МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт
з дисципліни

«КОМП'ЮТЕРНІ МЕРЕЖІ»

Івано-Франківськ
2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Фізико-технічний факультет

Кафедра комп’ютерної інженерії та електроніки

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт
з дисципліни
«КОМП'ЮТЕРНІ МЕРЕЖІ»
для здобувачів вищої освіти всіх форм навчання
першого (бакалаврського) рівня вищої освіти
спеціальностей: F7 «Комп’ютерна інженерія»,
G5 «Електроніка, електронні комунікації,
приладобудування та радіотехніка»,
015 «Професійна освіта (за спеціалізаціями)»
спеціалізація 015.39 «Цифрові технології»

Електронне видання

ЗАТВЕРДЖЕНО
кафедрою КІЕ
Протокол № 9 від 16.04.2026 р.

Івано-Франківськ
2026

Рекомендовано до друку засіданням кафедри комп’ютерної інженерії та електроніки фізико-технічного факультету Карпатського національного університету імені Василя Стефаника (протокол № 9 від 16.04.2026 р.).

Методичні вказівки до лабораторних робіт з дисципліни «Комп'ютерні мережі» для здобувачів вищої освіти всіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальностей: F7 «Комп’ютерна інженерія», G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка», 015 «Професійна освіта (за спеціалізаціями)» спеціалізація 015.39 «Цифрові технології». Упоряд.: І.В. Свид, Б.С. Дзундза. Електронне видання. Івано-Франківськ: КНУВС, 2026. 84 с. pdf 1,56 Мб.

Упорядники: І.В. Свид
Б.С. Дзундза

Рецензенти:

В.І. Голота, к.т.н., доц., доцент кафедри комп’ютерної інженерії та електроніки Карпатського національного університету імені Василя Стефаника.

І.Т. Когут, д.т.н., проф., професор кафедри комп’ютерної інженерії та електроніки Карпатського національного університету імені Василя Стефаника.

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Комп'ютерні мережі сьогодні є фундаментальною основою інформаційного суспільства, об'єднуючи окремі пристрої в єдину функціональну систему. Вони дозволяють обмінюватися даними, спільно використовувати ресурси та забезпечують роботу глобального Інтернету.

Впровадження комп'ютерних мереж є критично важливим для ефективної роботи організацій та приватних користувачів завдяки наступним перевагам:

- спільний доступ до ресурсів – це можливість використовувати один периферійний пристрій (принтер, сканер) або базу даних декількома користувачами одночасно, що значно економить кошти;
- обмін даними та комунікація – це миттєва передача інформації, електронна пошта, обмін файлами та спільна робота над документами (наприклад, через хмарні технології);
- централізоване керування та безпека – адміністратори можуть керувати безпекою, оновленнями та доступом до даних з одного місця (сервера);
- віддалений доступ – це можливість працювати з офісними ресурсами з будь-якої точки світу (дистанційна робота);
- економічна ефективність – це зниження витрат на придбання обладнання та підвищення продуктивності роботи.

Сучасне цифрове суспільство неможливе без надійних, швидкісних телекомунікаційний, інформаційних і комп’ютерних мереж, які є основою надання цифрових сервісів та послуг.

Дисципліна «Комп’ютерні мережі» відноситься дисциплін вільного вибору здобувача вищої освіти та забезпечує зальні компетентності та навики щодо побудови, модернізації та налаштування комп’ютерних мереж.

Дисципліна «Комп’ютерні мережі» пропонується до вибору здобувачам вищої освіти всіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальностей: F7 «Комп’ютерна інженерія», G5 «Електроніка, електронні

комунікації, приладобудування та радіотехніка», 015 «Професійна освіта (за спеціалізаціями)» спеціалізація 015.39 «Цифрові технології».

Метою дисципліни «Комп'ютерні мережі» є надання здобувачам вищої освіти знань щодо принципів функціонування комп'ютерних мереж, особливостей реалізації мережних технологій, ознайомлення з основними моделями, методами та технологіями комп'ютерних мереж та особливостями використання цих моделей і методів для вирішення задач проектування, модернізації та обслуговування комп'ютерних мереж різного призначення.

Завданням дисципліни «Комп'ютерні мережі» надання теоретичних і практичних знань у проектуванні, модернізації та обслуговуванні комп'ютерних мереж різного призначення.

Дисципліна «Комп'ютерні мережі» робота зі спеціалізації «Цифрові технології» спеціальності забезпечує програмні компетентності та результати навчання:

- спеціальність F7 «Комп'ютерна інженерія»:

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов.

ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ЗК12. Здатність до розуміння предметної галузі та професійної діяльності.

ЗК13. Здатність розв'язувати поставлені задачі та приймати відповідні рішення.

ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

ФК6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

ФК7. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

ФК8. Готовність брати участь у роботах з впровадження комп’ютерних систем та мереж, введення їх до експлуатації на об’єктах різного призначення.

ФК 10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.

ФК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп’ютерних засобів, систем та мереж.

ПРН2. Мати навички проведення експериментів, збирання даних та моделювання в комп’ютерних системах.

ПРН3. Знати новітні технології в галузі комп’ютерної інженерії.

ПРН4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

ПРН7. Вміти розв’язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

ПРН9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-

технічних засобів комп’ютерних систем та мереж для вирішення технічних задач спеціальності.

ПРН10. Вміти розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем, розраховувати, експлуатувати, типове для спеціальності обладнання.

ПРН13. Вміти ідентифікувати, класифікувати та описувати роботу комп’ютерних систем та їх компонентів.

ПРН15. Вміти виконувати експериментальні дослідження за професійною тематикою.

ПРН20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

ПРН21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

- спеціальність G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка»:

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми, що характеризуються комплексністю та невизначеністю умов, під час професійної діяльності у галузі електроніки, або у процесі навчання, що передбачає застосування теорій та методів електроніки.

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Навички використання інформаційних і комунікаційних технологій.

СК5. Здатність застосовувати відповідні математичні, наукові й технічні методи, сучасні інформаційні технології і комп'ютерне програмне забезпечення, навички роботи з комп'ютерними мережами, базами даних та Інтернет-ресурсами для вирішення інженерних задач в галузі електроніки.

СК10. Здатність застосовувати на практиці галузеві стандарти та стандарти якості функціонування пристроїв та систем електроніки.

Р1. Описувати принцип дії за допомогою наукових концепцій, теорій та методів та перевіряти результати при проектуванні та застосуванні приладів, пристроїв та систем електроніки.

Р5. Використовувати інформаційні та комунікаційні технології, прикладні та спеціалізовані програмні продукти для вирішення задач проектування та налагодження електронних систем, демонструвати навички програмування, аналізу та відображення результатів вимірювання та контролю.

Р7. Аналізувати складні цифрові та аналогові інформаційно-вимірювальні системи з розширеною архітектурою комп’ютерних та телекомунікаційних мереж з урахуванням специфікації вибраних технічних засобів електроніки та відповідної технічної документації.

- спеціальність 015 «Професійна освіта (за спеціалізаціями)» спеціалізація 015.39 «Цифрові технології»:

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми в професійній освіті, що передбачає застосування певних теорій і методів педагогічної науки та інших наук відповідно до спеціалізації і характеризується комплексністю та невизначеністю умов.

ЗК06. Навички використання інформаційних і комунікаційних технологій.

ЗК07. Здатність вчитися і оволодівати сучасними знаннями.

СК16 Здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище.

СК19. Здатність використовувати відповідне програмне забезпечення для вирішення професійних завдань у сфері цифрових технологій.

СК28. Базові знання в галузі інформатики й сучасних інформаційних технологій використовуючи сучасні комп'ютерні технології при вирішенні професійних задач, пов’язаних зі збором, передачею і обробкою інформації, побудовою графіків та діаграм.

СК30. Здатність застосовувати методи та засоби сучасних інформаційних технологій для проєктування та розроблення інформаційних систем та мереж.

Лабораторна робота № 1

Основи моделювання комп’ютерних мереж в Cisco Packet Tracer

1.1 Мета роботи

Опанувати основи роботи з Cisco Packet Tracer шляхом побудови простої мережі, налаштування IP-адресації та перевірки зв'язності між пристроями.

1.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і проробити відповідні теми за конспектом лекцій.

1.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням принципів моделювання комп’ютерних мереж у Cisco Packet Tracer шляхом побудови простої мережі, налаштування IP-адресації та перевірки зв'язності між пристроями.

1.4 Завдання на лабораторну роботу

1.4.1 Завантаження, встановлення та активація програми Cisco Packet Tracer

1.4.1.1 Перейдіть за посиланням https://www.netacad.com у веб-браузері. У правому верхньому куті сторінки натисніть кнопку «Login».

1.4.1.2 У вікні авторизації оберіть посилання «Sign up». Заповніть форму реєстрації як здобувач вищої освіти (студент), вказавши своє ім’я, прізвище, електронну пошту та інші необхідні дані. Після заповнення натисніть кнопку «Register» для створення облікового запису.

1.4.1.3 Після успішної реєстрації та входу до особистого кабінету перейдіть до розділу «Ресурси» у верхньому меню та оберіть пункт

«Завантажити Packet Tracer».

1.4.1.4 На сторінці завантажень виберіть версію програми, що відповідає вашій операційній системі (Windows, Linux або macOS). Завантажте інсталяційний файл на свій комп’ютер.

1.4.1.5 Запустіть завантажений файл і виконайте стандартну процедуру встановлення програми, слідуючи інструкціям майстра інсталяції. Для користувачів Linux-систем (наприклад, Linux Mint) перед запуском необхідно надати файлу права на виконання (chmod +x) та запустити його з правами суперкористувача (sudo ./CiscoPacketTracer_*.run).

1.4.1.6 Після першого запуску програми з’явиться вікно авторизації. Введіть логін і пароль від облікового запису Cisco Networking Academy, створеного на етапі 1.4.1.2.

1.4.1.7 Для зручності увімкніть опцію «Keep me logged in» (у вигляді перемикача або галочки залежно від версії програми), щоб уникнути необхідності повторного входу при кожному запуску.

1.4.1.8 Після успішної авторизації програма буде повністю активована і готова до виконання лабораторної роботи.

1.4.2 Створення та аналіз моделі комп'ютерної мережі

1.4.2.1 Запустить Packet Tracer. В нижній частині вікна послідовно вибрати: група [Network Devices], підгрупа [Hubs], пристрій [PT-HUB] та розмістити його в центрі робочої області (рис. 1.1).

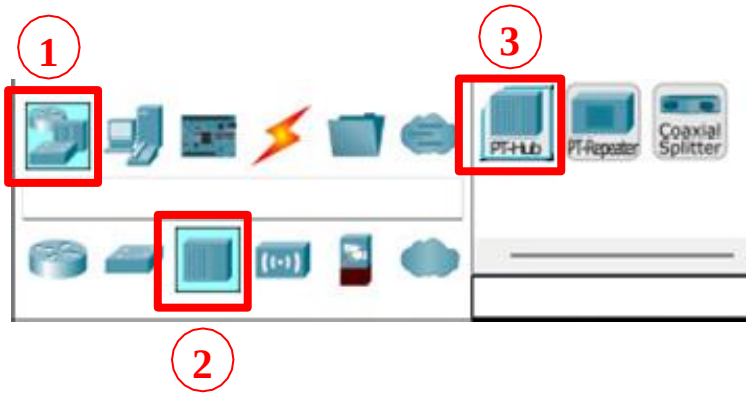

Рисунок 1.1 – Пристрої підгрупи «повторювачі»

1.4.2.2 Клікнути на піктограмі розміщеного пристрою повторювача і вибрати вкладку "Phisical". Вимнути пристрій (натиснути на зображенні вимикача), розмістити у вільних слотах модулі PT-REPEATER-NM-1CFE і знову ввімкнути пристрій (рис. 1.2).

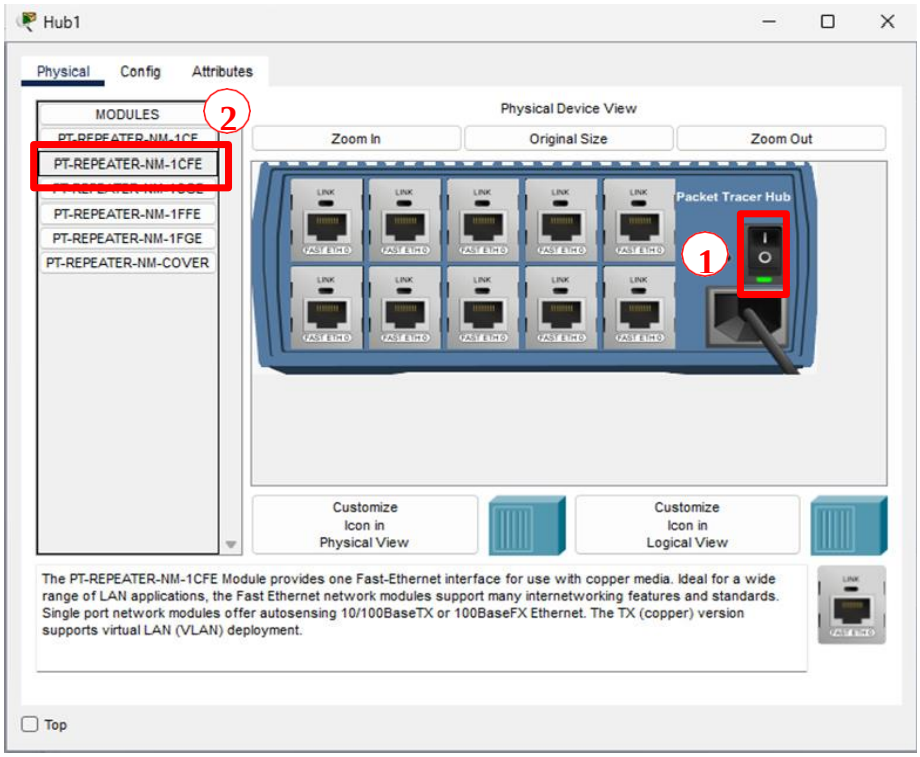

Рисунок 1.2 – Вікно апаратної конфігурації повторювача

1.4.2.3 Вибрати групу [End Devices], підгрупу [End Devices], пристрій робочої станції [PC] та розмістити його поряд з повторювачем.

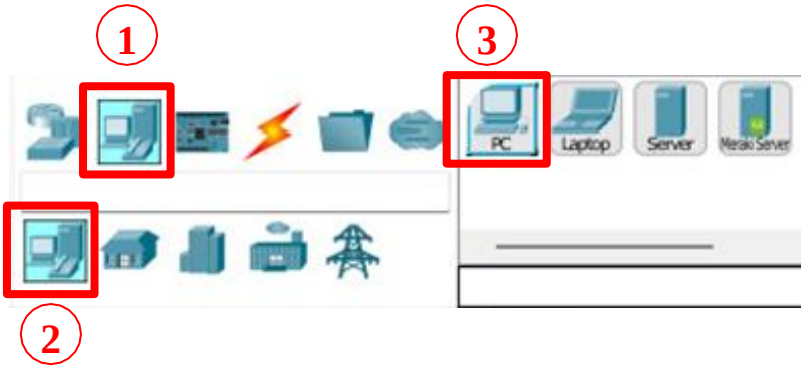

Рисунок 1.3 – Підгрупа кінцевих пристроїв

Згідно завдання необхідно розмістити три групи робочих станцій згідно таблиці 1.3. Приклад мережі наведено на рис. 1.4.

Таблиця 1.3 – Варіанти індивідуальних завдань

№ варіанту	Кількість робочих станцій			IP адреси
	група 1	група 2	група 3	
1	1	1	1	192.1.1.x
2	2	1	1	192.1.2.x
3	3	1	1	192.1.3.x
4	1	2	1	192.1.4.x
5	2	2	1	192.1.5.x
6	3	2	1	192.1.6.x
7	1	3	1	192.1.7.x
8	2	3	1	192.1.8.x
9	3	3	1	192.1.9.x
10	1	1	2	192.1.10.x
11	2	1	2	192.1.11.x
12	3	1	2	192.1.12.x
13	1	2	2	192.1.13.x
14	2	2	2	192.1.14.x
15	3	2	2	192.1.15.x
16	1	3	2	192.1.16.x
17	2	3	2	192.1.17.x
18	3	3	2	192.1.18.x
19	1	1	3	192.1.19.x
20	2	1	3	192.1.20.x
21	3	1	3	192.1.21.x
22	1	2	3	192.1.22.x
23	2	2	3	192.1.23.x
24	3	2	3	192.1.24.x
25	1	3	3	192.1.25.x
26	2	3	3	192.1.26.x
27	3	3	3	192.1.27.x
28	1	2	4	192.1.28.x
29	2	2	4	192.1.29.x
30	3	2	4	192.1.30.x

1.4.2.4 Клікнути на першому пристрої PC, на вкладці "Config" в розділі "GLOBAL-Settings" ввести ім'я PC1 для даного пристрою (поле Display name). Далі перейти в групу "Interface – FastEthernet0" і в полі "IPv4 Address" ввести адресу 192.168.x.1 згідно таблиці 1.3 (рис. 1.5, рис. 1.6). Аналогічно виконати конфігурування інших робочих станцій моделі мережі.

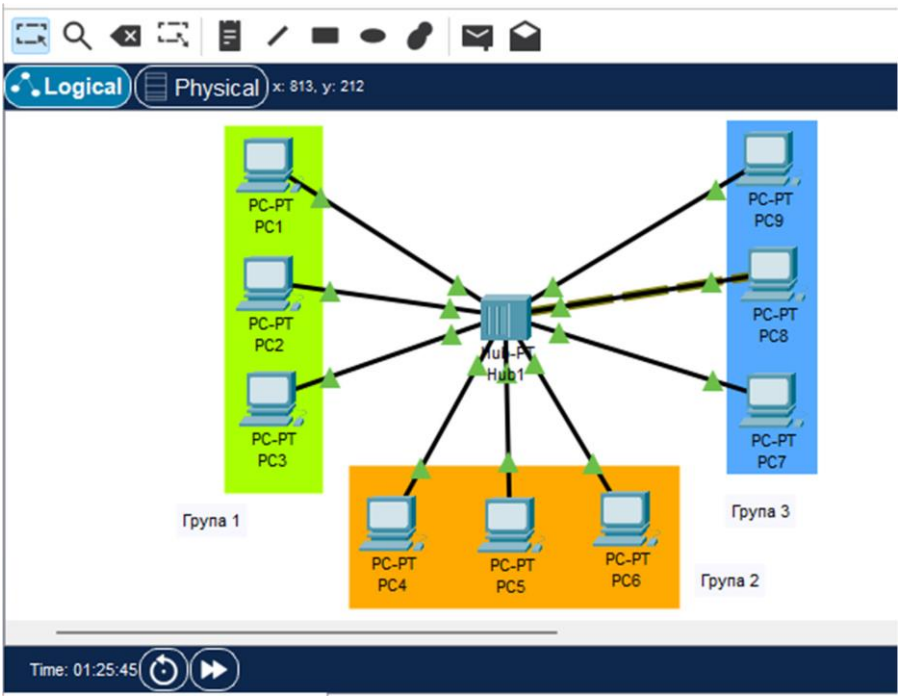

Рисунок 1.4 – Архітектура моделі мережі

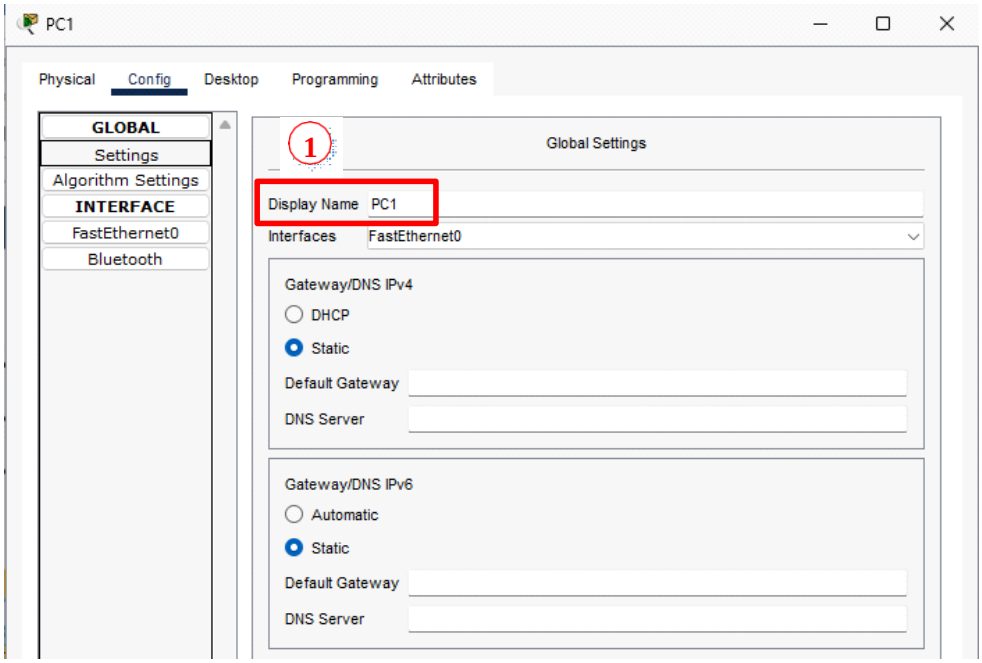

Рисунок 1.5 – Налаштування моделі робочої станції (назва)

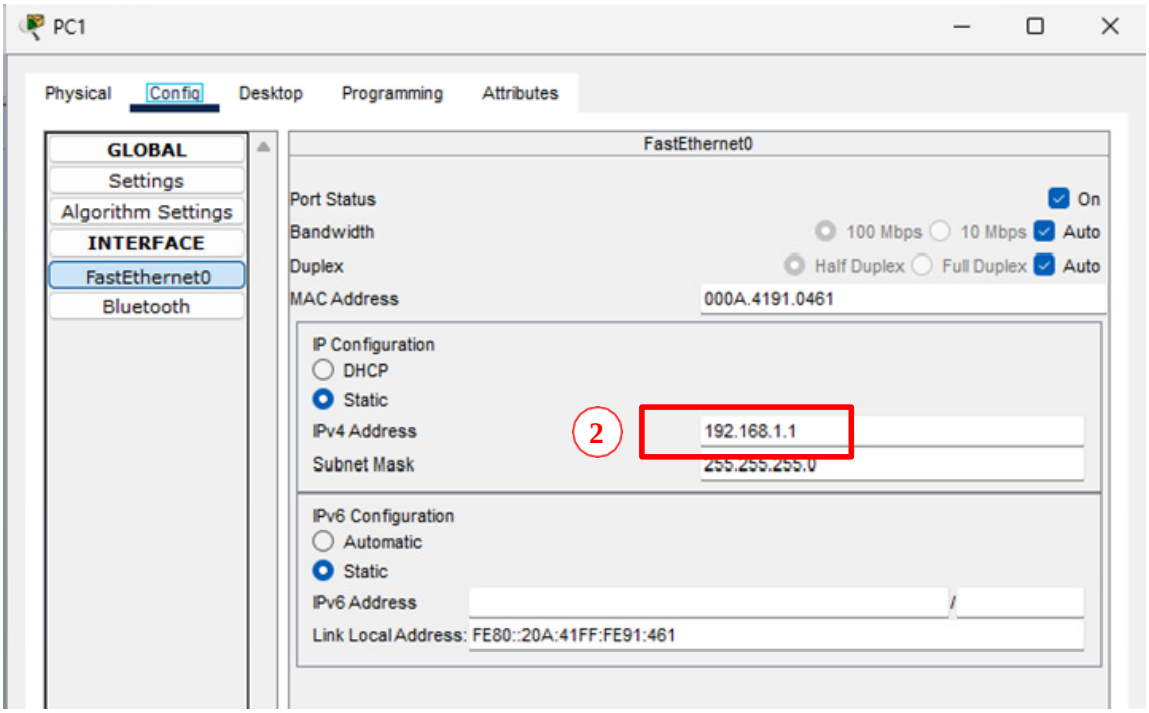

Рисунок 1.6 – Налаштування моделі робочої станції (IP адреса)

1.4.2.5 Клікнути на будь-якому пристрої робочої станції, наприклад, PC1. Перейти на вкладку "Desktop" і натиснути піктограму "Command Prompt" для запуску сесії командного рядка.

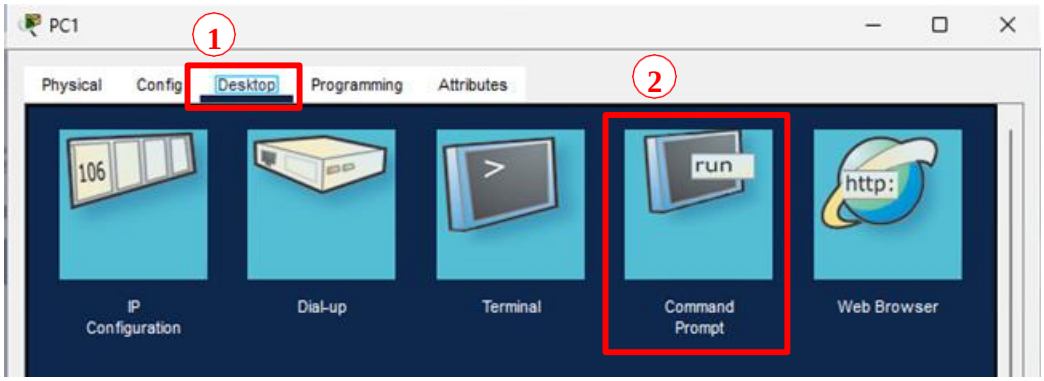

Рисунок 1.7 – Меню додатків моделі робочої станції

1.4.2.6 Ввести команду "ipconfig" для виводу налаштувань мережних інтерфейсів та впевнитись у відповідності IP адреси раніше введеному значенню (рис. 1.8).

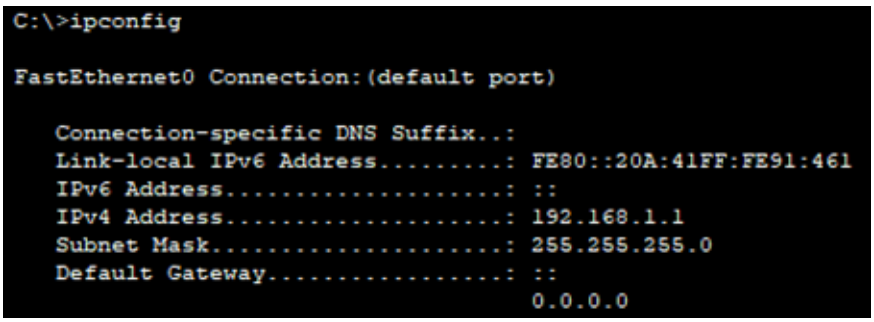

Рисунок 1.8 – Мережні налаштування моделі робочої станції

1.4.2.7 За допомогою команди ping перевірити наявність зв'язку із сусідніми робочими станціями (рис. 1.9).

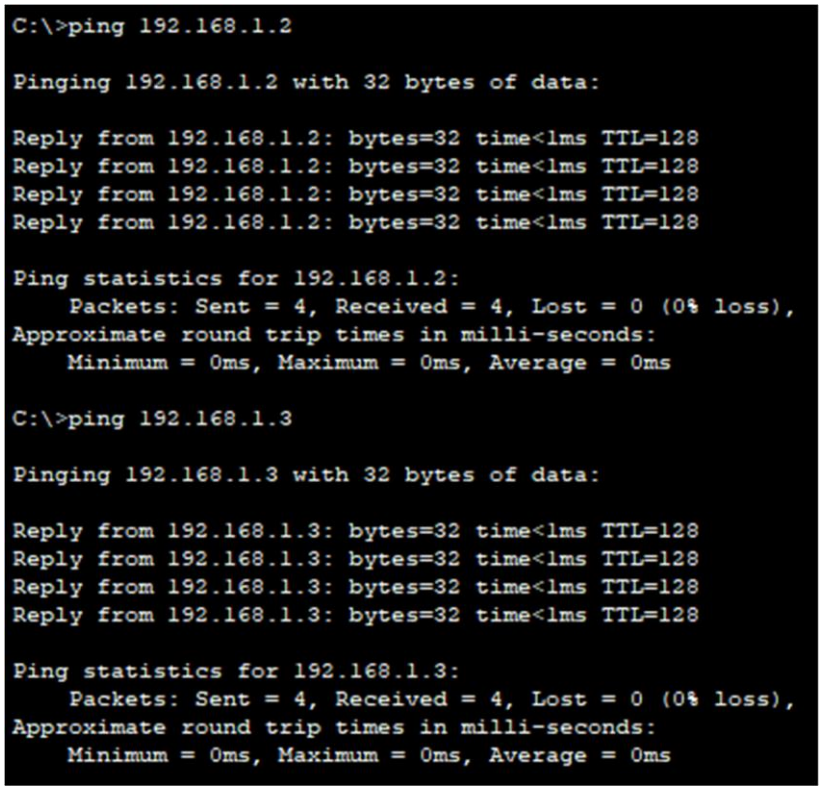

Рисунок 1.9 – Перевірка мережної зв'язності моделі робочої станції

1.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New

Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов’язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім’я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв’язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується цей розділ результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route,

show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

1.6 Контрольні запитання та завдання

1. Яке основне призначення програми Cisco Packet Tracer? Поясніть.
2. Наведіть переваги та недоліки Cisco Packet Tracer порівняні з іншими симуляторами мереж (наприклад, GNS3 або EVE-NG). Поясніть.
3. Наведіть та охарактеризуйте основні етапи процесу моделювання комп'ютерної мережі в Cisco Packet Tracer.
4. Яке призначення ієрархічних рівнів (доступу, розподілу, ядра) при проектуванні мереж?
5. Чому важливо виконувати етап планування та аналізу вимог перед створенням мережевої моделі?
6. Які основні типи пристроїв можна використовувати для побудови локальної мережі в Packet Tracer?
7. Як правильно виконати базову конфігурацію IP-адресації на кінцевому пристрої (PC) в Cisco Packet Tracer?
8. Які команди діагностики використовуються для перевірки зв'язності та налаштувань мережі, і як інтерпретувати їх результати?
9. У чому полягає різниця між фізичним і логічним моделюванням мережі в Packet Tracer?
10. Яке значення має правильне документування топології, IP-адресації та конфігурації пристроїв після завершення лабораторної роботи?

Лабораторна робота № 2

Базове конфігурування мережного обладнання Cisco

2.1 Мета роботи

Набути практичних навичок налаштування маршрутизатора Cisco.

2.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і проробити відповідні теми за конспектом лекцій.

2.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням принципів базового конфігурування мережного обладнання Cisco у Cisco Packet Tracer шляхом налаштування маршрутизатора Cisco.

2.4 Завдання на лабораторну роботу

2.4.1 Відкрити симулятор мереж Cisco Packet Tracer та побудувати схему мережі згідно рис. 2.1, що включає маршрутизатор 1841, а також дві робочі станції (PC0, PC1). Виконати з'єднання згідно табл. 2.1.

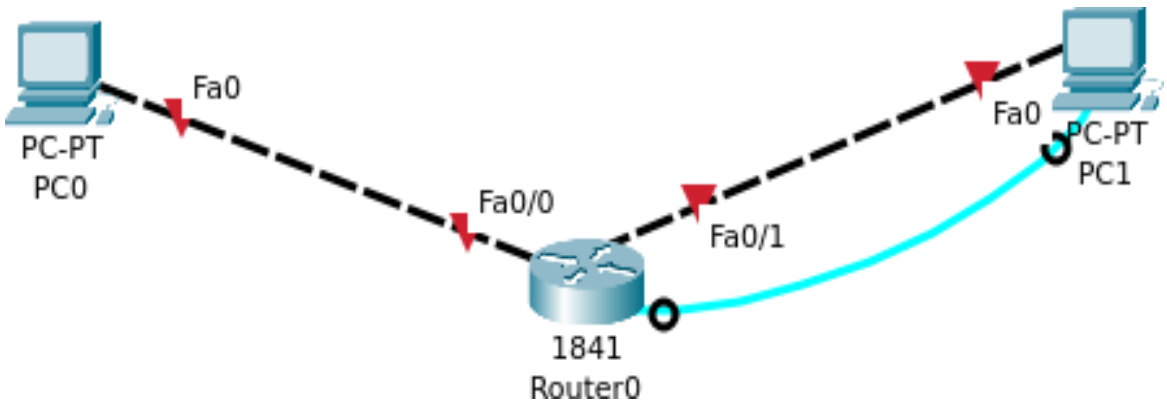

Рисунок 2.1 – Схема моделі мережі

Таблиця 2.1 – З'єднання інтерфейсів пристроїв

Тип лінії	Термінальне закінчення 1		Термінальне закінчення 2	
	пристрій	інтерфейс	пристрій	інтерфейс
Copper Cross-over	PC0	FastEthernet0	Cisco 1841	FastEthernet0/0
Copper Cross-over	PC1	FastEthernet0	Cisco 1841	FastEthernet0/1
Console	PC1	RS232	Cisco 1841	Console

2.4.2 Призначити PC0 та PC1 адреси IP згідно варіанту студента по журналу групи:

PC0 – 192.168.1.(N+10)

PC1 – 192.168.2.(N+20)

2.4.3 Клікнути курсором мишки на пристрої Cisco 1841, відкрити вкладку CLI та виконати налаштування інтерфейсів маршрутизатора

```
Router>show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
FastEthernet0/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
```

```
changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Після виконання даних команд з'єднувальні лінії перейдуть в активний стан і індикатори інтерфейсів змінять колір на зелений (рис. 2.2).

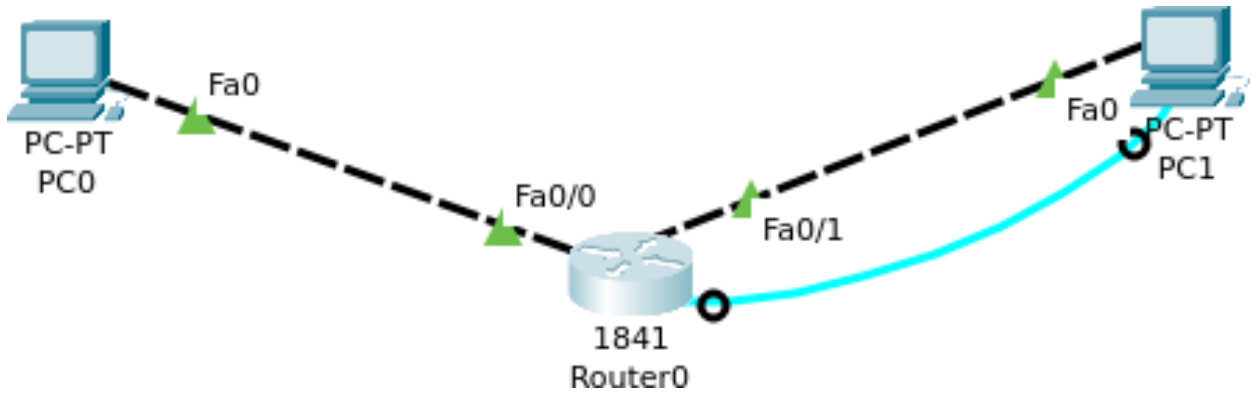

Рисунок 2.2 – Схема моделі мережі після налаштування мережних інтерфейсів

2.4.4 Виконати перевірку командою ping зв’язку між пристроями мережі.

```
Router#show ip int br
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.1.1 YES manual up up
FastEthernet0/1 192.168.2.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
Router#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/7/19
ms
Router#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8
ms
Router#ping 192.168.1.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
ms
Router>en
Router#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2
seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/7/19
ms
Router#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/7/17
ms
Router#ping 192.168.2.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.15, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0
ms
Router#ping 192.168.2.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.15, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
ms
Router#
```

2.4.5 Налаштувати дистанційний доступ до маршрутизатора 1841 по протоколу Telnet (замість cisco1 та cisco2 створити створити свої паролі):

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password cisco1
Router(config-line)#login
Router(config-line)#exit
```

```
Router(config)#enable secret cisco2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Перевірити працездатність підключення по Telnet. Для цього клікнути по PC0 або PC1, відкрити вкладку Desktop і клікнути на піктограмі Command Prompt (рис. 2.3).

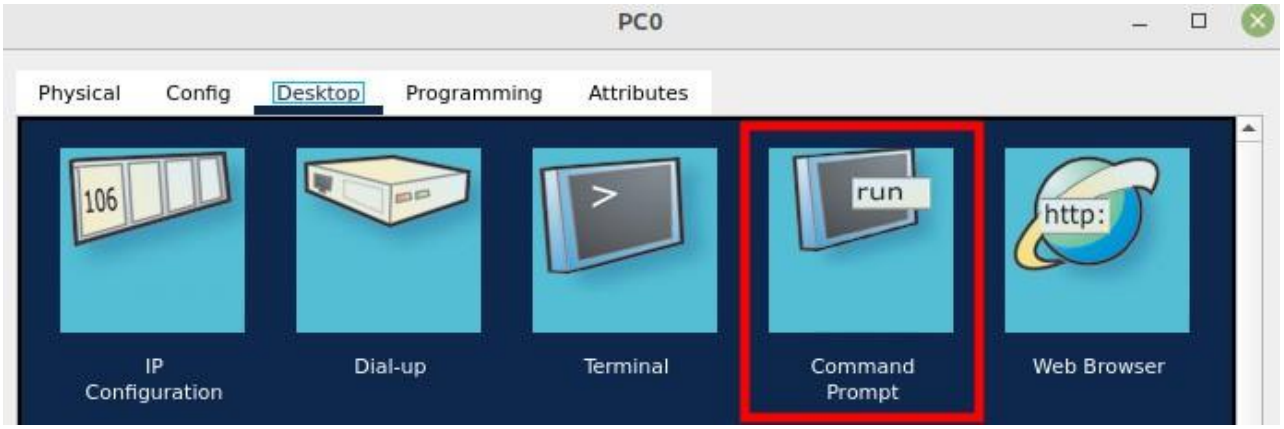

Рисунок 2.3 – Меню додатків моделі робочої станції

В командному рядку ввести команду

```
telnet ip_addr
```

де ip_addr – адреса інтерфейсу маршрутизатора, до якого відімкнена робоча станція, з якої відбувається підключення по протоколу Telnet (для PC0 це адреса 192.168.1.1) (рис. 2.4).

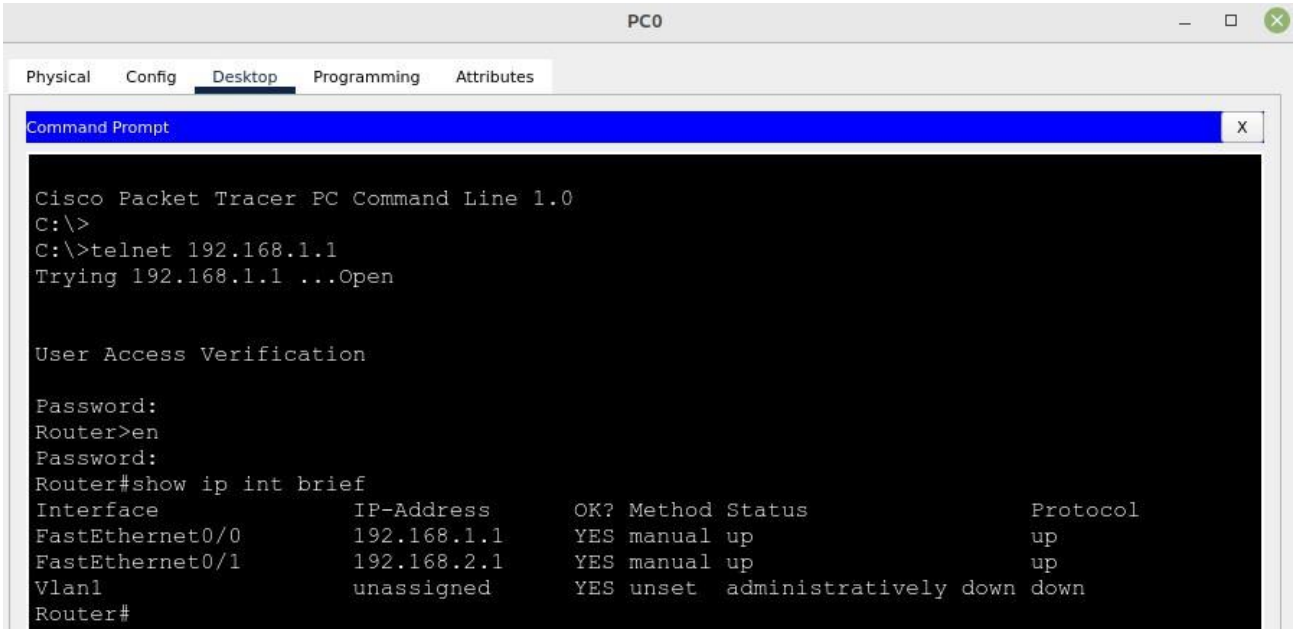

Рисунок 2.4 – Підключення до маршрутизатора через Telnet з PC

Після підключення по Telnet ви потрапите в режим користувача (Router>). Щоб зберегти конфігурацію, спочатку перейдіть у привілейований режим, ввівши команду enable та пароль *cisco2* (або ваш власний пароль, встановлений командою enable secret).

Після перевірки успішності налаштування віддаленого підключення, слід зберегти налаштування маршрутизатора:

```
Router>en
Password:
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

або

```
Router>en
Password:
Router#write memory
Building configuration...
[OK]
Router#
```

2.4.6 Протокол Telnet не передбачає шифрування пароля при організації сесії, тому він потенційно може бути перехоплений зловмисниками. Тому дистанційне підключення до пристроїв слід організовувати по захищеному SSH (Secure Shell) протоколу.

Переходимо в режим глобальної конфігурації

```
Router>en
Password:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Задати ім'я домену

```
Router(config)#ip domain-name mgu-it
```

Задати ім'я маршрутизатора

```
Router(config)#hostname R0
```

Згенерувати RSA ключ

```
R0(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R0.mgu-it
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
*Mar 1 0:46:47.48: %SSH-5-ENABLED: SSH 1.99 has been enabled
R0(config)#
```

Задати логін та пароль з'єднання SSH

```
R0(config)#username admin secret cisco
```

Задати логін

```
R0(config)#line vty 0 15
R0(config-line)#transport input ssh
R0(config-line)#login local
R0(config-line)#ip ssh version 2
R0(config-line)#end
R0#
```

Перевірити працездатність підключення по SSH. Для цього клікнути по PC0 або PC1, відкрити вкладку Desktop і клікнути на піктограмі Command Prompt.

```
C:\>ssh -l admin 192.168.1.1
Password: <пароль для підключення по SSH>
R0>en
Password: <пароль для привілейованого режиму>
R0#
```

2.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов'язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім'я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім'я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв'язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за

наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом студента. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується ця частина результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route, show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

2.6 Контрольні запитання та завдання

1. Які основні типи мережевого обладнання виробляє компанія Cisco, і які їхні основні функції?

2. Що таке операційна система Cisco IOS, і яке її значення для адміністрування мережевого обладнання?

3. Які існують режими роботи Cisco IOS, яка їх ієрархія, і як здійснюється перехід між ними?

4. Які основні команди Cisco IOS використовуються для перегляду стану пристрою та поточної конфігурації?

5. Як налаштовуються IP-адреси та активуються мережеві інтерфейси на маршрутизаторі Cisco?

6. Який процес завантаження Cisco IOS на пристрої, і яку роль відіграють пам'яті ROM, Flash, RAM та NVRAM?

7. Як налаштувати віддалений доступ до маршрутизатора за допомогою протоколу Telnet, і які його безпекові недоліки?

8. Які кроки необхідно виконати для налаштування безпечного віддаленого доступу до маршрутизатора за допомогою SSH?

9. Як зберегти поточну конфігурацію пристрою Cisco, щоб вона зберігалася після перезавантаження, і як видалити збережену конфігурацію?

10. Які основні діагностичні команди (наприклад, ping, show ip interface brief, show version) використовуються для перевірки працездатності мережі та налаштувань на пристроях Cisco?

Лабораторна робота № 3

Сегментація мереж з використанням VLAN

3.1 Мета роботи

Налаштування VLAN та забезпечення маршрутизації між віртуальними мережами через SVI-інтерфейси на комутаторах.

3.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і опрацювати відповідні теми за конспектом лекцій.

3.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням сегментації мереж з використанням VLAN у Cisco Packet Tracer.

3.4 Завдання на лабораторну роботу

3.4.1 У цій лабораторній роботі створюємо ієрархічну мережну топологію в програмі Cisco Packet Tracer, яка складається з двох комутаторів доступу та одного багаторівневого комутатора. Ця топологія моделює типову корпоративну мережу, де комутатори доступу підключають кінцеві пристрої, а комутатор розподілу забезпечує зв'язність між сегментами та виконує функції маршрутизації. Метою цього етапу є правильне фізичне з'єднання всіх пристроїв згідно з заданою схемою, що стане основою для подальшого логічного налаштування VLAN та між-VLAN маршрутизації у наступних пунктах завдання.

Топологія включає два комутатори моделі WS-C2960-24TT-L, які виступають у ролі комутаторів доступу S1 та S2, і один комутатор Cisco 3560-

24PS, який виступає у ролі центрального комутатора Core (рис. 3.1). До комутатора S1 підключаються робочі станції PC1, PC2, PC5, PC6, PC9, а до комутатора S2 — робочі станції PC3, PC4, PC7, PC8. Додатково, робоча станція PC10 підключається безпосередньо до комутатора Core. Зв'язок між комутаторами S1 та Core і між S2 та Core здійснюється за допомогою кросоверних кабелів, що підключаються до гігабітних інтерфейсів. Для з'єднання робочих станцій з комутаторами використовуються прямі кабелі. Ця архітектура дозволяє реалізувати сегментацію мережі за допомогою VLAN, де трафік ізольованих сегментів передається між комутаторами через trunk лінки, а взаємодія між сегментами забезпечується за рахунок маршрутизації на комутаторі Core.

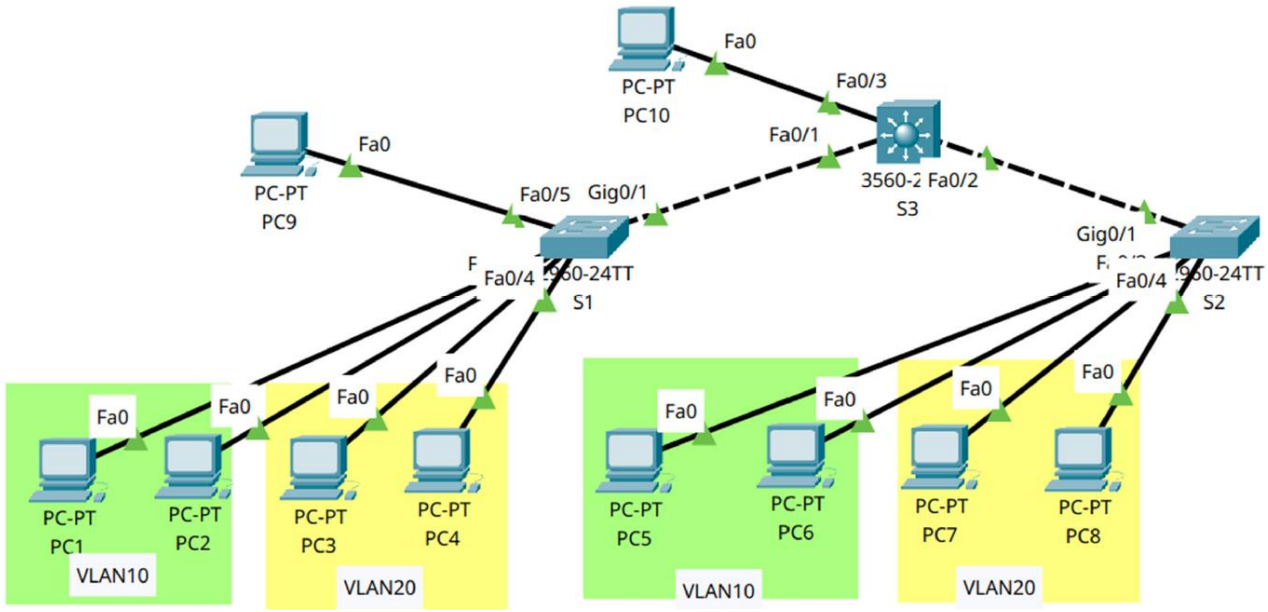

Рисунок 3.1 – Архітектура мережі зв’язку з використанням комутаторів L2 та L3

Кожен студент отримує індивідуальний варіант завдання, який визначає номери двох VLAN, що використовуються для сегментації користувацьких робочих станцій PC1-PC8 (табл. 3.1 та 3.2). Робочі станції PC9 та PC10 призначені виключно для цілей адміністрування мережі і завжди належать до VLAN 1. У таблиці варіантів вказано, які саме VLAN використовуються у кожному випадку, а також які робочі станції на кожному комутаторі доступу

належать до першої VLAN (вказаної в стовпці "VLAN 1"), а які – до другої VLAN (вказаної в стовпці "VLAN 2"). Наприклад, у варіанті 1 робочі станції PC1, PC2, PC5, PC6 належать до VLAN 10, а PC3, PC4, PC7, PC8 – до VLAN 20. У варіанті 16 ті ж самі номери VLAN використовуються, але розподіл змінюється: PC1, PC2, PC5, PC6 належать до VLAN 20, а PC3, PC4, PC7, PC8 – до VLAN 10. Це дозволяє забезпечити різноманітність завдань для всіх студентів.

Таблиця 3.1 – Таблиця зв'язності пристроїв

Пристрій 1	Інтерфейс (порт)	Кабель	Пристрій 2	Інтерфейс (порт)
PC1	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/1
PC2	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/2
PC3	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/3
PC4	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/4
PC5	FastEthernet0	Прямий (Copper Straight-Through)	S2	FastEthernet0/1
PC6	FastEthernet0	Прямий (Copper Straight-Through)	S2	FastEthernet0/2
PC7	FastEthernet0	Прямий (Copper Straight-Through)	S2	FastEthernet0/3
PC8	FastEthernet0	Прямий (Copper Straight-Through)	S2	FastEthernet0/4
PC9	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/5
PC10	FastEthernet0	Прямий (Copper Straight-Through)	Core	FastEthernet0/3
S1	GigabitEthernet0/1	Кросоверний (Copper Cross-Over)	Core	GigabitEthernet0/1
S2	GigabitEthernet0/1	Кросоверний (Copper Cross-Over)	Core	GigabitEthernet0/2

Таблиця 3.2 – Варіанти індивідуальних завдань

№	VLAN A (номер)	Робочі станції у VLAN A	VLAN B (номер)	Робочі станції у VLAN B
1	10	PC1, PC2, PC3, PC4	20	PC5, PC6, PC7, PC8
2	10	PC1, PC2, PC7, PC8	30	PC3, PC4, PC5, PC6
3	10	PC1, PC3, PC5, PC7	40	PC2, PC4, PC6, PC8
4	10	PC1, PC4, PC5, PC8	50	PC2, PC3, PC6, PC7
5	10	PC1, PC2, PC5, PC8	60	PC3, PC4, PC6, PC7
6	20	PC1, PC3, PC6, PC8	30	PC2, PC4, PC5, PC7
7	20	PC1, PC4, PC6, PC7	40	PC2, PC3, PC5, PC8
8	20	PC2, PC3, PC5, PC8	50	PC1, PC4, PC6, PC7
9	20	PC2, PC4, PC5, PC7	60	PC1, PC3, PC6, PC8
10	30	PC1, PC2, PC7, PC8	40	PC3, PC4, PC5, PC6
11	30	PC3, PC4, PC5, PC6	50	PC1, PC2, PC7, PC8
12	30	PC1, PC5, PC6, PC7	60	PC2, PC3, PC4, PC8
13	40	PC2, PC5, PC6, PC8	50	PC1, PC3, PC4, PC7
14	40	PC3, PC5, PC6, PC7	60	PC1, PC2, PC4, PC8
15	50	PC1, PC3, PC4, PC8	60	PC2, PC5, PC6, PC7
16	20	PC1, PC2, PC3, PC4	10	PC5, PC6, PC7, PC8
17	30	PC1, PC2, PC7, PC8	10	PC3, PC4, PC5, PC6
18	40	PC1, PC3, PC5, PC7	10	PC2, PC4, PC6, PC8
19	50	PC1, PC4, PC5, PC8	10	PC2, PC3, PC6, PC7
20	60	PC1, PC2, PC5, PC8	10	PC3, PC4, PC6, PC7
21	30	PC1, PC3, PC6, PC8	20	PC2, PC4, PC5, PC7
22	40	PC1, PC4, PC6, PC7	20	PC2, PC3, PC5, PC8
23	50	PC2, PC3, PC5, PC8	20	PC1, PC4, PC6, PC7
24	60	PC2, PC4, PC5, PC7	20	PC1, PC3, PC6, PC8
25	40	PC1, PC2, PC7, PC8	30	PC3, PC4, PC5, PC6
26	50	PC3, PC4, PC5, PC6	30	PC1, PC2, PC7, PC8
27	60	PC1, PC5, PC6, PC7	30	PC2, PC3, PC4, PC8
28	50	PC2, PC5, PC6, PC8	40	PC1, PC3, PC4, PC7
29	60	PC3, PC5, PC6, PC7	40	PC1, PC2, PC4, PC8
30	60	PC1, PC3, PC4, PC8	50	PC2, PC5, PC6, PC7

3.4.2 Налаштування комутатора доступу S1.

3.4.2.1 Створення VLAN та призначення портів. На комутаторі S1 створюються дві віртуальні мережі: VLAN 10 для відділу “Admin” та VLAN 20 для відділу “Sales”. Порти, до яких підключені робочі станції, налаштовуються

як access порти. Access порти призначені для підключення кінцевих пристроїв (PC, принтерів) і передають трафік лише одного VLAN без тегів. Порти Fa0/1 та Fa0/2 призначаються до VLAN 10, а порти Fa0/3 та Fa0/4 — до VLAN 20. Також налаштовується порт Fa0/5 для підключення PC9 до VLAN 1 (мережа керування).

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Admin
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name Sales
S1(config-vlan)#exit
S1(config)#interface range fastEthernet 0/1 - 2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#interface range fastEthernet 0/3 - 4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 20
S1(config-if-range)#exit
S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 1
S1(config-if)#exit
S1(config)#
```

3.4.2.2 Налаштування trunk порту. Порт GigabitEthernet0/1 налаштовується як trunk порт для підключення до комутатора Core. Trunk порти використовуються для передачі трафіку з декількох VLAN між комутаторами або між комутатором і маршрутизатором. Для цього використовується протокол тегування 802.1Q (dot1q), який додає до кадру Ethernet спеціальний тег (мітку) з ідентифікатором VLAN. Оскільки за замовчуванням інкапсуляція trunk може бути в режимі “Auto”, спочатку явно встановлюється switchport trunk encapsulation dot1q. Потім порт переводиться в режим trunk. Команда switchport trunk allowed vlan 1,10,20 явно вказує, які VLAN дозволено передавати по цьому лінку. Це важливо для безпеки та контролю трафіку.

```
S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 1,10,20
S1(config-if)#exit
S1(config)#
```

3.4.2.3 Налаштування інтерфейсу керування та шлюзу. Для віддаленого керування комутатором S1 створюється віртуальний інтерфейс VLAN 1 з IP-адресою 192.168.1.10. Цей інтерфейс дозволяє отримувати доступ до комутатора через мережу за допомогою протоколів Telnet або SSH. Команда no shutdown активує інтерфейс. Оскільки S1 є комутатором 2-го рівня (Layer 2), він не виконує маршрутизацію. Тому для доступу до пристроїв поза мережею 192.168.1.0/24 (наприклад, до інтерфейсів керування інших комутаторів або до PC у VLAN 10/20) встановлюється шлюз за замовчуванням (default gateway). У цій топології шлюзом є IP-адреса SVI VLAN 1 на комутаторі Core – 192.168.1.1. Всі пакети, призначені для інших мереж, будуть відправлятися на цей шлюз.

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.10 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.1.1
S1(config)#
```

3.4.3 Налаштування комутатора доступу S2. Налаштування S2 аналогічне S1, оскільки він виконує таку саму роль комутатора доступу.

3.4.3.1 Створення VLAN та призначення портів. Створюються VLAN 10 та VLAN 20. Порти Fa0/1 та Fa0/2 налаштовуються як access порти для VLAN 10. Порти Fa0/3 та Fa0/4 – для VLAN 20. Це забезпечує сегментацію трафіку користувачів на S2.

```
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Admin
S2(config-vlan)#exit
S2(config)#vlan 20
S2(config-vlan)#name Sales
S2(config-vlan)#exit
```

```
S2(config)#interface range fastEthernet 0/1 - 2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#exit
S2(config)#interface range fastEthernet 0/3 - 4
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#exit
S2(config)#
```

3.4.3.2 Налаштування trunk порту. Порт GigabitEthernet0/1 налаштовується як trunk порт з інкапсуляцією 802.1Q для передачі тегованого трафіку VLAN 1, 10 та 20 до комутатора Core. Явне вказання дозволених VLAN забезпечує контроль над трафіком.

```
S2(config)#interface gigabitEthernet 0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 1,10,20
S2(config-if)#exit
S2(config)#
```

3.4.3.3 Налаштування інтерфейсу керування та шлюзу. Створюється інтерфейс VLAN 1 для керування S2 з унікальною IP-адресою 192.168.1.11. Шлюз за замовчуванням встановлюється на 192.168.1.1 (Core), щоб забезпечити зв’язок з іншими мережами та пристроями керування.

```
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.11 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.1.1
S2(config)#
```

3.4.4 Налаштування багаторівневого комутатора Core (Cisco 3560-24PS).

3.4.4.1 Створення VLAN. Хоча VLAN 10 та 20 вже існують на комутаторах доступу, їх також потрібно створити на комутаторі Core. Це необхідно для того, щоб Core “розумів”, до яких VLAN належить трафік, що приходить по trunk портах. Без цього SVI (інтерфейси для маршрутизації) не зможуть бути правильно налаштовані.

```
Core#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core(config)#vlan 10
Core(config-vlan)#name Admin
Core(config-vlan)#exit
Core(config)#vlan 20
Core(config-vlan)#name Sales
Core(config-vlan)#exit
Core(config)#
```

3.4.4.2 Налаштування trunk портів. Порти fastEthernet0/1 та fastEthernet0/2 налаштовуються як trunk порти для підключення до S1 та S2. На комутаторах 3560 за замовчуванням trunk інкапсуляція може бути в режимі “Auto”, що не дозволяє вручну встановити режим trunk. Тому спочатку явно вказується switchport trunk encapsulation dot1q. Потім порти переводяться в режим trunk, і дозволяється передача трафіку VLAN 1, 10 та 20. Це забезпечує надходження всього необхідного трафіку від комутаторів доступу до Core.

```
Core(config)#interface range fastEthernet 0/1 - 2
Core(config-if-range)#switchport trunk encapsulation dot1q
Core(config-if-range)#switchport mode trunk
Core(config-if-range)#switchport trunk allowed vlan 1,10,20
Core(config-if-range)#exit
Core(config)#
```

3.4.4.3 Ввімкнення між-VLAN маршрутизації. Ключова функція комутатора 3560-24PS — це можливість виконувати маршрутизацію на рівні 3 (IP). За замовчуванням комутатор працює лише як комутатор 2-го рівня. Щоб ввімкнути функцію маршрутизатора, необхідно виконати команду ip routing. Після цього комутатор зможе аналізувати IP-адреси призначення в пакетах і приймати рішення про їх передачу між різними підмережами (VLAN).

```
Core(config)#ip routing
Core(config)#
```

3.4.4.4 Створення SVI для маршрутизації. Для кожної VLAN, між якими потрібно забезпечити зв’язок, створюється Switched Virtual Interface (SVI). SVI -

це віртуальний інтерфейс, який діє як шлюз за замовчуванням (default gateway) для всіх пристроїв у відповідній VLAN. Наприклад, SVI interface vlan 10 з IP-адресою 192.168.10.1 стає шлюзом для всіх PC у VLAN 10. Коли PC1 (192.168.10.10) хоче надіслати пакет до PC3 (192.168.20.10), він відправляє його на свій шлюз (192.168.10.1). Комутатор Core отримує цей пакет, аналізує IP-адресу призначення, знаходить маршрут до мережі 192.168.20.0/24 через SVI vlan 20 і передає пакет далі. Команда no shutdown обов'язково активує інтерфейс.

```
Core(config)#interface vlan 10
Core(config-if)#ip address 192.168.10.1 255.255.255.0
Core(config-if)#no shutdown
Core(config-if)#exit
Core(config)#interface vlan 20
Core(config-if)#ip address 192.168.20.1 255.255.255.0
Core(config-if)#no shutdown
Core(config-if)#exit
Core(config)#
```

3.4.4.5 Налаштування інтерфейсу керування. Для керування самим комутатором Core створюється SVI для VLAN 1 з IP-адресою 192.168.1.1. Це дозволяє адміністраторам підключатися до Core з будь-якого пристрою в мережі керування (VLAN 1), наприклад, з PC9 або PC10. Цей інтерфейс також використовується для відправки системних повідомлень (наприклад, за допомогою SNMP або Syslog).

```
Core(config)#interface vlan 1
Core(config-if)#ip address 192.168.1.1 255.255.255.0
Core(config-if)#no shutdown
Core(config-if)#exit
Core(config)#
```

3.4.4.6 Налаштування порту доступу для PC10. Щоб PC10 міг підключитися до мережі керування (VLAN 1) і отримати доступ до інтерфейсу 192.168.1.1, порт FastEthernet0/3 налаштовується як access порт і призначається до VLAN 1. Команда no shutdown гарантує, що порт буде активний.

```
Core(config)#interface fastEthernet 0/3
Core(config-if)#switchport mode access
Core(config-if)#switchport access vlan 1
Core(config-if)#no shutdown
Core(config-if)#exit
Core(config)#
```

3.4.5 Налаштування робочих станцій (PC).

Налаштуйте всі робочі станції з врахуванням підмереж (номерів VLAN) в таблиці 3.3. Адреси двох підмереж, до яких входять PC краще умовно співставити з номером VLAN:

1) для VLAN A – 192.168.($N_{VLAN\ A}$).0;

2) для VLAN B – 192.168.($N_{VLAN\ B}$).0;

Шлюз за замовчуванням для користувацьких PC (PC1-PC8) – це відповідна IP-адреса SVI їх VLAN на комутаторі Core. Для PC у VLAN 1 (PC9, PC10) шлюзом є IP-адреса SVI VLAN 1 на Core.

Таблиця 3.3 – Налаштування PC та портів комутатора в прикладі завдання до лабораторної роботи

Комп'ютер	VLAN	IP-адреса	Маска підмережі	Шлюз за замовчуванням
PC1	10	192.168.10.10	255.255.255.0	192.168.10.1
PC2	10	192.168.10.11	255.255.255.0	192.168.10.1
PC3	20	192.168.20.10	255.255.255.0	192.168.20.1
PC4	20	192.168.20.11	255.255.255.0	192.168.20.1
PC5	10	192.168.10.12	255.255.255.0	192.168.10.1
PC6	10	192.168.10.13	255.255.255.0	192.168.10.1
PC7	20	192.168.20.12	255.255.255.0	192.168.20.1
PC8	20	192.168.20.13	255.255.255.0	192.168.20.1
PC9	1	192.168.1.10	255.255.255.0	192.168.1.1
PC10	1	192.168.1.100	255.255.255.0	192.168.1.1

3.4.6 Тестування моделі мережі.

3.4.6.1 Перевірка зв'язності в межах VLAN: З PC1 виконайте команду ping до PC2 (192.168.10.11) та PC5 (192.168.10.12). З PC3 виконайте ping до PC4 (192.168.20.11) та PC7 (192.168.20.12). Успішний ping підтверджує правильну комутацію трафіку в межах VLAN.

3.4.6.2 Перевірка між-VLAN маршрутизації: З PC1 виконайте ping до PC3 (192.168.20.10), PC4 (192.168.20.11), PC7 (192.168.20.12) та PC8 (192.168.20.13).

Успішний ping підтверджує, що комутатор Core коректно маршрутизує трафік між VLAN 10 та VLAN 20.

3.4.6.3 Перевірка доступу до інтерфейсу керування: З PC9 виконайте ping до 192.168.1.1 (Core) та 192.168.1.10 (S1). З PC10 виконайте ping до 192.168.1.1 (себе), 192.168.1.10 (S1) та 192.168.1.11 (S2). Успішний ping підтверджує, що мережа керування (VLAN 1) працює і всі комутатори доступні для керування.

3.4.6.4 Перевірка маршрутизації з іншого сегменту: З PC9 (який знаходиться у VLAN 1) виконайте ping до PC1 (192.168.10.10). Це підтверджує, що Core може маршрутизувати трафік не тільки між користувацькими VLAN, але й між VLAN керування та користувацькими VLAN, що важливо для моніторингу та діагностики мережі.

3.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов’язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім’я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці

налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв’язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується цей розділ результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route, show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

3.6 Контрольні запитання та завдання

1. Що таке VLAN і які основні переваги використання віртуальних локальних мереж у корпоративній інфраструктурі?
2. Яку роль відіграє тегування IEEE 802.1Q у передачі трафіку між комутаторами, і як структурований VLAN-тег у кадрі Ethernet?
3. Чим відрізняються access-порти від trunk-портів, і в яких випадках використовується кожен тип порту?
4. Яка основна відмінність між комутаторами Cisco Catalyst 2960 та 3560, і чому комутатор 3560 може виконувати між-VLAN маршрутизацію?
5. Що таке SVI (Switched Virtual Interface), і як він забезпечує міжVLAN маршрутизацію на багаторівневому комутаторі?
6. Чому необхідно виконувати команду ip routing на комутаторі Cisco 3560, і що відбудеться, якщо цю команду не активувати?
7. Як правильно налаштувати trunk-порт між комутаторами S1 і Core, і для чого потрібно вказувати switchport trunk allowed vlan та native vlan?
8. Навіщо створюється окрема VLAN для керування (наприклад, VLAN 1 або VLAN 99), і як забезпечується доступ до інтерфейсів керування комутаторів?
9. Як визначається приналежність робочої станції до певної VLAN, і які параметри IP-налаштування мають бути вказані на PC для коректної роботи в сегментованій мережі?
10. Які діагностичні команди Cisco IOS використовуються для перевірки конфігурації VLAN, стану trunk-портів та таблиці маршрутизації, і яку інформацію вони надають?

Лабораторна робота № 4

Вивчення принципів сегментації мережі за допомогою технології VLSM

4.1 Мета роботи

Опрацювати навички розрахунку підмереж змінної довжини та налаштування мережевого обладнання для забезпечення міжмережевої взаємодії.

4.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і опрацювати відповідні теми за конспектом лекцій.

4.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням принципів сегментації мережі за допомогою технології VLSM у Cisco Packet Tracer.

4.4 Завдання на лабораторну роботу

Індивідуальне завдання для студента складається з двох основних частин: теоретичної та практичної. Теоретична частина передбачає виконання розрахунків схеми IP-адресації на основі індивідуального варіанта, визначеного за табл. 4.6 з 30 можливих варіантів. Кожен варіант містить базову мережу класу C (з маскою /24), яку необхідно розділити на чотири підмережі згідно із заданими кількістю хостів у кожній. Використовуючи метод VLSM (змінна маска підмережі), студент повинен визначити мінімально необхідний розмір кожної підмережі з урахуванням службових адрес (мережева та широкомовна), підібрати відповідну маску, розрахувати межі діапазонів адрес і сформувати структуровану таблицю адресації. Усі розрахунки мають бути виконані з

дотриманням принципів VLSM для ефективного використання адресного простору.

Таблиця 4.1 – Варіанти завдань для індивідуального завдання

№ варіанта	Базова мережа	Кількість хостів у підмережі			
		Підмережа 1	Підмережа 2	Підмережа 3	Підмережа 4
1	192.168.10.0/24	60	30	14	6
2	192.168.15.0/24	50	25	12	8
3	10.10.5.0/24	70	35	18	10
4	172.16.20.0/24	45	22	11	5
5	192.168.25.0/24	80	40	20	12
6	10.15.8.0/24	55	28	15	7
7	172.20.12.0/24	65	32	16	9
8	192.168.30.0/24	40	20	10	4
9	10.25.3.0/24	75	38	19	11
10	172.25.18.0/24	35	18	9	3
11	192.168.35.0/24	85	42	21	13
12	10.30.7.0/24	48	24	13	6
13	172.30.15.0/24	62	31	17	8
14	192.168.40.0/24	52	26	14	7
15	10.35.12.0/24	68	34	18	10
16	172.35.22.0/24	42	21	12	5
17	192.168.45.0/24	78	39	20	12
18	10.40.6.0/24	58	29	16	8
19	172.40.28.0/24	46	23	13	6
20	192.168.50.0/24	72	36	19	11
21	10.45.9.0/24	54	27	15	7
22	172.45.35.0/24	66	33	18	9
23	192.168.55.0/24	44	22	12	5
24	10.50.14.0/24	82	41	22	13
25	172.50.42.0/24	38	19	11	4
26	192.168.60.0/24	76	38	20	12
27	10.55.11.0/24	56	28	16	8
28	172.55.48.0/24	64	32	17	9
29	192.168.65.0/24	49	25	14	6
30	10.60.16.0/24	74	37	19	11

Практична реалізація розрахованої схеми підмережування виконується в середовищі Cisco Packet Tracer з використанням типового мережевого обладнання. Топологія мережі включає один маршрутизатор з додатковим модулем, чотири комутатори та вісім комп’ютерів, розподілених по підмережах відповідно до розрахунків.

На рис. 4.1 зображена структурна схема мережі з центральним маршрутизатором Router0 типу 2811, обладнаним модулем NM-2FE2W для розширення кількості інтерфейсів. До маршрутизатора підключені чотири комутатори Switch0, Switch1, Switch2 та Switch3 типу 2960-24TT через інтерфейси FastEthernet 0/0, 0/1, 1/0 та 1/1 відповідно. До кожного комутатора підключено по два комп'ютери: PC0 та PC1 до Switch0, PC2 та PC3 до Switch1, PC4 та PC5 до Switch2, PC6 та PC7 до Switch3. З'єднання між маршрутизатором та комутаторами здійснюється прямими кабелями типу Straight-Through, а між комутаторами та комп'ютерами також використовуються прямі кабелі.

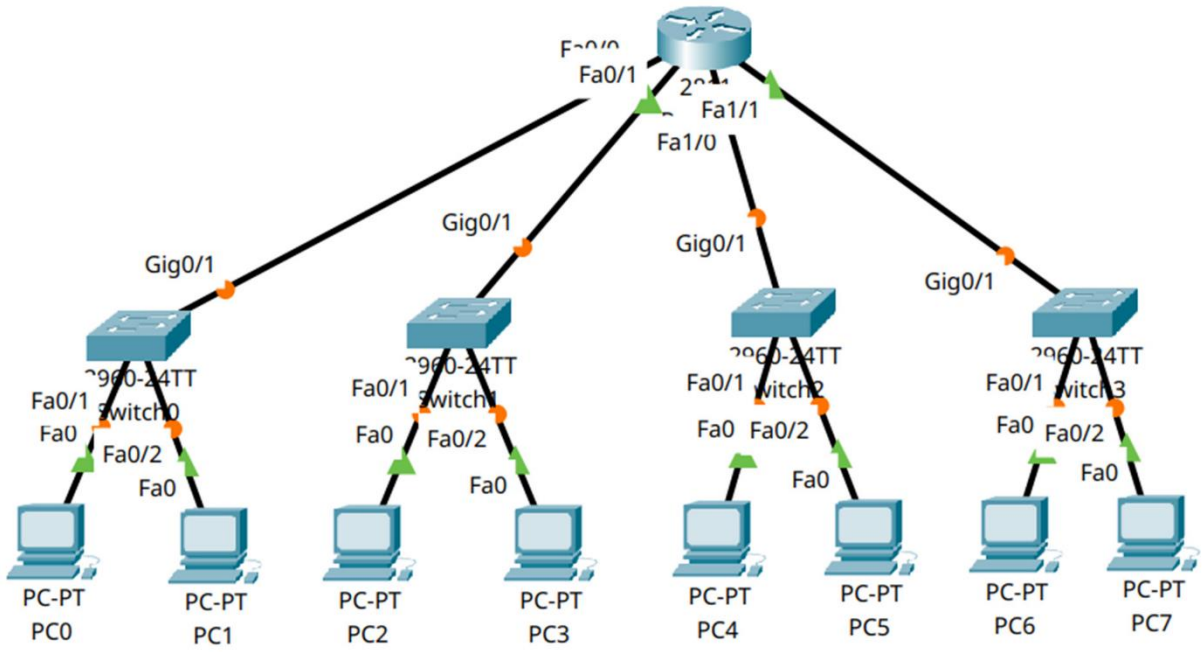

Рисунок 4.1 – Топологія мережі з підмережуванням

4.4.1 Створення топології мережі.

4.4.1.1 Розміщення обладнання. В робочій області Packet Tracer розмістіть маршрутизатор типу 2811 у центрі топології. Вимкніть маршрутизатор, натиснувши кнопку Power. Перетягніть модуль NM-2FE2W з панелі модулів до слота 1 маршрутизатора для розширення кількості FastEthernet інтерфейсів. Після встановлення модуля ввімкніть маршрутизатор. Додайте чотири комутатори типу 2960-24TT, розташувавши їх навколо маршрутизатора. До

кожного комутатора додайте по два комп’ютери типу PC-PT, розмістивши їх симетрично для зручності сприйняття схеми.

4.4.1.2. З’єднання пристроїв. Підключіть комутатор Switch0 до інтерфейсу FastEthernet 0/0 маршрутизатора за допомогою прямого кабелю Copper Straight-Through. Аналогічно підключіть Switch1 до FastEthernet 0/1, Switch2 до FastEthernet 1/0, Switch3 до FastEthernet 1/1. Завдяки модулю NM-2FE2W маршрутизатор тепер має чотири FastEthernet інтерфейси: два вбудованих (0/0, 0/1) та два додаткових (1/0, 1/1). Кожен комп’ютер підключіть до відповідного комутатора через порти FastEthernet прямими кабелями.

4.4.2 Налаштування маршрутизатора.

4.4.2.1 Вхід в режим конфігурації та перевірка інтерфейсів. Клацніть на маршрутизаторі та перейдіть на вкладку CLI. Введіть команди для входу в привілейований режим та перевірте доступні інтерфейси. Завдяки встановленому модулю NM-2FE2W маршрутизатор має чотири FastEthernet інтерфейси. Встановіть ім’я маршрутизатора для зручності ідентифікації.

```
Router> enable
Router# show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
FastEthernet0/1 unassigned YES unset administratively down down
FastEthernet1/0 unassigned YES unset administratively down down
FastEthernet1/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
Router# configure terminal
Router(config)# hostname R1
R1(config)#
```

4.4.2.2 Налаштування інтерфейсу FastEthernet 0/0. Інтерфейс FastEthernet 0/0 налаштовується для обслуговування першої підмережі з 60 хостами. IP-адреса 192.168.10.1 призначається як шлюз за замовчуванням для цієї підмережі. Маска 255.255.255.192 відповідає префіксу /26, що забезпечує 62 доступні адреси хостів. Команда description додає текстовий опис інтерфейсу для документування, a no shutdown активує інтерфейс.

```
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.192
R1(config-if)# description "Subnet1 - 60 hosts /26"
R1(config-if)# no shutdown
R1(config-if)# exit
```

4.4.2.3 Налаштування інтерфейсу FastEthernet 0/1. Другий інтерфейс обслуговує підмережу з 30 хостами. IP-адреса 192.168.10.65 є першою доступною адресою в другій підмережі після завершення діапазону першої. Маска 255.255.255.224 (/27) забезпечує 30 адрес хостів з урахуванням адреси мережі та широкомовної адреси.

```
R1(config)# interface fastEthernet 0/1
R1(config-if)# ip address 192.168.10.65 255.255.255.224
R1(config-if)# description "Subnet2 - 30 hosts /27"
R1(config-if)# no shutdown
R1(config-if)# exit
```

4.4.2.4 Налаштування інтерфейсу FastEthernet 1/0. Третій інтерфейс призначений для підмережі з 14 хостами. Адреса 192.168.10.97 продовжує послідовність адресації після другої підмережі. Маска 255.255.255.240 (/28) дозволяє розмістити 14 хостів в межах блоку з 16 адрес.

```
R1(config)# interface fastEthernet 1/0
R1(config-if)# ip address 192.168.10.97 255.255.255.240
R1(config-if)# description "Subnet3 - 14 hosts /28"
R1(config-if)# no shutdown
R1(config-if)# exit
```

4.4.2.5 Налаштування інтерфейсу FastEthernet 1/1. Останній інтерфейс обслуговує найменшу підмережу з 6 хостами. IP-адреса 192.168.10.113 забезпечує безперервність адресації. Маска 255.255.255.248 (/29) створює блок з 8 адрес, що достатньо для 6 хостів плюс службові адреси.

```
R1(config)# interface fastEthernet 1/1
R1(config-if)# ip address 192.168.10.113 255.255.255.248
R1(config-if)# description "Subnet4 - 6 hosts /29"
R1(config-if)# no shutdown
R1(config-if)# exit
```

4.4.2.6 Збереження конфігурації маршрутизатора. Після завершення налаштування всіх інтерфейсів необхідно зберегти поточну конфігурацію у стартову, щоб налаштування збереглися після перезавантаження пристрою.

```
R1(config)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

4.4.3 Налаштування комутаторів.

4.4.3.1 Налаштування комутатора Switch0. Комутатор, що обслуговує першу підмережу, потребує базової конфігурації для забезпечення керування. Встановлюється ім’я хоста для ідентифікації та налаштовується віртуальний інтерфейс VLAN 1 для адміністративного доступу.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.10.10 255.255.255.192
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# ip default-gateway 192.168.10.1
```

4.4.3.2 Налаштування комутатора Switch1. Другий комутатор налаштовується для другої підмережі з відповідною IP-адресою керування та шлюзом за замовчуванням.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW2
SW2(config)# interface vlan 1
SW2(config-if)# ip address 192.168.10.70 255.255.255.224
SW2(config-if)# no shutdown
SW2(config-if)# exit
SW2(config)# ip default-gateway 192.168.10.65
```

4.4.3.3 Налаштування комутатора Switch2. Третій комутатор отримує IP-адресу з третьої підмережі для адміністративних цілей.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW3
SW3(config)# interface vlan 1
SW3(config-if)# ip address 192.168.10.100 255.255.255.240
SW3(config-if)# no shutdown
SW3(config-if)# exit
SW3(config)# ip default-gateway 192.168.10.97
```

4.4.3.4 Налаштування комутатора Switch3. Останній комутатор налаштовується для четвертої підмережі з найменшою кількістю хостів.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW4
SW4(config)# interface vlan 1
SW4(config-if)# ip address 192.168.10.116 255.255.255.248
SW4(config-if)# no shutdown
SW4(config-if)# exit
SW4(config)# ip default-gateway 192.168.10.113
```

4.4.4 Налаштування комп’ютерів.

У таблиці 4.2 представлено детальні налаштування мережевих параметрів для всіх комп’ютерів у кожній підмережі.

Таблиця 4.2 - Налаштування IP-параметрів комп’ютерів

Комп’ютер	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Підмережа
PC0	192.168.10.2	255.255.255.192	192.168.10.1	1
PC1	192.168.10.3	255.255.255.192	192.168.10.1	1
PC2	192.168.10.66	255.255.255.224	192.168.10.65	2
PC3	192.168.10.67	255.255.255.224	192.168.10.65	2
PC4	192.168.10.98	255.255.255.240	192.168.10.97	3
PC5	192.168.10.99	255.255.255.240	192.168.10.97	3
PC6	192.168.10.114	255.255.255.248	192.168.10.113	4
PC7	192.168.10.115	255.255.255.248	192.168.10.113	4

4.4.4.1 Налаштування комп’ютерів першої підмережі. Комп’ютери PC0 та PC1 налаштовуються для роботи в першій підмережі з 60 хостами. Клацніть на PC0, перейдіть на вкладку Desktop та оберіть IP Configuration. Встановіть статичну IP-адресу 192.168.10.2, маску підмережі 255.255.255.192 та шлюз за замовчуванням 192.168.10.1. Аналогічно налаштуйте PC1 з адресою 192.168.10.3.

4.4.4.2 Налаштування комп’ютерів другої підмережі. Для PC2 встановіть IP-адресу 192.168.10.66, маску 255.255.255.224 та шлюз 192.168.10.65. Комп’ютер PC3 отримує адресу 192.168.10.67 з тими ж параметрами маски та шлюзу.

4.4.4.3 Налаштування комп’ютерів третьої підмережі. PC4 налаштовується з адресою 192.168.10.98, маскою 255.255.255.240 та шлюзом 192.168.10.97. PC5 отримує наступну доступну адресу 192.168.10.99 з ідентичними параметрами маски та шлюзу.

4.4.4.4 Налаштування комп’ютерів четвертої підмережі. Останні два комп’ютери PC6 та PC7 налаштовуються з адресами 192.168.10.114 та 192.168.10.115 відповідно, маскою 255.255.255.248 та шлюзом 192.168.10.113.

4.4.5 Перевірка конфігурації мережі.

4.4.5.1 Перевірка стану інтерфейсів маршрутизатора. На маршрутизаторі R1 виконайте команду show ip interface brief для перевірки стану всіх інтерфейсів. Результат повинен показувати статус “up up” для інтерфейсів FastEthernet 0/0, 0/1, 1/0 та 1/1, що підтверджує їхню активність та готовність до передачі даних.

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.10.1 YES manual up up
FastEthernet0/1 192.168.10.65 YES manual up up
FastEthernet1/0 192.168.10.97 YES manual up up
FastEthernet1/1 192.168.10.113 YES manual up up
```

4.4.5.2 Аналіз таблиці маршрутизації. Команда show ip route відображає таблицю маршрутизації маршрутизатора. В результаті повинні бути присутні чотири безпосередньо підключені мережі (Connected routes) з префіксами /26, /27, /28 та /29, що підтверджує правильність налаштування підмереж.

```
R1# show ip route
192.168.10.0/24 is variably subnetted, 4 subnets, 4 masks
C 192.168.10.0/26 is directly connected, FastEthernet0/0
C 192.168.10.64/27 is directly connected, FastEthernet0/1
C 192.168.10.96/28 is directly connected, FastEthernet1/0
C 192.168.10.112/29 is directly connected, FastEthernet1/1
```

4.4.6 Тестування зв’язності.

4.4.6.1 Тестування в межах підмережі. З командного рядка PC0 виконайте ping до PC1 для перевірки зв’язності в межах першої підмережі. Успішна передача чотирьох пакетів з мінімальною затримкою підтверджує правильність налаштування локального сегмента мережі.

4.4.6.2 Тестування міжмережевої зв’язності. Виконайте ping з PC0 до PC2 (192.168.10.66) для перевірки маршрутизації між першою та другою підмережами. Аналогічно протестуйте зв’язність з PC4 (192.168.10.98) та PC6 (192.168.10.114). Успішні відповіді підтверджують правильність конфігурації маршрутизатора.

4.4.6.3 Перевірка доступності шлюзів. З кожного комп’ютера виконайте ping до відповідного шлюзу за замовчуванням. Наприклад, з PC0 до 192.168.10.1, з PC2 до 192.168.10.65. Ці тести підтверджують правильність налаштування мережевих параметрів на кінцевих пристроях.

4.4.7 Діагностика та усунення проблем.

4.4.7.1 Аналіз конфігурації інтерфейсів. У разі проблем зі зв’язністю використовуйте команду show ip interface для детального аналізу конфігурації конкретного інтерфейсу. Команда показує IP-адресу, маску, стан інтерфейсу та додаткові параметри.

4.4.7.2 Перевірка ARP-таблиці. Команда show arp на маршрутизаторі відображає таблицю відповідності IP та MAC-адрес. Наявність записів для активних комп'ютерів підтверджує успішне встановлення комунікації на канальному рівні.

4.4.7.3 Аналіз статистики інтерфейсів. Команда show interfaces надає детальну статистику роботи інтерфейсів, включаючи кількість переданих та отриманих пакетів, помилки передачі та колізії. Ця інформація допомагає виявити фізичні проблеми з підключенням.

У результаті виконання роботи створюється функціональна мережа з чотирма підмережами, оптимально розподіленим адресним простором та повною зв'язністю між усіма сегментами. Використання технології VLSM дозволило ефективно використати 47% доступного адресного простору базової мережі, залишивши достатньо місця для майбутнього розширення системи.

4.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов'язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім'я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім'я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці

налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв’язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується цей розділ результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route, show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

4.6 Контрольні запитання та завдання

1. Що таке IP-адреса і з яких двох основних частин вона складається? Як маска підмережі допомагає визначити ці частини?

2. Які діапазони IP-адрес відносяться до класів A, B і C, і які маски за замовчуванням їм відповідають? Наведіть приклади.

3. Що таке приватні IP-адреси? Які діапазони визначені стандартом RFC 1918 для класів A, B і C?

4. У чому полягає суть технології VLSM (Variable Length Subnet Mask)? Як вона відрізняється від класичного підмережування з фіксованою маскою?

5. Чому при використанні VLSM важливо сортувати підмережі за спаданням кількості хостів перед розрахунком? Як це впливає на ефективність використання адресного простору?

6. Як визначається кількість підмереж і кількість хостів у кожній підмережі при підмережуванні? Наведіть відповідні формули.

7. Поясніть, як було розраховано маску /26 для підмережі з 60 хостами в прикладі з мережею 192.168.10.0/24. Чому саме /26, а не /25 чи /27?

8. Яку роль відіграє маршрутизатор у сегментованій мережі з кількома підмережами? Як налаштовуються його інтерфейси для обслуговування різних підмереж у Cisco Packet Tracer?

9. Навіщо комутатору потрібна IP-адреса (на інтерфейсі VLAN 1), і чому він потребує шлюзу за замовчуванням? Як це налаштовується на прикладі Switch0?

10. Які команди використовуються для перевірки конфігурації маршрутизатора в Cisco Packet Tracer? Поясніть, що показують команди show ip interface brief та show ip route, і як за їхнім виводом можна підтвердити правильність налаштування підмереж.

Лабораторна робота № 5

Статична маршрутизація в комп'ютерних мережах

5.1 Мета роботи

Набути практичних навичок налаштування статичної маршрутизації в комп'ютерних мережах.

5.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і опрацювати відповідні теми за конспектом лекцій.

5.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням принципів статичної маршрутизація в комп'ютерних мережах у Cisco Packet Tracer.

5.4 Завдання на лабораторну роботу

5.4.1 Відкрити симулятор мереж Cisco Packet Tracer. Побудувати схему мережі згідно рис. 5.1, що включає: три комутатори типу 2960-24TT, три маршрутизатори 1841 та три робочі станції (PC1 – PC3). IP-адреси підмереж для побудови мережі визначаються згідно з таблицею вихідних даних (табл. 5.1) на основі індивідуального варіанта студента (номера у журналі). На основі цих даних необхідно довільно призначити IP-адреси робочим станціям у межах відповідної підмережі, враховуючи необхідність виділення адрес для інтерфейсів маршрутизаторів.

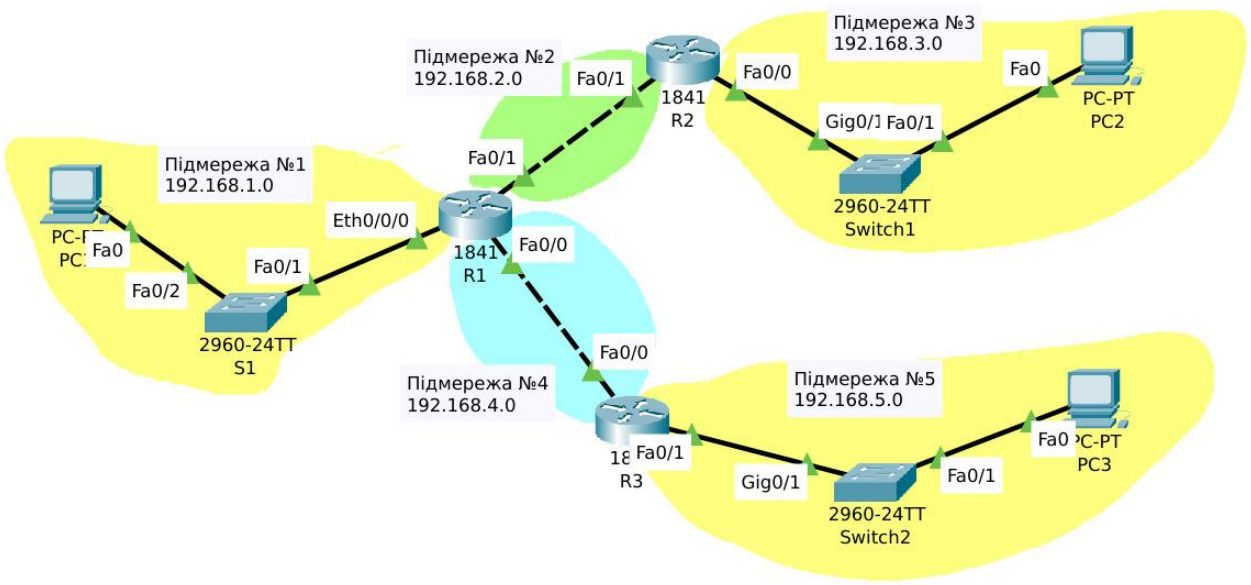

Рисунок 5.1 – Топологія мережі для вивчення статичної маршрутизації

Схема лабораторного завдання включає чотири маршрутизатори моделі Cisco 1841, розміщені у центральній частині діаграми. Маршрутизатор R1 знаходиться зліва та має три інтерфейси: Ethernet0/0/0 з'єднаний з комутатором S1 у підмережі 192.168.1.0/24 (лівий з'єднувач), FastEthernet0/1 підключений до маршрутизатора R2 у підмережі 192.168.2.0/24 (верхній з'єднувач), та FastEthernet0/0 з'єднаний з маршрутизатором R3 у підмережі 192.168.4.0/24 (нижній з'єднувач).

Маршрутизатор R2 розташований у верхній частині схеми з трьома інтерфейсами: FastEthernet0/1 підключений до R1 (нижній з'єднувач), FastEthernet0/0 з'єднаний через Gigabit0/1 з комутатором Switch1 у підмережі 192.168.3.0/24 (правий з'єднувач), та FastEthernet0/1 підключений до R3 через інтерфейс Gig0/1.

Маршрутизатор R3 знаходиться у нижній частині діаграми з інтерфейсами: FastEthernet0/1 підключений до підмережі 192.168.4.0/24 (лівий з'єднувач до R1), та Gigabit0/1 з'єднаний з комутатором Switch2 у підмережі 192.168.5.0/24 (правий з'єднувач).

Кожна з підмереж №1, №3 та №5 представлена комутатором Cisco 2960- 24TT та робочою станцією, з'єднаними прямими лініями.

Підмережа №1 (192.168.1.0/24) містить комутатор S1 та PC1, підмережа №3 (192.168.3.0/24) включає Switch1 та PC2, а підмережа №5 (192.168.5.0/24) – Switch2 та PC3. Підмережі №2 (192.168.2.0/24) та №4 (192.168.4.0/24) є транзитними мережами між маршрутизаторами без кінцевих пристроїв.

З'єднання між маршрутизаторами виконані за допомогою кабелів FastEthernet та Gigabit Ethernet, що відображають фізичну топологію мережі з можливістю резервування шляхів. Підмережі візуально виділені різними кольорами: жовтим для №1, №3, №5, зеленим для №2 та блакитним для № 4.

Після налаштування всіх інтерфейсів і статичних маршрутів, студенти можуть переглянути кінцевий стан таблиці маршрутизації на будь-якому маршрутизаторі за допомогою команди show ip route. Приклад виводу цієї команди для маршрутизатора R2 може виглядати наступним чином:

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - ISIS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user
static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
192.168.1.0/24 is directly connected, Ethernet0/0/0
192.168.2.0/24 is directly connected, FastEthernet0/1
192.168.3.0/24 [120/1] via 192.168.2.1, 00:00:15,
FastEthernet0/1
192.168.4.0/24 is directly connected, FastEthernet0/0
192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:23,
FastEthernet0/0
[120/2] via 192.168.2.1, 00:00:15,
FastEthernet0/1
```

Вивід команди show ip route для маршрутизатора R1 надає повний огляд його таблиці маршрутизації, що є ключовим інструментом для аналізу стану мережі та роботи протоколів. На початку виводу наведено легенду з кодами, які вказують на джерело отримання маршрутної інформації: C позначає

безпосередньо підключені мережі, S – статичні маршрути, а R, D, O та інші – маршрути, отримані від відповідних динамічних протоколів маршрутизації, таких як RIP, EIGRP чи OSPF. У даному випадку присутні коди C і R, що вказує на комбінацію статичних і динамічних маршрутів, хоча в лабораторному завданні передбачалася лише статична маршрутизація. Рядок "Gateway of last resort is not set" повідомляє, що маршрут за замовчуванням (default route) не визначений, тому маршрутизатор не знатиме, куди спрямовувати пакети, призначені для мереж, які відсутні в його таблиці.

Основна частина виводу містить список усіх відомих мереж з деталізацією способу їх досягнення. Мережі 192.168.1.0/24, 192.168.2.0/24 та 192.168.4.0/24 позначені кодом C, що підтверджує їх безпосереднє підключення до інтерфейсів Ethernet0/0/0, FastEthernet0/1 та FastEthernet0/0 відповідно. Це відповідає налаштуванням інтерфейсів маршрутизатора R1, який фізично з'єднаний з цими підмережами. Особливу увагу приділяється записам для мереж 192.168.3.0/24 та 192.168.5.0/24, які не є безпосередньо підключеними до R1. Мережа 192.168.3.0/24 вказана з кодом R, що свідчить про отримання цієї інформації від протоколу RIP. Вказаний шлях [120/1] означає, що адміністративна відстань (AD) для RIP дорівнює 120, а метрика (вартість шляху) – 1. IP-адреса 192.168.2.1 є наступним стрибком (next-hop), а FastEthernet0/1 – вихідним інтерфейсом для досягнення цієї мережі. Для мережі 192.168.5.0/24 спостерігається ситуація з кількома шляхами: один шлях [120/1] через 192.168.4.1 (наступний стрибок на R3), інший шлях [120/2] через 192.168.2.1 (наступний стрибок на R2). Оскільки метрика першого шляху нижча (1 < 2), саме він буде використовуватися для маршрутизації трафіку, а другий залишиться як резервний. Цей вивід демонструє, як маршрутизатор об'єднує інформацію з різних джерел для побудови повної картини мережі.

Таблиця 5.1 – Варіанти індивідуальних завдань

Номер підмережі	IP адреса підмережі
1	192.168.*N*.0
2	192.168.(*N*+1).0
3	192.168.(*N*+2).0
4	192.168.(*N*+3).0
5	192.168.(*N*+4).0

де *N*- номер студента по журналу.

Оскільки в маршрутизаторі R1 є тільки два вбудованих порти Fast Ethernet, слід доповнити його інтерфейсною платою WIC-1ENET перед виконанням з'єднань між вузлами мережі (рис. 5.2).

Рисунок 5.2 – Розміщення інтерфейсної плати WIC-1ENET у маршрутизатор Cisco 1841

5.4.2 Налаштування мережних інтерфейсів маршрутизаторів.

5.4.2.1 Налаштовуємо маршрутизатор R1 для об'єднання підмереж № 1, № 2 та № 4.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface Ethernet0/0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
```

5.4.2.2 Налаштовуємо маршрутизатор R2 для об'єднання підмереж № 2 та № 3.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
```

5.4.2.3 Налаштовуємо маршрутизатор R3 для об'єднання підмереж № 4 та № 5.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface interface FastEthernet0/0
Router(config-if)# ip address 192.168.4.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface FastEthernet0/1
Router(config-if)# ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
```

5.4.3 Налаштування статичної маршрутизації.

5.4.3.1 Маршрутизатор R1.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip route 192.168.3.0 255.255.255.0
FastEthernet0/1
Router(config)# ip route 192.168.5.0 255.255.255.0
FastEthernet0/0
Router(config)# show ip route
```

5.4.3.2 Маршрутизатор R2.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip route 192.168.1.0 255.255.255.0
FastEthernet0/1
Router(config)# ip route 192.168.5.0 255.255.255.0
FastEthernet0/1
Router(config)# ip route 192.168.4.0 255.255.255.0
FastEthernet0/1
Router(config)# show ip route
```

5.4.3.3 Маршрутизатор R3.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip route 192.168.1.0 255.255.255.0
FastEthernet0/0
Router(config)# ip route 192.168.3.0 255.255.255.0
FastEthernet0/0
Router(config)# ip route 192.168.2.0 255.255.255.0
FastEthernet0/0
Router(config)# show ip route
```

5.4.4 Перевірка маршрутів.

Виконати перевірку працездатності мережі за допомогою команд ping та tracert.

```
C:\>tracert 192.168.3.10
Tracing route to 192.168.3.10 over a maximum of 30 hops:
1 13 ms 1 ms 3 ms 192.168.1.1
2 * * 1 ms 192.168.2.2
3 * 0 ms 0 ms 192.168.3.10
Trace complete.
C:\>tracert 192.168.3.10
Tracing route to 192.168.3.10 over a maximum of 30 hops:
1 0 ms 0 ms 6 ms 192.168.1.1
2 0 ms 0 ms 0 ms 192.168.2.2
3 0 ms 0 ms 0 ms 192.168.3.10
Trace complete.
```

```
C:\>ping 192.168.3.10
Pinging 192.168.3.10 with 32 bytes of data:
Reply from 192.168.3.10: bytes=32 time=13ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.3.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

5.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов'язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім'я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім'я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв'язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за

наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується цей розділ результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route, show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

5.6 Контрольні запитання та завдання

1. У чому полягає основна відмінність між маршрутизацією на мережевому рівні та комутацією на канальному рівні моделі OSI?

2. Які основні переваги та недоліки статичної маршрутизації порівняно з динамічною маршрутизацією?

3. Які ключові поля містить запис у таблиці маршрутизації маршрутизатора і яку інформацію вони передають?

4. Чому для коректної роботи маршрутизатора R1 в лабораторному завданні необхідно встановити додаткову інтерфейсну плату WIC-1ENET?

5. Яка логіка визначення IP-адрес підмереж для виконання лабораторного завдання залежно від номера студента у журналі?

6. У чому полягає різниця між використанням IP-адреси наступного стрибка та вихідного інтерфейсу при налаштуванні статичного маршруту за допомогою команди ip route?

7. Які команди Cisco IOS використовуються для перегляду поточної конфігурації маршрутизатора та для збереження цієї конфігурації у постійній пам'яті?

8. Яким чином команда show ip route допомагає адміністратору перевірити правильність налаштування статичних маршрутів?

9. Які діагностичні команди використовуються для перевірки зв'язності між кінцевими вузлами в різних підмережах після налаштування маршрутизації, і чим вони відрізняються за призначенням?

10. Використовуючи топологію з рис. 5.1, поясніть, чому маршрутизатор R2 повинен мати статичні маршрути до підмереж 192.168.1.0, 192.168.4.0 та 192.168.5.0, навіть якщо він безпосередньо з ними не з'єднаний.

Лабораторна робота № 6

Налаштування безпеки маршрутизатора та керування трафіком за допомогою списків контролю доступу ACL

6.1 Мета роботи

Навчитися налаштовувати базовий захист на маршрутизаторі та керувати трафіком між мережами за допомогою ACL у середовищі Packet Tracer.

6.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і опрацювати відповідні теми за конспектом лекцій.

6.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням принципів налаштування безпеки маршрутизатора та керування трафіком за допомогою списків контролю доступу ACL у Cisco Packet Tracer.

6.4 Завдання на лабораторну роботу

6.4.1 Створення топології мережі.

6.4.1.1 Розміщення обладнання. У робочій області Cisco Packet Tracer розмістіть маршрутизатор типу 2811 у центрі топології (рис. 6.1). Вимкніть маршрутизатор, натиснувши кнопку Power. Перетягніть модуль NM-2FE2W з панелі модулів до слота 1 маршрутизатора для розширення кількості FastEthernet-інтерфейсів. Після встановлення модуля ввімкніть маршрутизатор. Додайте чотири комутатори типу 2960-24TT, розташувавши їх навколо маршрутизатора. До перших трьох комутаторів (Switch0, Switch1, Switch2) додайте по одному комп’ютеру типу PC-PT, а до четвертого комутатора

(Switch3) – один сервер типу Server-PT. Розмістіть пристрої симетрично для зручності сприйняття схеми.

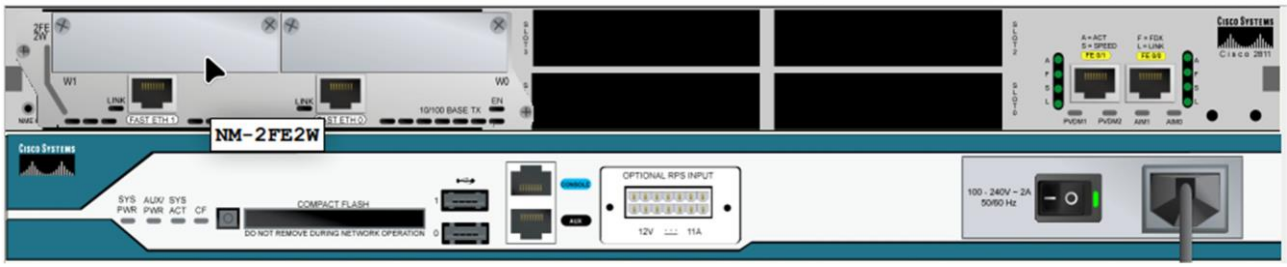

Рисунок 6.1 – Маршрутизатор Cisco 2811 з модулем NM-2FE2W

6.4.1.2 З’єднання пристроїв. Підключіть комутатор Switch0 до інтерфейсу FastEthernet 0/0 маршрутизатора за допомогою прямого кабелю Copper Straight-Through. Аналогічно підключіть Switch1 до FastEthernet 0/1, Switch2 до FastEthernet 1/0, Switch3 до FastEthernet 1/1. Завдяки модулю NM-2FE2W маршрутизатор має чотири FastEthernet-інтерфейси: два вбудованих (0/0, 0/1) та два додаткових (1/0, 1/1). Кожен комп’ютер та сервер підключіть до відповідного комутатора через порти FastEthernet прямими кабелями (рис. 6.2).

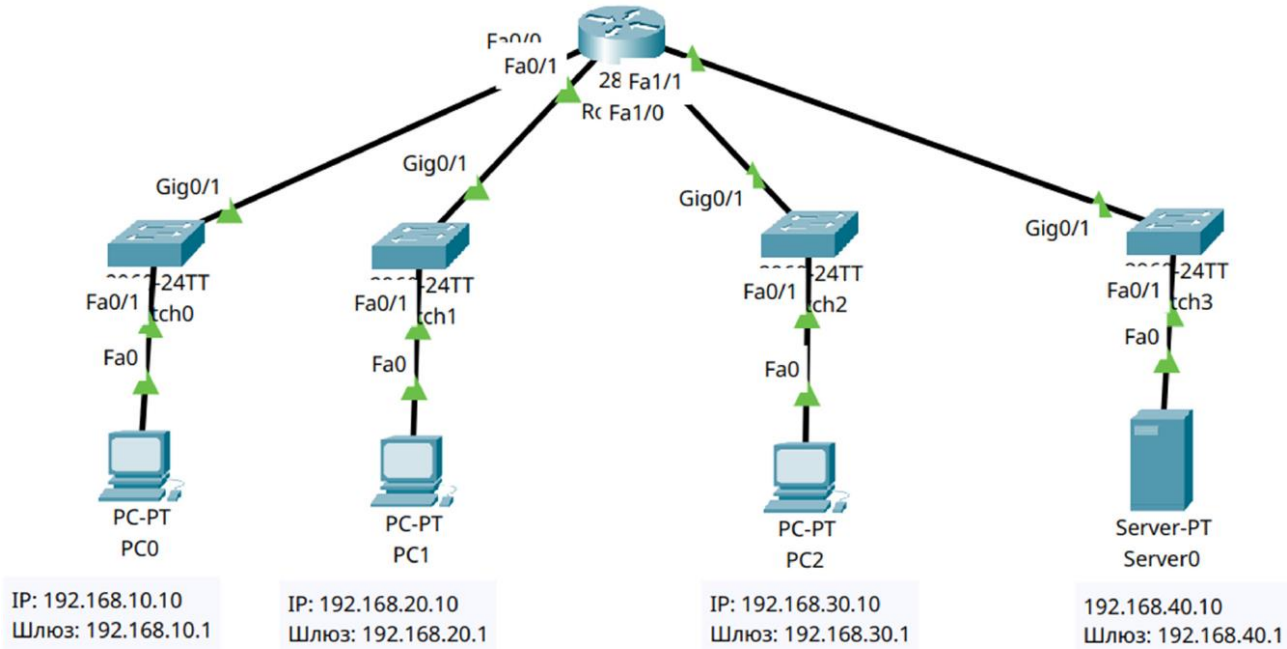

Рисунок 6.2 – Архітектура мережі для лабораторного завдання

Таблиця 6.4 – Варіанти індивідуальних завдань

№ варіанта	Підмережа A (PC1)	Підмережа B (PC2)	Підмережа C (PC3)	Підмережа D (Server)	Заборонити трафік між	Заборонити HTTP з
1	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24	192.168.40.0/24	A → B	B → Server
2	192.168.20.0/24	192.168.30.0/24	192.168.40.0/24	192.168.50.0/24	B → C	C → Server
3	192.168.30.0/24	192.168.40.0/24	192.168.50.0/24	192.168.60.0/24	C → A	A → Server
4	192.168.40.0/24	192.168.50.0/24	192.168.60.0/24	192.168.70.0/24	A → C	B → Server
5	192.168.50.0/24	192.168.60.0/24	192.168.70.0/24	192.168.80.0/24	B → A	C → Server
6	192.168.60.0/24	192.168.70.0/24	192.168.80.0/24	192.168.90.0/24	C → B	A → Server
7	192.168.70.0/24	192.168.80.0/24	192.168.90.0/24	192.168.100.0/24	A → B	B → Server
8	192.168.80.0/24	192.168.90.0/24	192.168.100.0/24	192.168.110.0/24	B → C	C → Server
9	192.168.90.0/24	192.168.100.0/24	192.168.110.0/24	192.168.120.0/24	C → A	A → Server
10	192.168.100.0/24	192.168.110.0/24	192.168.120.0/24	192.168.130.0/24	A → C	B → Server
11	192.168.110.0/24	192.168.120.0/24	192.168.130.0/24	192.168.140.0/24	B → A	C → Server
12	192.168.120.0/24	192.168.130.0/24	192.168.140.0/24	192.168.150.0/24	C → B	A → Server
13	192.168.130.0/24	192.168.140.0/24	192.168.150.0/24	192.168.160.0/24	A → B	B → Server
14	192.168.140.0/24	192.168.150.0/24	192.168.160.0/24	192.168.170.0/24	B → C	C → Server
15	192.168.150.0/24	192.168.160.0/24	192.168.170.0/24	192.168.180.0/24	C → A	A → Server
16	192.168.160.0/24	192.168.170.0/24	192.168.180.0/24	192.168.190.0/24	A → C	B → Server
17	192.168.170.0/24	192.168.180.0/24	192.168.190.0/24	192.168.200.0/24	B → A	C → Server
18	192.168.180.0/24	192.168.190.0/24	192.168.200.0/24	192.168.210.0/24	C → B	A → Server
19	192.168.190.0/24	192.168.200.0/24	192.168.210.0/24	192.168.220.0/24	A → B	B → Server
20	192.168.200.0/24	192.168.210.0/24	192.168.220.0/24	192.168.230.0/24	B → C	C → Server
21	192.168.210.0/24	192.168.220.0/24	192.168.230.0/24	192.168.240.0/24	C → A	A → Server
22	192.168.220.0/24	192.168.230.0/24	192.168.240.0/24	192.168.250.0/24	A → C	B → Server
23	192.168.230.0/24	192.168.240.0/24	192.168.250.0/24	192.168.10.0/24	B → A	C → Server
24	192.168.240.0/24	192.168.250.0/24	192.168.10.0/24	192.168.20.0/24	C → B	A → Server
25	192.168.250.0/24	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24	A → B	B → Server
26	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24	192.168.40.0/24	B → C	C → Server
27	192.168.20.0/24	192.168.30.0/24	192.168.40.0/24	192.168.50.0/24	C → A	A → Server
28	192.168.30.0/24	192.168.40.0/24	192.168.50.0/24	192.168.60.0/24	A → C	B → Server
29	192.168.40.0/24	192.168.50.0/24	192.168.60.0/24	192.168.70.0/24	B → A	C → Server
30	192.168.50.0/24	192.168.60.0/24	192.168.70.0/24	192.168.80.0/24	C → B	A → Server

6.4.2 Налаштування маршрутизатора.

6.3.2.1 Вхід в режим конфігурації та перевірка інтерфейсів. Клацніть на маршрутизаторі та перейдіть на вкладку CLI. Введіть команди для входу в привілейований режим та перевірте доступні інтерфейси. Завдяки встановленому модулю NM-2FE2W маршрутизатор має чотири FastEthernet-інтерфейси. Встановіть ім’я маршрутизатора для зручності ідентифікації.

```
Router> enable
Router# show ip interface brief
Interface IP-Address OK? Method Status
Protocol
FastEthernet0/0 unassigned YES unset administratively
down down
FastEthernet0/1 unassigned YES unset administratively
down down
FastEthernet1/0 unassigned YES unset administratively
down down
FastEthernet1/1 unassigned YES unset administratively
down down
Vlan1 unassigned YES unset administratively
down down
Router# configure terminal
Router(config)# hostname R1
R1(config)#
```

6.4.2.2 Налаштування інтерфейсів маршрутизатора. Налаштуйте кожен інтерфейс маршрутизатора відповідно до варіанта згідно з таблицею нижче. IP-адреса кожного інтерфейсу повинна бути першою адресою в підмережі (наприклад, .1). Маска підмережі – 255.255.255.0 (/24). Команда description додає пояснення призначення інтерфейсу, а no shutdown активує інтерфейс.

Приклад для варіанта 1 (підмережі 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, 192.168.40.0/24):

```
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description "PC Subnet A"
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface fastEthernet 0/1
```

```
R1(config-if)# ip address 192.168.20.1 255.255.255.0
R1(config-if)# description "PC Subnet B"
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface fastEthernet 1/0
R1(config-if)# ip address 192.168.30.1 255.255.255.0
R1(config-if)# description "PC Subnet C"
R1(config-if)# no shutdown R1(config-if)#
exit
R1(config)# interface fastEthernet 1/1
R1(config-if)# ip address 192.168.40.1 255.255.255.0
R1(config-if)# description "Server Subnet"
R1(config-if)# no shutdown
R1(config-if)# exit
```

Примітка. Адреси підмереж визначаються за варіантом. Перші три підмережі призначені для комп'ютерів, четверта - для сервера.

6.4.2.3 Налаштування паролів та банеру. Забезпечте базовий захист маршрутизатора, налаштувавши паролі та банер доступу. Використовуйте унікальний банер, який попереджає про обмежений доступ.

```
R1(config)# enable secret classpass
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password telnet
R1(config-line)# login
R1(config-line)# exit
R1(config)# banner motd "Authorized access only! Unauthorized
entry is prohibited."
```

6.4.2.4 Перевірка зв'язності між пристроями мережі до налаштувань ACL. Для перевірки зв'язності між комп'ютерами та веб-сервером у середовищі Cisco Packet Tracer необхідно налаштувати сервер так, щоб він міг обслуговувати HTTP-запити, а також налаштувати клієнтський комп'ютер для доступу до нього. На сервері (Server0) потрібно відкрити конфігураційну панель і перейти до вкладки "Services", де слід увімкнути службу "Web Server". Після цього необхідно вказати правильну IP-адресу, маску підмережі та шлюз, які повинні бути синхронізовані з налаштуваннями маршрутизатора. Увімкнення опції

"Enable Web Server" активує веб-сервіс на порті 80, що дозволить приймати запити від клієнтів.

На клієнтському комп’ютері (PC0, PC1 або PC2) спочатку слід перевірити, чи правильно встановлені параметри мережі: IP-адреса, маска підмережі та шлюз мають відповідати налаштуванням згідно з варіантом завдання. Після цього потрібно відкрити програму "Web Browser", яка є частиною стандартного набору інструментів для моделі PC-PT у Packet Tracer. Ця програма є вбудованим браузером, який може працювати безпосередньо в інтерфейсі симулятора і виконує функції класичних браузерів, таких як Internet Explorer або Chrome, але в обмеженому режимі. В адресному рядку вбудованого браузера слід ввести IP-адресу сервера, наприклад, http://192.168.40.10, і натиснути кнопку "Go".

Якщо всі налаштування виконані правильно, в браузері відобразиться сторінка веб-сервера, що свідчить про успішне встановлення HTTP-з’єднання між клієнтом і сервером. Цей крок є важливим елементом тестування, оскільки він демонструє роботу протоколу TCP/IP на рівні застосувань. Особливо важливо, щоб студенти зрозуміли, що браузер у Packet Tracer — це не реальний браузер, а імітація, яка дозволяє перевірити доступ до веб-ресурсів у симульованій мережі. Це дозволяє ефективно перевіряти роботу ACL, якщо вони забороняють доступ до сервера з певних підмереж: у такому випадку браузер повинен показати помилку "Connection refused" або "Page not found", що підтверджує ефективність фільтрації трафіку.

Важливо враховувати, що вбудований браузер у Packet Tracer має обмежені можливості порівняно з реальними браузерами, але він достатньо функціональний для базових тестів доступу до веб-серверів. Його головним призначенням є демонстрація роботи HTTP-протоколу та перевірка налаштування мережі, а не робота з складними веб-додатками. При тестуванні рекомендується спочатку виконати ping від клієнта до сервера, щоб переконатися у фізичній зв’язності, а потім вже використовувати браузер. Якщо

ping працює, але браузер не відображає сторінку, це може свідчити про блокування трафіку на рівні ACL або неправильну конфігурацію сервера. Таким чином, послідовна перевірка дозволяє систематично виявити проблеми і вирішити їх.

6.4.3. Налаштування ACL.

6.4.3.1 Стандартний ACL (заборона трафіку між підмережами). Створіть стандартний ACL, який забороняє трафік між двома підмережами з комп'ютерами (наприклад, між PC Subnet A і PC Subnet B). Застосуйте ACL на вихідному інтерфейсі призначення або на вході до джерела. Приклад:

```
R1(config)# access-list 1 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 1 permit any
R1(config)# interface fastEthernet 0/1
R1(config-if)# ip access-group 1 in
Це заборонить трафік з підмережі 192.168.10.0/24 до
192.168.20.0/24.
```

6.4.3.2 Розширений ACL (заборона HTTP-доступу до сервера). Створіть розширений ACL, який забороняє доступ до сервера за протоколом HTTP (порт 80) з однієї з підмереж. Дозвольте інший трафік. Приклад:

```
R1(config)# ip access-list extended NO-HTTP-TO-SERVER
R1(config-ext-nacl)# deny tcp 192.168.20.0 0.0.0.255 host
192.168.40.10 eq 80
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface fastEthernet 1/1
R1(config-if)# ip access-group NO-HTTP-TO-SERVER in
```

Примітка. IP-адреса сервера – 192.168.40.10. Перевірте роботу за допомогою веб-браузера на PC.

6.4.3.3 Перевірка зв'язності між пристроями мережі після налаштувань ACL. Після завершення налаштування списків контролю доступу (ACL) необхідно повторно перевірити зв'язність між пристроями, щоб переконатися, що політики безпеки працюють очікуваним чином. На комп'ютері, який, згідно

з конфігурацією ACL, має бути заблокований для доступу до сервера, спробуйте відкрити веб-сторінку за адресою http://192.168.40.10 за допомогою вбудованого браузера у Packet Tracer. Якщо ACL налаштовано правильно, браузер відобразить повідомлення про помилку підключення, що свідчить про те, що HTTP-трафік був успішно заблокований на рівні маршрутизатора. На іншому комп'ютері, для якого доступ до сервера дозволений, та сама адреса має відкриватися без перешкод, підтверджуючи вибіркову природу фільтрації. Крім того, виконайте команду ping з обох комп'ютерів до сервера: ICMP-трафік має проходити, якщо ACL не блокує його, що демонструє різницю між фільтрацією на рівні IP та на рівні застосувань. Ці тести підтверджують, що ACL працює коректно — він дозволяє загальну зв'язність, але ефективно обмежує доступ до певних сервісів згідно з визначеною політикою безпеки.

6.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов'язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім'я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім'я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці

налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв’язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується цей розділ результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route, show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

6.6 Контрольні запитання та завдання

1. У чому полягає принцип багаторівневого захисту (defense in depth) у мережевій безпеці, і які його основні компоненти реалізуються на рівні маршрутизатора?

2. Чому використання команди enable secret є безпечнішим, ніж enable password, і який механізм шифрування використовується для збереження пароля?

3. Які режими доступу налаштовуються за допомогою команд line console 0 та line vty 0 4, і чому важливо встановлювати паролі для обох цих ліній?

4. Яке призначення має команда banner motd, і яке правове значення вона може мати у контексті мережевої безпеки?

5. У чому різниця між стандартним і розширеним ACL у Cisco IOS, і чому розширені ACL застосовуються ближче до джерела трафіку?

6. Як обчислюється WildCard-маска, і чому для мережі 192.168.10.0/24 вона дорівнює 0.0.0.255?

7. Як правильно застосувати ACL для заборони HTTP-трафіку (порт 80) від підмережі 192.168.20.0/24 до сервера з IP-адресою 192.168.40.10? Наведіть приклад команди конфігурації.

8. Чому в кінці кожного ACL рекомендується додавати правило permit ip any any, і що станеться, якщо це правило відсутнє?

9. Які команди використовуються для перевірки налаштування та роботи ACL на маршрутизаторі, і яку інформацію вони виводять?

10. Як впливає застосування директиви transport input ssh на VTY-лінії, і чому SSH є безпечнішим способом віддаленого доступу порівняно з Telnet?

Лабораторна робота № 7

Налаштування автономної бездротової точки доступу Cisco

7.1 Мета роботи

Опанувати конфігурування автономної точки доступу Cisco AIR-CAP2702 у режимі прозорого моста з інтеграцією бездротових клієнтів до провідної мережі.

7.2 Методичні вказівки з організації самостійної роботи здобувачів вищої освіти

Під час підготовки до лабораторної роботи слід детально вивчити і опрацювати відповідні теми за конспектом лекцій.

7.3 Зміст лабораторної роботи

Зміст роботи пов'язаний з вивченням принципів налаштування автономної бездротової точки доступу Cisco у Cisco Packet Tracer.

7.4 Завдання на лабораторну роботу

7.4.1 Підключення до точки доступу через консоль та вхід у привілейований режим.

Після фізичного підключення до консольного порту точки доступу через серійний адаптер із параметрами 9600 8N1, відбувається завантаження пристрою. За замовчуванням точка доступу не має пароля для EXEC-режиму, але для переходу в привілейований режим (enable) використовується стандартний пароль Cisco (з великої літери). Це дозволяє адміністратору одразу отримати повний доступ до CLI без попереднього налаштування.

```
AP> enable
Password: Cisco
AP#
```

7.4.2 Базова ідентифікація та сервіси.

Точка доступу отримує унікальне ім’я CAP2702I для зручності ідентифікації в мережі, а також налаштовується базова безпека та зручність адміністрування: вимикається застарілий сервіс pad, увімкнені часові мітки для логів і налагодження, вимкнено автоматичне перетворення невідомих команд у DNS-запити, що прискорює роботу CLI, а також активовані веб-сервери HTTP та HTTPS для віддаленого управління через браузер.

```
AP# configure terminal
AP(config)# hostname CAP2702I
CAP2702I(config)# no service pad
CAP2702I(config)# service timestamps debug datetime msec
CAP2702I(config)# service timestamps log datetime msec
CAP2702I(config)# no ip domain-lookup
CAP2702I(config)# ip http server
CAP2702I(config)# ip http secure-server
```

7.4.3 Налаштування провідного аплінку та Bridge Group.

Фізичний Ethernet-порт GigabitEthernet0 налаштовується як точка підключення до основної мережі (аплінк) і активується. Потім створюється логічна Bridge Group 1 з використанням стандартного протоколу IEEE 802.1D, яка дозволяє точці доступу працювати як мережевий міст на канальному рівні (L2), об’єднуючи бездротові та провідні інтерфейси в одну broadcast-домену. Команда bridge 1 route ip дозволяє мосту передавати IP-трафік, що необхідно для роботи віртуального інтерфейсу управління BVI1.

```
CAP2702I(config)# interface GigabitEthernet0
CAP2702I(config-if)# description Uplink
CAP2702I(config-if)# no shutdown
CAP2702I(config-if)# exit
CAP2702I(config)# bridge 1 protocol ieee
CAP2702I(config)# bridge 1 route ip
```

7.4.4 Створення субінтерфейсів та приєднання до Bridge Group 1.

Для коректної роботи з VLAN створюються субінтерфейси на фізичному Ethernet-порті (GigabitEthernet0.1) та на обох радіоінтерфейсах (Dot11Radio0.1 для 2.4 ГГц та Dot11Radio1.1 для 5 ГГц). Кожен субінтерфейс налаштовується на роботу з нативним (untagged) трафіком VLAN 1 і явно приєднується до Bridge Group 1. Згідно з рекомендаціями Cisco, для радіоінтерфейсів додатково вимикається навчання MAC-адрес і unicast flooding, а також блокується unknown-source трафік – це підвищує безпеку та ефективність роботи моста.

```
CAP2702I(config)# interface GigabitEthernet0.1
CAP2702I(config-subif)# encapsulation dot1Q 1 native
CAP2702I(config-subif)# bridge-group 1
CAP2702I(config-subif)# bridge-group 1 spanning-disabled
CAP2702I(config-subif)# no bridge-group 1 source-learning
CAP2702I(config-subif)# exit
CAP2702I(config)# interface Dot11Radio0.1
CAP2702I(config-subif)# encapsulation dot1Q 1 native
CAP2702I(config-subif)# bridge-group 1
CAP2702I(config-subif)# bridge-group 1 subscriber-loopcontrol
CAP2702I(config-subif)# bridge-group 1 block-unknown-source
CAP2702I(config-subif)# no bridge-group 1 source-learning
CAP2702I(config-subif)# no bridge-group 1 unicast-flooding
CAP2702I(config-subif)# exit
CAP2702I(config)# interface Dot11Radio1.1
CAP2702I(config-subif)# encapsulation dot1Q 1 native
CAP2702I(config-subif)# bridge-group 1
CAP2702I(config-subif)# bridge-group 1 subscriber-loopcontrol
CAP2702I(config-subif)# bridge-group 1 block-unknown-source
CAP2702I(config-subif)# no bridge-group 1 source-learning
CAP2702I(config-subif)# no bridge-group 1 unicast-flooding
CAP2702I(config-subif)# exit
```

7.4.5 Налаштування інтерфейсу управління (BVI1).

Віртуальний інтерфейс BVI1 (Bridge Virtual Interface) створюється для надання точки доступу власної IP-адреси на рівні мережі (L3), що необхідно для її віддаленого управління (SSH, веб-інтерфейс, пінг). Цей інтерфейс отримує IP-адресу автоматично через DHCP від вашого роутера або комутатора лабораторної мережі, що спрощує інтеграцію в існуючу інфраструктуру без необхідності ручного призначення адреси.

```
CAP2702I(config)# interface BVI1
CAP2702I(config-if)# ip address dhcp
CAP2702I(config-if)# no shutdown
CAP2702I(config-if)# exit
```

7.4.6 Створення глобального профілю SSID.

Створюється єдиний профіль бездротової мережі з ім’ям Cisco_2702I, який буде транслюватися в обох діапазонах (2.4 ГГц та 5 ГГц). Цей SSID прив’язаний до VLAN 1, використовує відкриту аутентифікацію на першому етапі, але з подальшим управлінням ключами за стандартом WPA2-Personal (найбезпечніший варіант для навчальних та домашніх мереж) і паролем mywifipass у відкритому вигляді. Команда guest-mode гарантує, що SSID буде видимим у бездротових маячках (beacon frames), що дозволяє клієнтам виявляти мережу.

```
CAP2702I(config)# dot11 ssid Cisco_2702I
CAP2702I(config-ssid)# vlan 1
CAP2702I(config-ssid)# authentication open
CAP2702I(config-ssid)# authentication key-management wpa
version 2
CAP2702I(config-ssid)# wpa-psk ascii 0 mywifipass
CAP2702I(config-ssid)# guest-mode
CAP2702I(config-ssid)# exit
```

7.4.7 Активація та налаштування радіоінтерфейсів.

Обидва радіомодулі (Dot11Radio0 для 2.4 ГГц та Dot11Radio1 для 5 ГГц) активуються командою no shutdown. На кожному налаштовується шифрування AES-CCM, що є обов’язковим для WPA2, призначається SSID Cisco_2702I, встановлюється роль кореневого пристрою (station-role root), а для 2.4 ГГц фіксується канал 6 для уникнення інтерференції та забезпечення стабільності. Це дозволяє сучасним клієнтам автоматично підключатися до найкращого доступного діапазону, використовуючи один пароль.

```
CAP2702I(config)# interface Dot11Radio0
CAP2702I(config-if)# no shutdown
CAP2702I(config-if)# encryption vlan 1 mode ciphers aes-ccm
CAP2702I(config-if)# ssid Cisco_2702I
CAP2702I(config-if)# station-role root
CAP2702I(config-if)# channel 6
CAP2702I(config-if)# exit
CAP2702I(config)# interface Dot11Radio1
CAP2702I(config-if)# no shutdown
CAP2702I(config-if)# encryption vlan 1 mode ciphers aes-ccm
CAP2702I(config-if)# ssid Cisco_2702I
CAP2702I(config-if)# station-role root
CAP2702I(config-if)# exit
```

7.4.8 Налаштування локального облікового запису та збереження конфігурації.

Для забезпечення доступу через веб-інтерфейс або SSH створюється локальний користувач із повними привілеями. Після завершення всіх налаштувань виконується вихід з конфігураційного режиму, і конфігурація записується в постійну пам’ять (NVRAM) за допомогою команди write memory. Це гарантує, що всі зміни збережуться після перезавантаження пристрою.

```
CAP2702I(config)# username student privilege 15 secret
student123
CAP2702I(config)# line vty 0 4
CAP2702I(config-line)# login local
CAP2702I(config-line)# transport input ssh
CAP2702I(config-line)# exit
CAP2702I(config)# end
CAP2702I# write memory
```

7.4.9 Перевірка роботи.

Після завершення конфігурування точка доступу підключається до навчальної мережі через Ethernet-порт. Адміністратор перевіряє, чи пристрій отримав IP-адресу від DHCP-сервера за допомогою команди show ip interface brief. Потім з клієнтських пристроїв (ноутбуків або смартфонів) здійснюється пошук бездротової мережі Cisco_2702I. Після введення пароля mywifipass клієнт має успішно асоціюватися з точкою доступу та отримати IP-адресу з того ж підмережі, що й інші хости мережі. Успішність роботи підтверджується

можливістю доступу до внутрішніх мережевих ресурсів або Інтернету, а також (опційно) можливістю входу в веб-інтерфейс точки доступу за її IP-адресою BVI1 з використанням облікових даних student / student123.

7.5 Зміст звіту

Звіт з лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації (ДСТУ-3008-2015): шрифт Times New Roman, розмір 14 pt, міжрядковий інтервал 1,5. Звіт складається з наступних обов'язкових частин:

Титульний аркуш. Тут зазначаються тема та мета лабораторної роботи, прізвище, ім'я та по батькові здобувача вищої освіти, назва академічної групи, а також прізвище, ім'я та по батькові викладача.

Вступна частина. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також тут подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі та демонструвати розуміння здобувачем вищої освіти ключових положень теми.

Основна частина (виконання лабораторного завдання). Цей розділ починається із загального опису архітектури досліджуваної мережі та таблиці налаштувань обладнання. Архітектура мережі включає повну схему топології, що відображає взаємозв'язок усіх компонентів: маршрутизаторів, комутаторів, серверів, робочих станцій тощо. У таблиці налаштувань обладнання для кожного блоку вказуються IP-адреса та маска підмережі, роль у мережі (наприклад, шлюз, DHCP-клієнт, точка доступу), VLAN-приналежність (за наявності) та інші специфічні параметри, такі як ACL, маршрути чи бездротові SSID.

Далі послідовно описується виконання кроків лабораторного завдання згідно з індивідуальним варіантом. Для кожного кроку наводяться:

- короткий коментар щодо суті виконуваної дії;

- конфігураційні команди (за наявності) з поясненням їх призначення та синтаксису;

- результати виконання кроку, включаючи вивід CLI, стан інтерфейсів, таблиці маршрутизації тощо, підтверджені скріншотом (наприклад, вікно CLI, графічна топологія в Packet Tracer, результат команди ping тощо).

Завершується цей розділ результатами тестування працездатності мережі: наводяться виводи діагностичних команд (ping, tracert/traceroute, show ip route, show interfaces тощо), що підтверджують коректну взаємодію між усіма сегментами мережі.

Висновки. У цій частині здобувач вищої освіти формулює висновки щодо знань, практичних умінь та професійних компетенцій, отриманих у процесі виконання роботи. Також аналізуються типові помилки або проблеми, які виникали під час виконання завдання, та наводяться способи їх усунення. Особлива увага приділяється практичному значенню набутих навичок для майбутньої професійної діяльності.

7.6 Контрольні запитання та завдання

1. Яку роль відіграють Bridge Group і BVI-інтерфейс у забезпеченні роботи автономної точки доступу Cisco на рівнях L2 та L3?

2. Навіщо створюють субінтерфейси з native VLAN і приєднують їх до однієї Bridge Group при налаштуванні точки доступу?

3. Чому для радіоінтерфейсів у Bridge Group вимикають функції source-learning та unicast-flooding, і як це впливає на безпеку мережі?

4. Як відбувається процес аутентифікації та шифрування при використанні WPA2-Personal з паролем у конфігурації точки доступу?

5. Що означає команда guest-mode у профілі SSID, і чи надає вона гостьовим користувачам обмежений доступ до мережі?

6. Як точка доступу інтегрує бездротових клієнтів у провідну мережу за допомогою мосту, VLAN і субінтерфейсів?

7. Чому IP-адреса для управління автономною точкою доступу призначається на BVI-інтерфейс, а не на фізичний порт?

8. Чому для віддаленого доступу до точки доступу рекомендовано використовувати SSH замість Telnet, і як правильно налаштувати локального користувача?

9. У чому полягає принципова різниця між автономним і контролерним режимами роботи точок доступу Cisco, і коли доцільно застосовувати автономний режим?

10. Якими командами CLI та діями клієнта можна підтвердити коректну роботу точки доступу після завершення конфігурації?

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації та основні вимоги до структури, змісту та оформлення навчальних видань / схвалено на засіданні Науково-методичної ради ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» 23 квітня 2013 р. (протокол № 3).

2. Державний стандарт України ДСТУ 3008-2025: Документація. Звіти у сфері науки і техніки. Структура і правила оформлення. К.: Держстандарт України, 2015.

3. Комп’ютерні мережі: Методичні рекомендації для практичних та лабораторних занять (частина 1) [Електронне видання] / Педяш В.В., Йона Л.Г., Мазур Г.Д. Кафедра комп’ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. Одеса, 2025. 123 с.

4. Жураковський Б. Ю. Комп’ютерні мережі. Частина 1. [навчальний посібник] / Б. Ю. Жураковський, І.О. Зенів. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

5. Б. Ю. Жураковський. Комп’ютерні мережі. Частина 2. [навчальний посібник] / Б. Ю. Жураковський, І.О. Зенів. Електронні текстові дані. Київ : КПІ ім. Ігоря Сікорського, 2020. 372 с.

6. Карпенко М. Ю. Конспект лекцій з курсу «Комп’ютерні мережі» / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 99 с.

7. Безрук В.М., Бідний Ю.М., Колтун Ю.М., Астраханцев А.А., Свид І.В., Ширяєв А.В., Харченко Н.А. Інформаційні мережі зв’язку. Ч. 2. Телекомунікаційні технології стаціонарних мереж зв’язку: навч. посібник. Харків: ХНУРЕ, 2011. 492 с.

8. Ємельянов В.В., Свид І.В. Системи стільникового рухомого радіозв'язку: навч. посіб. с грифом МОН. Харків, ТОВ «Компанія СМІТ», 2011 336 с.

9. Свид І.В., Сухоруков Д.О., Коротіч О.В., Мачоніс Т.С. Метод підвищення якості обслуговування сигналів запиту в інформаційних системах. // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 122-127. doi: https://doi.org/10.30837/rt.2023.4.215.12.

10. Свид І.В., Обод І.І., Сєріков А.О. Застосування MATLAB для моделювання радіолокаційних систем // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 211. С. 154-158. doi: https://doi.org/10.30837/rt.2022.4.211.13.

11. Безрук В.М., Свид І.В., Корсун І.В. Нейронні технології в телекомунікаціях та системах управління: навч. посібник с грифом МОН. Харків, СМІТ, 2008. 230 с.

12. Управління оптичною мережею контролером SDN на базі ONOS / О.І. Романов, І.В. Свид, Н.І. Корнієнко, А.О. Романов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 210. С. 188-196. doi: https://doi.org/10.30837/rt.2022.3.210.16.

13. Аналіз технології управління каналами передачі цифрових даних з ущільненням в комп'ютерних системах / Довгий, В., Грига, В., Дзундза, Б., Свид, І., Терлецький, А. і Павлюк, М. // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 222. С. 161-171. doi: https://doi.org/10.30837/rt.2025.3.222.15.

14. Zapukhlyak R., Pavliuk M., Svyd I., Dzundza B., Dovhyi V., Martyuniuk V., Haider Th. Salim ALRikabi. Analysis and Improvement of Information Security Technologies in Distributed and Asymmetric Systems // Advances in Cyber-Physical Systems, Volume 10, Number 2, 2025, pp. 158-162. doi: https://doi.org/10.23939/acps2025.02.158.

15. І.І. Обод, І.В. Свид, І.В. Рубан, Г.Е. Заволодько. Математичне моделювання інформаційних систем: навчальний посібник. / За редакцією І.І. Обода. Харків : Друкарня Мадрид, 2019. 270 с.

16. Проєктування вбудованих систем. Лабораторний практикум: Навч. посіб. / Б. С. Дзундза, І. В. Свид. К.: ФОП Гуляєва В.М., 2025. 88 с.

Електронне навчальне видання

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт
з дисципліни
«КОМП'ЮТЕРНІ МЕРЕЖІ»

для здобувачів вищої освіти всіх форм навчання
першого (бакалаврського) рівня вищої освіти
спеціальностей: F7 «Комп’ютерна інженерія»,
G5 «Електроніка, електронні комунікації,
приладобудування та радіотехніка»,
015 «Професійна освіта (за спеціалізаціями)»
спеціалізація 015.39 «Цифрові технології»

Упорядники: СВИД Ірина Вікторівна
ДЗУНДЗА Богдан Степанович

Авторська редакція
Комп’ютерна верстка І.В. Свид

КНУВС, 76018, Івано-Франківськ, вул. Шевченко, 57. E-mail: kkie@pnu.edu.ua

Підготовлено на кафедрі комп’ютерної інженерії та електроніки ФТФ КНУВС