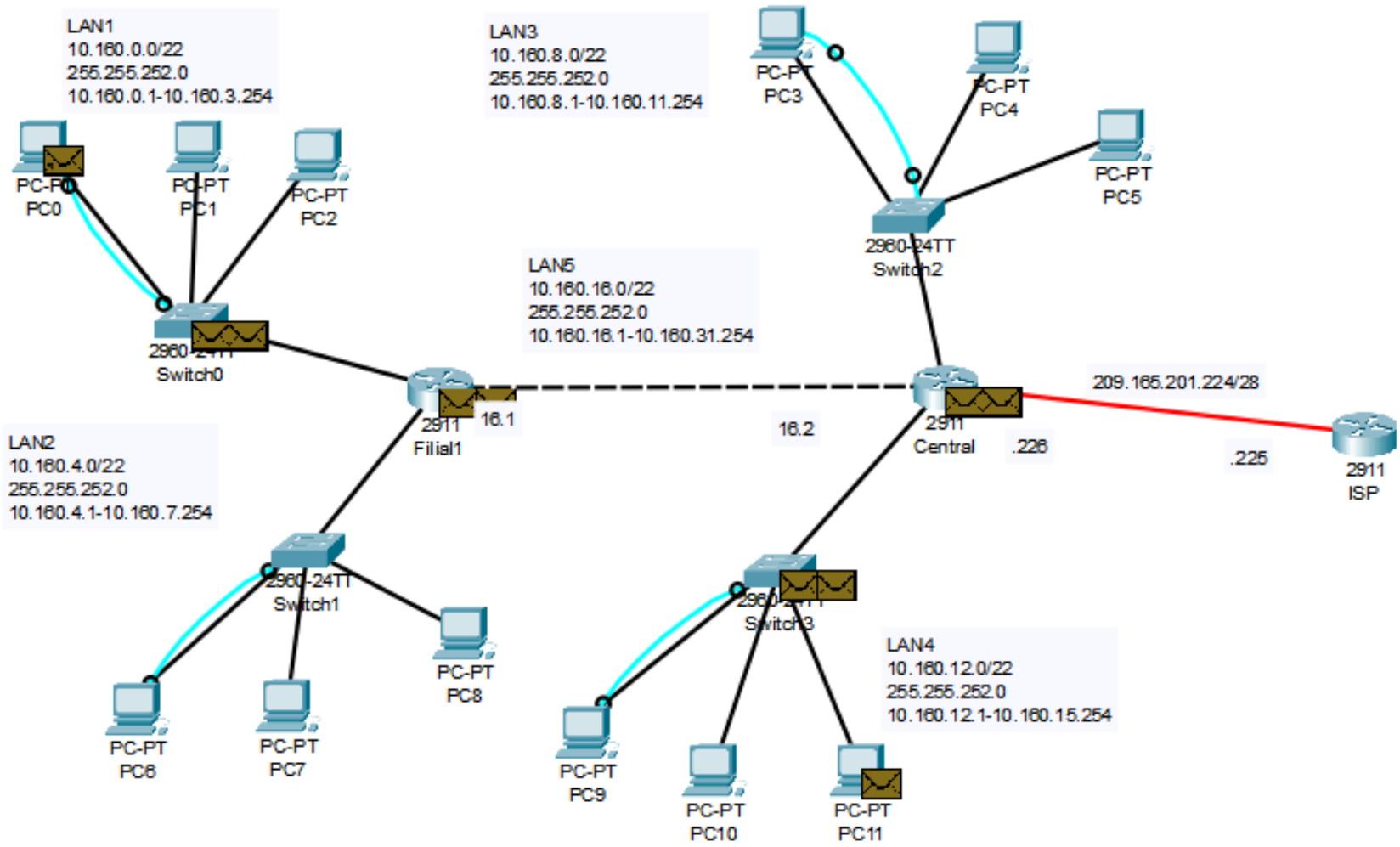


Рисунок 21.1 - Дослідження передачі пакетів між PC0 і PC11

Трасування шляху проходження пакетів від PC0 до PC11

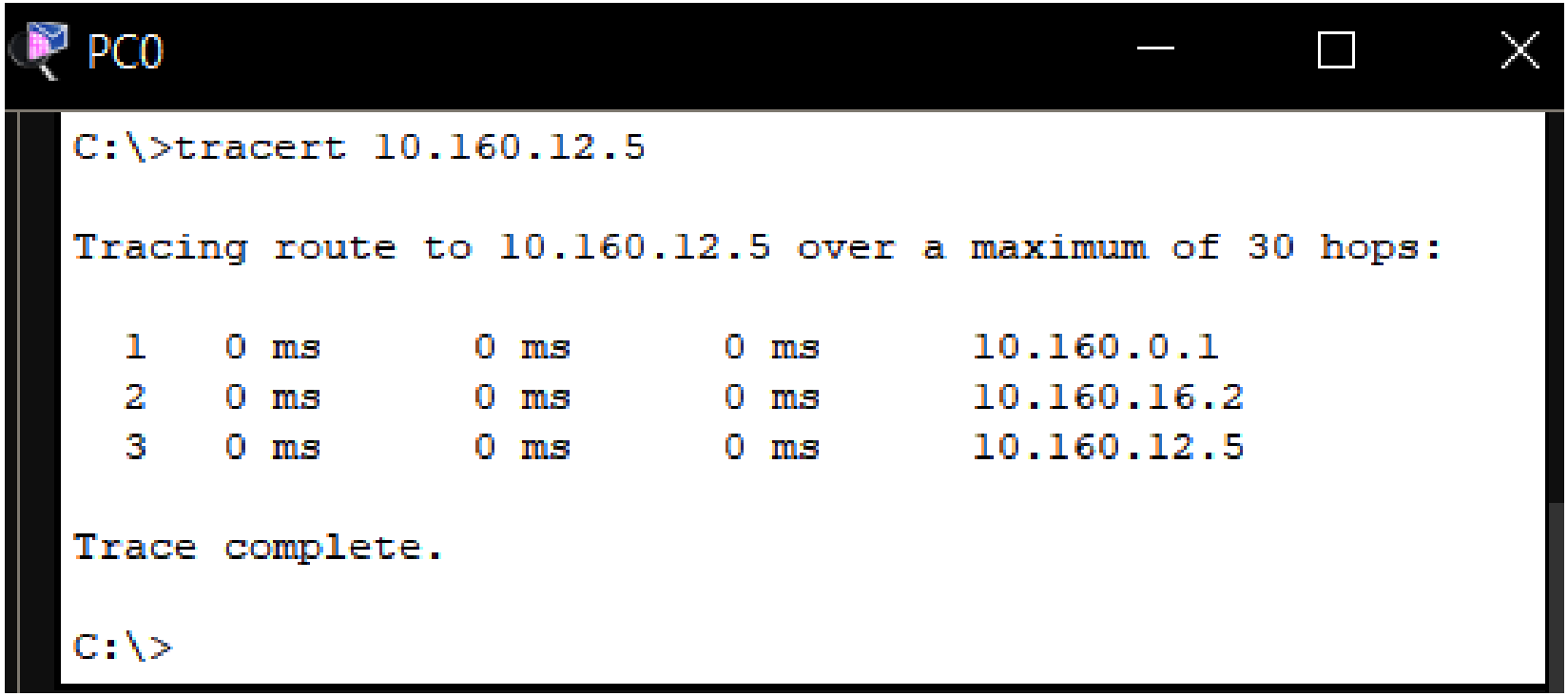


Рисунок 3.24 – Трасування шляху проходження пакетів від PC0 до PC11

Симуляція передачі пакетів між PC5 і PC6

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC5	ICMP
	0.001	PC5	Switch2	ICMP
	0.002	Switch2	Central	ICMP
	0.003	Central	Filial1	ICMP
	0.004	Filial1	Switch1	ICMP
	0.005	Switch1	PC6	ICMP
	0.006	PC6	Switch1	ICMP
	0.007	Switch1	Filial1	ICMP
	0.008	Filial1	Central	ICMP
	0.009	Central	Switch2	ICMP
	0.010	Switch2	PC5	ICMP
	0.150	--	PC5	ICMP
	0.151	PC5	Switch2	ICMP
	0.152	Switch2	Central	ICMP
	0.153	Central	Filial1	ICMP
	0.154	Filial1	Switch1	ICMP

Reset Simulation ☑ Constant Delay

Play Controls

Рисунок 23.1 – Панель симуляції передачі пакетів між PC5 і PC6

ВИСНОВКИ

1. В результаті виконання кваліфікаційного проекту на тему «Телекомунікаційна мережа сучасного офісу» побудована модель мережі в середовищі Cisco Packet Tracer, виконано розбиття адресного простору, проведено налаштування мережевих пристроїв, прописані таблиці маршрутизації для маршрутизаторів.
2. Проведена симуляція відправки пакетів між вузлами в різних підмережах. Підтверджена вірність введених налаштувань.
3. Проведена діагностика мережі, яка показала високу навантажувальну здатність мережі і швидкість передачі пакетів.

Відгук на кваліфікаційний проєкт виконану за темою
«Телекомунікаційна мережа сучасного офісу»
студента гр. ТР2-21-1 Кланцатого Д.Ю.

У сучасних умовах цифровізації та зростаючої залежності від інформаційних технологій, телекомунікаційна інфраструктура офісу відіграє ключову роль у забезпеченні ефективної роботи підприємства. Тому тема роботи є актуальною.

У кваліфікаційному проєкті студента Кланцатого Д.Ю. Зроблений аналітичний огляд літературних джерел по принципам проєктування мереж сучасного офісу. Відповідно до заданих вимог виконано розбиття адресного простору телекомунікаційної мережі, виділений адресний простір з врахуванням можливого розширення кількості вузлів в кожній підмережі. Побудована модель мережі у середовищі Cisco Packet Tracer, виконано базове налаштування пристроїв: комутаторів, маршрутизаторів, ПК. Налаштований віртуальний інтерфейс VLAN 1 для керування комутатором по мережі, перевірений стан активованих портів. Налаштовані всі активні інтерфейси маршрутизаторів, задані IP-адреси, маски підмереж, налаштований loopback-інтерфейс маршрутизатора ISP. Виконаний тест перехресних команд ping з PC11 на PC0 і з PC5 на PC6, який показав хорошу навантажувальну здатність мережі, прописані таблиці маршрутизації для маршрутизаторів.

В цілому під час роботи над кваліфікаційним проєктом студент Кланцатий Д.Ю. проявив себе як грамотний спеціаліст в галузі телекомунікацій, показав вміння та навички і набуті компетентності в дослідженні методів побудови телекомунікаційної мережі сучасного офісу.

Кваліфікаційний проєкт виконано на високому технічному рівні, він має безперечну актуальність в області сучасних телекомунікацій, а студент Кланцатий Д.Ю. заслуговує оцінки «відмінно».

Професор кафедри телекомунікацій, медійних
та інтелектуальних технологій Бойко Ю.М.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

Дипломник: *Кланцатий Дмитро Юрійович*
Тема роботи: *Телекомунікаційна мережа сучасного офісу*
Спеціальність *172 «Телекомунікації та радіотехніка»*

Обсяг дипломної роботи

Кількість листів креслень 4 Кількість сторінок записки 87

1. Короткий зміст роботи та прийнятих рішень в результаті виконаного наукового дослідження *Кваліфікаційний проєкт присвячений розробці телекомунікаційної мережі. Зроблений аналітичний огляд літературних джерел по особливостям проектування телекомунікаційних мереж. Найчастіше мережі будують на основі комутаторів і маршрутизаторів. Виконано розбиття адресного простору телекомунікаційної мережі. Визначено схему поділу на підмережі, враховуючи кількість комп'ютерів в кожній підмережі. При цьому IP-адреси назначені для кожного інтерфейсу локальної мережі кожного маршрутизатора. Для побудови мережі використані комутатори Cisco Catalyst 2960 і маршрутизатори 2911. Побудована телекомунікаційна мережа в середовищі в Cisco Packet Tracer і проведено базове налаштування пристроїв. Налаштовані інтерфейси комутаторів і маршрутизаторів. Налаштовані персональні комп'ютери та проведена перевірка підключень до мережі. Проведено налаштування статичних маршрутів і маршрутів за замовчуванням. Проведена симуляція відправки пакетів між вузлами в різних підмережах. Підтверджена вірність введених налаштувань. Проведена діагностика мережі, яка показала високу пропускну здатність мережі і швидкість передачі.*

2. Висновок про відповідність роботи дипломному завданню *Кваліфікаційний проєкт відповідає виданому завданню*

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки та техніки і передових методів роботи: *В першому розділі дипломної роботи здійснено огляд принципів побудови телекомунікаційних мереж, розглянуті сучасні технології зв'язку. У другому розділі роботи виконано розбиття адресного простору телекомунікаційної мережі, побудована модель мережі у середовищі Cisco Packet Tracer, налаштовані всі активні інтерфейси маршрутизаторів, задані IP-адреси, маски підмереж. В третьому розділі роботи виконано налаштування статичних маршрутів і*

маршрутів за замовчуванням, проведено тестування навантажувальної здатності мережі.

4. Позитивні сторони роботи: *Побудована модель телекомунікаційної мережі сучасного офісу в середовищі Cisco Packet Tracer, проведена симуляція відправки пакетів між вузлами в різних підмережах. Підтверджена вірність введених налаштувань. Проведена діагностика мережі, яка показала високу навантажувальну здатність мережі і швидкість передачі пакетів*

5. Негативні сторони роботи: *У роботі бажано було би привести числові показники навантажувальної здатності, пропускної спроможності мережі. Присутні невеликі граматичні помилки. Однак, ці недоліки не мають принципового значення, суттєво не впливають на кінцевий результат і не знижують загального враження від проведеної роботи.*

6. Оцінка графічного оформлення та пояснювальної записки роботи: *Графічне оформлення та пояснювальна записка виконані згідно вимог ЄСКД*

7. Відгук про роботу в цілому: *Кваліфікаційний проєкт виконаний на високому рівні, має безперечну актуальність в області телекомунікацій. Результати дослідження мають важливе практичне застосування при налагоджуванні телекомунікаційних мереж.*

8. Інші зауваження: *немає*

9. Оцінка дипломної роботи: *Кваліфікаційний проєкт відповідає встановленим вимогам і заслуговує оцінки «відмінно», а її автор Кланцатий Д.Ю - присвоєння кваліфікації бакалавра за спеціальністю «Телекомунікації та радіотехніка»*

10. Рецензент (прізвище, ім'я, по батькові, місце роботи) *Єрьоменко Олександр Іванович – к.т.н., доцент кафедри фізики та електротехніки*

«06» червня 2025р.

підпис

Завідувачу кафедри телекомунікацій,
медійних та інтелектуальних технологій
д.т.н., професору ПІДЧЕНКУ Сергію
здобувача вищої освіти
КЛАНЦАТОГО Дмитра
ФІТ, гр. ТР2-21-1

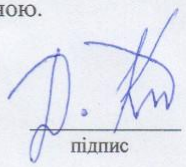
ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу мого кваліфікаційного проєкту для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом мого кваліфікаційного проєкта «Телекомунікаційна мережа сучасного офісу» в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія мого кваліфікаційного проєкту збігається (ідентична) з друкованою.

29 травня 2025 р.
дата



підпис

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 3.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 14%**

ID: 242732 Title: Телекомунікаційна мережа сучасного офісу Added in a DB: 2025-06-02 Authors: Кланцатий Дмитро Юрійович Heads: Бойко Юлій Миколайович Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	75171	1132	2658 (4%)	34 (3%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Дмитро КЛАНЦАТИЙ (ТР2-21-1)

Співавтор:

Назва: Телекомунікаційна мережа сучасного офісу

Експерт: Ливбар О.С

Підрозділ: Кафедра телекомунікацій, медійних та інтелектуальних технологій

Коефіцієнт подібності 1:13.5%

Коефіцієнт подібності 2:4.6%

Мікропробіли: 0

Заміна букв: 5

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-03 02:24:15.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування: Виявлені запозичення не є плагіатом так як відносяться до термінологічних та загальновживаних типових фраз

Дата 3.06.2025 експерт Ливбар О.С

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ КАФЕДРИ ТМІТ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи: Телекомунікаційна мережа сучасного офісу
Автор Кланцатий Дмитро Юрійович
Освітня програма: «Телекомунікації, медійні технології та інтелектуальні мережі»
Рівень вищої освіти Бакалавр
Спеціальність 172 «Телекомунікації та радіотехніка»
Науковий керівник: д.т.н., професор Бойко Ю.М

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	+
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження: Виявлені запозичення не є плагіатом так як відповідають до термінологічних та загальновживаних шаблонних фраз

Дата 05.06.2025

Завідувач кафедри _____ Підпис Підченко О. Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Підпис Стецюк В. Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Підпис Юрій Бойко Ім'я, ПРІЗВИЩЕ