Педяш В.В., Йона Л.Г., Мазур Г.Д.

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації для практичних та лабораторних занять (частина 1)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Міжнародний гуманітарний університет
Кафедра комп’ютерної інженерії та інноваційних технологій

Педяш В.В., Йона Л.Г., Мазур Г.Д.

КОМП’ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації для практичних та лабораторних занять (частина 1)
здобувачів вищої освіти зі спеціальностей:

A4.09 Середня освіта (Інформатика),
F2 Інженерія програмного забезпечення,
F3 Комп'ютерні науки,
F7 Комп'ютерна інженерія,
F5 Кібербезпека та захист інформації,
G5 Електроніка, електронні комунікації, приладобудування та радіотехніка

Одеса 2025

Затверджено Вченою Радою Міжнародного гуманітарного університету (протокол № 12 від 23 червня 2025 року)

Педяш В.В., Йона Л.Г., Мазур Г.Д.

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.

Методичні рекомендації до практичних та лабораторних занять з дисципліни «Комп’ютерні мережі» (перша частина) розроблено відповідно до навчального плану підготовки здобувачів вищої освіти. Посібник охоплює перші сім лабораторних робіт, спрямованих на освоєння базових принципів побудови, налаштування та діагностики локальних комп’ютерних мереж. Матеріали містять детальні інструкції щодо виконання завдань, від базової конфігурації обладнання Cisco до створення VLAN, реалізації статичної маршрутизації, налаштування безпеки за допомогою ACL та інтеграції бездротових клієнтів.

Посібник призначено для здобувачів першого (бакалавського) рівня вищої освіти спеціальностей: A4 Середня освіта (Інформатика), F2 Інженерія програмного забезпечення, F3 Комп’ютерні науки, F7 Комп’ютерна інженерія, F5 Кібербезпека та захист інформації, G5 Електроніка, електронні комунікації, приладобудування та радіотехніка.

Завдання можуть виконуватися як у навчальному симуляторі Cisco Packet Tracer, так і в більш просунутих середовищах (наприклад, GNS3) або на реальному мережевому обладнанні, доступному в лабораторіях факультету кібербезпеки, програмної інженерії та комп’ютерних наук. Такий підхід забезпечує гнучкість навчального процесу та сприяє формуванню практичних інженерних навичок, необхідних для подальшого вивчення сучасних мережевих технологій, проходження міжнародних сертифікацій (зокрема CCNA) та виконання кваліфікаційних робіт у галузі інформаційно-комунікаційних технологій.

ЗМІСТ

ВСТУП

Сучасна інформаційна інфраструктура будь-якої організації – від невеликого підприємства до глобальної корпорації ґрунтується на комп’ютерних мережах. Розуміння принципів їх побудови, функціонування та управління є фундаментальною компетенцією фахівця в галузі інформаційних технологій. Перша частина курсу «Комп’ютерні мережі», що викладається у першому семестрі навчання, спрямована на формування базових практичних навичок проєктування, налаштування, діагностики та безпечного адміністрування локальних мереж.

Дані методичні вказівки призначені для використання під час проведення практичних і лабораторних занять з дисципліни «Комп’ютерні мережі» та охоплюють матеріали першої частини курсу, яка включає перші сім навчальних робіт. Кожна робота побудована за єдиною логічною схемою, що забезпечує послідовний перехід від опрацювання теоретичних положень до виконання практичних завдань і сприяє цілісному засвоєнню навчального матеріалу.

Практичні заняття проводяться на основі розділу «Ключові положення», у якому викладено необхідні теоретичні відомості, подано пояснення принципів роботи мережевих технологій і протоколів, а також наведено технічні характеристики обладнання та аналітичні узагальнення. Опрацювання цього матеріалу дозволяє студентам сформувати розуміння теми, підготуватися до виконання практичних дій і усвідомлено підійти до розв’язання завдань лабораторної роботи.

Після засвоєння ключових положень практичного заняття навчальний процес логічно продовжується лабораторним заняттям з тієї ж тематики, яке виконується відповідно до розділу «Лабораторне завдання». У цьому розділі подано структуровану покрокову інструкцію з виконання конкретних завдань, що передбачають налаштування мережевих пристроїв, перевірку працездатності мережі та фіксацію отриманих результатів. Лабораторні роботи виконуються переважно в середовищах комп’ютерного моделювання, таких як Cisco Packet Tracer або GNS3, а за наявності відповідних умов – також на реальному мережевому обладнанні.

Запропонована організація навчального матеріалу забезпечує логічну послідовність навчання, за якої теоретичні знання, отримані під час практичних занять, закріплюються та поглиблюються в процесі виконання лабораторних робіт. Використання середовищ моделювання дозволяє наочно відтворювати мережеві сценарії та відпрацьовувати конфігурації без залучення фізичного обладнання, водночас зберігаючи можливість переходу до більш складних і наближених до реальних умов рішень.

Сформовані у першому семестрі компетенції створюють основу для подальшого вивчення дисципліни в другому семестрі, зокрема більш складних технологій маршрутизації, мережевої безпеки, моніторингу та централізованого управління мережами, а також для підготовки до міжнародних сертифікацій, таких як Cisco Certified Network Associate (CCNA).

Лабораторна робота № 1

Тема: Основи моделювання комп’ютерних мереж в Cisco Packet Tracer

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

1 КЛЮЧОВІ ПОЛОЖЕННЯ

Комп'ютерні мережі є основою сучасного цифрового світу, проникаючи в усі сфери життя та промисловості. У побуті вони об’єднують смартфони, комп’ютери, пристрої «розумного дому» та IoT, забезпечуючи доступ до інтернету, хмарних сервісів і обмін даними. У промисловості мережі автоматизують виробництво, контролюють обладнання й збирають дані в реальному часі, стаючи основою «Індустрії 4.0». У бізнесі вони зв’язують філії, підтримують документообіг, відеоконференції та захищені комунікації. Банки й фінансові установи залежать від мереж для транзакцій і обміну конфіденційною інформацією. У освіті мережі дозволяють дистанційне навчання, доступ до електронних ресурсів і співпрацю між закладами. У медицині — обмін даними, телеконсультації та моніторинг пацієнтів. Таким чином, комп’ютерні мережі є ключовим елементом цифрової інфраструктури сьогодення.

Моделювання комп'ютерних мереж є критично важливим етапом при проектуванні, впровадженні та оптимізації мережевих рішень, оскільки дозволяє тестувати різні сценарії роботи без ризику порушення функціонування реальних систем. Використання програмних симуляторів мереж надає можливість експериментувати з різними топологіями, протоколами маршрутизації, налаштуваннями безпеки та політиками якості обслуговування в контрольованому середовищі. Таблиця 1.1 містить порівняльну характеристику найпопулярніших програм для моделювання комп'ютерних мереж, що використовуються в освітніх та комерційних цілях.

Cisco Packet Tracer розробляється компанією Cisco Systems з 2007 року як частина програми Cisco Networking Academy та призначений для навчання студентів основам мережних технологій. Програма пройшла значну еволюцію від простого інструменту візуалізації до потужного симулятора мереж, що підтримує широкий спектр мережевих протоколів та технологій. Сучасні версії Packet Tracer включають підтримку IPv6, бездротових технологій, мереж IoT, хмарних сервісів та технологій програмно-конфігурованих мереж. Основним призначенням програми є надання студентам безпечного середовища для вивчення принципів роботи мереж, експериментування з конфігураціями та відпрацювання практичних навичок без ризику пошкодження реального обладнання. Таблиця 1.2 містить детальну класифікацію пристроїв та технологій, що підтримуються в Cisco Packet Tracer.

Таблиця 1.1 – Порівняння програм для моделювання комп'ютерних мереж

Назва програми	Розробник	Тип ліцензії	Операційні системи	Основні переваги	Недоліки
Cisco Packet Tracer	Cisco Systems	Безкоштовна (освітня)	Windows, Linux, macOS	Простий інтерфейс, інтеграція з Cisco Academy, підтримка багатьох протоколів	Обмежений набір пристроїв, тільки обладнання Cisco
GNS3	GNS3 Technologies	Відкритий код	Windows, Linux, macOS	Використання реальних образів ОС, підтримка різних вендорів	Складна конфігурація, вимагає потужного обладнання
EVE-NG	EVE-NG Team	Freemium	Linux, Windows (через VM)	Багатокористувацька робота, підтримка віртуалізації	Складний у налаштуванні, платна версія для повного функціоналу
NS-3	Open Source Community	Відкритий код	Linux, Windows, macOS	Гнучкість програмування, академічна спрямованість	Потребує знання програмування, відсутність графічного інтерфейсу

Таблиця 1.2 – Групи та моделі пристроїв у Cisco Packet Tracer

Група пристроїв	Підгрупа	Приклади моделей	Основне призначення
Network Devices	Routers	2811, 2901, 4331, ISR4000	Маршрутизація трафіку між мережами
Network Devices	Switches	2950-24, 2960, 3560, 9300	Комутація в локальних мережах
Network Devices	Hubs	Generic Hub, PT-HUB	Повторення сигналу (застарілі пристрої)
Network Devices	Wireless Devices	Linksys WRT300N, WLC2504	Бездротовий доступ та управління
Network Devices	Security	ASA 5505, ISE	Захист мережі та контроль доступу
End Devices	Computers	PC, Laptop, Tablet PC	Кінцеві пристрої користувачів
End Devices	Servers	Server-PT, Web Server	Надання мережевих сервісів
End Devices	Printers	Printer-PT	Мережеві принтери
End Devices	IoT Devices	Smart Home Gateway, Sensors	Пристрої інтернету речей
Connections	Cables	Straight-through, Crossover, Fiber	Фізичні з'єднання пристроїв

Моделювання комп'ютерних мереж у Cisco Packet Tracer здійснюється за чітко визначеними етапами, що забезпечують системний підхід до створення та

тестування мережевих топологій. Рисунок 1.1 ілюструє послідовність основних етапів моделювання мереж, починаючи від аналізу вимог і завершуючи документуванням результатів.

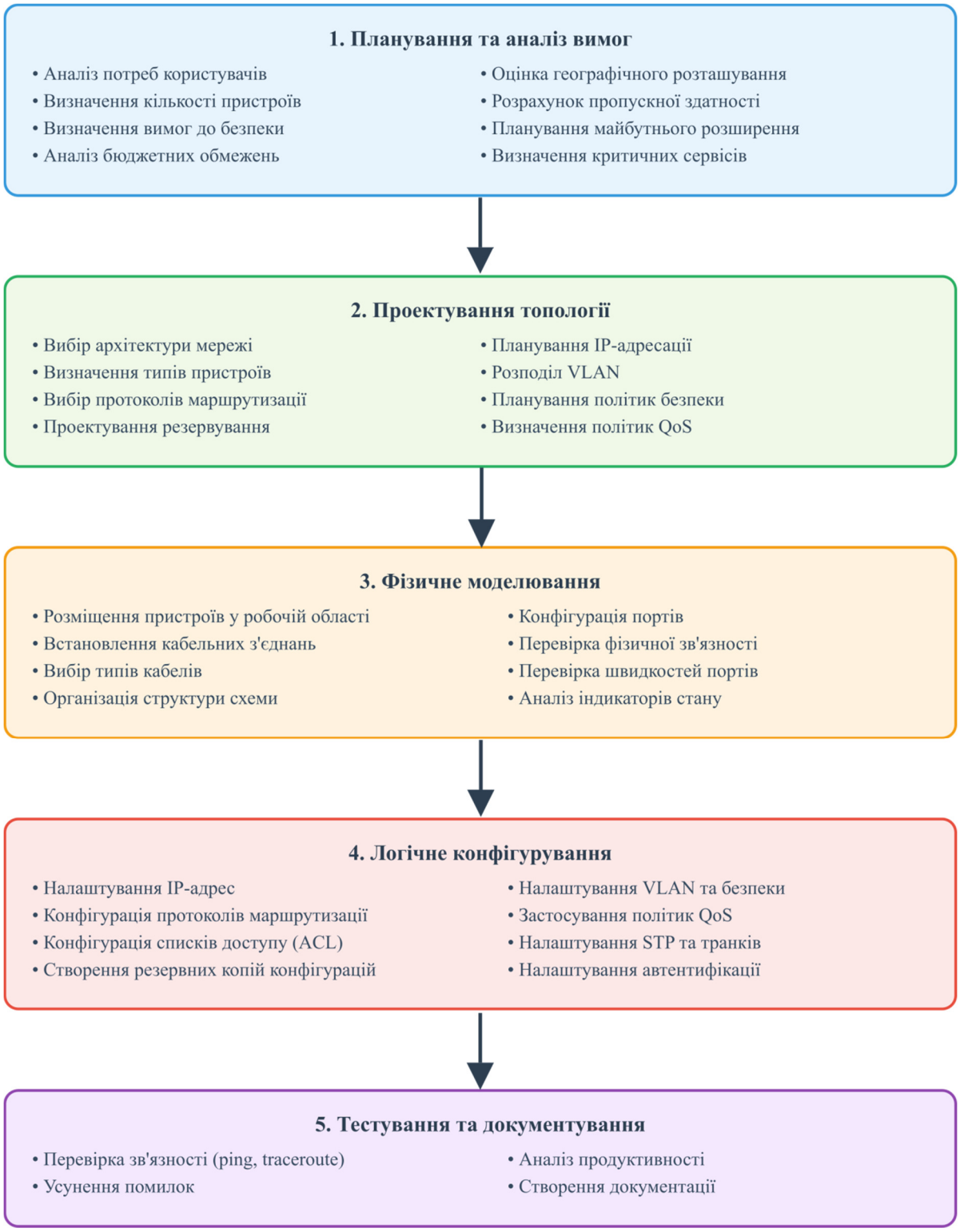

Рисунок 1.1 – Етапи моделювання комп'ютерних мереж у Cisco Packet Tracer

Етап планування та аналізу вимог є фундаментальною основою для успішного моделювання мережі та потребує детального вивчення всіх аспектів майбутньої системи. На цьому етапі необхідно провести ретельний аналіз

потреб користувачів, визначити типи додатків, які будуть використовуватися, та їх вимоги до пропускної здатності, затримки та надійності. Важливо оцінити кількість кінцевих пристроїв, які планується підключити до мережі, їх географічне розташування та можливості для майбутнього розширення системи. Аналіз також має включати визначення критично важливих сервісів, вимог до безпеки, політик резервного копіювання та планів відновлення після збоїв. Результатом цього етапу має стати документ з технічними вимогами, який слугуватиме основою для всіх подальших рішень щодо архітектури та конфігурації мережі. Правильне виконання цього етапу дозволяє уникнути серйозних помилок на пізніших стадіях проекту та забезпечує відповідність кінцевого рішення реальним потребам організації.

Етап проектування топології передбачає вибір оптимальної архітектури мережі, що найкраще відповідає визначеним на попередньому етапі вимогам та обмеженням. Цей процес включає вибір між різними топологіями (зіркоподібна, кільцева, деревоподібна, повнос в'язна) з урахуванням факторів надійності, масштабованості та вартості реалізації. Необхідно визначити типи мережевих пристроїв для кожного рівня ієрархії мережі, враховуючи їх технічні характеристики, підтримувані протоколи та можливості інтеграції з існуючою інфраструктурою. Важливою частиною проектування є планування схеми IP-адресації з використанням принципів VLSM та CIDR для оптимального використання адресного простору. Також необхідно спроектувати структуру VLAN для логічного розділення трафіку, визначити політики безпеки та якості обслуговування. Результатом цього етапу є детальна схема мережі з технічними специфікаціями всіх компонентів, план адресації та документація з описом прийнятих архітектурних рішень.

Етап фізичного моделювання включає практичну реалізацію спроектованої топології у середовищі Cisco Packet Tracer шляхом розміщення віртуальних пристроїв та встановлення з'єднань між ними. Процес починається з вибору необхідних пристроїв з палітри інструментів та їх розташування у робочій області відповідно до логічної схеми мережі. Важливо дотримуватися принципів читабельності схеми, розміщуючи пристрої логічно згруповано та забезпечуючи достатній простір для кабельних з'єднань. Наступним кроком є встановлення фізичних з'єднань між пристроями з використанням відповідних типів кабелів (прямий, кросовий, оптоволоконний) залежно від типів інтерфейсів та вимог підключення. Необхідно перевірити правильність підключень та відповідність швидкостей портів, а також врахувати обмеження щодо максимальної довжини кабельних сегментів для різних типів з'єднань. На цьому етапі також виконується базова перевірка фізичної зв'язності шляхом аналізу індикаторів стану портів та з'єднань.

Етап логічного конфігурування є найбільш складним та відповідальним процесом, що включає налаштування всіх програмних параметрів мережевих пристроїв для забезпечення їх правильної взаємодії. Конфігурація починається з призначення IP-адрес всім інтерфейсам згідно з розробленою схемою адресації, включаючи налаштування масок підмережі та адрес шлюзів за замовчуванням. Далі виконується конфігурація протоколів маршрутизації (RIP,

OSPF, EIGRP) для забезпечення автоматичного обміну маршрутною інформацією між маршрутизаторами. На комутаторах налаштовуються VLAN для логічного розділення мережевого трафіку, конфігуруються транкові з'єднання та протоколи, що запобігають утворенню петель (STP). Важливою частиною конфігурації є налаштування політик безпеки, включаючи списки контролю доступу (ACL), автентифікацію користувачів та шифрування трафіку. Також може виконуватися конфігурація сервісів якості обслуговування (QoS) для пріоритизації критично важливого трафіку. Всі налаштування повинні бути задокументовані та збережені для можливості відновлення конфігурації у разі необхідності.

Етап тестування та документування завершує процес моделювання мережі та включає комплексну перевірку працездатності всіх компонентів системи та створення повної технічної документації. Тестування починається з базової перевірки зв'язності за допомогою команди ping між всіма сегментами мережі для підтвердження правильності конфігурації маршрутизації. Далі виконується детальний аналіз таблиць маршрутизації, ARP-таблиць та конфігурацій VLAN для виявлення можливих помилок або неоптимальних налаштувань. Важливо протестувати роботу мережі під навантаженням, перевірити відмовостійкість системи шляхом імітації відмов окремих компонентів та оцінити час відновлення зв'язності. Режим симуляції Packet Tracer дозволяє детально проаналізувати проходження пакетів через мережу та переконатися в правильності роботи протоколів на всіх рівнях моделі OSI. Завершальним кроком є створення повної технічної документації, включаючи схеми мережі, таблиці IP-адресації, конфігураційні файли пристроїв, результати тестування та інструкції з усунення типових проблем, що може виникнути під час експлуатації системи.

Особливу увагу при моделюванні мереж слід приділяти принципам ієрархічного дизайну, що передбачає розділення мережі на три рівні: доступу, розподілу та ядра. Рівень доступу забезпечує підключення кінцевих пристроїв до мережі та включає комутатори доступу, точки бездротового доступу та пристрої безпеки. Рівень розподілу виконує функції агрегації трафіку, застосування політик безпеки та якості обслуговування, маршрутизації між VLAN та фільтрації трафіку. Рівень ядра забезпечує високошвидкісну комутацію між різними сегментами мережі та підключення до зовнішніх мереж. Такий підхід спрощує управління мережею, підвищує її масштабованість та полегшує усунення несправностей.

IP-адресація є фундаментальним аспектом мережевого дизайну, що потребує ретельного планування для забезпечення оптимального використання адресного простору та уникнення конфліктів. При роботі з приватними адресами класів A (10.0.0.0/8), B (172.16.0.0/12) та C (192.168.0.0/16) необхідно враховувати принципи VLSM (Variable Length Subnet Masking) для ефективного розподілу адрес. Використання підмереж різного розміру дозволяє мінімізувати втрати адрес та забезпечити можливості для майбутнього розширення мережі. Документування схеми адресації є критично важливим для подальшого адміністрування мережі та усунення проблем зв'язності.

Конфігурація мережевих пристроїв у Packet Tracer здійснюється через інтуїтивний графічний інтерфейс, що імітує роботу з реальним обладнанням Cisco. Вкладка "Physical" надає доступ до апаратної конфігурації пристрою, включаючи можливість вимикання живлення, додавання модулів розширення, заміни компонентів та перегляду індикаторів стану. Вкладка "Config" призначена для налаштування логічних параметрів, таких як імена інтерфейсів, IP-адреси, маски підмережі, VLAN, протоколи маршрутизації та політики безпеки. Вкладка "CLI" емулює інтерфейс командного рядка Cisco IOS, що дозволяє використовувати традиційні команди конфігурації для більш детального налаштування пристроїв.

Діагностика та усунення несправностей мережі є невід'ємною частиною роботи мережевого інженера та включає використання різноманітних інструментів та методик. Основні команди діагностики включають ping для перевірки базової зв'язності, traceroute для визначення шляху проходження пакетів, ipconfig/ifconfig для перегляду конфігурації інтерфейсів та arp для аналізу таблиці ARP. Packet Tracer надає додаткові інструменти візуалізації, такі як Simulation Mode, що дозволяє покроково відстежувати проходження пакетів через мережу та аналізувати роботу протоколів на різних рівнях моделі OSI. Режим Real Time забезпечує нормальну роботу мережі з реальним часом передачі пакетів.

Успішне завершення лабораторної роботи потребує дотримання послідовності виконання всіх етапів: створення облікового запису Cisco Networking Academy, завантаження та інсталяція Packet Tracer, побудова топології відповідно до варіанту завдання, конфігурація IP-адресації та тестування зв'язності мережі. Особлива увага повинна приділятися точності введення мережевих параметрів, дотриманню вимог індивідуального варіанту та документуванню всіх виконаних налаштувань. Результати тестування за допомогою команд ping та ipconfig мають підтвердити правильність конфігурації та працездатність усіх з'єднань у створеній мережі, що є основою для подальшого вивчення більш складних мережевих технологій та протоколів.

2 КЛЮЧОВІ ПИТАННЯ

1. Яке основне призначення програми Cisco Packet Tracer у навчальному процесі?
2. Які переваги та недоліки має Cisco Packet Tracer порівняно з іншими симуляторами мереж (наприклад, GNS3 або EVE-NG)?
3. Які основні етапи включає процес моделювання комп'ютерної мережі в Cisco Packet Tracer?
4. Яке призначення ієрархічних рівнів (доступу, розподілу, ядра) у проектуванні мереж?
5. Чому важливо виконувати етап планування та аналізу вимог перед створенням мережевої моделі?
6. Які основні типи пристроїв (згідно з Таблицею 1.2) 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 (наприклад, `ping`, `ipconfig`) 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?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1 Завантаження, встановлення та активація програми Cisco Packet Tracer

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

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

3.1.3. Після успішної реєстрації та входу до особистого кабінету перейдіть до розділу «Ресурси» у верхньому меню та оберіть пункт «Завантажити Packet Tracer».

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

3.1.5. 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).

3.1.6. Після першого запуску програми з’явиться вікно авторизації. Введіть логін і пароль від облікового запису Cisco Networking Academy, створеного на етапі 3.1.2.

3.1.7. 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.

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

3.2 Створення та аналіз моделі комп'ютерної мережі

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

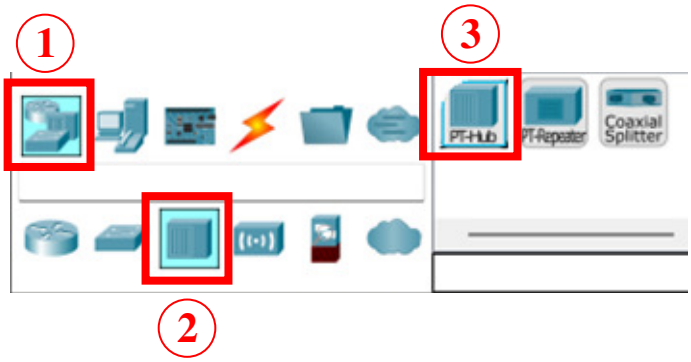

Рисунок 1.2 – Пристрої підгрупи "повторювачі"

3.2.2 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.

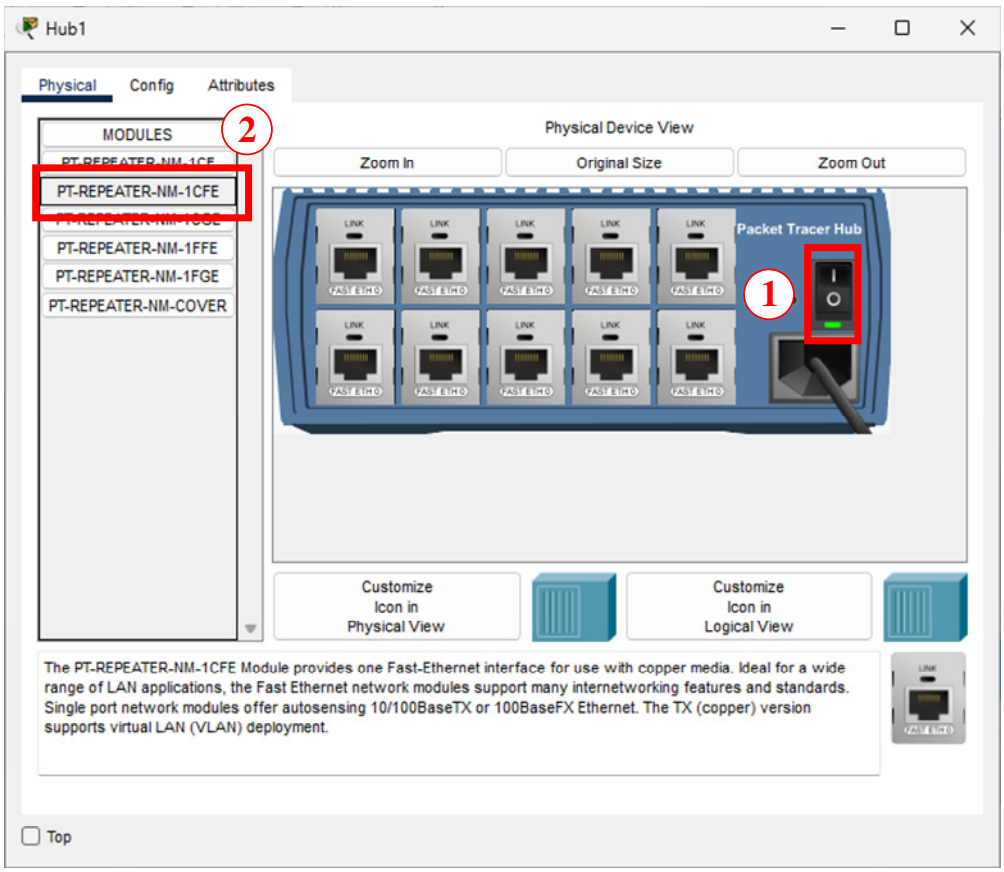

Рисунок 1.3 – Вікно апаратної конфігурації повторювача

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

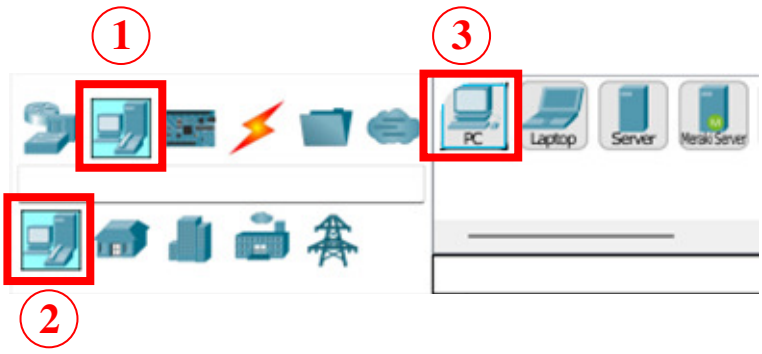

Рисунок 1.4 – Підгрупа кінцевих пристроїв

Згідно завдання необхідно розмістити три групи робочих станцій згідно таблиці 1.3.

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

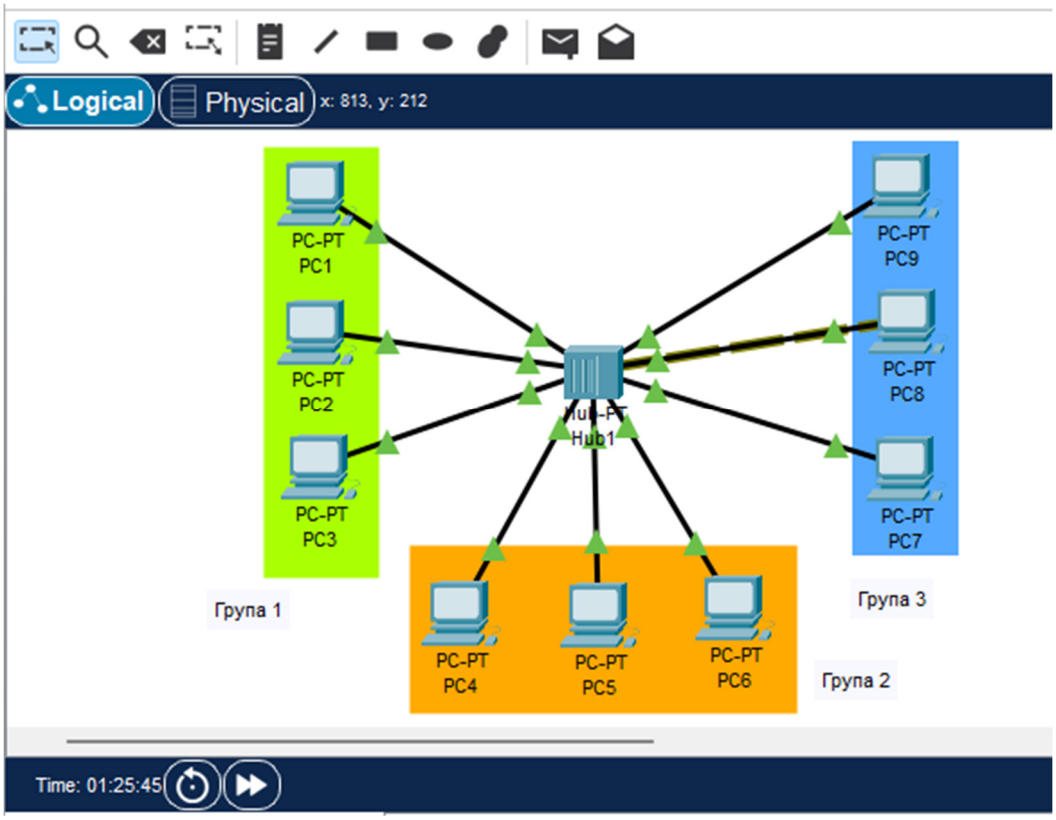

Рисунок 1.5 – Архітектура моделі мережі

3.2.4 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. Аналогічно виконати конфігурування інших робочих станцій моделі мережі.

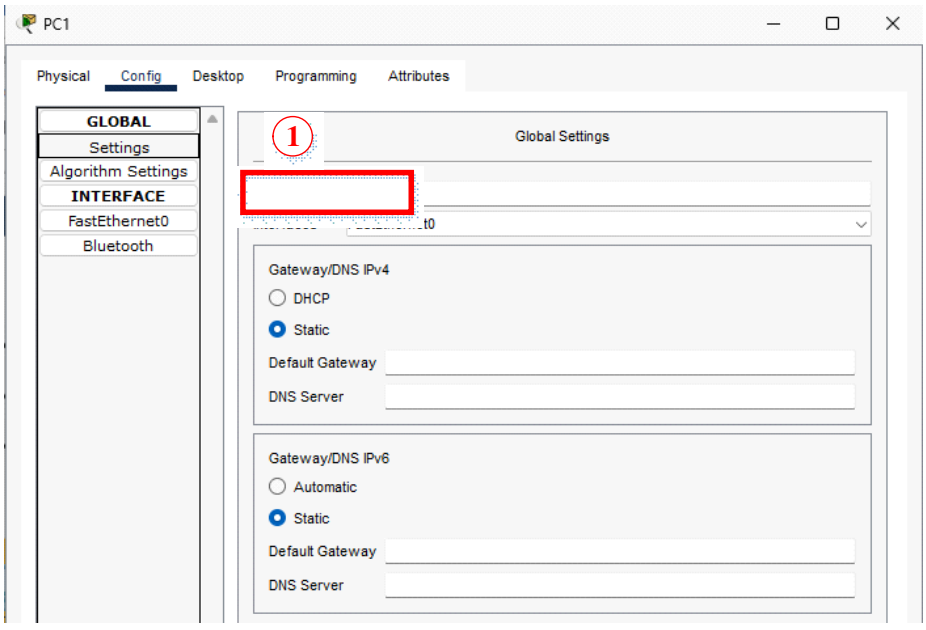

Рисунок 1.6 – Налаштування моделі робочої станції (назва)

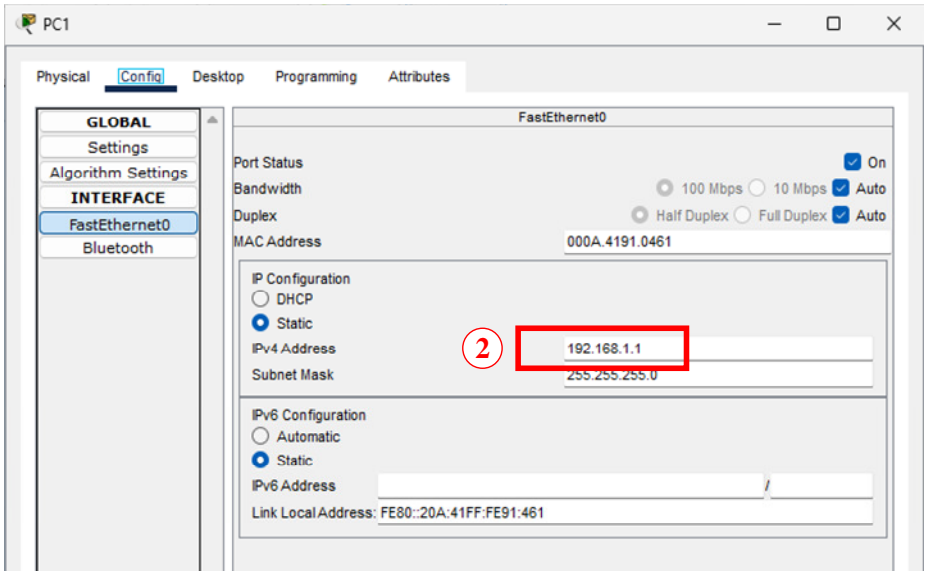

Рисунок 1.7 – Налаштування моделі робочої станції (IP адреса)

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

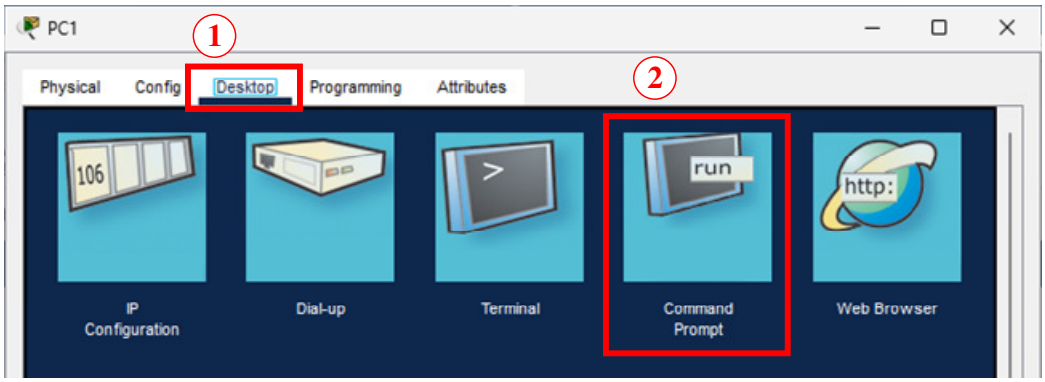

Рисунок 1.8 – Меню додатків моделі робочої станції

3.2.6 Ввести команду "ipconfig" для виводу налаштувань мережних інтерфейсів та впевнитись у відповідності IP адреси раніше введеному значенню.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20A:41FF:FE91:461
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 1.9 – Мережні налаштування моделі робочої станції

3.2.7 За допомогою команди ping перевірити наявність зв'язку із сусідніми робочими станціями.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 1.10 – Перевірка мережної зв'язності моделі робочої станції

4 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

Лабораторна робота № 2

Тема: Базове конфігурування мережного обладнання Cisco

Мета роботи: Набути практичних навичок налаштування маршрутизатора Cisco.

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Типи телекомунікаційного обладнання фірми Cisco

Компанія Cisco Systems була заснована в 1984 році подружжям Сенді та Лен Босак у Стенфордському університеті, коли вони зіткнулися з проблемою з'єднання різних комп'ютерних мереж. Назва компанії походить від міста Сан-Франциско, а логотип символізує знаменитий міст Golden Gate. Перший продукт компанії - багатопротокольний маршрутизатор AGS (Advanced Gateway Server) - дозволив об'єднувати мережі з різними протоколами передачі даних, що стало революційним рішенням для того часу. Протягом 1990-х років Cisco активно розширювала свій продуктовий портфель через численні поглинання інноваційних компаній, що дозволило їй стати лідером у галузі мережевого обладнання. До кінця XX століття компанія контролювала понад 80% ринку маршрутизаторів корпоративного класу та стала синонімом надійності в телекомунікаційній індустрії.

Внесок Cisco у розвиток телекомунікаційних технологій важко переоцінити, оскільки компанія стояла у витоків сучасного Інтернету та корпоративних мереж. Компанія розробила та стандартизувала численні мережеві протоколи, включаючи EIGRP (Enhanced Interior Gateway Routing Protocol), HSRP (Hot Standby Router Protocol) та CDP (Cisco Discovery Protocol), які широко використовуються в сучасних мережах. Операційна система Cisco IOS (Internetwork Operating System), вперше представлена в 1986 році, стала де-факто стандартом для управління мережевим обладнанням і впливала на розвиток інтерфейсів командного рядка в усій індустрії.

Сьогодні Cisco випускає широкий спектр телекомунікаційного обладнання, що охоплює всі рівні мережевої інфраструктури від домашніх пристроїв до обладнання для центрів обробки даних рівня підприємства. Основними категоріями продуктів є маршрутизатори (Router), комутатори (Switch), точки доступу бездротових мереж (Wireless Access Point), міжмережеві екрани (Firewall), телефонні системи (IP Telephony), а також спеціалізовані пристрої для відеоконференцій та колаборації. Кожна категорія включає десятки моделей, що розрізняються за продуктивністю, функціональністю та цільовою аудиторією - від малих офісів до великих корпорацій та інтернет-провайдерів.

Особливістю обладнання Cisco є модульна архітектура більшості пристроїв, що дозволяє гнучко налаштовувати конфігурацію під конкретні потреби замовника. Наприклад, маршрутизатори серії ISR (Integrated Services

Router) можуть комплектуватися різними типами інтерфейсних модулів, модулями безпеки, голосовими картами та іншими компонентами. Всі пристрої Cisco працюють під управлінням операційної системи IOS або її модифікацій, що забезпечує уніфікований підхід до управління та адміністрування незалежно від типу обладнання.

1.2 Основні групи комутаторів Cisco

У таблиці 2.1 представлено основні серії комутаторів Cisco, що випускалися протягом останніх двох десятиліть та актуальні на сьогоднішній день.

Таблиця 2.1 – Основні серії комутаторів Cisco

Покоління	Серія	Роки випуску	Особливості
Catalyst 2960	2960, 2960-X, 2960-XR, 2960-L	2006-2023	Комутатори рівня доступу, FastEthernet/GigabitEthernet, PoE підтримка
Catalyst 3560	3560, 3560-X, 3560-CX	2005-2020	Комутатори L3, стекування, розширена безпека
Catalyst 3650/3850	3650, 3850	2013-2021	Конвергентна інфраструктура, UADP ASIC, StackWise-480
Catalyst 9200/9300/9400/9500	9200, 9300, 9300L, 9400, 9500, 9600	2017-теперішній час	Intent-based networking, programmable ASIC, Cisco DNA
Nexus	3000, 5000, 7000, 9000 серії	2008-теперішний час	Центри обробки даних, 10/40/100GbE, FCoE підтримка
Industrial Ethernet	IE-2000, IE-3000, IE-4000, IE-5000	2008-теперішний час	Промислові умови, розширений температурний діапазон

Комутатори серії Catalyst 2960 традиційно позиціонуються як пристрої рівня доступу для малих та середніх офісів, забезпечуючи базові функції комутації на другому рівні моделі OSI. Ці пристрої відрізняються простотою налаштування, енергоефективністю та підтримкою технології Power over Ethernet для живлення IP-телефонів, точок доступу Wi-Fi та IP-камер. Модифікації з індексами X та XR додали підтримку стекування StackWise Plus, розширені можливості QoS та вдосконалені функції безпеки. Останні моделі серії 2960-L позиціонуються як бюджетні рішення з обмеженим функціоналом, призначені для найпростіших завдань комутації в невеликих мережах.

Серія Catalyst 3560 представляє комутатори третього рівня з можливостями маршрутизації, що робить їх ідеальними для використання як aggregation switch у середніх корпоративних мережах. Ці пристрої підтримують динамічні протоколи маршрутизації, VLAN inter-routing, розширені списки доступу та функції multicast. Технологія StackWise дозволяє об'єднувати до дев'яти комутаторів у єдиний логічний блок з пропускною здатністю стекового з'єднання до 32 Гбіт/с. Серія 3560-CX призначена для компактних інсталяцій та

підтримує сучасні стандарти, включаючи 802.11ac Wave 2 для бездротової інфраструктури.

Платформи Catalyst 3650 та 3850 стали перехідною ланкою до сучасної архітектури програмованих мереж, вперше впроваджуючи концепцію Unified Access Data Plane (UADP). Ці комутатори забезпечують конвергентну інфраструктуру для дротових та бездротових підключень з централізованим управлінням через контролер бездротової мережі. Технологія StackWise-480 забезпечує пропускну здатність стека до 480 Гбіт/с, а вбудовані можливості аналітики дозволяють отримувати детальну телеметрію про роботу мережі.

Сучасне покоління комутаторів Catalyst 9000 представляє повністю програмовану мережеву платформу, побудовану навколо концепції Intent-Based Networking (IBN). Серія 9200 призначена для рівня доступу, 9300 - для агрегації, 9400 - для ядра кампусу, а 9500 та 9600 - для високопродуктивних центрів обробки даних. Всі моделі оснащені програмованими ASIC чіпами, що дозволяє додавати нові функції через оновлення мікрокоду без заміни апаратного забезпечення. Інтеграція з платформою Cisco DNA Center забезпечує централізоване управління, автоматизацію та аналітику мережі.

1.3 Основні групи маршрутизаторів Cisco

У таблиці 2.2 наведено класифікацію основних серій маршрутизаторів Cisco за їх призначенням та технічними характеристиками.

Таблиця 2.2 - Основні серії маршрутизаторів Cisco

Покоління	Серія	Роки випуску	Особливості
ISR G1	1800, 2800, 3800	2005-2016	Перше покоління ISR, модульна архітектура, VPN підтримка
ISR G2	1900, 2900, 3900	2009-2020	Покращена продуктивність, PVDM3 модулі, UC готовність
ISR 4000	4200, 4300, 4400, 4500	2013-теперішній час	Multicore архітектура, Application hosting, SD-WAN
ASR	ASR 1000, ASR 9000, ASR 920	2008-теперішній час	Carrier-class, MPLS, високошвидкісні інтерфейси
ISR 1000	1100, 1000v	2016-теперішній час	SD-WAN ready, хмарне управління, компактні розміри
Branch	800, 1000	2007-2018	Малі філії, ADSL/3G/4G модеми, Wi-Fi інтеграція

Маршрутизатори серії Integrated Services Router (ISR) першого покоління заклали основи модульної архітектури, що стала стандартом для корпоративних маршрутизаторів Cisco. Серії 1800, 2800 та 3800 забезпечували інтеграцію голосових послуг, безпеки та передачі даних у єдиній платформі, що значно спростило управління мережевою інфраструктурою філій. Ці пристрої підтримували різноманітні інтерфейсні модуле - від традиційних WAN підключень до T1/E1 ліній, а також забезпечували апаратне шифрування VPN

трафіку. Архітектура дозволяла гнучко нарощувати функціональність шляхом встановлення додаткових модулів без необхідності заміни основного пристрою.

Друге покоління ISR (серії 1900, 2900, 3900) принесло суттєве покращення продуктивності завдяки використанню більш потужних процесорів та оптимізованої архітектури. Впровадження цифрових сигнальних процесорів PVDM3 дозволило значно збільшити кількість одночасних голосових викликів та поліпшити якість обробки медіа-потоків. Ці маршрутизатори стали основою для розгортання комплексних UC (Unified Communications) рішень, інтегруючи IP-телефонію, відеоконференції та обмін повідомленнями. Підтримка технологій віртуалізації дозволила запускати гостьові операційні системи безпосередньо на маршрутизаторі.

Сучасні маршрутизатори ISR 4000 серії представляють кардинально нову архітектуру, побудовану на багатоядерних процесорах з роздільними площинами управління та даних. Серії 4200, 4300, 4400 та 4500 різняться за продуктивністю та кількістю інтерфейсних слотів, але всі підтримують технології програмно-визначених мереж SD-WAN. Можливість хостингу додатків дозволяє запускати віртуальні мережеві функції (VNF) безпосередньо на маршрутизаторі, зменшуючи потребу в окремих апаратних пристроях. Інтеграція з хмарними сервісами Cisco забезпечує централізоване управління та моніторинг розподіленої мережевої інфраструктури.

Серія ASR (Aggregation Services Router) призначена для операторів зв'язку та великих підприємств, які потребують високої продуктивності та надійності на рівні carrier-class. Маршрутизатори ASR 1000 забезпечують пропускну здатність до декількох терабіт на секунду та підтримують розширені MPLS функції, включаючи L3VPN, L2VPN та VPLS. ASR 9000 серія позиціонується як платформа для побудови ядер IP/MPLS мереж з підтримкою 100GbE інтерфейсів та модульною архітектурою для максимальної масштабованості. Компактні моделі ASR 920 призначені для агрегації трафіку в точках присутності та підтримують синхронізацію за протоколами IEEE 1588v2.

1.4 Архітектура типового обладнання Cisco

Мережеві пристрої компанії Cisco, зокрема комутатори та маршрутизатори платформ ISR (Integrated Services Router), побудовані на базі модульної архітектури, яка забезпечує високу надійність, масштабованість та гнучкість конфігурування. Ця архітектура, представлена на рисунку 2.1, демонструє інтегрований підхід до побудови мережевого обладнання, де всі компоненти працюють як єдиний комплекс. Основу архітектури становить процесорна плата з інтегрованими функціями комутації та маршрутизації, яка виконує всі критично важливі операції з обробки мережевого трафіку в реальному часі. Ця плата містить спеціалізовані ASIC-мікросхеми та мережеві процесори, що дозволяють забезпечити високошвидкісну обробку пакетів навіть при пікових навантаженнях мережі. Центральний процесор координує роботу всіх підсистем, управляє процесами Layer 2 та Layer 3 обробки трафіку,

а також забезпечує виконання складних мережевих протоколів та алгоритмів маршрутизації.

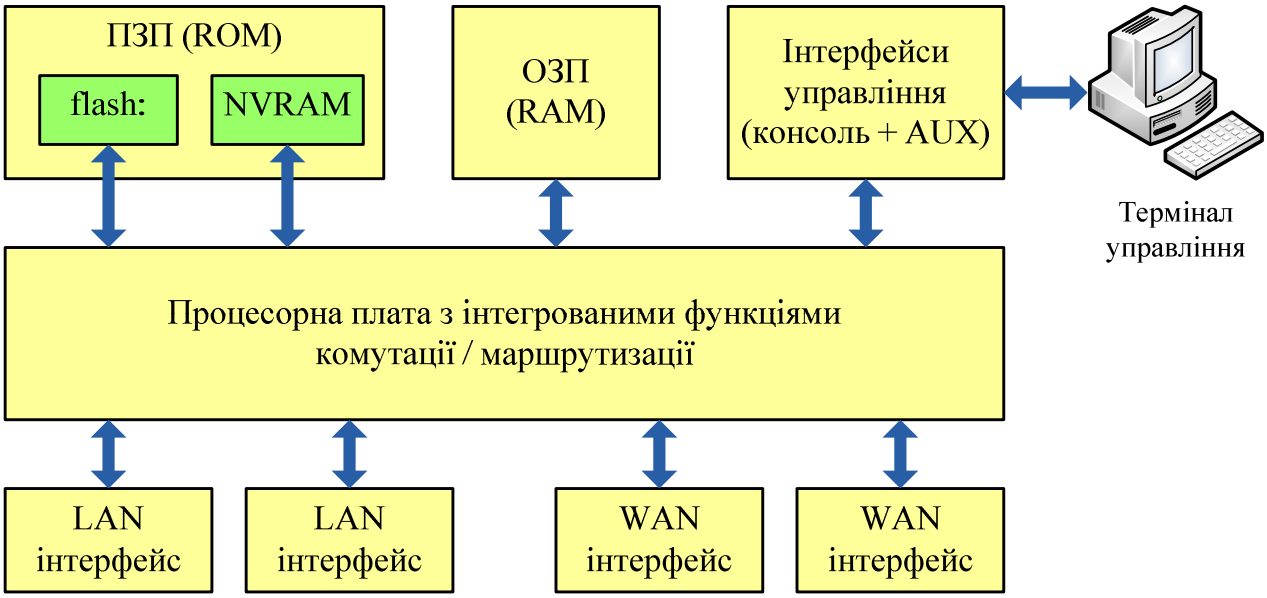

Рисунок 2.1 – Структурна схема маршрутизатора

Інтегрована природа архітектури дозволяє оптимізувати міжкомпонентну взаємодію та мінімізувати затримки при передачі даних між різними функціональними блоками пристрою. Така організація особливо важлива для маршрутизаторів ISR, які поєднують функції маршрутизації, комутації, забезпечення безпеки та надання різноманітних мережевих сервісів в одному корпусі.

Система зберігання даних у пристроях Cisco організована за ієрархічним принципом, що забезпечує як швидкий доступ до критично важливої інформації, так і довгострокове зберігання конфігурацій та програмного забезпечення. Як показано на архітектурній схемі, кожен тип пам'яті виконує специфічні функції у загальній системі. Постійний запам'ятовуючий пристрій (ПЗП або ROM) містить базову програму завантаження ROMMON (ROM Monitor) та набір діагностичних утиліт, які забезпечують початкову ініціалізацію системи та перевірку працездатності апаратних компонентів. Ця підсистема є критично важливою для відновлення пристрою в аварійних ситуаціях та забезпечення можливості оновлення програмного забезпечення.

Flash-пам'ять використовується для зберігання операційної системи Cisco IOS, конфігураційних файлів та додаткових програмних модулів, що дозволяє легко оновлювати програмне забезпечення без необхідності заміни апаратних компонентів. Оперативна пам'ять (ОЗП або RAM) відіграє центральну роль у забезпеченні високої продуктивності пристрою. Вона містить активну конфігурацію running-config, таблиці маршрутизації, кеш ARP, буфери пакетів та робочі дані всіх активних процесів операційної системи. NVRAM (Non-Volatile RAM) забезпечує збереження стартової конфігурації startup-config навіть при повному знеструмленні пристрою, що гарантує автоматичне відновлення налаштувань при наступному включенні.

Процес завантаження пристроїв Cisco, детально ілюстрований на рисунку 2.2, відбувається у суворо визначеній послідовності, що забезпечує надійну та передбачувану ініціалізацію всіх компонентів системи. Початковий етап розпочинається при увімкненні живлення, коли пристрій автоматично виконує POST (Power-On Self Test) та запускає стартовий завантажувач ROMMON з постійної пам'яті. Цей компонент містить мінімальний набір інструкцій, необхідних для базової діагностики апаратури, ініціалізації системної шини та підготовки пристрою до завантаження основної операційної системи. На цьому етапі перевіряється працездатність процесора, різних типів пам'яті, системних шин та критично важливих інтерфейсів.

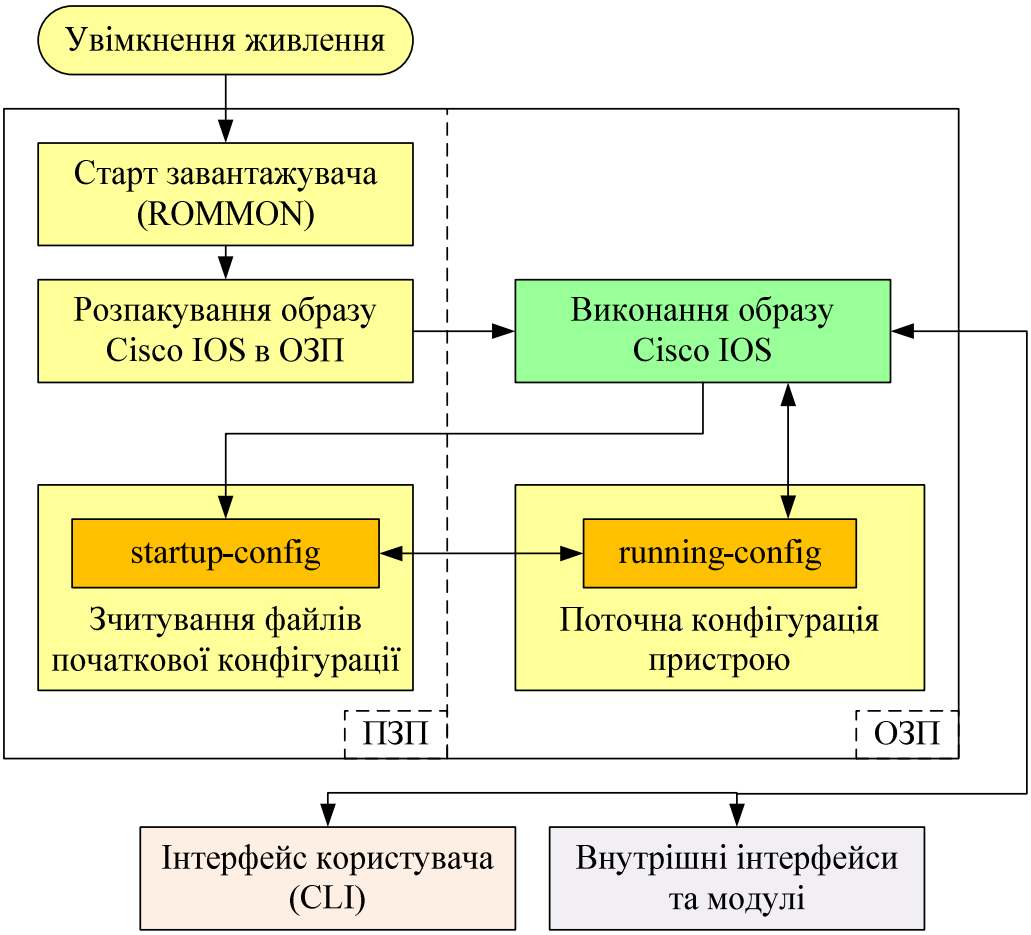

Рисунок 2.2 – Завантаження IOS із ОЗП (маршрутизатор RFR)

Після успішного завершення початкової діагностики система переходить до ключового етапу розпакування образу операційної системи Cisco IOS. Цей процес включає читання стисненого образу з flash-пам'яті та його розгортання в оперативній пам'яті, що може тривати від кількох секунд до кількох хвилин залежно від розміру образу IOS, швидкості роботи пам'яті та потужності процесора. Під час розпакування система також виконує перевірку цілісності образу за допомогою контрольних сум, що запобігає завантаженню пошкоджених файлів.

Після завершення успішного розпакування система починає виконання образу Cisco IOS безпосередньо з оперативної пам'яті, що забезпечує

максимальну швидкість роботи операційної системи та мінімізує час відгуку на мережеві події. На заключному етапі завантаження відбувається критично важливий процес зчитування та застосування конфігураційних параметрів. Спочатку система завантажує файл startup-config з NVRAM та створює його активну копію running-config в оперативній пам'яті, після чого ініціалізує всі мережеві інтерфейси, запускає необхідні мережеві протоколи та активує інтерфейс командного рядка (CLI) для взаємодії з адміністраторами.

1.5 Інтерфейсна підсистема та мережева зв'язність

Інтерфейсна підсистема пристроїв Cisco представлена широким спектром портів різного призначення, що забезпечують універсальність підключення до різноманітних типів мереж та телекомунікаційних систем. Локальні мережеві інтерфейси (LAN) зазвичай реалізовані у вигляді портів Ethernet з підтримкою різних швидкостей передачі даних - від традиційного Fast Ethernet (100 Мбіт/с) до сучасного Gigabit Ethernet (1 Гбіт/с) та вище, залежно від моделі пристрою та його позиціонування в лінійці продуктів. Ці інтерфейси забезпечують підключення до корпоративних локальних мереж, серверних сегментів та кінцевого обладнання користувачів.

Глобальні мережеві інтерфейси (WAN) призначені для з'єднання з провайдерськими мережами та можуть включати серійні порти для підключення до традиційних телекомунікаційних ліній, оптичні інтерфейси для високошвидкісних з'єднань, а також спеціалізовані порти для роботи з xDSL, кабельними модемами та іншими технологіями доступу. Модульна архітектура маршрутизаторів ISR дозволяє гнучко налаштовувати конфігурацію інтерфейсів відповідно до специфічних потреб мережевої інфраструктури організації.

Система управління пристроями Cisco забезпечує адміністраторам різноманітні способи доступу для конфігурування, моніторингу та діагностики мережевого обладнання. Консольний порт (Console) є основним засобом локального управління та використовується для прямого підключення термінала або комп'ютера через послідовний інтерфейс RS-232. Цей тип з'єднання особливо важливий при первинному налаштуванні пристрою, відновленні після збоїв та виконанні складних діагностичних процедур, коли мережеве підключення недоступне або не функціонує належним чином.

Допоміжний порт (AUX) розширює можливості віддаленого управління, дозволяючи здійснювати адміністрування через модемне з'єднання або інші асинхронні лінії зв'язку. Це особливо корисно для пристроїв, розташованих у віддалених офісах або філіях, де фізичний доступ до обладнання обмежений. Термінал управління може бути реалізований як спеціалізований комп'ютер з відповідним програмним забезпеченням для емуляції терміналу та роботи з командним рядком IOS, що забезпечує повноцінний доступ до всіх функцій управління та конфігурування пристрою.

Однією з ключових переваг архітектури маршрутизаторів ISR є їх висока модульність, що дозволяє адаптувати функціональність пристрою до

специфічних потреб мережевої інфраструктури. Система розширення базується на використанні різноманітних модулів, які можуть додавати нові інтерфейси, розширювати функціональність безпеки, забезпечувати підтримку голосових сервісів або надавати спеціалізовані можливості обробки трафіку. Модулі розширення для маршрутизаторів ISR включають HWIC (High-Speed WAN Interface Card), VWIC (Voice/WAN Interface Card) та EHWIC (Enhanced High-Speed WAN Interface Card), які забезпечують різні комбінації інтерфейсів та функцій.

Платформи ISR G1 та ISR G2 мають певні відмінності в підтримці модулів розширення, причому друге покоління пристроїв забезпечує більшу пропускну здатність та розширені можливості інтеграції сервісів.

Таблиця 2.3 – Модулі розширення для маршрутизаторів ISR G1 та ISR G2

Тип модуля	Призначення	ISR G1	ISR G2	Особливості
HWIC-4ESW	4-портовий Ethernet комутатор	✓	✓	10/100 Мбіт/с
EHWIC-4ESG	4-портовий Gigabit Ethernet	✗	✓	10/100/1000 Мбіт/с
VWIC2-1MFT-T1/E1	Голосовий/WAN інтерфейс	✓	✓	T1/E1 підключення
HWIC-1T	Серійний T1 інтерфейс	✓	✓	WAN підключення
HWIC-2T	Подвійний T1 інтерфейс	✓	✓	Два T1 канали
EHWIC-3G-HSPA-U	3G стільниковий модем	✗	✓	GPRS/EDGE/UMTS/HSPA
EHWIC-D-8ESG-P	8-портовий PoE Gigabit	✗	✓	Power over Ethernet
HWIC-4A/S	4-портовий асинхронний	✓	✓	Послідовні з'єднання
VWIC3-4MFT-T1/E1	Голосовий модуль 3-го покоління	✗	✓	Покращена продуктивність
EHWIC-VA-DSL-A	ADSL/ADSL2+ інтерфейс	✗	✓	Широкосмуговий доступ

Ця модульна архітектура дозволяє організаціям поступово нарощувати функціональність своїх мережевих пристроїв відповідно до зростаючих потреб, не вимагаючи повної заміни основного обладнання. Крім того, використання стандартизованих модулів забезпечує сумісність та спрощує процеси планування, закупівлі та технічного обслуговування мережевої інфраструктури.

1.6 Режими роботи операційної системи Cisco IOS

Cisco IOS (Internetwork Operating System) являє собою операційну систему, спеціально розроблену для управління мережевими пристроями компанії Cisco. Її основне призначення полягає в забезпеченні функціональності та управління мережевими пристроями, такими як маршрутизатори та комутатори. Cisco IOS забезпечує ефективне управління та

маршрутизацію даних у комп'ютерних мережах. Вона надає надійну та безпечну платформу для обміну інформацією між пристроями в мережі. Однією з ключових функцій Cisco IOS є підтримка різних мережевих протоколів, що робить її універсальним інструментом для побудови та підтримки різних мережевих топологій. Вона забезпечує високий ступінь гнучкості, даючи змогу налаштовувати й адаптувати мережеві пристрої під конкретні потреби підприємства. Cisco IOS також надає механізми безпеки, включно з аутентифікацією, авторизацією та обліком, для забезпечення захисту мережевих ресурсів. Вона підтримує віддалене керування мережевими пристроями через протоколи, як-от Telnet і SSH, забезпечуючи зручність адміністрування. Cisco IOS сприяє оптимізації мережевого трафіку, що підвищує продуктивність і ефективність мережі. Вона також надає можливості моніторингу та діагностики для оперативного виявлення та вирішення проблем у мережі. Cisco IOS забезпечує масштабованість, даючи змогу інтегрувати нові пристрої та технології в наявну інфраструктуру. Ця операційна система є основою для розробки та впровадження різних сервісів, таких як віртуальні приватні мережі (VPN) і мережеві служби. Вона підтримує технології QoS (Quality of Service), забезпечуючи пріоритет передавання даних та оптимізацію мережевого трафіку. Cisco IOS сприяє створенню надійних і ефективних мережевих рішень, що робить її кращим вибором для різних підприємств і провайдерів послуг зв'язку.

Операційна система Cisco IOS організована за принципом ієрархічних режимів доступу, що забезпечує різні рівні привілеїв та функціональних можливостей для користувачів залежно від їх ролі та потреб. Ця архітектура режимів була розроблена з метою забезпечення безпеки системи шляхом обмеження доступу до критично важливих команд конфігурації для неавторизованих користувачів. Кожен режим має свій унікальний набір доступних команд, власний формат командного рядка та специфічні правила переходу до інших режимів. Розуміння структури режимів є фундаментальним для ефективної роботи з мережевим обладнанням Cisco, оскільки воно визначає логіку навігації по системі та доступність функцій адміністрування. Правильне використання режимів також дозволяє мінімізувати ризики випадкових змін критично важливих параметрів мережевої конфігурації.

Рисунок 2.3 ілюструє повну діаграму переходів між режимами операційної системи Cisco IOS, демонструючи логічну структуру доступу до функцій управління мережевим обладнанням.

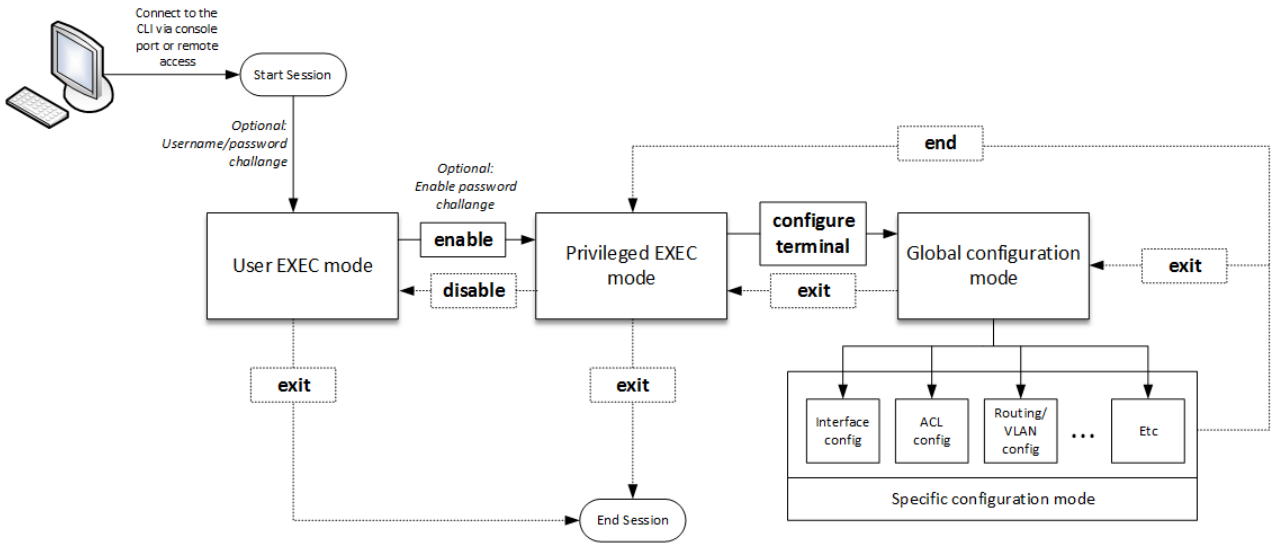

Рисунок 2.3 – Діаграма режимів роботи Cisco IOS

Діаграма відображає ієрархічну структуру режимів, що починається з початкової точки підключення до пристрою через консольний порт або віддалений доступ. Початковий стан "Start Session" представляє момент встановлення з'єднання з пристроєм, після якого система автоматично переходить у режим User EXEC mode, що позначається запрошенням командного рядка у форматі "Router>". З цього базового режиму користувач може виконувати лише обмежений набір команд діагностики та перегляду стану системи, не маючи можливості змінювати конфігурацію пристрою. Перехід до привілейованого режиму здійснюється командою "enable" та може вимагати введення пароля, якщо такий налаштований адміністратором системи.

Privileged EXEC mode являє собою розширений режим управління з запрошенням у форматі "Router#", який надає доступ до всіх команд діагностики, моніторингу та управління файлами конфігурації. У цьому режимі адміністратор може виконувати команди збереження та відновлення конфігурації, перезавантаження системи, оновлення програмного забезпечення та детальної діагностики роботи всіх компонентів пристрою. Для переходу до режиму зміни конфігурації використовується команда "configure terminal", що переводить систему в Global configuration mode з характерним запрошенням "Router(config)#". Цей режим дозволяє виконувати глобальні зміни конфігурації пристрою, такі як встановлення імені хоста, налаштування паролів, конфігурація протоколів маршрутизації та інші параметри, що стосуються всього пристрою в цілому.

З режиму глобальної конфігурації система надає можливість переходу до специфічних підрежимів конфігурації, кожен з яких призначений для налаштування окремих компонентів або функцій пристрою. Interface config mode активується командою "interface" з вказівкою конкретного інтерфейсу та дозволяє налаштовувати параметри мережевих портів, включаючи IP-адреси, маски підмереж, швидкість передачі даних та інші специфічні параметри інтерфейсів. ACL config mode призначений для створення та модифікації списків контролю доступу, що забезпечують фільтрацію трафіку на основі

різних критеріїв. Routing/VLAN config mode використовується для конфігурації протоколів маршрутизації та налаштування віртуальних локальних мереж відповідно. Діаграма також показує наявність додаткових специфічних режимів конфігурації, позначених як "Etc", що включають режими налаштування ліній термінального доступу, криптографічних параметрів та інших спеціалізованих функцій.

Навігація між режимами здійснюється за допомогою спеціальних команд переходу, основними з яких є "exit" для повернення на один рівень вгору та "end" для безпосереднього переходу з будь-якого режиму конфігурації до привілейованого режиму. Команда "disable" дозволяє повернутися з привілейованого режиму до користувацького режиму, а завершення сесії відбувається через команди "exit" або "logout" з відповідним переходом до стану "End Session". Така структурована організація режимів забезпечує логічну та безпечну роботу з конфігурацією мережевого обладнання, дозволяючи адміністраторам ефективно управляти складними мережевими інфраструктурами з мінімальними ризиками несанкціонованих змін або випадкових помилок конфігурації.

1.7 Основні команди Cisco IOS

У таблиці 2.4 представлено систематизовані групи команд операційної системи Cisco IOS, що використовуються для конфігурації та управління мережевим обладнанням.

Таблиця 2.4 – Основні команди Cisco IOS

Група команд	Команда	Призначення	Приклад використання
Навігація та режими	enable	Перехід у привілейований режим	Router> enable
	configure terminal	Перехід у режим глобальної конфігурації	Router# configure terminal
	interface	Перехід у режим конфігурації інтерфейсу	Router(config)# interface fa0/0
	exit	Повернення на попередній рівень	Router(config-if)# exit
	end	Повернення у привілейований режим	Router(config)# end
Інформаційні команди	show running-config	Перегляд поточної конфігурації	Router# show running-config
	show ip interface brief	Стислий перегляд стану інтерфейсів	Router# show ip int brief
	show version	Інформація про систему та версію IOS	Router# show version
	show ip route	Перегляд таблиці маршрутизації	Router# show ip route
Конфігурація інтерфейсів	ip address	Призначення IP адреси інтерфейсу	Router(config-if)# ip address 192.168.1.1 255.255.255.0

Група команд	Команда	Призначення	Приклад використання
	no shutdown	Активація інтерфейсу	Router(config-if)# no shutdown
	shutdown	Деактивація інтерфейсу	Router(config-if)# shutdown
	description	Опис інтерфейсу	Router(config-if)# description LAN Interface
Збереження конфігурації	copy running-config startup-config	Збереження конфігурації	Router# copy run start
	write memory	Альтернативна команда збереження	Router# write memory
	erase startup-config	Видалення збереженої конфігурації	Router# erase startup-config
Діагностика	ping	Перевірка зв'язку	Router# ping 192.168.1.10
	traceroute	Трасування маршруту	Router# traceroute 8.8.8.8
	debug	Включення діагностичних повідомлень	Router# debug ip routing
Віддалений доступ	line vty	Конфігурація віртуальних терміналів	Router(config)# line vty 0 4
	password	Встановлення пароля	Router(config-line)# password cisco
	login	Активація аутентифікації	Router(config-line)# login
	transport input	Дозволені протоколи підключення	Router(config-line)# transport input ssh

Команди навігації та переходу між режимами становлять основу роботи з інтерфейсом командного рядка Cisco IOS та дозволяють адміністратору переміщуватися між різними рівнями конфігурації. Команда enable переводить пристрій із користувацького режиму (User EXEC) у привілейований режим (Privileged EXEC), що дозволяє виконувати команди діагностики та управління. Для входу в режим конфігурації використовується команда configure terminal, після якої стає доступною зміна параметрів пристрою. Команди interface дозволяють перейти до налаштування конкретного інтерфейсу, а exit та end забезпечують повернення на попередні рівні або безпосередньо в привілейований режим.

Інформаційні команди групи show є найчастіше використовуваними у повсякденній роботі мережевих адміністраторів, оскільки вони дозволяють отримувати актуальну інформацію про стан пристрою та мережі. Команда show running-config відображає поточну активну конфігурацію пристрою в текстовому форматі, що особливо корисно для діагностики проблем або створення резервних копій. Команда show ip interface brief надає стислу таблицю всіх інтерфейсів з їх IP-адресами та станом, дозволяючи швидко оцінити топологію підключень. Використання команди show version дає змогу отримати детальну інформацію про модель пристрою, версію операційної системи, час роботи та встановлені модулі.

1.8 Алгоритм базового налаштування маршрутизатора/комутатора

Процес приведення мережевого обладнання Cisco до робочого стану включає послідовність обов'язкових кроків, що забезпечують базову функціональність та безпеку пристрою. Початковий етап передбачає фізичне підключення до пристрою через консольний порт за допомогою спеціального кабелю RS-232 або USB-to-Serial адаптера, після чого встановлюється термінальне з'єднання зі швидкістю 9600 бод, 8 біт даних, без парності та з одним стоп-бітом. При першому увімкненні пристрій завантажується з заводськими налаштуваннями та пропонує запустити майстер початкової конфігурації, який доцільно відхилити для ручного налаштування. Наступним кроком є перехід у привілейований режим командою enable та встановлення паролів для забезпечення базової безпеки доступу.

Конфігурація мережевих інтерфейсів починається з переходу в режим глобальної конфігурації командою configure terminal, після чого для кожного необхідного інтерфейсу виконується послідовність команд налаштування. Спочатку здійснюється перехід до конфігурації конкретного інтерфейсу командою interface, потім призначається IP-адреса та маска підмережі командою ip address, після чого інтерфейс активується командою no shutdown. Для комутаторів додатково може знадобитися конфігурація VLAN та портів доступу або trunk портів залежно від топології мережі. Після налаштування всіх інтерфейсів необхідно перевірити їх стан командою show ip interface brief та переконатися, що всі потрібні інтерфейси перебувають у стані "up/up".

Налаштування віддаленого доступу є критично важливим для подальшого адміністрування пристрою без необхідності фізичного підключення. Конфігурація Telnet доступу включає перехід до налаштування віртуальних терміналів командою line vty 0 4, встановлення пароля командою password та активацію аутентифікації командою login. Для забезпечення більшої безпеки рекомендується налаштувати SSH доступ, що потребує попереднього створення RSA ключів командою crypto key generate rsa, встановлення доменного імені командою ip domain-name та конфігурації локальних користувачів з унікальними паролями. Завершальним етапом є збереження конфігурації командою copy running-config startup-config, що забезпечує відновлення налаштувань після перезавантаження пристрою та створює основу для подальшого розширення функціональності мережі.

2 КЛЮЧОВІ ПИТАННЯ

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?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. Відкрити симулятор мереж Cisco Packet Tracer та побудувати схему мережі згідно рис. 2.4, що включає маршрутизатор 1841, а також дві робочі станції (PC0, PC1). Виконати з'єднання згідно табл. 2.5.

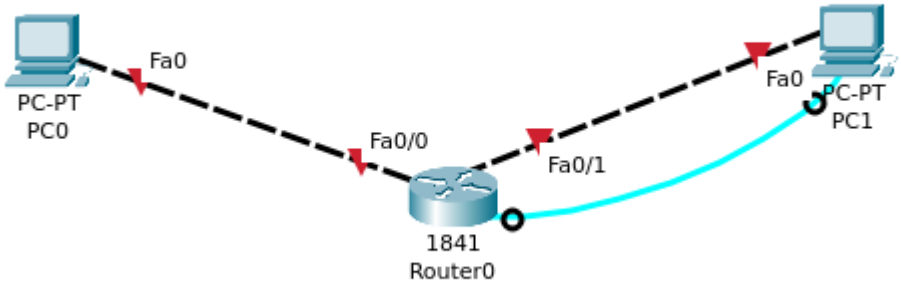

Рисунок 2.4 – Схема моделі мережі

Таблиця 2.5 – 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

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

PC0 – 192.168.1.(N+10)
PC1 – 192.168.2.(N+20)

3.3. 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. 2.5).

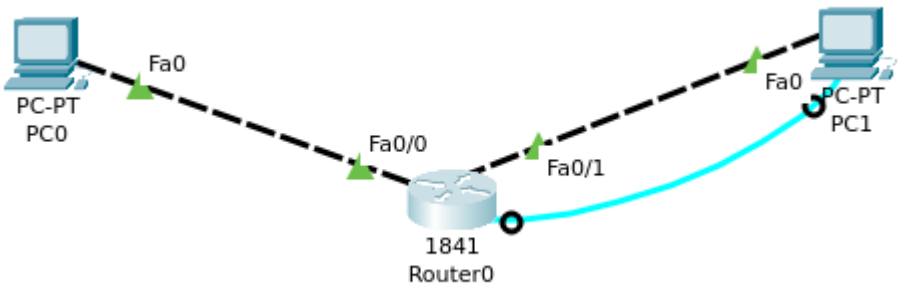

Рисунок 2.5 – Схема моделі мережі після налаштування мережних інтерфейсів

3.4. 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#
```

3.5. 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.

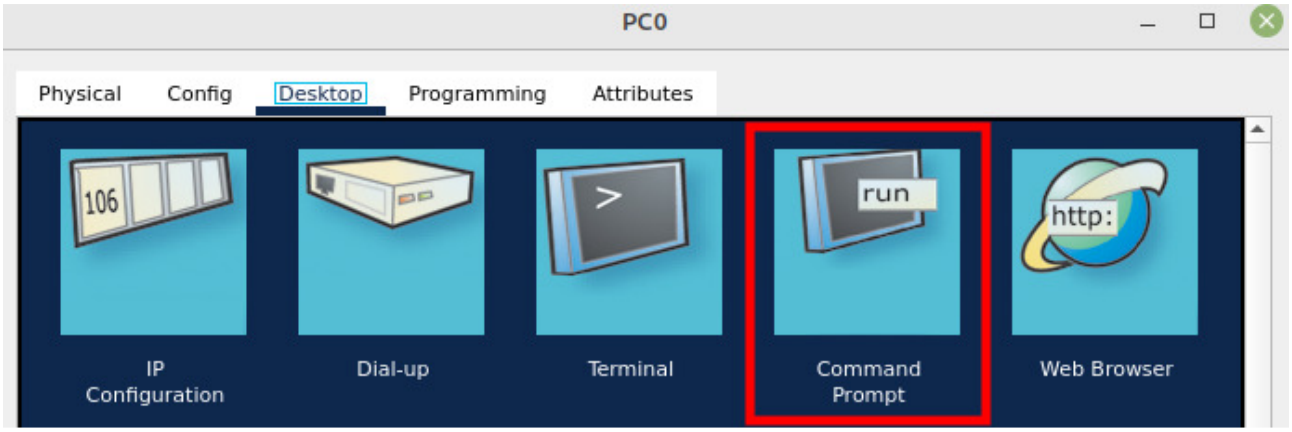

Рисунок 2.6 – Меню додатків моделі робочої станції

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).

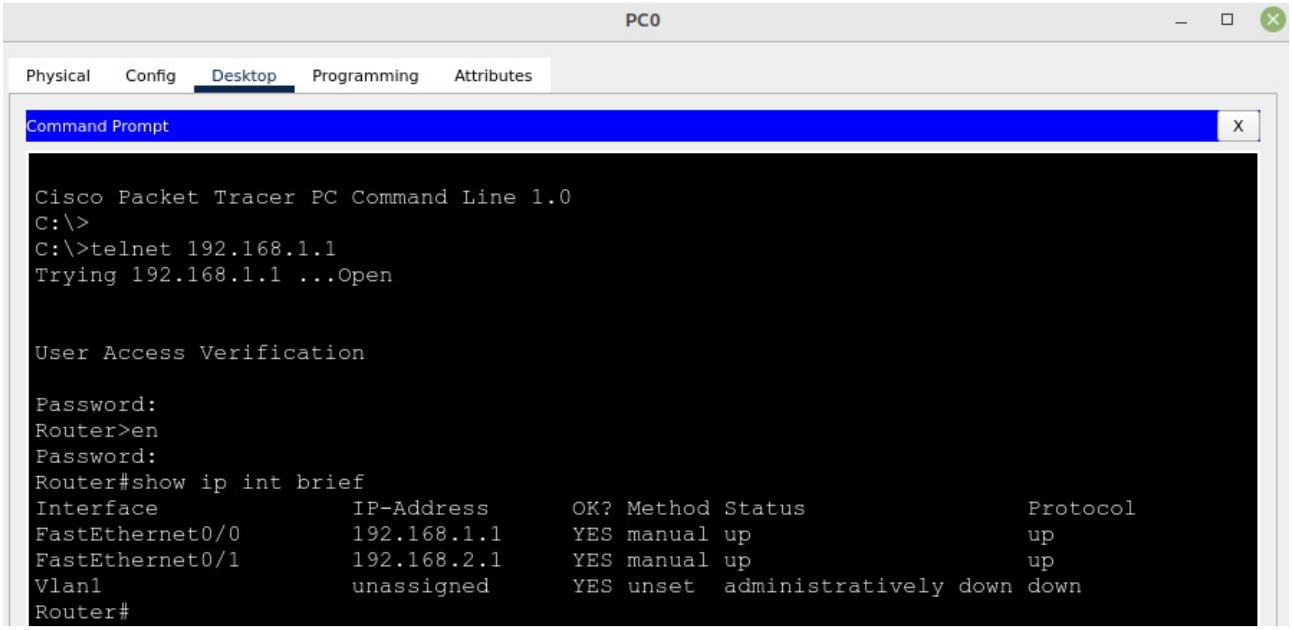

Рисунок 2.7 – Підключення до маршрутизатора через Telnet з PC

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#
```

3.6. 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.

Переходим в режим глобальной конфигурации

```
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#
```

4 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

Лабораторна робота № 3

Тема: Сегментація мереж з використанням VLAN

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

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Принципи побудови VLAN з тегуванням трафіку

Сучасні корпоративні мережі складаються з великої кількості пристроїв, які потребують різних рівнів доступу до мережевих ресурсів та безпеки. Без належної сегментації всі пристрої знаходяться в одному широкомовному домені, що створює проблеми з продуктивністю мережі через надмірний широкомовний трафік та ускладнює забезпечення безпеки. Традиційна сегментація за допомогою окремих фізичних комутаторів для кожного відділу є неефективною з економічної точки зору та складною в управлінні. VLAN (Virtual Local Area Network) вирішує ці проблеми шляхом створення логічних сегментів мережі на рівні комутаторів без необхідності фізичного розділення пристроїв. Використання VLAN дозволяє адміністраторам мережі створювати віртуальні робочі групи, які можуть включати пристрої, підключені до різних комутаторів та розташовані в різних географічних точках.

Кожна VLAN функціонує як окрема підмережа з власним широкомовним доменом, що зменшує навантаження на мережу та покращує її продуктивність. Важливою перевагою VLAN є можливість легкої реконфігурації мережі програмно, без фізичного переміщення кабелів або зміни топології мережі. Це особливо актуально для динамічних організацій, де співробітники часто змінюють робочі місця або переходять між проектними групами. Додатково, VLAN забезпечують підвищений рівень безпеки за рахунок ізоляції трафіку різних відділів та можливості застосування різних політик безпеки для кожної віртуальної мережі.

VLAN представляють собою логічні групи пристроїв, які функціонують як окремі мережі незалежно від їх фізичного розташування. Основою функціонування VLAN є механізм тегування кадрів Ethernet, який дозволяє комутаторам ідентифікувати приналежність трафіку до конкретної віртуальної мережі. Стандарт IEEE 802.1Q визначає структуру цих міток та правила їх обробки комутаторами, забезпечуючи сумісність обладнання різних виробників. Тегування може здійснюватися як самими кінцевими пристроями, які підтримують VLAN, так і комутаторами доступу при отриманні нетегованого трафіку від звичайних пристроїв. Цей механізм дозволяє передавати трафік декількох VLAN по одному фізичному з’єднанню, що значно підвищує ефективність використання мережевої інфраструктури.

Ідентифікація VLAN здійснюється за допомогою унікального номеру - VLAN ID, який може мати значення від 1 до 4094. Деякі значення зарезервовані для спеціальних цілей: VLAN 1 за замовчуванням призначена для управління

мережею, а VLAN 4095 зарезервована системою. Кожен комутатор підтримує базу даних VLAN (VLAN database), в якій зберігається інформація про створені віртуальні мережі, їх назви та налаштування. При проходженні кадру через комутатор система аналізує VLAN тег та приймає рішення про подальшу обробку кадру відповідно до конфігурації портів та таблиці комутації для відповідної VLAN.

Структура кадру Ethernet з VLAN тегом представлена на рисунку 3.1. Тег VLAN розміщується між полями Source Address та Type/Length оригінального кадру Ethernet та складається з двох частин: Tag Protocol Identifier (TPID) розміром 2 байти зі значенням 0x8100, що ідентифікує наявність VLAN тегу, та Tag Control Information (TCI) також розміром 2 байти. Поле TCI містить Priority Code Point (PCP) розміром 3 біти для визначення пріоритету кадру, Drop Eligible Indicator (DEI) розміром 1 біт для позначення можливості відкидання кадру при перевантаженні, та VLAN Identifier (VID) розміром 12 біт, що дозволяє створювати до 4094 унікальних VLAN. Додавання VLAN тегу збільшує розмір кадру на 4 байти, що може вплинути на максимальний розмір кадру (MTU) в мережі.

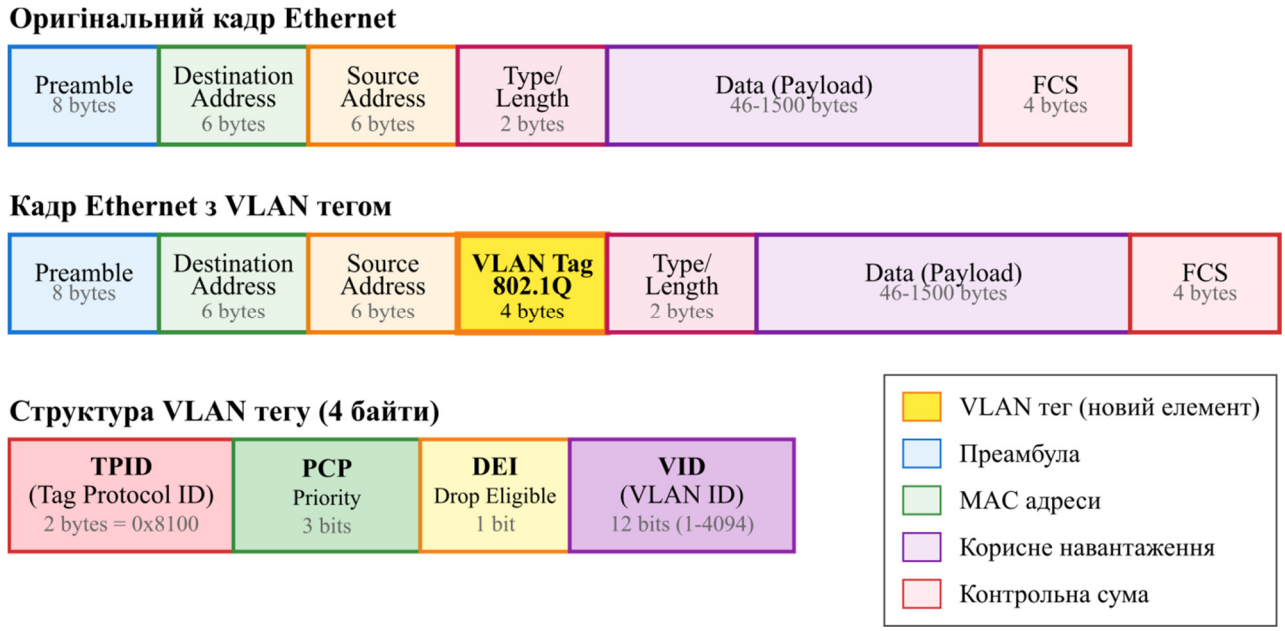

Рисунок 3.1 – Структура кадру Ethernet з VLAN тегом

Комутатори використовують два основні типи портів для роботи з VLAN: access порти та trunk порти, кожен з яких має специфічне призначення та принципи функціонування. Access порти призначені для підключення кінцевих пристроїв (комп'ютерів, принтерів, телефонів) і передають трафік лише одного VLAN без тегів у напрямку до кінцевого пристрою. Коли кінцевий пристрій надсилає нетегований кадр на access порт, комутатор автоматично додає відповідний VLAN тег відповідно до конфігурації порту. При передачі кадру з комутатора до кінцевого пристрою через access порт тег автоматично видаляється, оскільки більшість кінцевих пристроїв не розуміють тегований трафік.

Trunk порти призначені для з'єднання комутаторів між собою або для підключення серверів та маршрутизаторів, які підтримують роботу з множинними VLAN. Ці порти передають тегований трафік декількох VLAN одночасно, зберігаючи теги при проходженні кадрів. Це дозволяє віддаленому пристрою правильно ідентифікувати приналежність трафіку до конкретної VLAN та обробити його відповідним чином. На trunk портах можна налаштувати список дозволених VLAN для підвищення безпеки та контролю трафіку. Також існує поняття native VLAN - це VLAN, трафік якої передається через trunk порт без тегів, що забезпечує сумісність із застарілим обладнанням.

1.2 Технічні характеристики та призначення комутаторів Cisco

Компанія Cisco Systems пропонує широку лінійку комутаторів, організованих у серії відповідно до їх функціонального призначення та технічних можливостей. Серія Catalyst включає комутатори для всіх рівнів корпоративної мережі: від простих неуправляємих моделей для малого бізнесу до високопродуктивних модульних систем для центрів обробки даних. Кожна серія оптимізована для конкретних завдань та характеризується певним набором функцій, портфелем протоколів та рівнем продуктивності. Нумерація моделей у Cisco Catalyst відображає покоління технології та функціональні можливості: чим вищий номер серії, тим більше сучасних функцій підтримує обладнання. Розуміння позиціонування різних серій комутаторів є критично важливим для правильного проектування мережевої архітектури підприємства.

Комутатор Cisco Catalyst 2960 серії позиціонується як рішення для рівня доступу (Access Layer) в ієрархічній моделі корпоративної мережі та призначений для безпосереднього підключення кінцевих пристроїв користувачів. Модель WS-C2960-24TT-L представляє собою некерований комутатор другого рівня, який забезпечує основні функції комутації Ethernet та підтримку VLAN без можливості виконання маршрутизації IP трафіку. Цей комутатор оптимізований для середовища офісних мереж, де потрібна надійна та економічно ефективна комутація для підключення робочих станцій, принтерів та іншого периферійного обладнання. Серія 2960 характеризується простотою налаштування, енергоефективністю та підтримкою базових функцій безпеки мережі.

Комутатор Cisco Catalyst 3560 серії є багаторівневим пристроєм, який може функціонувати як на рівні доступу, так і на рівні розподілу (Distribution Layer) корпоративної мережі. Модель 3560-24PS підтримує як функції комутації другого рівня, так і маршрутизації третього рівня моделі OSI, що робить його ідеальним вибором для ролі центрального комутатора (Core Switch) у невеликих та середніх мережах. Додатковою перевагою цієї моделі є вбудована підтримка Power over Ethernet (PoE), що дозволяє живити підключені пристрої безпосередньо через мережевий кабель. Це особливо корисно для підключення IP телефонів, точок доступу Wi-Fi та камер відеоспостереження без необхідності прокладання окремих кабелів живлення.

Детальні технічні характеристики цих комутаторів наведені в таблиці 3.1. Основною функціональною відмінністю між цими моделями є підтримка Layer 3 функцій комутатором 3560-24PS, що дозволяє йому виконувати міжVLAN маршрутизацію без використання зовнішнього маршрутизатора. Це суттєво спрощує топологію мережі та зменшує загальну вартість володіння системою.

Таблиця 3.1 – Технічні характеристики комутаторів

Характеристика	**Cisco WS-C2960-24TT-L**	**Cisco 3560-24PS**
Призначення	Access Layer Switch	Distribution/Core Layer Switch
Кількість портів FastEthernet	24 x 10/100 Mbps	24 x 10/100 Mbps
Кількість портів GigabitEthernet	2 x 1000 Mbps (SFP)	2 x 1000 Mbps + 2 SFP
Підтримка Layer 2	Так	Так
Підтримка Layer 3 (маршрутизація)	Ні	Так
Підтримка PoE	Ні	Так (до 15.4W на порт)
Максимальна кількість VLAN	255	1005
Підтримка SVI інтерфейсів	Тільки VLAN 1	Всі VLAN
Комутаційна здатність	8.8 Gbps	32 Gbps
Розмір таблиці MAC адрес	8K	12K

1.3 SVI інтерфейси та принципи міжVLAN маршрутизації

Switched Virtual Interface (SVI) представляє собою ключову технологію, яка забезпечує взаємодію між віртуальними локальними мережами на багаторівневих комутаторах. SVI є віртуальним інтерфейсом третього рівня моделі OSI, який існує програмно в операційній системі комутатора та не має фізичного еквівалента у вигляді порту або роз’єму. Кожен SVI інтерфейс асоціюється з конкретною VLAN і функціонує як IP шлюз для всіх пристроїв, підключених до цієї віртуальної мережі. Номер VLAN та відповідного SVI інтерфейсу завжди співпадають: для VLAN 10 створюється інтерфейс vlan 10, для VLAN 20 створюється інтерфейс vlan 20, і так далі. Цей прямий зв’язок забезпечує логічну структуру конфігурації та спрощує адміністрування мережі.

Основне призначення SVI інтерфейсів полягає в забезпеченні IP зв’язності між різними VLAN без необхідності використання зовнішнього маршрутизатора. Традиційно, для організації взаємодії між VLAN потрібен був окремий маршрутизатор з фізичними підінтерфейсами для кожної віртуальної мережі. SVI технологія дозволяє виконувати цю функцію безпосередньо на комутаторі, що значно спрощує топологію мережі та знижує затримки при передачі даних між VLAN. Коли комутатор отримує пакет, призначений для іншої підмережі, він використовує свою таблицю маршрутизації для визначення оптимального шляху та SVI інтерфейс для подальшої передачі пакету. Це відбувається на апаратному рівні сучасних комутаторів, забезпечуючи швидкість комутації, близьку до швидкості обробки трафіку другого рівня.

Функціонування SVI інтерфейсів базується на принципах класичної IP маршрутизації, але адаптованих для роботи в середовищі комутатора. Коли пристрій у певній VLAN потребує передати дані в іншу VLAN або зовнішню мережу, він відправляє пакет на MAC адресу свого шлюзу за замовчуванням, якою є MAC адреса SVI інтерфейсу його VLAN. Комутатор отримує цей Ethernet кадр через один з access портів, ідентифікує його приналежність до VLAN за налаштуваннями порту або наявним тегом, та передає кадр на обробку відповідному SVI інтерфейсу. SVI виконує декапсуляцію Ethernet кадру, отримує IP пакет та аналізує IP адресу призначення. На основі таблиці маршрутизації комутатора приймається рішення про подальшу передачу пакету: якщо адреса призначення належить іншій VLAN в тому ж комутаторі, пакет передається на відповідний SVI інтерфейс цільової VLAN.

Важливою особливістю роботи SVI інтерфейсів є їх стан активності, який залежить від наявності активних портів у відповідній VLAN. SVI інтерфейс переходить у стан “up” тільки тоді, коли в асоційованій з ним VLAN є хоча б один активний порт (access або trunk), що знаходиться в стані “forwarding”. Якщо всі порти VLAN стають неактивними, SVI автоматично переходить у стан “down”, що впливає на доступність відповідної підмережі. Ця поведінка забезпечує автоматичне відключення недоступних мережних сегментів та запобігає появі неправильних записів у таблицях маршрутизації. Адміністратори можуть контролювати цю поведінку за допомогою додаткових команд конфігурації, якщо потрібна інша логіка роботи SVI.

Процес створення та налаштування SVI інтерфейсів потребує виконання кількох обов’язкових кроків на багаторівневому комутаторі. Спочатку необхідно ввімкнути функцію IP маршрутизації командою “ip routing” в режимі глобальної конфігурації, оскільки за замовчуванням більшість комутаторів працюють тільки як пристрої другого рівня. Після цього створюється відповідна VLAN у базі даних комутатора, якщо вона ще не існує. Далі створюється SVI інтерфейс командою “interface vlan [номер]”, призначається IP адреса та маска підмережі, і обов’язково виконується команда “no shutdown” для активації інтерфейсу. IP адреса, призначена SVI інтерфейсу, автоматично стає адресою шлюзу за замовчуванням для всіх пристроїв у відповідній VLAN.

Рисунок 3.2 ілюструє детальний процес міжVLAN маршрутизації через SVI інтерфейси в практичному сценарії. На схемі зображено багаторівневий комутатор з трьома VLAN (10, 20, 30) та відповідними SVI інтерфейсами з IP адресами 192.168.10.1/24, 192.168.20.1/24 та 192.168.30.1/24. Коли комп’ютер PC1 з VLAN 10 (IP адреса 192.168.10.10) намагається відправити дані комп’ютеру PC3 з VLAN 20 (IP адреса 192.168.20.10), відбувається наступна послідовність дій: PC1 визначає, що цільова адреса знаходиться в іншій підмережі, та відправляє Ethernet кадр на MAC адресу свого шлюзу (SVI vlan 10). Комутатор отримує кадр через access порт VLAN 10, передає його SVI інтерфейсу vlan 10, який виконує маршрутизацію до підмережі 192.168.20.0/24 через SVI інтерфейс vlan 20. Нарешті, SVI vlan 20 формує новий Ethernet кадр та передає його до PC3 через відповідний access порт VLAN 20.

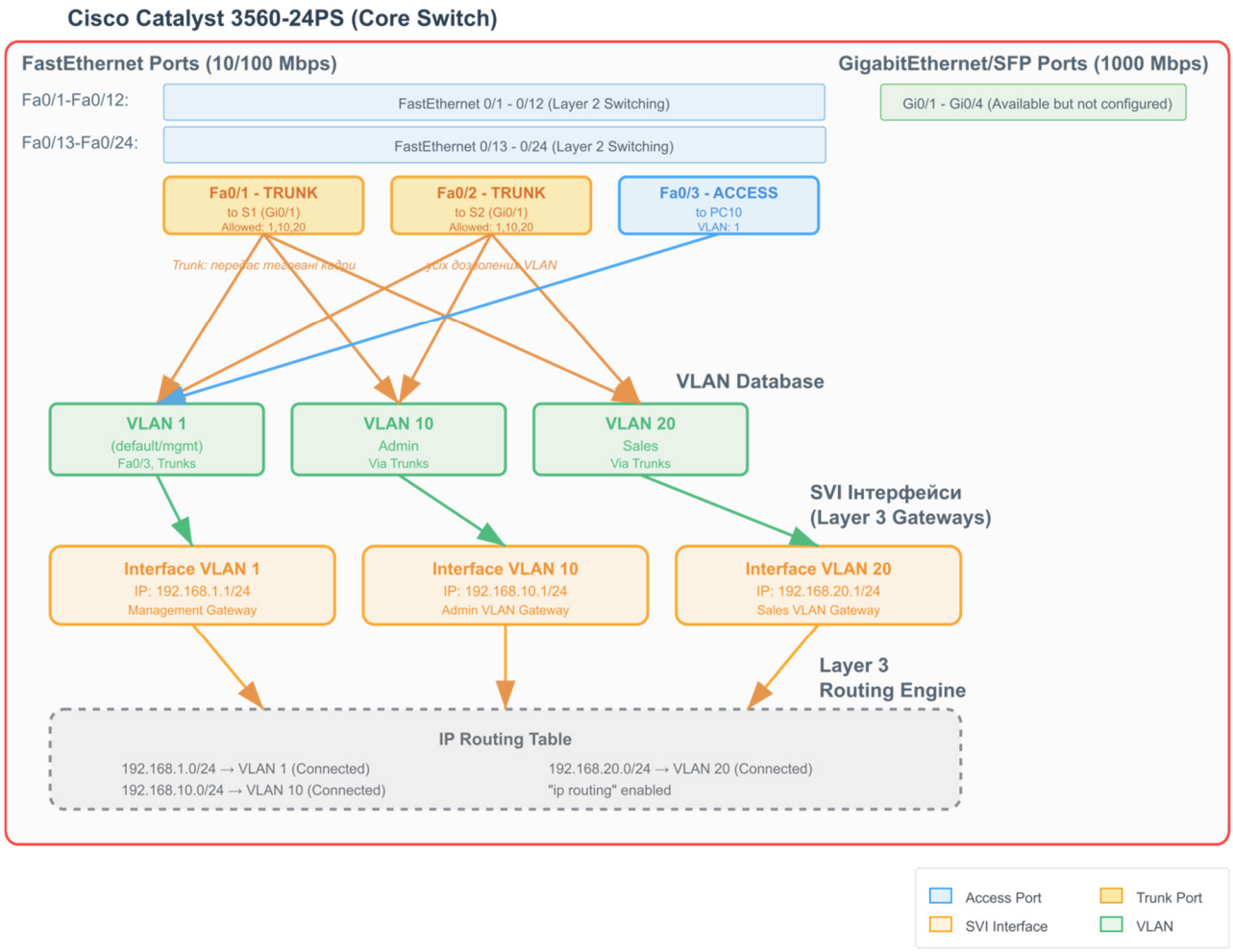

Рисунок 3.2 – Схема міжVLAN маршрутизації через SVI інтерфейси

1.4 Команди Cisco IOS для конфігурації VLAN та комутаторів

Управління комутаторами Cisco здійснюється через потужний інтерфейс командного рядка Cisco IOS (Internetwork Operating System), який надає повний контроль над всіма функціями пристрою та забезпечує високий рівень гнучкості конфігурації. Команди IOS організовані в ієрархічну структуру режимів конфігурації, де кожен режим дозволяє виконувати певний набір операцій з відповідними правами доступу. Основними режимами роботи є User EXEC (позначається символом >), який надає обмежений доступ до команд перегляду інформації, Privileged EXEC (позначається #) для виконання діагностичних команд та перегляду конфігурації, Global Configuration (позначається (config)#) для внесення змін у глобальні налаштування системи, та спеціалізовані режими конфігурації інтерфейсів, протоколів та сервісів. Розуміння структури цих режимів та правил переходу між ними є fundamental для ефективної роботи з обладнанням Cisco.

Таблиця 3.2 систематизує основні команди Cisco IOS, які використовуються для конфігурації VLAN, налаштування портів комутаторів та моніторингу стану мережі. Команди згруповані за функціональним призначенням для полегшення вивчення та практичного застосування, кожна команда супроводжується конкретним прикладом використання та поясненням

результату виконання. Ця систематизація допомагає студентам швидко знаходити потрібні команди для вирішення конкретних завдань конфігурації мережі.

Таблиця 3.2 – Команди Cisco IOS для роботи з VLAN та комутаторами

Категорія	Команда	Приклад використання	Призначення
Режими роботи	enable	Switch> enable	Перехід в привілейований режим
	configure terminal	Switch# conf t	Вхід в режим глобальної конфігурації
	exit	Switch(config)# exit	Повернення в попередній режим
	end	Switch(config-if)# end	Повернення в привілейований режим
Створення VLAN	vlan [номер]	vlan 10	Створення нової VLAN з номером 10
	name [назва]	name Admin	Призначення імені “Admin” для поточної VLAN
	show vlan brief	show vlan brief	Перегляд списку всіх VLAN
Налаштування access портів	interface [тип порту]	int fa0/1	Вхід в режим конфігурації порту FastEthernet 0/1
	switchport mode access	switchport mode access	Налаштування порту як access (для кінцевих пристроїв)
	switchport access vlan [номер]	switchport access vlan 10	Призначення access порту до VLAN 10
	interface range [діапазон]	int range fa0/1-4	Одночасне налаштування портів 1-4
Налаштування trunk портів	switchport mode trunk	switchport mode trunk	Налаштування порту як trunk (між комутаторами)
	switchport trunk encapsulation dot1q	switchport trunk encapsulation dot1q	Встановлення інкапсуляції 802.1Q
	switchport trunk allowed vlan [список]	switchport trunk allowed vlan 1,10,20	Дозвіл передачі VLAN 1, 10, 20 через trunk
	switchport trunk native vlan [номер]	switchport trunk native vlan 99	Встановлення native VLAN 99 для trunk
SVI інтерфейси	interface vlan [номер]	int vlan 10	Створення SVI інтерфейсу для VLAN 10

Категорія	Команда	Приклад використання	Призначення
	ip address [IP] [маска]	ip address 192.168.10.1 255.255.255.0	Призначення IP адреси SVI інтерфейсу
	no shutdown	no shutdown	Активація інтерфейсу
	shutdown	shutdown	Деактивація інтерфейсу
Маршрутизація	ip routing	ip routing	Ввімкнення функції маршрутизації Layer 3
	ip default-gateway [IP]	ip default-gateway 192.168.1.1	Встановлення шлюзу для комутатора Layer 2
	show ip route	show ip route	Перегляд таблиці маршрутизації
Моніторинг та діагностика	show interfaces	show int	Детальна інформація про всі інтерфейси
	show interfaces switchport	show int switchport	Стан switchport налаштувань усіх портів
	show ip interface brief	show ip int brief	Короткий статус всіх IP інтерфейсів
	show running-config	show run	Поточна активна конфігурація
	show startup-config	show start	Збережена конфігурація
	show mac address-table	show mac address-table	Таблиця MAC адрес комутатора

1.4 Практичні приклади конфігурації комутаторів для роботи з VLAN

Розглянемо практичні приклади типових сценаріїв конфігурації комутаторів, які найчастіше зустрічаються при налаштуванні корпоративних мереж з використанням технології VLAN. Ці приклади демонструють покрокові інструкції з поясненням логіки кожної команди та очікуваних результатів.

Приклад 1. Створення VLAN та базове налаштування.

Припустимо, що потрібно створити дві VLAN для відділів компанії: VLAN 10 для відділу адміністрації та VLAN 20 для відділу продажів.

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Administration
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name Sales
```

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

У цьому прикладі спочатку відбувається перехід у привілейований режим, потім у режим глобальної конфігурації. Команда vlan 10 створює нову VLAN з номером 10 і переводить систему в режим конфігурації VLAN. Команда name Administration присвоює VLAN описову назву для спрощення адміністрування. Аналогічно створюється VLAN 20. Команда show vlan brief дозволяє перевірити успішність створення VLAN та переглянути їх стан.

Приклад 2. Налаштування access портів для кінцевих пристроїв.

Налаштуємо порти FastEthernet 0/1-0/8 як access порти: порти 1-4 для VLAN 10 (адміністрація), порти 5-8 для VLAN 20 (продажі).

```
Switch# configure terminal
Switch(config)# interface range fastEthernet 0/1 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# description Admin Department PCs
Switch(config-if-range)# exit
Switch(config)# interface range fastEthernet 0/5 - 8
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# description Sales Department PCs
Switch(config-if-range)# exit
```

Команда interface range дозволяє одночасно налаштувати кілька послідовних портів, що значно прискорює процес конфігурації. switchport mode access явно встановлює режим access, що означає передачу трафіку тільки одної VLAN без тегів. switchport access vlan 10 призначає порти до конкретної VLAN. Команда description додає текстовий опис, який допомагає в майбутньому адмініструванні мережі.

Приклад 3. Конфігурація trunk порту для з'єднання комутаторів.

Налаштуємо порт GigabitEthernet 0/1 як trunk для передачі трафіку кількох VLAN між комутаторами.

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1,10,20,30
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# description Trunk to Core Switch
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

У цьому прикладі switchport trunk encapsulation dot1q встановлює стандарт IEEE 802.1Q для тегування кадрів. switchport mode trunk активує режим trunk. Команда switchport trunk allowed vlan явно вказує, які VLAN можуть передаватися цим портом, що підвищує безпеку. switchport trunk native vlan 99 встановлює VLAN 99 як native (трафік цієї VLAN передається без тегів),

що є кращою практикою безпеки. no shutdown гарантує, що інтерфейс активний.

Приклад 4. Створення SVI інтерфейсів для міжVLAN маршрутизації.

На багаторівневому комутаторі (наприклад, Cisco 3560) налаштуємо SVI інтерфейси для забезпечення зв'язку між VLAN 10 та VLAN 20.

```
Switch# configure terminal
Switch(config)# ip routing
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)#  description  Gateway  for  Administration
VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# description Gateway for Sales VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# description Management Interface
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Команда ip routing є критично важливою - вона вмикає функцію маршрутизації Layer 3 на комутаторі. Без неї SVI інтерфейси не зможуть маршрутизувати трафік між VLAN. Кожен SVI отримує IP адресу, яка стає шлюзом за замовчуванням для пристроїв у відповідній VLAN. Наприклад, всі комп'ютери в VLAN 10 повинні мати налаштування шлюзу 192.168.10.1. Команда no shutdown обов'язкова для активації віртуального інтерфейсу.

Приклад 5. Налаштування порту для управління мережею.

Створимо окремий порт для підключення адміністративної робочої станції до VLAN управління.

```
Switch# configure terminal
Switch(config)# vlan 99
Switch(config-vlan)# name Management
Switch(config-vlan)# exit
Switch(config)# interface fastEthernet 0/24
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 99
Switch(config-if)# description Admin Workstation
Switch(config-if)# spanning-tree portfast
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan 99
Switch(config-if)# ip address 192.168.99.1 255.255.255.0
Switch(config-if)# description Management Network Gateway
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

У цьому прикладі створюється окрема VLAN 99 для управління, що є кращою практикою безпеки. Порт FastEthernet 0/24 налаштовується для підключення адміністративної станції. Команда spanning-tree portfast прискорює перехід порту в стан forwarding, оскільки до нього підключений кінцевий пристрій, а не інший комутатор. SVI інтерфейс для VLAN 99 забезпечує IP зв'язність для адміністрування.

Приклад 6. Перевірка та діагностика конфігурації VLAN.

Після налаштування важливо перевірити правильність конфігурації за допомогою діагностичних команд.

```
Switch# show vlan brief
Switch# show interfaces switchport
Switch# show ip interface brief
Switch# show running-config interface vlan 10
Switch# show mac address-table vlan 10
Switch# show spanning-tree vlan 10
```

Команда show vlan brief відображає список усіх VLAN та порти, призначені до них. show interfaces switchport показує детальну інформацію про налаштування switchport для всіх портів. show ip interface brief дає огляд стану всіх IP інтерфейсів, включаючи SVI. show running-config interface vlan 10 показує поточну конфігурацію конкретного SVI інтерфейсу. show mac address-table vlan 10 відображає MAC адреси, вивчені в конкретній VLAN. show spanning-tree vlan 10 показує стан протоколу Spanning Tree для VLAN.

Приклад 7. Налаштування безпеки VLAN

Реалізуємо базові заходи безпеки для VLAN конфігурації.

```
Switch# configure terminal
Switch(config)# vlan 999
Switch(config-vlan)# name Unused_Ports
Switch(config-vlan)# exit
Switch(config)# interface range fastEthernet 0/9 - 23
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 999
Switch(config-if-range)# shutdown
Switch(config-if-range)# description Unused - Security
Switch(config-if-range)# exit
Switch(config)# interface range gigabitEthernet 0/1 - 2
Switch(config-if-range)# switchport trunk allowed vlan remove
999
Switch(config-if-range)# exit
```

Цей приклад демонструє створення "чорної діри" VLAN 999 для невикористовуваних портів. Усі порти, які не використовуються, призначаються до цієї VLAN та відключаються командою shutdown. Це запобігає несанкціонованому доступу через невикористовувані порти. Команда switchport trunk allowed vlan remove 999 гарантує, що VLAN 999 не передається через trunk порти, додатково ізолюючи потенційно скомпрометовані порти.

2 КЛЮЧОВІ ПИТАННЯ

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 між-VLAN 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?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1 Створення моделі мережі в Cisco Packet Tracer

У цій лабораторній роботі студенти створюють 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. 3.3). 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.

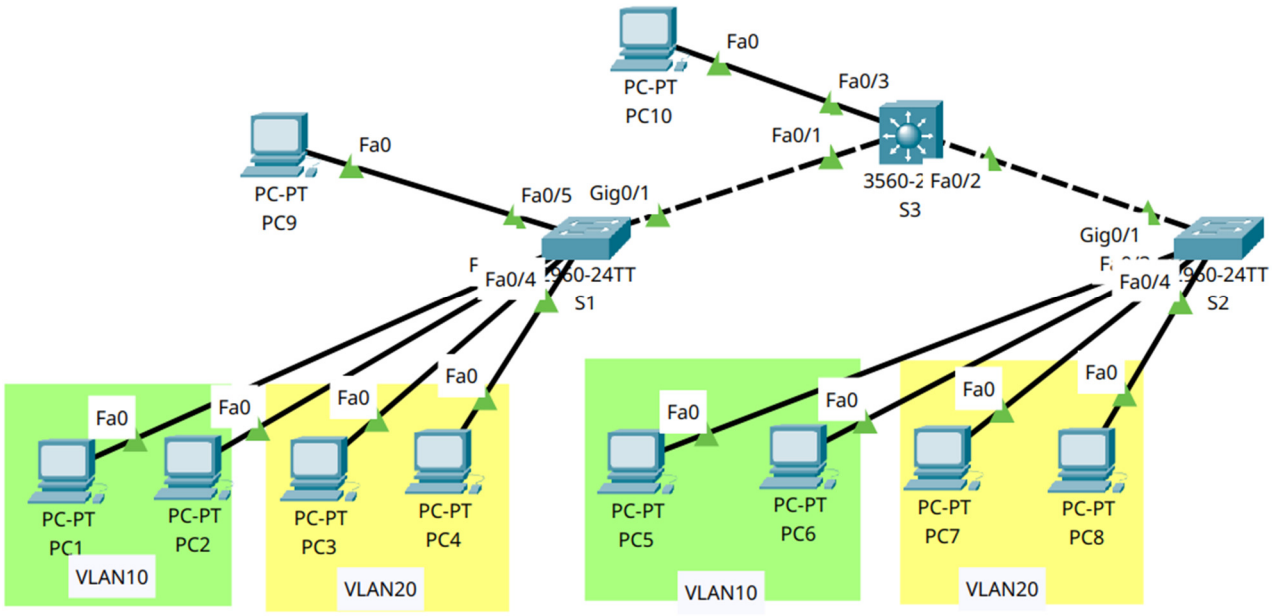

Рисунок 3.3 – Архітектура мережі звязку з використанням комутаторів L2 та L3

Кожен студент отримує індивідуальний варіант завдання, який визначає номери двох VLAN, що використовуються для сегментації користувацьких робочих станцій PC1-PC8 (табл. 3.3 та 3.4). 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 3.3 – 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)	S2	FastEthernet0/1
PC4	FastEthernet0	Прямий (Copper Straight-Through)	S2	FastEthernet0/2
PC5	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/3
PC6	FastEthernet0	Прямий (Copper Straight-Through)	S1	FastEthernet0/4
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 3.4 – 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

№	VLAN A (НОМЕР)	РОБОЧІ СТАНЦІЇ У VLAN A	VLAN B (НОМЕР)	РОБОЧІ СТАНЦІЇ У VLAN B
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

3.2 Налаштування комутатора доступу S1

3.2.1 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)#
```

3.2.2 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)#
```

3.2.3 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)#
```

3.3 Налаштування комутатора доступу S2

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

3.3.1 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)#
```

3.3.2 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)#
```

3.3.3 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 Налаштування багаторівневого комутатора Core (Cisco 3560-24PS)

3.4.1 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)#
```

3.4.2 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)#
```

3.4.3 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 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)#
```

3.4.5 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)#
```

3.4.6 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)#
```

3.5 Налаштування робочих станцій (PC)

Налаштуйте всі робочі станції з врахуванням підмереж (номерів VLAN) в таблиці 1. 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 3.5 – 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

3.6 Тестування моделі мережі

3.6.1 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.

3.6.2 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.

3.6.3 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.

3.6.4 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.

4 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

Лабораторна робота № 4

Тема: Вивчення принципів сегментації мережі за допомогою технології VLSM

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

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Основи IP-адресації та адресний простір

Сучасні комп’ютерні мережі базуються на принципах багаторівневої архітектури, де кожен рівень виконує специфічні функції забезпечення надійної передачі даних між пристроями. Ця архітектура, відома як модель OSI (Open Systems Interconnection), складається з семи рівнів: фізичного, канального, мережевого, транспортного, сеансового, представлення та прикладного. Кожен рівень інкапсулює дані попереднього рівня, додаючи власні заголовки з керуючою інформацією, що забезпечує модульність та незалежність функціонування окремих компонентів мережевої системи. Такий підхід дозволяє розробляти, модернізувати та обслуговувати мережеві протоколи незалежно один від одного, забезпечуючи сумісність обладнання різних виробників та гнучкість у виборі технологічних рішень.

Основою функціонування глобальних та локальних мереж є протокол IP (Internet Protocol), який відповідає за логічну адресацію пристроїв та маршрутизацію пакетів у складних мережевих топологіях. IP протокол функціонує на третьому (мережевому) рівні моделі OSI і забезпечує доставку дейтаграм (пакетів даних) від джерела до призначення через мережі з різною фізичною архітектурою. Протокол IP є протоколом без встановлення з’єднання (connectionless), що означає відсутність попереднього встановлення логічного каналу між відправником та отримувачем. Кожен IP-пакет обробляється незалежно та містить повну адресну інформацію, необхідну для доставки до пункту призначення. Цей механізм забезпечує високу надійність мережі, оскільки вихід з ладу окремих маршрутизаторів не призводить до повної втрати зв’язності, а альтернативні маршрути автоматично використовуються для доставки пакетів.

Структура IP-пакета включає заголовок фіксованої довжини (20 байт для IPv4) та змінну частину даних. Заголовок містить критично важливі поля: версію протоколу (4 біти), довжину заголовка (4 біти), тип сервісу (8 біт), загальну довжину пакета (16 біт), ідентифікатор фрагмента (16 біт), прапорці фрагментації (3 біти), зсув фрагмента (13 біт), час життя або TTL (8 біт), протокол наступного рівня (8 біт), контрольну суму заголовка (16 біт), адресу джерела (32 біти) та адресу призначення (32 біти). Поле TTL (Time To Live) виконує критично важливу функцію запобігання циклічній маршрутизації пакетів, автоматично зменшуючись на одиницю при проходженні кожного

маршрутизатора і призводячи до знищення пакета при досягненні нульового значення.

Механізм фрагментації дозволяє IP протоколу адаптуватися до різних значень MTU (Maximum Transmission Unit) в гетерогенних мережах. Коли пакет перевищує максимально допустимий розмір кадру на певному сегменті мережі, маршрутизатор розбиває його на менші фрагменти, кожен з яких отримує унікальний ідентифікатор та інформацію про своє положення в оригінальному пакеті. Збирання фрагментів відбувається виключно на кінцевому пристрої призначення, що зменшує навантаження на проміжні маршрутизатори, але створює додаткові вимоги до буферної пам’яті та процесорних ресурсів кінцевих станцій.

IP-адреса являє собою унікальний 32-бітний ідентифікатор пристрою в мережі, який записується у десятковому форматі через крапку у вигляді чотирьох октетів, кожен з яких може мати значення від 0 до 255. Ця система запису, відома як десяткова нотація з крапками (dotted decimal notation), була введена для спрощення сприйняття людиною двійкових адрес та зменшення ймовірності помилок при конфігуруванні мережевого обладнання. Загальний адресний простір IPv4 становить 2^32 = 4,294,967,296 унікальних адрес, що на момент розробки протоколу в 1980-х роках здавалося достатнім для покриття всіх потреб глобальної мережі. Однак стрімкий розвиток Інтернету та збільшення кількості підключених пристроїв призвело до вичерпання адресного простору, що стимулювало розробку технологій NAT (Network Address Translation) та нового протоколу IPv6.

Структура IP-адреси складається з двох основних частин: мережевої частини (Network ID), що ідентифікує конкретну мережу або підмережу, та хостової частини (Host ID), яка визначає конкретний пристрій в межах цієї мережі. Розмежування між цими частинами здійснюється за допомогою маски підмережі, яка також записується у 32-бітному форматі і визначає, які біти IP-адреси відносяться до мережевої частини, а які до хостової. Маска підмережі складається з послідовних одиничних біт (мережева частина) та послідовних нульових біт (хостова частина), що забезпечує чітке розмежування адресних компонентів. Операція логічного множення (AND) між IP-адресою та маскою підмережі дає адресу мережі, а інверсія маски визначає діапазон можливих хостових адрес у межах конкретної мережі.

Маска підмережі може бути представлена у трьох основних форматах: десятковому (наприклад, 255.255.255.0), двійковому (11111111.11111111.11111111.00000000) та префіксному записі CIDR (наприклад, /24), де число після косої риски вказує кількість біт мережевої частини. Префіксна нотація CIDR (Classless Inter-Domain Routing) стала стандартною для сучасних мережевих технологій, оскільки вона компактна, зрозуміла та підтримується всіма сучасними протоколами маршрутизації. Використання CIDR дозволяє більш гнучко планувати адресний простір, створювати супермережі (супернети) та ефективно агрегувати маршрутну інформацію в таблицях маршрутизації.

Класична система IP-адресації, розроблена в 1980-х роках, передбачає поділ адресного простору на п’ять основних класів (A, B, C, D, E), три з яких (A, B, C) призначені для адресації хостів, один (D) для багатоадресної розсилки (multicast), а останній (E) зарезервований для експериментальних цілей. У таблиці 4.1 наведено детальні характеристики класів IP-адрес з їхніми діапазонами та можливостями.

Таблиця 4.1 – Класи IP-адрес та їхні характеристики

Клас	Діапазон адрес	Маска за замовчуванням	Префікс CIDR	Кількість мереж	Кількість хостів	Перші біти
A	1.0.0.0 - 126.255.255.255	255.0.0.0	/8	126	16,777,214	0
B	128.0.0.0 - 191.255.255.255	255.255.0.0	/16	16,384	65,534	10
C	192.0.0.0 - 223.255.255.255	255.255.255.0	/24	2,097,152	254	110
D	224.0.0.0 - 239.255.255.255	-	-	Multicast	-	1110
E	240.0.0.0 - 255.255.255.255	-	-	Зарезервований	-	1111

Клас A призначений для великих мережевих структур з невеликою кількістю мереж, але великою кількістю хостів у кожній мережі. Перший біт адрес класу A завжди дорівнює 0, що дозволяет автоматично визначити клас за першим октетом. Діапазон 127.0.0.0/8 (127.0.0.1 - 127.255.255.255) зарезервований для адрес зворотного зв’язку (loopback), найбільш відомою з яких є 127.0.0.1 (localhost). Мережі класу A використовуються переважно великими корпораціями та інтернет-провайдерами, оскільки забезпечують можливість адресації понад 16 мільйонів пристроїв у межах однієї мережі. Адреси класу A вважаються найбільш цінними в глобальному адресному просторі через свою універсальність та великий діапазон хостів.

Клас B забезпечує баланс між кількістю мереж та хостів, підходячи для середніх організацій з кількістю пристроїв від кількох сотень до кількох десятків тисяч. Перші два біти адрес класу B завжди мають значення 10, що відповідає діапазону 128-191 у першому октеті. Мережі класу B широко використовуються університетами, великими підприємствами та регіональними інтернет-провайдерами. Стандартна маска 255.255.0.0 дозволяє створювати гнучкі схеми підмережування з використанням третього та четвертого октетів для внутрішнього розподілу адрес.

Клас C орієнтований на невеликі мережі з обмеженою кількістю пристроїв, типові для малих офісів, домашніх мереж та філій великих організацій. Перші три біти адрес класу C мають значення 110, що відповідає діапазону 192-223 у першому октеті. Незважаючи на обмеження в 254 можливих хости, мережі класу C є найбільш численними в глобальному Інтернеті через простоту планування та адміністрування. Стандартна маска

255.255.255.0 залишає лише один октет для адресації хостів, що вимагає ретельного планування при розширенні мережі.

Особливо важливими є приватні IP-адреси, визначені стандартом RFC 1918 "Address Allocation for Private Internets", які використовуються в локальних мережах і не маршрутизуються в глобальному інтернеті. Приватний адресний простір включає три діапазони: 10.0.0.0/8 (10.0.0.0 - 10.255.255.255) для класу A з 16,777,216 адресами, 172.16.0.0/12 (172.16.0.0 - 172.31.255.255) для класу B з 1,048,576 адресами та 192.168.0.0/16 (192.168.0.0 - 192.168.255.255) для класу C з 65,536 адресами. Ці діапазони дозволяють організаціям створювати внутрішні мережі без необхідності отримання унікальних глобальних IP-адрес для кожного внутрішнього пристрою, що значно економить адресний простір Інтернету та забезпечує додатковий рівень безпеки через приховування внутрішньої структури мережі від зовнішніх користувачів.

Крім приватних адрес, існують інші спеціальні діапазони: 169.254.0.0/16 для автоматичної конфігурації APIPA (Automatic Private IP Addressing) при недоступності DHCP-сервера, 224.0.0.0/4 для багатоадресної розсилки (multicast), 255.255.255.255 для обмеженої широкомовної розсилки (limited broadcast) та 0.0.0.0/8 для позначення невизначених адрес. Розуміння призначення цих спеціальних діапазонів критично важливе для правильного проектування та налаштування мережевих систем.

1.2 Підмережування та технології FLSM і VLSM

Підмережування (subnetting) представляє собою фундаментальну технологію мережевого проектування, що дозволяє поділити велику мережу на менші логічні сегменти з метою ефективного використання IP-адрес, покращення продуктивності мережі, підвищення безпеки та спрощення адміністрування. Основним інструментом підмережування є модифікація стандартної маски підмережі шляхом "позичання" біт з хостової частини для створення додаткових мережевих адрес. Цей процес дозволяє створювати ізольовані сегменти мережі, які можуть бути налаштовані з різними політиками безпеки, якості обслуговування та адміністративними правилами, забезпечуючи більш гнучке управління мережевою інфраструктурою та можливість реалізації принципу мінімальних привілеїв на мережевому рівні.

Математичні основи підмережування базуються на двійковій арифметиці та степенях числа 2. Кількість можливих підмереж визначається формулою 2^n, де n - кількість позичених біт з хостової частини адреси. Кількість доступних хостів у кожній підмережі обчислюється як 2^h - 2, де h - кількість хостових біт, що залишилися після позичання, а віднняття двиці враховує адресу мережі (всі хостові біти дорівнюють 0) та широкомовну адресу (всі хостові біти дорівнюють 1), які не можуть бути призначені звичайним пристроям. Наприклад, при підмережуванні мережі класу C (192.168.1.0/24) з позичанням 3 біт можна створити 2^3 = 8 підмереж, кожна з яких матиме 2^5 - 2 = 30 доступних хостових адрес.

Процес розрахунку підмережування вимагає розуміння двійкової математики та вміння працювати з бітовими операціями. Для визначення меж підмережі необхідно знати "магічне число" - різницю між 256 та значенням останнього ненульового октета маски підмережі. Це число визначає крок між сусідніми підмережами та дозволяє швидко розрахувати всі адресні діапазони. Наприклад, для маски 255.255.255.224 (/27) магічне число становить 256 - 224 = 32, що означає підмережі з кроком 32: 0-31, 32-63, 64-95, 96-127 і так далі.

Технологія FLSM (Fixed Length Subnet Mask) представляє традиційний підхід до підмережування, який передбачає використання однакових масок підмереж для всіх сегментів мережі. Цей метод спрощує планування, налаштування та адміністрування мережі, оскільки всі підмережі мають ідентичну структуру та кількість доступних адрес. FLSM особливо ефективний у гомогенних мережевих середовищах, де всі сегменти мають приблизно однакові вимоги до кількості пристроїв. Однак основний недолік FLSM полягає в неефективному використанні адресного простору, коли розмір кожної підмережі визначається за найбільшою потребою в кількості хостів.

При застосуванні FLSM всі менші підмережі отримують надлишкову кількість адрес, які залишаються невикористаними та не можуть бути перерозподілені на інші сегменти. Це призводить до значних втрат адресного простору, особливо критичних в умовах дефіциту IPv4 адрес. Наприклад, якщо найбільша підмережа потребує 100 хостів (вимагає /25 з 126 адресами), то всі інші підмережі також отримують /25, навіть якщо деякі з них потребують лише 10-20 адрес. Такий підхід може призвести до втрати до 70-80% адресного простору в неоднорідних мережевих структурах.

Технологія VLSM (Variable Length Subnet Mask) революціонізувала підхід до проектування мереж, дозволяючи використовувати маски підмереж різної довжини в межах однієї батьківської мережі. Ця технологія забезпечує оптимальне використання адресного простору відповідно до реальних потреб кожного сегмента, дозволяючи досягти економії до 50-70% адрес порівняно з традиційним підходом FLSM. VLSM особливо ефективна в складних корпоративних мережах з гетерогенними сегментами, що мають суттєво відмінні вимоги до кількості адрес.

Ключовим принципом успішного застосування VLSM є правильне планування адресного простору з урахуванням поточних та майбутніх потреб. Рекомендується спочатку планувати підмережі, починаючи з найбільшої за кількістю хостів, і поступово переходити до менших, що дозволяє уникнути фрагментації адресного простору та забезпечити можливість майбутнього розширення мережі. Цей підхід, відомий як "принцип найбільшого першого" (largest first principle), гарантує оптимальне використання доступних адрес та мінімізує ймовірність конфліктів адресації при розширенні мережі.

Процедура проектування мережі з VLSM включає кілька етапів: аналіз вимог до кількості хостів у кожному сегменті, сортування підмереж за спаданням розміру, розрахунок необхідних масок для кожної підмережі, послідовний розподіл адресних блоків та верифікація отриманої схеми на предмет перекриття адресних діапазонів. Критично важливо забезпечити, щоб

адресні діапазони різних підмереж не перетинались, оскільки це призведе до конфліктів маршрутизації та порушення зв’язності мережі.

VLSM вимагає використання протоколів маршрутизації класу classless (безкласові), які підтримують передачу інформації про маски підмереж разом з маршрутною інформацією. До таких протоколів належать RIPv2, EIGRP, OSPF, IS-IS та BGP. Класичні протоколи маршрутизації (RIPv1, IGRP) не можуть коректно обробляти мережі з різними масками в межах одного адресного класу, оскільки вони передають лише інформацію про мережеві адреси без масок підмереж. Це обмеження робить їх непридатними для сучасних мережевих інфраструктур, де VLSM є стандартною практикою.

Додатковою перевагою VLSM є можливість створення суперефективних схем адресації для point-to-point з’єднань між маршрутизаторами. Використання масок /30 (4 адреси: мережева, 2 хости, широкомовна) або навіть /31 (2 адреси за RFC 3021 для point-to-point каналів) дозволяє мінімізувати втрати адрес на міжмережевих з’єднаннях. Такий підхід особливо важливий у великих мережевих топологіях з множинними WAN-з’єднаннями між філіями організації.

Сучасні мережеві архітектури також використовують концепцію суммаризації маршрутів (route summarization або route aggregation), яка тісно пов’язана з VLSM. Правильно спланована ієрархічна адресація дозволяє агрегувати множинні маршрути в один сумарний маршрут, що зменшує розмір таблиць маршрутизації, прискорює процес прийняття рішень про пересилання пакетів та підвищує стабільність мережі за рахунок локалізації змін топології. Ефективна суммаризація вимагає використання безперервних адресних блоків та правильного планування ієрархії мережі на етапі проектування.

Приклад 1. Розбиття мережі без використання технології VLSM

Розглянемо приклад розбиття мережі 192.168.10.0/24 на чотири підмережі з використанням класичного підходу, коли всі підмережі мають однаковий розмір — так званий метод FLSM (Fixed Length Subnet Mask). Вихідні вимоги залишаються незмінними: необхідно створити чотири підмережі, що обслуговують 60, 30, 14 та 6 хостів відповідно. Однак, на відміну від VLSM, у цьому випадку всі підмережі повинні мати однакову кількість адрес, що призводить до менш ефективного використання IP-адресного простору.

Мережа 192.168.10.0/24 належить до класу C, оскільки перший октет (192) знаходиться в діапазоні від 192 до 223. Це приватна мережа, визначена в RFC 1918, із загальною кількістю 256 IP-адрес, з яких 254 можуть бути призначені хостам. Метою є розбиття цієї мережі на чотири окремі підмережі, але без застосування змінних масок.

Оскільки технологія VLSM не використовується, всі підмережі повинні мати однаковий розмір. Розмір кожної підмережі визначається за найбільшою потребою — у нашому випадку це 60 хостів. Для розміщення 60 хостів потрібно мінімум 62 адреси (з урахуванням мережевої та широкомовної). Найближча степінь двійки, що забезпечує цю кількість, — 64. Отже, кожна

підмережа повинна мати 64 адреси, що відповідає масці /26 або 255.255.255.192.

Оскільки загальна кількість адрес у мережі становить 256, а кожна підмережа займає 64 адреси, можна створити рівно чотири підмережі, що цілком вписується в доступний діапазон. Однак варто зазначити, що такий підхід призводить до значних втрат адресного простору, особливо для менших підмереж.

Перша підмережа починається з базової адреси 192.168.10.0. З огляду на маску /26, вона займає діапазон від 192.168.10.0 до 192.168.10.63. Мережева адреса — 192.168.10.0, широкомовна — 192.168.10.63, а хости можуть використовувати адреси від 192.168.10.1 до 192.168.10.62.

Друга підмережа розпочинається з наступної доступної адреси — 192.168.10.64 — і займає діапазон до 192.168.10.127. Мережева адреса — 192.168.10.64, широкомовна — 192.168.10.127, хости — від 192.168.10.65 до 192.168.10.126.

Третя підмережа починається з 192.168.10.128 і закінчується на 192.168.10.191. Мережева адреса — 192.168.10.128, широкомовна — 192.168.10.191, хости — від 192.168.10.129 до 192.168.10.190.

Четверта підмережа займає останній блок: від 192.168.10.192 до 192.168.10.255. Мережева адреса — 192.168.10.192, широкомовна — 192.168.10.255, хости — від 192.168.10.193 до 192.168.10.254.

Хоча всі підмережі відповідають вимогам за кількістю адрес, насправді більшість з них використовує значно менше хостів, ніж доступно. Наприклад, підмережа 2 (30 хостів) отримує 62 адреси, підмережа 3 (14 хостів) — також 62, і підмережа 4 (6 хостів) — теж 62. Це означає, що велика кількість IP-адрес залишається невикористаною.

Загальна кількість використаних хостових адрес становить: 60 + 30 + 14 + 6 = 110. Загальна кількість доступних хостових адрес у чотирьох підмережах: 4 × 62 = 248. Отже, втрачено 248 – 110 = 138 адрес через неефективне розподілення.

У порівнянні з підходом VLSM, де використано лише 120 адрес і залишено простір для розширення, у разі FLSM використано всі 256 адрес, і немає можливості створити додаткові підмережі у межах 192.168.10.0/24. Це робить мережу менш гнучкою та масштабованою.

Нижче наведено підсумкову таблицю розподілу підмереж за методом FLSM.

Таблиця 4.2 – Двійкове представлення адрес і масок підмереж (FLSM)

Підмережа	**Двійкові адреси та маска**
1 (/26, 62 хости)	Для підмережі з 60 хостами потрібно щонайменше 62 адреси. Найближча степінь двійки — 64, що відповідає 6 хостовим бітам. Використовується маска /26 (255.255.255.192), що дає 62 доступних адрес для хостів. 11000000.10101000.00001010.00000000 — мережева адреса (192.168.10.0) 11000000.10101000.00001010.00000001 — перший хост (192.168.10.1) 11000000.10101000.00001010.00000010 — другий хост (192.168.10.2) ... 11000000.10101000.00001010.00111110 — останній хост (192.168.10.62) 11000000.10101000.00001010.00111111 — широкомовна адреса (192.168.10.63) Маска підмережі: 11111111.11111111.11111111.11000000 — (255.255.255.192)
2 (/26, 62 хости)	Друга підмережа починається з адреси 192.168.10.64. Маска залишається /26. 11000000.10101000.00001010.01000000 — мережева адреса (192.168.10.64) 11000000.10101000.00001010.01000001 — перший хост (192.168.10.65) 11000000.10101000.00001010.01000010 — другий хост (192.168.10.66) ... 11000000.10101000.00001010.01111110 — останній хост (192.168.10.126) 11000000.10101000.00001010.01111111 — широкомовна адреса (192.168.10.127) Маска підмережі: 11111111.11111111.11111111.11000000 — (255.255.255.192)
3 (/26, 62 хости)	Третя підмережа починається з 192.168.10.128. 11000000.10101000.00001010.10000000 — мережева адреса (192.168.10.128) 11000000.10101000.00001010.10000001 — перший хост (192.168.10.129) 11000000.10101000.00001010.10000010 — другий хост (192.168.10.130) ... 11000000.10101000.00001010.10111110 — останній хост (192.168.10.190) 11000000.10101000.00001010.10111111 — широкомовна адреса (192.168.10.191) Маска підмережі: 11111111.11111111.11111111.11000000 — (255.255.255.192)
4 (/26, 62 хости)	Четверта підмережа починається з 192.168.10.192. 11000000.10101000.00001010.11000000 — мережева адреса (192.168.10.192) 11000000.10101000.00001010.11000001 — перший хост (192.168.10.193) 11000000.10101000.00001010.11000010 — другий хост (192.168.10.194) ... 11000000.10101000.00001010.11111110 — останній хост (192.168.10.254) 11000000.10101000.00001010.11111111 — широкомовна адреса (192.168.10.255) Маска підмережі: 11111111.11111111.11111111.11000000 — (255.255.255.192)

Таблиця 4.3 – Розрахунок підмереж без використання VLSM (FLSM)

Підмережа	Мережева адреса	Маска підмережі	Діапазон хостів	Широкомовна адреса	Кількість хостів у підмережі
1	192.168.10.0/26	255.255.255.192	192.168.10.1 – 192.168.10.62	192.168.10.63	62
2	192.168.10.64/26	255.255.255.192	192.168.10.65 – 192.168.10.126	192.168.10.127	62
3	192.168.10.128/26	255.255.255.192	192.168.10.129 – 192.168.10.190	192.168.10.191	62
4	192.168.10.192/26	255.255.255.192	192.168.10.193 – 192.168.10.254	192.168.10.255	62

Цей приклад демонструє основний недолік методу FLSM — неефективне використання IP-адресного простору у випадках, коли підмережі мають різну кількість хостів. Хоча метод простий у реалізації та підходить для однотипних мереж, він не рекомендується для сучасних мережевих інфраструктур, де важлива економія адрес та гнучкість проектування. Технологія VLSM є значно кращим вибором у більшості практичних сценаріїв.

Приклад 2. Застосування технології VLSM

Розглянемо детальний приклад застосування технології VLSM (Variable Length Subnet Mask) для ефективного розподілу IP-адрес у мережі. Базовою мережею є 192.168.10.0/24, яка потребує розбиття на чотири підмережі з різною кількістю хостів: перша підмережа має обслуговувати 60 пристроїв, друга — 30, третя — 14, а четверта — 6. Метою є мінімізація втрат адресного простору шляхом використання змінних масок підмереж.

Аналізуючи базову мережу, встановлюємо, що IP-адреса 192.168.10.0 належить до класу C, оскільки її перший октет (192) знаходиться в діапазоні від 192 до 223. Це приватна мережа, визначена в стандарті RFC 1918, із маскою за замовчуванням 255.255.255.0 або префіксом /24. Така мережа забезпечує загалом 256 IP-адрес, з яких 254 можуть бути призначені хостам (дві адреси використовуються для мережевої та широкомовної).

Для ефективного використання адресного простору за технологією VLSM необхідно спочатку впорядкувати підмережі за спаданням кількості потрібних хостів. Це дозволяє розміщувати найбільші підмережі на початку діапазону, уникнути фрагментації та забезпечити можливість майбутнього розширення. У нашому випадку послідовність розподілу буде такою: підмережа 1 (60 хостів), підмережа 2 (30 хостів), підмережа 3 (14 хостів), підмережа 4 (6 хостів).

Для кожної підмережі визначається необхідна кількість адрес із урахуванням мережевої та широкомовної. Для підмережі з 60 хостами потрібно щонайменше 62 адреси. Найближча степінь двійки, що перевищує це значення, — 64, що відповідає 6 хостовим бітам. Відповідно, префікс підмережі становить /26, а маска — 255.255.255.192. Ця підмережа забезпечує 62 використовуваних адрес для хостів.

Наступна підмережа, що потребує 30 хостів, потребує 32 адреси. Найближча степінь двійки — 32, що вимагає 5 хостових бітів. Таким чином,

префікс становить /27, а маска — 255.255.255.224. Кількість доступних хостів — 30, що повністю відповідає вимогам.

Для підмережі з 14 хостами потрібно 16 адрес. Використовується 2^4 = 16, що відповідає 4 хостовим бітам. Префікс — /28, маска — 255.255.255.240, кількість хостів — 14.

Остання підмережа, що обслуговує 6 пристроїв, потребує 8 адрес. Використовується 2^3 = 8, що вимагає 3 хостових біти. Префікс — /29, маска — 255.255.255.248, кількість хостів — 6.

Розподіл адрес виконується послідовно, починаючи з першої підмережі. Перша підмережа /26 починається з адреси 192.168.10.0 і займає діапазон від 192.168.10.0 до 192.168.10.63. Мережева адреса — 192.168.10.0, широкомовна — 192.168.10.63, хости — від 192.168.10.1 до 192.168.10.62. Наступна вільна адреса — 192.168.10.64.

Друга підмережа /27 розпочинається з 192.168.10.64 і займає 32 адреси, завершуючись на 192.168.10.95. Мережева адреса — 192.168.10.64, широкомовна — 192.168.10.95, хости — від 192.168.10.65 до 192.168.10.94. Наступна вільна адреса — 192.168.10.96.

Третя підмережа /28 починається з 192.168.10.96 і займає 16 адрес, завершуючись на 192.168.10.111. Хости призначені від 192.168.10.97 до 192.168.10.110, широкомовна адреса — 192.168.10.111. Наступна вільна адреса — 192.168.10.112.

Четверта підмережа /29 розпочинається з 192.168.10.112 і займає 8 адрес, завершуючись на 192.168.10.119. Хости — від 192.168.10.113 до 192.168.10.118, широкомовна — 192.168.10.119.

У результаті використано 120 IP-адрес (включаючи мережеві та широкомовні), що становить менше половини загального адресного простору. Загалом доступно 256 адрес, отже, залишається 136 адрес для майбутнього розширення мережі. Це демонструє високу ефективність технології VLSM порівняно з класичним підходом з фіксованою маскою, де всі підмережі мали б однаковий розмір і значна кількість адрес була б втрачена.

Нижче наведено підсумкову таблицю розподілу підмереж.

Таблиця 4.4 – Розрахунок підмереж з використанням VLSM

ПІДМЕРЕЖА	МЕРЕЖЕВА АДРЕСА	МАСКА ПІДМЕРЕЖІ	ДІАПАЗОН ХОСТІВ	ШИРОКОМОВНА АДРЕСА	ПРИКЛАД АДРЕСИ ШЛЮЗУ
1	192.168.10.0/26	255.255.255.192	192.168.10.1 – 192.168.10.62	192.168.10.63	192.168.10.1
2	192.168.10.64/27	255.255.255.224	192.168.10.65 – 192.168.10.94	192.168.10.95	192.168.10.65
3	192.168.10.96/28	255.255.255.240	192.168.10.97 – 192.168.10.110	192.168.10.111	192.168.10.97
4	192.168.10.112/29	255.255.255.248	192.168.10.113 – 192.168.10.118	192.168.10.119	192.168.10.113

Таблиця 4.5 – Двійкове представлення адрес і масок підмереж (VLSM)

Підмережа	Двійкові адреси та маска
1 (/26, 62 хости)	Для 60 хостів потрібно 62 адреси — найближча степінь двійки 64 відповідає 6 хостовим бітам, тому використовується префікс /26 (маска 255.255.255.192), що дає 62 доступних хостів. 11000000.10101000.00001010.00000000 — мережева (192.168.10.0) 11000000.10101000.00001010.00000001 — хост 1 (192.168.10.1) 11000000.10101000.00001010.00000010 — хост 2 (192.168.10.2) ... 11000000.10101000.00001010.00111110 — останній хост (192.168.10.62) 11000000.10101000.00001010.00111111 — широкомовна (192.168.10.63) 11111111.11111111.11111111.11000000 — маска (255.255.255.192)
2 (/27, 30 хостів)	Підмережа 2 (30 хостів): 30 хостів вимагають 32 адреси, що відповідає 5 хостовим бітам; отже, використовується маска /27 (255.255.255.224), яка забезпечує рівно 30 хостів. 11000000.10101000.00001010.01000000 — мережева (192.168.10.64) 11000000.10101000.00001010.01000001 — хост 1 (192.168.10.65) 11000000.10101000.00001010.01000010 — хост 2 (192.168.10.66) ... 11000000.10101000.00001010.01011110 — останній хост (192.168.10.94) 11000000.10101000.00001010.01011111 — широкомовна (192.168.10.95) 11111111.11111111.11111111.11100000 — маска (255.255.255.224)
3 (/28, 14 хостів)	Підмережа 3 (14 хостів): Для 14 хостів потрібно 16 адрес, що вимагає 4 хостових біти; тому застосовується префікс /28 (маска 255.255.255.240) з 14 доступними хостами. 11000000.10101000.00001010.01100000 — мережева (192.168.10.96) 11000000.10101000.00001010.01100001 — хост 1 (192.168.10.97) 11000000.10101000.00001010.01100010 — хост 2 (192.168.10.98) ... 11000000.10101000.00001010.01101110 — останній хост (192.168.10.110) 11000000.10101000.00001010.01101111 — широкомовна (192.168.10.111) 11111111.11111111.11111111.11110000 — маска (255.255.255.240)
4 (/29, 6 хостів)	Підмережа 4 (6 хостів): 6 хостів потребують 8 адрес — це 3 хостових біти, отже, використовується маска /29 (255.255.255.248), яка забезпечує рівно 6 хостів. 11000000.10101000.00001010.01110000 — мережева (192.168.10.112) 11000000.10101000.00001010.01110001 — хост 1 (192.168.10.113) 11000000.10101000.00001010.01110010 — хост 2 (192.168.10.114) ... 11000000.10101000.00001010.01111010 — останній хост (192.168.10.118) 11000000.10101000.00001010.01111011 — широкомовна (192.168.10.119) 11111111.11111111.11111111.11111000 — маска (255.255.255.248)

Для спрощення процесу розрахунку підмереж за допомогою методу VLSM (Variable Length Subnet Mask) студентам може бути рекомендована використання спеціалізованої програми — VLSM Calculator, доступної за посиланням https://github.com/belavina/VLSMCalculator. Ця програма дозволяє

швидко та точно виконати розподіл адресного простору базової мережі на кілька підмереж з різними потребами у хостах, що значно економить час на виконанні практичних завдань і дозволяє зосередитися на аналізі результатів та їх реалізації в симуляторі (рис. 4.1).

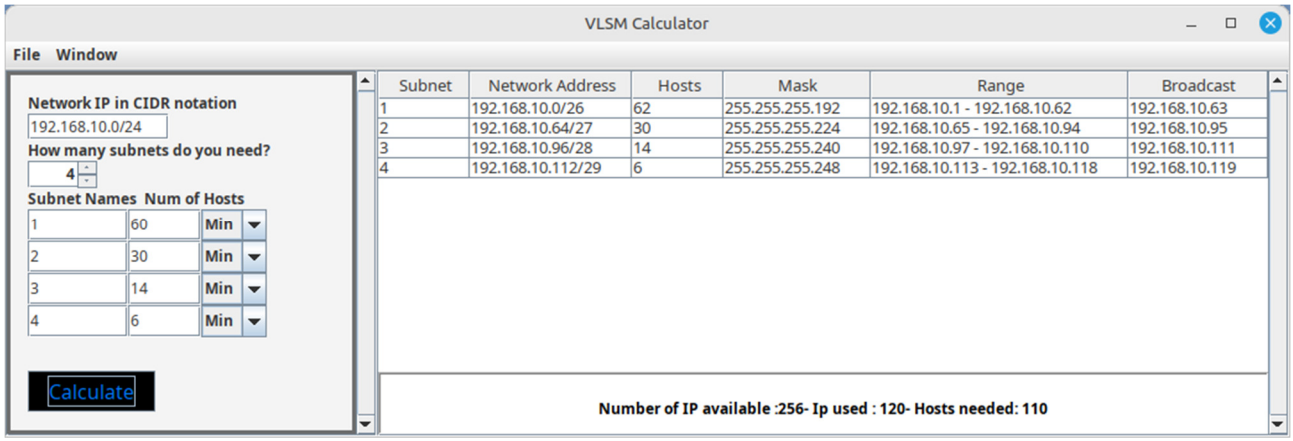

Рисунок 4.1 – Вікно програми VLSM Calculator

Робота з програмою полягає у введенні вихідних даних: початкової IP-адреси мережі у форматі CIDR (наприклад, `192.168.10.0/24`) та кількості необхідних підмереж разом із кількістю хостів у кожній. У лівій частині інтерфейсу користувач вказує параметри задачі, а після натискання кнопки "Calculate" програма автоматично обчислює оптимальні маски для кожної підмережі, враховуючи принципи VLSM. Результати виводяться у таблиці праворуч, де для кожної підмережі вказано мережеву адресу, маску, кількість хостів, діапазон використовуваних IP-адрес та широкомовну адресу. Такий підхід дозволяє отримати повну інформацію про структуру мережі без необхідності ручних розрахунків, що особливо корисно при виконанні складних завдань з великим числом підмереж.

Використання VLSM Calculator не замінює розуміння теоретичних основ підмережування, але є цінним інструментом для перевірки правильності ручних розрахунків та швидкого отримання результатів. Студентам слід використовувати програму як допоміжний інструмент, щоб зберегти час на виконанні практичної частини заняття, наприклад, при побудові моделі мережі в Cisco Packet Tracer. Після отримання результатів з програми, необхідно вручну ввести отримані IP-адреси та маски в конфігурацію пристроїв, що забезпечує глибоке розуміння взаємозв’язку між теорією та практикою. Важливо пам’ятати, що програма використовує алгоритм, який починає з найбільшої підмережі, що відповідає стандартному підходу до VLSM, і тому результати будуть максимально ефективними у використанні адресного простору.

Цей приклад ілюструє, як технологія VLSM дозволяє гнучко планувати IP-адресацію, уникати втрат адресного простору та забезпечувати масштабованість мережі. Він може бути використаний як основа для проектування реальних мережевих інфраструктур або як навчальний матеріал

при вивченні безкласової адресації (CIDR) та протоколів маршрутизації, що підтримують VLSM, таких як OSPF, EIGRP або RIP v2.

2 КЛЮЧОВІ ПИТАННЯ

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.

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

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 таблицею 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 4.6 – 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. 4.2 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.

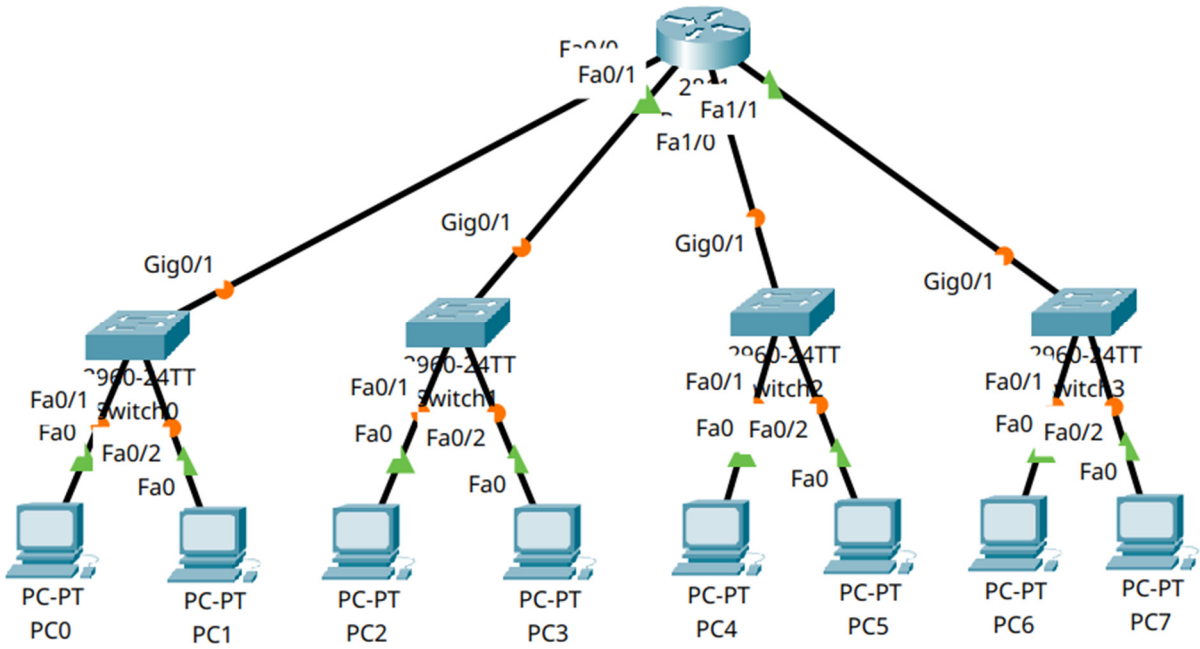

Рисунок 4.2 – Топологія мережі з підмережуванням

3.1. Створення топології мережі

3.1.1 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.

3.1.2 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.

3.2. Налаштування маршрутизатора

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)#
```

3.2.2 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, а 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
```

3.2.3 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
```

3.2.4 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
```

3.2.5 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
```

3.2.6 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]
```

3.3. Налаштування комутаторів

3.3.1 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
```

3.3.2 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
```

3.3.3 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
```

3.3.4 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
```

3.4. Налаштування комп’ютерів

У таблиці 4.4 представлено детальні налаштування мережевих параметрів для всіх комп’ютерів у кожній підмережі.

Таблиця 4.7 - 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

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.5. Перевірка конфігурації мережі

3.5.1 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
```

3.5.2 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
```

3.6. Тестування зв'язності

3.6.1 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.

3.6.2 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.

3.6.3 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.

3.7. Діагностика та усунення проблем

3.7.1 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.

3.7.2 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.

3.7.3 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 практичної 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 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

Лабораторна робота № 5

Тема: Статична маршрутизація в комп'ютерних мережах

Мета роботи: набути практичних навичок налаштування статичної маршрутизації в комп'ютерних мережах.

1 КЛЮЧОВІ ПОЛОЖЕННЯ

Архітектура глобальних комп'ютерних мереж будується за модульним принципом, який передбачає створення складної системи шляхом об'єднання менших, незалежних і функціонально завершених компонентів . Ці компоненти, як правило, є окремими локальними мережами (LAN), що обслуговують певні географічні локації або підрозділи організації. Така ієрархічна побудова дозволяє ефективно керувати складністю, полегшити масштабування та покращити надійність мережі. Для забезпечення зв'язку між цими окремими модулями необхідно використовувати спеціалізовані пристрої, які виконують функцію передачі даних від одного сегменту до іншого. Цей процес відомий як маршрутизація. Маршрутизація — це процес визначення оптимального шляху для передачі пакетів даних між різними мережами на основі їх IP-адрес призначення. Вона відрізняється від комутації, яка відбувається на канальному рівні моделі OSI і здійснюється на основі MAC-адрес у межах однієї таємної мережі . Маршрутизація ж працює на мережевому рівні і забезпечує зв'язок між різними мережами, використовуючи логічні IP-адреси. Без ефективної маршрутизації неможлива була б інтеграція розрізнених мережних сегментів в єдину функціонуючу глобальну мережу.

Статична маршрутизація є одним із фундаментальних методів керування трафіком у комп'ютерних мережах, який полягає в ручному налаштуванні маршрутів між різними підмережами через адміністратора мережі. На відміну від динамічної маршрутизації, де маршрути визначаються автоматично за допомогою спеціальних протоколів, статичні маршрути створюються та підтримуються вручну, що забезпечує повний контроль над шляхами проходження пакетів даних. Цей підхід особливо ефективний у невеликих та середніх мережах із стабільною топологією, де зміни в структурі відбуваються рідко. Статична маршрутизація характеризується високою надійністю та передбачуваністю, оскільки маршрути не змінюються автоматично при зміні мережевих умов. Головними перевагами статичної маршрутизації є мінімальне навантаження на процесор маршрутизатора, відсутність додаткового трафіку для обміну маршрутною інформацією та високий рівень безпеки через відсутність автоматичного обміну даними про топологію мережі. Проте її основним недоліком є низька масштабованість і необхідність ручного втручання при будь-якій зміні в топології мережі.

Маршрутизатор є ключовим елементом мережевої інфраструктури, що працює на третьому рівні моделі OSI та забезпечує передачу пакетів між різними мережевими сегментами на основі IP-адрес призначення. Основна функція маршрутизатора полягає в аналізі заголовків IP-пакетів та прийнятті

рішень щодо оптимального шляху їх передачі до кінцевого призначення. Кожен маршрутизатор містить таблицю маршрутизації, яка є базою даних, що зберігає інформацію про доступні мережеві шляхи, включаючи адреси призначення, маски підмереж та інтерфейси виходу. Таблиця маршрутизації є центральним компонентом системи маршрутизації, що містить записи про всі відомі мережеві призначення та способи їх досягнення. Як показано в табл. 5.1, кожен запис таблиці маршрутизації включає кілька ключових елементів, що визначають правила передачі пакетів.

Таблиця 5.1 – Структура запису таблиці маршрутизації

Поле	Опис	Приклад
Мережа призначення	IP-адреса цільової підмережі	192.168.3.0
Маска підмережі	Визначає межі підмережі	255.255.255.0
Шлюз наступного переходу	IP-адреса наступного маршрутизатора	192.168.2.2
Інтерфейс виходу	Фізичний порт для передачі пакета	FastEthernet0/1
Метрика	Вартість маршруту	1
Адміністративна відстань	Пріоритет джерела маршруту	1 (для статичних)

Процес конфігурування статичних маршрутів в операційній системі Cisco IOS здійснюється через інтерфейс командного рядка з використанням спеціальних команд налаштування. Базова команда для створення статичного маршруту має синтаксис ip route [мережа_призначення] [маска_підмережі] [наступний_перехід або інтерфейс], де параметри визначають всі необхідні характеристики маршруту. Налаштування починається з переходу в привілейований режим за допомогою команди enable, після чого необхідно увійти в режим глобальної конфігурації командою configure terminal. Важливо розуміти, що статичні маршрути мають найвищий пріоритет серед усіх типів маршрутів, за винятком безпосередньо підключених мереж. Інтерфейси маршрутизатора потребують попереднього налаштування перед створенням статичних маршрутів, оскільки вони є точками підключення до різних мережевих сегментів. Кожен інтерфейс має отримати унікальну IP-адресу, що відповідає адресному простору підключеної підмережі, та бути активованим командою no shutdown. Типові інтерфейси маршрутизаторів Cisco включають FastEthernet, Ethernet та серіальні порти, кожен з яких має свою специфічну номенклатуру та характеристики пропускної здатності. Правильне налаштування інтерфейсів є критично важливим для забезпечення коректної роботи статичної маршрутизації.

Команди, що безпосередньо стосуються процесу маршрутизації, є основним інструментарієм для побудови та діагностики шляхів передачі даних у мережі (табл. 5.2). Команда *ip route [мережа] [маска] [next-hop або інтерфейс]* є фундаментальною для налаштування статичної маршрутизації, оскільки вона дозволяє вручну визначити шлях до певної цільової мережі. Ця команда вимагає вказати IP-адресу мережі призначення та її маску, а також визначити, куди надсилати пакети — або на IP-адресу наступного стрибка (next-hop), або через конкретний вихідний інтерфейс маршрутизатора. Використання адреси наступного стрибка є більш універсальним підходом,

особливо в мережах з кількома пристроями на одному сегменті, тоді як вказівка інтерфейсу напряму найчастіше застосовується для точкових з'єднань, таких як серіальні лінії. Протилежною до неї є команда *no ip route*, яка використовується для видалення конкретного статичного маршруту з конфігурації, і для її коректної роботи необхідно точно вказати всі параметри видаляємого маршруту, які були використані при його створенні.

Таблиця 5.2 – Команди Cisco IOS для налаштування та перевірки маршрутизації

Команда	Режим	Призначення
enable	User EXEC	Перехід в привілейований режим
disable	Privileged EXEC	Повернення в режим користувача
configure terminal	Privileged EXEC	Вхід в режим глобальної конфігурації
interface [ім'я_інтерфейсу]	Global Config	Вхід в режим конфігурації вказаного інтерфейсу
ip address [IP_адреса] [маска]	Interface Config	Призначення IP-адреси інтерфейсу
no shutdown	Interface Config	Активування (ввімкнення) інтерфейсу
shutdown	Interface Config	Деактивування (вимкнення) інтерфейсу
ip route [мережа] [маска] [next-hop або інтерфейс]	Global Config	Додавання статичного маршруту
no ip route [мережа] [маска] [next-hop або інтерфейс]	Global Config	Видалення статичного маршруту
show ip route	Privileged EXEC	Перегляд таблиці маршрутизації
show running-config	Privileged EXEC	Перегляд поточної конфігурації
show startup-config	Privileged EXEC	Перегляд конфігурації, що завантажується при запуску
ping [IP_адреса]	User EXEC / Privileged EXEC	Перевірка зв'язності з вказаним хостом
traceroute [IP_адреса]	Privileged EXEC	Відстеження шляху до вказаного хоста

Ключовою командою для аналізу стану маршрутизації є *show ip route*, яка відображає вміст таблиці маршрутизації — центрального реєстру, за яким маршрутизатор приймає рішення про передачу пакетів. Ця команда надає детальний огляд усіх відомих мережевих шляхів, включаючи як безпосередньо підключені мережі (позначені C), так і статичні (позначені S) та динамічні маршрути. Вивід містить критично важливу інформацію: для кожного маршруту вказується адреса призначення, маска, наступний стрибок (якщо є) та вихідний інтерфейс, що дозволяє адміністратору перевірити, чи правильно налаштовані всі необхідні шляхи. Команда *show running-config* доповнює цю інформацію, оскільки вона виводить поточну активну конфігурацію маршрутизатора, включаючи всі внесені зміни, зокрема команди ip route. Це дозволяє порівняти те, що було сконфігуровано (*running-config*), з тим, що завантажиться після перезавантаження (*startup-config*), і переконатися, що всі зміни були збережені командою copy running-config startup-config.

Для перевірки працездатності налаштованих маршрутів використовуються діагностичні команди *ping* та *traceroute*. Команда *ping* є першим і найпростішим інструментом для перевірки базової зв'язності між двома вузлами мережі. Вона працює шляхом відправлення ICMP-пакетів запиту (Echo Request) до вказаної IP-адреси та очікування відповіді (Echo Reply). Успішні відповіді підтверджують, що шлях до цільового хоста існує, а час відгуку дає уявлення про затримку в мережі. Проте ping не показує, яким саме шляхом пройшов пакет. Саме для цього призначена команда *traceroute*. Вона відстежує весь шлях проходження пакета від джерела до призначення, послідовно виявляючи кожен проміжний маршрутизатор (стрибок) на цьому шляху. Це досягається за рахунок маніпуляції з полем TTL (Time To Live) у заголовку IP-пакета. Вивід traceroute показує IP-адреси кожного хоста на шляху та час відгуку для кожного стрибка, що є незамінним інструментом для локалізації проблем у мережі, наприклад, визначення, на якому саме маршрутизаторі виникає висока затримка або втрати пакетів. Разом ці команди утворюють повний набір інструментів для конфігурування, візуалізації та тестування 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).

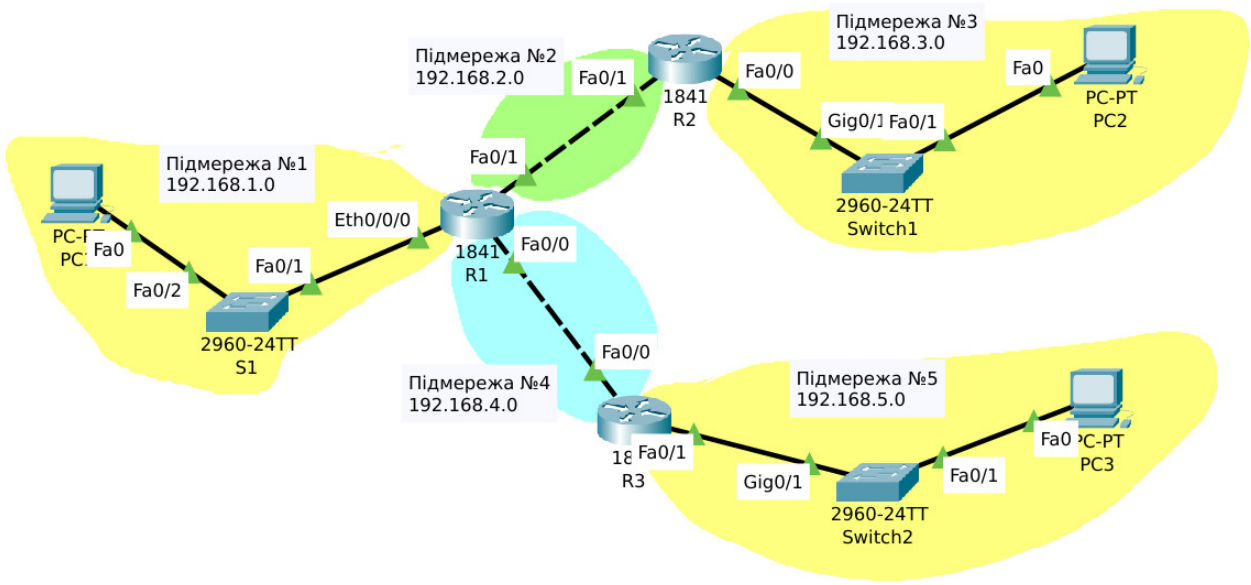

Рисунок 5.1 – Топологія мережі для вивчення статичної маршрутизації

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 - IS-
IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     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.

2 КЛЮЧОВІ ПИТАННЯ

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.

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. 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. 5.3) 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.

Таблиця 5.3 – 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

3.2 Налаштування мережних інтерфейсів маршрутизаторів

3.2.1 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
```

3.2.2 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
```

3.2.3 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 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
```

3.3 Налаштування статичної маршрутизації

3.3.1 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
```

3.3.2 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
```

3.3.3 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
```

3.4 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
```

4 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

Лабораторна робота № 6

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

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

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Загальні принципи мережевої безпеки та керування трафіком

Сучасна мережева безпека базується на принципі багаторівневого захисту (defense in depth), який передбачає створення декількох незалежних рівнів контролю для забезпечення комплексного захисту мережевої інфраструктури від різноманітних загроз. Цей підхід включає фізичну безпеку обладнання, захист мережевого рівня, контроль доступу до пристроїв та моніторинг трафіку, що створює ешелоновану систему захисту, де компрометація одного рівня не призводить до повного порушення безпеки системи. Ефективна система безпеки повинна забезпечувати конфіденційність, цілісність та доступність мережевих ресурсів, дотримуючись принципу найменших привілеїв, коли кожен користувач або система отримує мінімально необхідні права для виконання своїх функцій. Особливо важливим є забезпечення безперервності роботи критично важливих сервісів навіть в умовах активних атак або технічних збоїв, що вимагає впровадження резервування та систем аварійного відновлення.

Керування мережевим трафіком є невід'ємною частиною забезпечення безпеки та ефективної роботи мережевої інфраструктури, оскільки дозволяє контролювати потоки даних між різними сегментами мережі відповідно до встановлених політик безпеки та вимог продуктивності. Основними цілями керування трафіком є запобігання несанкціонованому доступу до критичних ресурсів, оптимізація використання пропускної здатності мережевих каналів, забезпечення якості обслуговування для пріоритетних додатків та мінімізація впливу шкідливого або надмірного трафіку на загальну продуктивність мережі. Сегментація мережі на логічні зони з різними рівнями довіри дозволяє застосовувати диференційовані політики безпеки та обмежувати поширення потенційних загроз між критичними та менш важливими системами.

Принцип найменших привілеїв у мережевій безпеці передбачає надання мінімально необхідних прав доступу для виконання конкретних завдань, що значно зменшує потенційну поверхню атаки та обмежує можливості зловмисників у разі компрометації облікових записів або систем. Цей підхід реалізується через детальну класифікацію користувачів, пристроїв та додатків за рівнями довіри, встановлення чітких правил взаємодії між різними сегментами мережі та регулярний аудит прав доступу для виявлення та усунення надмірних привілеїв. Важливим аспектом є також принцип явного

дозволу (default deny), коли весь трафік за замовчуванням блокується, а дозволяються лише явно визначені типи з'єднань, що забезпечує більш контрольоване та безпечне середовище.

Моніторинг та аналіз мережевого трафіку відіграють ключову роль у своєчасному виявленні аномалій, атак та порушень безпеки, забезпечуючи можливість швидкого реагування на інциденти та мінімізацію їх наслідків. Ефективна система моніторингу повинна включати збір та аналіз метрик мережевої активності в реальному часі, ведення детальних журналів подій, автоматичне виявлення підозрілих патернів поведінки та генерацію сповіщень для адміністраторів безпеки. Особливу увагу слід приділяти аналізу базових показників мережевої активності (baseline), що дозволяє швидко ідентифікувати відхилення від нормальної поведінки системи та потенційні загрози безпеці.

Політики безпеки мережевої інфраструктури повинні бути чітко документовані, регулярно переглядатися та оновлюватися відповідно до еволюції загроз та зміни бізнес-вимог організації. Ці політики визначають правила доступу до мережевих ресурсів, процедури аутентифікації та авторизації користувачів, вимоги до шифрування даних, стандарти конфігурації обладнання та процедури реагування на інциденти безпеки. Важливим елементом є також навчання персоналу основам мережевої безпеки та регулярне проведення тестувань на проникнення для оцінки ефективності впроваджених заходів захисту та виявлення потенційних вразливостей системи.

1.2 Налаштування безпеки мережних пристроїв

Базова безпека маршрутизатора ґрунтується на системі багаторівневого контролю доступу, який включає фізичний доступ через консольний порт, віддалений доступ через мережеві протоколи та привілейований доступ до конфігураційних команд (табл. 6.1). Пароль привілейованого режиму (enable secret) є першою лінією захисту від несанкціонованого доступу до критичних функцій пристрою та повинен бути надійно зашифрованим. Консольний та віртуальний доступ контролюються окремими паролями, які забезпечують захист відповідно фізичного та мережевого підключення до маршрутизатора. Банер повідомлення дня служить не тільки інформаційним, але й правовим попередженням для користувачів про правила використання системи.

Таблиця 6.1 – Команди налаштування безпеки маршрутизатора

Команда	Режим	Призначення
enable secret <пароль>	Global Config	Встановлення зашифрованого пароля привілейованого режиму
enable password <пароль>	Global Config	Встановлення незашифрованого пароля (менш безпечний)
line console 0	Global Config	Вхід в конфігурацію консольної лінії
line vty 0 4	Global Config	Вхід в конфігурацію віртуальних терміналів

password <пароль>	Line Config	Встановлення пароля для лінії
login	Line Config	Активація перевірки пароля
login local	Line Config	Використання локальної бази користувачів
username <ім'я> password <пароль>	Global Config	Створення локального користувача
crypto key generate rsa	Global Config	Генерація RSA ключів для SSH
ip ssh version 2	Global Config	Встановлення версії SSH
transport input ssh	Line Config	Дозвіл лише SSH підключень
transport input telnet	Line Config	Дозвіл лише Telnet підключень
transport input ssh telnet	Line Config	Дозвіл SSH та Telnet підключень
banner motd "<текст>"	Global Config	Встановлення банера повідомлення дня
exec-timeout <хвилини> <секунди>	Line Config	Встановлення тайм-ауту сесії

Конфігурування консольного доступу забезпечує захист прямого фізичного підключення до маршрутизатора та є найбезпечнішим методом первинного налаштування пристрою. Приклад базової конфігурації консольного доступу:

```
Router(config)# line console 0
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exec-timeout 5 0
Router(config-line)# exit
```

Команда line console 0 переводить систему в режим конфігурації консольної лінії, password cisco встановлює пароль доступу до консолі, login активує перевірку пароля при підключенні, а exec-timeout 5 0 встановлює автоматичне відключення сесії через 5 хвилин бездіяльності для підвищення безпеки.

Налаштування Telnet-доступу дозволяє віддалене керування маршрутизатором через мережу, але слід пам’ятати про передачу даних у незашифрованому вигляді. Конфігурація Telnet-доступу:

```
Router(config)# line vty 0 4
Router(config-line)# password telnetpass
Router(config-line)# login
Router(config-line)# transport input telnet
Router(config-line)# exec-timeout 10 0
Router(config-line)# exit
```

Команда line vty 0 4 конфігурує п’ять віртуальних терміналів (лінії від 0 до 4), що дозволяє одночасне підключення п’яти користувачів, password telnetpass встановлює пароль для Telnet-сесій, transport input telnet явно дозволяє лише Telnet підключення, а exec-timeout 10 0 встановлює тайм-аут сесії у 10 хвилин.

SSH (Secure Shell) є найбезпечнішим методом віддаленого доступу завдяки шифруванню всього трафіку між клієнтом та сервером. Повна конфігурація SSH-доступу:

```
Router(config)# hostname R1
Router(config)# ip domain-name example.com
Router(config)# crypto key generate rsa
Router(config)# ip ssh version 2
Router(config)# username admin password adminpass
Router(config)# username user1 password userpass
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# transport input ssh
Router(config-line)# exec-timeout 15 0
Router(config-line)# exit
```

Ця конфігурація починається з встановлення імені хоста (hostname R1) та доменного імені (ip domain-name example.com), які необхідні для генерації RSA ключів. Команда crypto key generate rsa створює криптографічні ключі для SSH, ip ssh version 2 активує більш безпечну версію SSH. Створення локальних користувачів (username admin password adminpass) дозволяє індивідуальну аутентифікацію, а login local вказує системі використовувати локальну базу користувачів замість загального пароля лінії.

1.3 Списки контролю доступу (Access Control Lists, ACL)

Списки контролю доступу представляють собою потужний інструмент керування мережевим трафіком, який дозволяє адміністраторам створювати детальні політики безпеки для контролю потоків даних між різними сегментами мережі. ACL працюють на основі принципу послідовної перевірки правил: кожен пакет порівнюється з правилами списку по порядку, і як тільки знаходиться відповідне правило, воно застосовується без перевірки наступних. В кінці кожного ACL існує неявне правило "deny all", яке блокує весь трафік, що не відповідає жодному з явно визначених правил, тому важливо завжди включати правило "permit any" в кінці списку для дозволу легітимного трафіку.

У операційній системі Cisco IOS існують два основні типи списків доступу: стандартні та розширені ACL, які відрізняються за можливостями фільтрації та областю застосування. Стандартні списки доступу можуть фільтрувати трафік виключно на основі IP-адреси джерела та мають номери від 1 до 99 або від 1300 до 1999, що обмежує їх функціональність, але спрощує конфігурацію для базових завдань фільтрації. Розширені списки доступу надають значно більші можливості, дозволяючи контролювати трафік на основі IP-адрес джерела та призначення, типів протоколів, номерів портів, напрямків з'єднання та інших параметрів, і використовують номери від 100 до 199 або від 2000 до 2699.

Класифікація списків доступу в Cisco IOS включає кілька основних типів, кожен з яких має свої особливості та область застосування. Таблиця 6.2 наводить детальну інформацію про типи списків доступу та їх характеристики.

Таблиця 6.2 - Типи списків доступу в Cisco IOS

Тип ACL	**Номерний діапазон**	**Можливості фільтрації**	**Швидкість обробки**	**Застосування**
Стандартний	1-99	Лише адреси джерела	Висока	Базова фільтрація по IP-адресах
Розширений	100-199	Адреси джерела/призначення, протоколи, порти	Середня	Детальна фільтрація трафіку
Динамічний	100-199 + налаштування	Тимчасовий доступ після автентифікації	Низька	Контрольований доступ до ресурсів
Рефлексивний	Іменований розширений	Відстеження стану з'єднань	Низька	Захист від несанкціонованих з'єднань
За часом	Будь-який + розклад	Активація по розкладу	Залежно від типу	Обмеження доступу по часу

Стандартні списки доступу є найпростішим типом ACL та можуть перевіряти лише адреси джерела пакетів, що робить їх швидкими у обробці, але обмеженими за функціональністю. Розширені списки доступу надають значно більше можливостей для фільтрації, оскільки можуть аналізувати адреси джерела та призначення, тип протоколу (TCP, UDP, ICMP тощо), номери портів, що дозволяє створювати точні правила фільтрації для специфічних додатків та сервісів. Динамічні списки доступу забезпечують механізм тимчасового доступу, коли користувач спочатку автентифікується через Telnet, після чого йому відкривається доступ до ресурсів на певний період часу (зазвичай 10 хвилин за замовчуванням).

Рефлексивні ACL розроблені для вирішення проблеми асиметричного трафіку та забезпечення безпеки при встановленні з'єднань з внутрішньої мережі. Вони працюють шляхом динамічного створення тимчасових правил дозволу для відповідного трафіку на основі вихідних з'єднань, ініційованих з локальної мережі. Списки доступу з обмеженням за часом дозволяють активувати або деактивувати певні правила згідно з встановленим розкладом, що корисно для обмеження доступу співробітників до певних ресурсів у робочий час.

Принцип розміщення ACL у мережі є критично важливим для ефективної фільтрації трафіку та оптимізації мережевої продуктивності. Стандартні ACL рекомендується застосовувати якомога ближче до мережі призначення, оскільки вони фільтрують трафік лише за адресою джерела і можуть блокувати легітимний трафік, якщо будуть застосовані занадто рано в мережевому шляху. Розширені ACL, навпаки, слід розміщувати якомога ближче до джерела трафіку, оскільки їх детальні критерії фільтрації дозволяють точно ідентифікувати небажаний трафік на ранній стадії та економити мережеві ресурси.

Для адресації в списках доступу використовується спеціальний тип маски, відомий як WildCard-маска або обернена маска. WildCard-маска обчислюється шляхом віднімання звичайної мережевої маски від шаблонного значення 255.255.255.255, наприклад, для мережевої маски 255.255.255.0 відповідна WildCard-маска становитиме 0.0.0.255. У WildCard-масці біти зі значенням 0 означають, що відповідні біти в IP-адресі повинні точно збігатися, тоді як біти зі значенням 1 можуть мати будь-яке значення. Це дозволяє гнучко визначати діапазони IP-адрес для застосування правил ACL, наприклад, маска 0.0.0.255 дозволить збігатися будь-яким адресам у межах однієї підмережі класу C.

Таблиця 6.3 - Команди створення та управління ACL

Команда	**Режим**	**Призначення**
access-list <номер> permit/deny <умови>	Global Config	Створення стандартного ACL правила
access-list <номер> permit/deny <протокол> <джерело> <призначення> <порт>	Global Config	Створення розширеного ACL правила
ip access-list standard <ім'я>	Global Config	Створення іменованого стандартного ACL
ip access-list extended <ім'я>	Global Config	Створення іменованого розширеного ACL
permit/deny <умови>	Named ACL Config	Додавання правила в іменований ACL
ip access-group <ACL> in/out	Interface Config	Застосування ACL до інтерфейсу
show access-lists	Privileged EXEC	Відображення всіх налаштованих ACL
show access-lists <номер/ім'я>	Privileged EXEC	Відображення конкретного ACL
show ip interface <інтерфейс>	Privileged EXEC	Відображення ACL, застосованих до інтерфейсу
clear access-list counters	Privileged EXEC	Очищення лічильників ACL
no access-list <номер>	Global Config	Видалення всього ACL
no ip access-group <ACL> in/out	Interface Config	Видалення ACL з інтерфейсу

Створення стандартних списків доступу здійснюється для фільтрації трафіку на основі IP-адреси джерела з використанням інверсних масок (wildcard masks), які визначають які біти адреси мають точно співпадати. Приклад стандартного ACL для блокування трафіку з конкретної підмережі:

```
Router(config)# access-list 1 deny 192.168.10.0 0.0.0.255
Router(config)# access-list 1 permit any
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip access-group 1 in
Router(config-if)# exit
```

Команда access-list 1 deny 192.168.10.0 0.0.0.255 створює правило стандартного ACL номер 1, яке забороняє весь трафік з мережі 192.168.10.0/24, де інверсна маска 0.0.0.255 означає, що перші три октети повинні точно співпадати, а четвертий октет може бути будь-яким. Правило access-list 1 permit any дозволяє весь інший трафік, а команда ip access-group 1 in застосовує ACL до вхідного трафіку на зазначеному інтерфейсі.

Розширені списки доступу надають можливості детального контролю трафіку з урахуванням протоколів, портів та напрямків з'єднання. Приклад розширеного ACL для блокування HTTP-трафіку до конкретного сервера:

```
Router(config)# access-list 100 deny tcp 192.168.20.0 0.0.0.255
host 192.168.40.10 eq 80
Router(config)# access-list 100 permit ip any any
Router(config)# interface fastEthernet 1/1
Router(config-if)# ip access-group 100 in
Router(config-if)# exit
```

Правило access-list 100 deny tcp 192.168.20.0 0.0.0.255 host 192.168.40.10 eq 80 створює розширений ACL номер 100, який блокує TCP-трафік з мережі 192.168.20.0/24 до конкретного хоста 192.168.40.10 на порт 80 (HTTP). Ключове слово host еквівалентне інверсній масці 0.0.0.0 і вказує на конкретний хост, а eq 80 означає рівність номеру порту 80.

Іменовані списки доступу забезпечують кращу організацію та управління складними конфігураціями завдяки використанню описових назв замість номерів. Приклад створення іменованого розширеного ACL:

```
Router(config)# ip access-list extended BLOCK-HTTP-TO-SERVER
Router(config-ext-nacl)# deny tcp 192.168.30.0 0.0.0.255 host
192.168.40.10 eq 80
Router(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host
192.168.40.10 eq 443
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# interface fastEthernet 1/1
Router(config-if)# ip access-group BLOCK-HTTP-TO-SERVER in
Router(config-if)# exit
```

Команда ip access-list extended BLOCK-HTTP-TO-SERVER створює іменований розширений ACL з описовою назвою, що робить конфігурацію більш зрозумілою для адміністрування. Наступні правила в режимі конфігурації розширеного іменованого ACL (config-ext-nacl) послідовно забороняють HTTP-трафік (порт 80), дозволяють HTTPS-трафік (порт 443) та дозволяють весь інший IP-трафік, демонструючи гнучкість селективного контролю доступу.

Перевірка та діагностика роботи ACL здійснюється за допомогою спеціальних команд перегляду та тестових утиліт. Команда show access-lists відображає всі налаштовані списки доступу та статистику їх використання, включаючи кількість пакетів, які відповідали кожному правилу. Для тестування функціональності ACL використовуються команди ping, traceroute, telnet та веб-браузер для перевірки HTTP/HTTPS доступу, що дозволяє систематично перевіряти правильність роботи кожного правила фільтрації.

2 КЛЮЧОВІ ПИТАННЯ

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?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. Створення топології мережі

3.1.1 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.

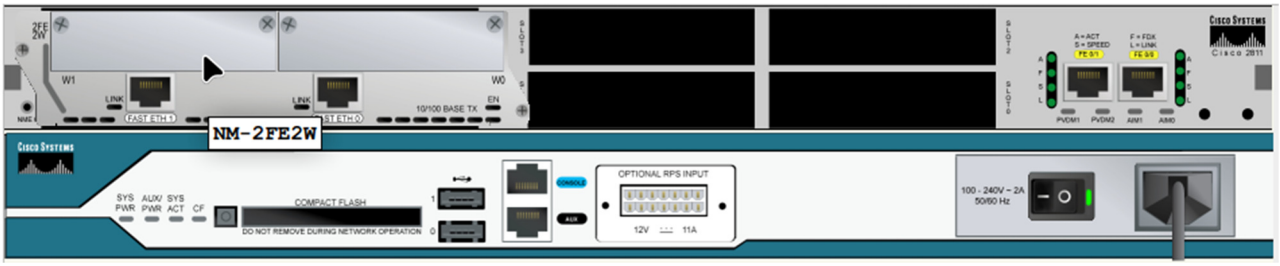

Рисунок 6.1 – Маршрутизатор Cisco 2811 з модулем NM-2FE2W

3.1.2 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).

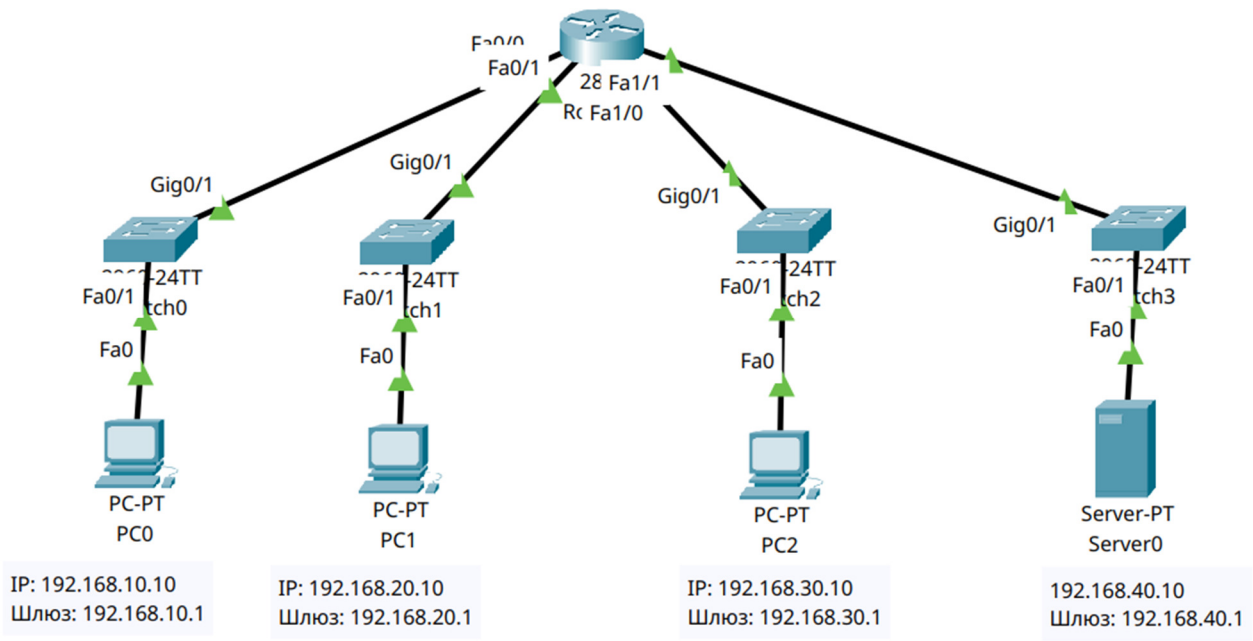

Рисунок 6.2 – Архітектура мережі для лабораторного завдання

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

3.2. Налаштування маршрутизатора

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)#
```

3.2.2 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.

3.2.3 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."
```

3.2.4 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.

3.3. Налаштування ACL

3.3.1 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.
```

3.3.2 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.

3.3.3 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.

4 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

Лабораторна робота № 7

Тема: Налаштування автономної бездротової точки доступу Cisco

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

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Розвиток стандартів бездротових мереж Wi-Fi

Бездротові мережі передачі даних пройшли значний еволюційний шлях від перших комерційних реалізацій до сучасних високошвидкісних систем. Розвиток технології Wi-Fi характеризувався послідовним збільшенням пропускної здатності, розширенням частотних діапазонів, удосконаленням методів модуляції та впровадженням механізмів множинного доступу. Кожне нове покоління стандартів IEEE 802.11 вирішувало конкретні технічні обмеження попередніх версій.

Таблиця 7.1 – Порівняльні характеристики стандартів Wi-Fi

Стандарт	Рік ухвалення	Частотний діапазон	Максимальна швидкість (теор.)	Модуляція	Канальна ширина
IEEE 802.11b	1999	2,4 ГГц	до 11 Мбіт/с	DSSS, CCK	22 МГц
IEEE 802.11a	1999	5 ГГц	до 54 Мбіт/с	OFDM	20 МГц
IEEE 802.11g	2003	2,4 ГГц	до 54 Мбіт/с	OFDM	20 МГц
IEEE 802.11n (Wi-Fi 4)	2009	2,4 та 5 ГГц	до 600 Мбіт/с	OFDM, MIMO	20/40 МГц
IEEE 802.11ac (Wi-Fi 5)	2013	5 ГГц	до 6,9 Гбіт/с	OFDM, MU-MIMO, 256-QAM	20/40/80/160 МГц
IEEE 802.11ax (Wi-Fi 6)	2019	2,4 та 5 ГГц	до 9,6 Гбіт/с	OFDMA, MU-MIMO, 1024-QAM	20/40/80/160 МГц
IEEE 802.11ax (Wi-Fi 6E)	2021	6 ГГц (крім 2,4 та 5)	до 9,6 Гбіт/с	OFDMA, MU-MIMO	20/40/80/160 МГц
IEEE 802.11be (Wi-Fi 7)	очікується 2024	2,4/5/6 ГГц	до 46 Гбіт/с	OFDMA, MLO, 4096-QAM	20–320 МГц

Перші стандарти IEEE 802.11b та IEEE 802.11a (1999 рік) заклали фундамент для майбутнього розвитку. Стандарт 802.11b працював у діапазоні 2,4 ГГц з максимальною швидкістю до 11 Мбіт/с. Стандарт 802.11a використовував діапазон 5 ГГц та метод ортогонального частотного мультиплексування (OFDM), досягаючи швидкості до 54 Мбіт/с. Стандарт IEEE 802.11g (2003) об’єднав переваги попередників, використовуючи OFDM-модуляцію в діапазоні 2,4 ГГц зі швидкістю до 54 Мбіт/с при зворотній сумісності з 802.11b.

Революційний прорив відбувся зі стандартом IEEE 802.11n (2009), який запровадив технологію MIMO (множинного входу-множинного виходу), що дозволяла використовувати кілька антен для одночасної передачі просторових потоків даних. Стандарт підтримував обидва діапазони (2,4 та 5 ГГц), пропонував об’єднання каналів для створення 40 МГц каналів і забезпечував швидкість до 600 Мбіт/с при чотирьох просторових потоках. Технологія beamforming дозволяла формувати спрямований радіопромінь, збільшуючи дальність до 70 метрів.

Стандарт IEEE 802.11ac (2013) працював виключно в діапазоні 5 ГГц. Wave 1 забезпечував швидкості до 1,3 Гбіт/с при каналах 80 МГц, тоді як Wave 2 (2015) впровадив багатокористувацьке MU-MIMO, підтримував до восьми просторових потоків та канали 160 МГц, досягаючи швидкості до 6,9 Гбіт/с. Використання 256-QAM модуляції підвищило спектральну ефективність на 33%.

Сучасне покоління IEEE 802.11ax (Wi-Fi 6, 2019) принципово змінило підхід через перехід до OFDMA, який дозволяє ділити канал на субканали та обслуговувати кілька клієнтів одночасно, підвищуючи ефективність у щільних середовищах. Стандарт також впровадив BSS Coloring для зменшення взаємних завад, 1024-QAM модуляцію та Target Wake Time для зниження енергоспоживання. Wi-Fi 6E (2021) додав підтримку діапазону 6 ГГц без застарілого обладнання.

1.2 Еволюція корпоративних точок доступу Cisco Aironet

Компанія Cisco Systems протягом двох десятиліть займає провідні позиції на ринку корпоративного бездротового обладнання. Лінійка Cisco Aironet, а пізніше Catalyst, еволюціонувала від простих точок доступу до інтелектуальних пристроїв з функціями радіочастотного моніторингу, виявлення вторгнень та інтеграції з системами управління мережею. Кожне покоління характеризувалося підтримкою нових стандартів Wi-Fi та впровадженням власних технологій для підвищення надійності, безпеки та ефективності.

Ранні моделі Aironet 1200 підтримували стандарти 802.11b/a/g з базовим шифруванням WEP та ранніми версіями WPA. Моделі 1130 та 1240 додали підтримку декількох SSID та режиму mesh-мережі для розширення покриття.

Перехід до 802.11n ознаменувався серіями Aironet 1600, 2600 та 3600 з підтримкою MIMO. Модель 3600 з конфігурацією 4×4:3 MIMO забезпечувала швидкість до 450 Мбіт/с. Технологія CleanAir використовувала спектральний

процесор для моніторингу радіочастотного середовища та виявлення завад. ClientLink покращував зв’язок зі старими пристроями через beamforming.

Таблиця 7.2 – Еволюція точок доступу Cisco за поколіннями Wi-Fi

Покоління Wi-Fi	Стандарт IEEE	Орієнтовні роки	Серії Cisco (приклади)	Просторові потоки (MIMO)	Основні технології	Типові швидкості
Wi-Fi 1/2	802.11b (1999), 802.11a/g (2003)	2000-2005	Aironet 1200, 1130, 1240	1×1 (без MIMO)	WEP/WPA, 2.4 і 5 ГГц, базові радіомодулі	до 11 Мбіт/с (b), до 54 Мбіт/с (a/g)
Wi-Fi 3	802.11n	2007-2012	Aironet 1600, 2600, 3600, також 3500, 3700 (із модулем ac)	2×2:2, 3×3:2, 4×4:3	MIMO, Channel Bonding (40 МГц), ClientLink, CleanAir	до 450 Мбіт/с (3 SS)
Wi-Fi 4 → перехід на ac	802.11ac Wave 1	2013-2015	Aironet 1700, 2700, 3700	3×3:3, 4×4:3	80 МГц канали, Beamforming, ClientLink 3.0	до ~1,3 Гбіт/с
Wi-Fi 5	802.11ac Wave 2	2015-2018	Aironet 1800, 2800, 3800, 4800	4×4:4 (MU-MIMO)	MU-MIMO, 160 МГц канали, CleanAir, wIPS	до ~2,6–3,5 Гбіт/с
Wi-Fi 6	802.11ax	2019-2021	Catalyst 9105, 9115, 9120, 9130	4×4, 8×8 (залежно від моделі)	OFDMA, MU-MIMO uplink/downlink, BSS Coloring	до ~5 Гбіт/с
Wi-Fi 6E	802.11ax (з 6 ГГц)	2021-тепер	Catalyst 9136, 9162/9164/9166	4×4, 8×8	Додатковий діапазон 6 ГГц, вбудовані датчики, IoT-радіо	5–10 Гбіт/с
Wi-Fi 7	802.11be	~2024+	очікувані Catalyst наступного покоління	до 16×16 (теоретично)	Multi-Link Operation, 320 МГц канали	> 30 Гбіт/с (теоретично)

Серія Aironet 2700 (включаючи AIR-CAP2702I-E-K9) представляє покоління 802.11ac Wave 1. Ці точки підтримують гігабітні швидкості в діапазоні 5 ГГц. Модель 2702I має конфігурацію 4×4:3 MIMO, забезпечуючи швидкість до 1,3 Гбіт/с при каналах 80 МГц та 256-QAM модуляції. Індекс “I” означає внутрішні інтегровані антени, “E” – відповідність європейським нормам.

Технологічний стек серії 2700 включає ClientLink 3.0 для адаптивного beamforming, VideoStream для оптимізації відеоконтенту та BandSelect для балансування навантаження між діапазонами 2,4 та 5 ГГц.

Серії 1800, 2800, 3800 та 4800 підтримують 802.11ac Wave 2 з MU-MIMO, що дозволяє одночасну передачу даних кільком клієнтам. Моделі підтримують канали 160 МГц, досягаючи швидкостей 2,6-3,5 Гбіт/с при 4×4:4 MIMO, та включають вбудовані можливості wIPS.

Сучасна серія Catalyst 9100 підтримує Wi-Fi 6 (802.11ax) та працює під управлінням Cisco IOS-XE. Моделі 9120 та 9130 пропонують конфігурації до 8×8:8 MIMO зі швидкостями близько 5 Гбіт/с. Серія 9136 та моделі 916x представляють Wi-Fi 6E з діапазоном 6 ГГц та інтегрованими IoT-радіомодулями для Bluetooth Low Energy та Zigbee.

1.3 Архітектурні режими роботи точок доступу Cisco

Корпоративні точки доступу Cisco підтримують дві принципово різні архітектури розгортання: автономний та контролерний режими. Ці підходи відображають еволюцію від децентралізованих до централізованих систем. Розуміння архітектур критично важливе для проектування ефективних мереж, оскільки перехід між режимами потребує зміни прошивки та переналаштування інфраструктури.

Автономний режим (Autonomous/Standalone) представляє децентралізовану архітектуру, де кожна точка доступу функціонує як самостійний пристрій з повним набором функцій управління, маршрутизації та безпеки. Точка працює під управлінням Cisco IOS і надає адміністратору повний CLI-доступ. Автономні точки маркуються префіксом AIR-AP (наприклад, AIR-AP2702I-E-K9).

В автономному режимі вся обробка даних (розшифрування, фільтрація, застосування QoS, інкапсуляція в VLAN) виконується локально на процесорі точки доступу. Це створює розподілену архітектуру з високою відмовостійкістю – вихід з ладу однієї точки не впливає на решту. Конфігурація виконується індивідуально через CLI, веб-інтерфейс або SNMP. Цей підхід оптимальний для невеликих мереж (до 10-20 точок доступу) або спеціалізованих сценаріїв (бездротові мости, mesh-топології).

Контролерний режим (Controller-based/Lightweight), або CAPWAP режим, представляє централізовану архітектуру, де точки функціонують як “тонкі” пристрої, делегуючи логіку управління центральному контролеру (WLC). Точки маркуються префіксом AIR-CAP (наприклад, AIR-CAP2702I-E-K9) і після завантаження автоматично виявляють контролер через широкомовні запити, DNS-запити, DHCP-опцію 43 або статичну адресу.

Після встановлення захищеного CAPWAP-тунелю легковагова точка отримує від контролера всю конфігурацію (параметри радіо, SSID, політики безпеки, прошивку). Трафік за замовчуванням інкапсулюється в CAPWAP-тунель та передається до контролера для централізованої обробки. Це дозволяє контролеру приймати глобальні рішення щодо балансування навантаження, роумінгу без втрати сесії, централізованих політик безпеки та функцій wIDS/wIPS. Контролерна архітектура оптимальна для середніх та великих мереж з десятками або сотнями точок доступу.

Принципова різниця: автономні точки не потребують додаткової інфраструктури та працюють відразу, але вимагають індивідуального адміністрування. Контролерні точки потребують WLC, але забезпечують централізоване управління через єдиний інтерфейс. Автономні точки

виконують локальну комутацію трафіку, тоді як контролерні використовують централізовану комутацію за замовчуванням (з підтримкою режиму FlexConnect для віддалених локацій).

У даній лабораторній роботі використовується точка доступу Cisco AIR-CAP2702I-E-K9, яка є пристроєм класу Enterprise, призначеним для встановлення у корпоративних та навчальних мережах. Її корпус має компактну квадратну форму з заокругленими кутами та виконаний з білого ударостійкого пластику, що забезпечує стійкість до механічних пошкоджень та відповідає вимогам естетики сучасних офісів та аудиторій (рис. 7.1). На верхній панелі розташовано логотип Cisco та індикаторний світлодіод, який візуально відображає стан пристрою: зелений — нормальна робота, помаранчевий (амбру) — режим конфігурації або оновлення ПЗ, червоний — помилка або завантаження. Цей дизайн дозволяє легко ідентифікувати пристрій навіть з відстані та швидко оцінити його робочий стан без необхідності підключення до CLI.

Рисунок 7.1 – Зовнішній вигляд точки доступу Cisco AIR-CAP2702I-E-K9

На задній панелі точки доступу розміщено всі фізичні порти та кнопки управління. У центрі — один гігабітний Ethernet-порт (GigabitEthernet0), який використовується як основний аплінк до комутатора навчальної мережі. Праворуч від нього розташований консольний порт (RJ-45) для початкового налаштування через серійний кабель, а також AUX-порт, який може використовуватися для додаткових службових функцій. Нижче розташована кнопка MODE, яка служить для перемикання режимів роботи пристрою (наприклад, автономний/контролерний) або запуску процедури скидання налаштувань. Поруч з нею знаходиться індикатор STATUS, який показує поточний режим роботи (червоний — резерв, зелений — активний). Також на задній панелі видно маркування 802.11ac Wave 1, що підтверджує підтримку сучасних стандартів Wi-Fi, а також інформацію про напругу живлення (DC 48 В) та серійний номер пристрою. Живлення подається через гніздо DC IN 48V, але точка доступу може отримувати живлення також через PoE (Power over Ethernet) з порту GigabitEthernet0.

Підключення до точки доступу здійснюється через стандартний RJ-45 Ethernet-кабель до порту GigabitEthernet0, який у конфігурації використовується як основний аплінк до комутатора навчальної мережі. Для конфігурування пристрою спочатку використовується консольний порт, до якого підключається кабель RJ-45 → DB-9 або USB-serial адаптер. Після завершення базового налаштування доступ до пристрою можна отримати через веб-інтерфейс або SSH за IP-адресою, отриманою через DHCP на віртуальному інтерфейсі BVI1. Важливо підключати точку доступу лише до мережевих пристроїв, які підтримують PoE (Power over Ethernet), оскільки живлення надходить через Ethernet-кабель, а не окремий блок живлення.

Фізична конструкція пристрою передбачає можливість монтажу на стелі або стіні за допомогою спеціального кріплення (не показано на фото), що дозволяє оптимально розмістити антени для покриття бездротової зони. Два внутрішніх радіомодулі (2.4 ГГц та 5 ГГц) забезпечують одночасну роботу у двох діапазонах, а їхня продуктивність контролюється через CLI-команди, які дозволяють фіксувати канали, встановлювати потужність сигналу та налаштовувати безпеку. Таким чином, хоча зовнішній вигляд пристрою простий та лаконічний, його внутрішня архітектура та функціональність дозволяють реалізовувати складні мережеві сценарії, включаючи прозоре мостування, WPA2-безпеку та віддалене управління.

Точка доступу Cisco AIR-CAP2702I-E-K9, працюючи в автономному (standalone) режимі під управлінням операційної системи Cisco IOS, реалізує складну внутрішню архітектуру, яка поєднує фізичні, логічні та віртуальні компоненти для забезпечення повноцінної інтеграції бездротових клієнтів у провідну інфраструктуру (рис. 7.2). Ця архітектура побудована навколо концепції мосту на канальному рівні (L2), що дозволяє пристрою функціонувати як прозорий комутатор, об'єднуючи провідні та бездротові інтерфейси в єдину broadcast-домену.

Фізичні інтерфейси формують апаратну основу пристрою:

– GigabitEthernet0 — єдиний гігабітний Ethernet-порт, призначений для підключення до провідної мережі (аплінк). Він є єдиною точкою входу та виходу для всього трафіку, який проходить між бездротовою зоною та зовнішньою інфраструктурою;

– Dot11Radio0 — радіомодуль, що працює в діапазоні 2.4 ГГц і підтримує стандарти 802.11b/g/n;

– Dot11Radio1 — радіомодуль, що працює в діапазоні 5 ГГц і підтримує стандарти 802.11a/n/ac (Wave 1).

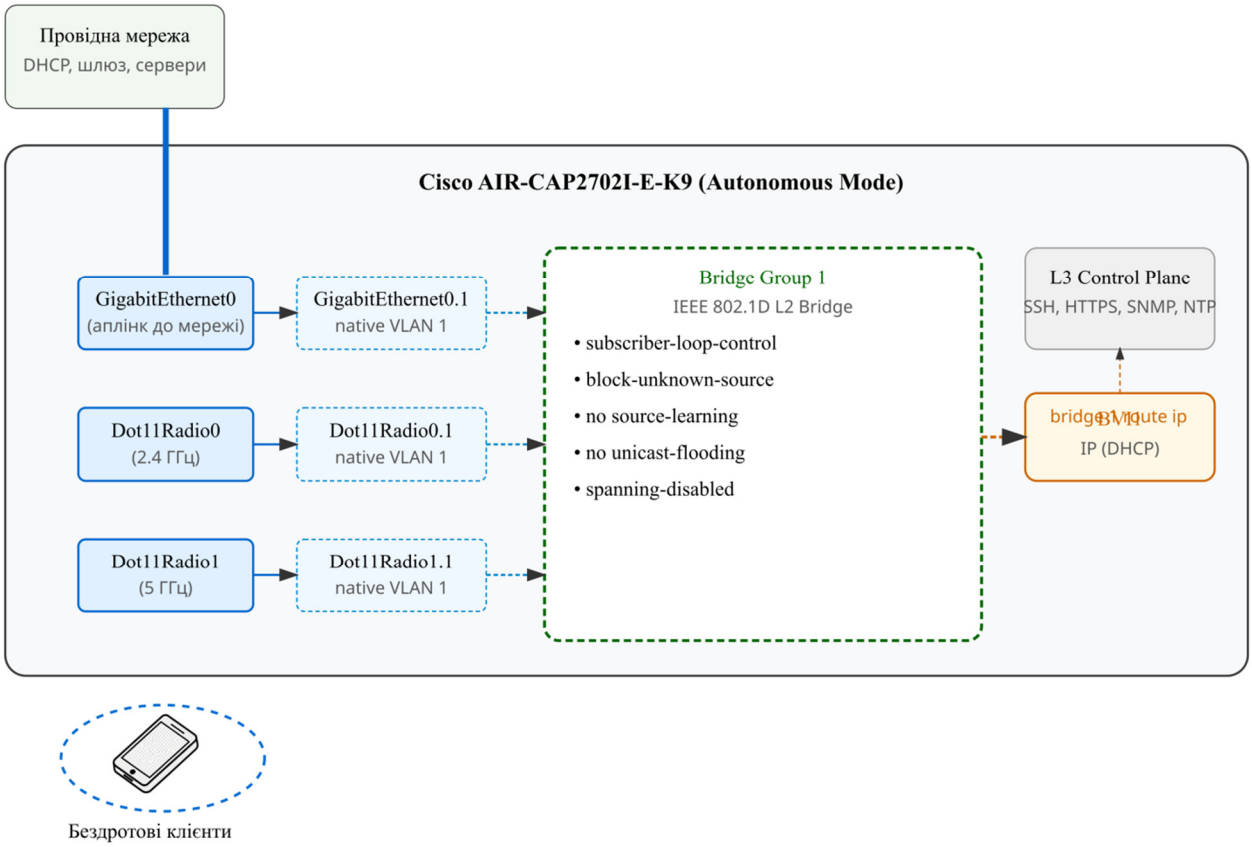

Рисунок 7.2 – Внутрішня архітектура точки доступу Cisco AIR-CAP2702I-E-K9 в автономному режимі

Для підтримки VLAN та гнучкої сегментації трафіку на кожному фізичному інтерфейсі створюються логічні субінтерфейси. Найпоширенішою конфігурацією для невеликих мереж є створення субінтерфейсів для native VLAN (як правило, VLAN 1). Ці субінтерфейси GigabitEthernet0.1, Dot11Radio0.1 та Dot11Radio1.1 всі налаштовуються з командою encapsulation dot1Q 1 native і служать для передачі untagged-трафіку.

Ключовим елементом архітектури є Bridge Group — логічний міст, який об'єднує всі субінтерфейси в єдину комутаційну таблицю на рівні L2. За замовчуванням використовується Bridge Group 1 з протоколом ieee (802.1D). Команда bridge 1 route ip активує можливість обробки IP-трафіку, що критично для роботи віртуального інтерфейсу управління.

Для забезпечення можливості віддаленого управління (через SSH, веб-інтерфейс, SNMP) на рівні мережі (L3) створюється Bridge Virtual Interface (BVI1). Цей віртуальний інтерфейс не бере участі у передачі клієнтського трафіку. Замість цього, він асоційований з Bridge Group 1 і отримує власну IP-адресу (наприклад, через DHCP), що дозволяє адміністратору підключатися до пристрою як до звичайного мережевого хоста.

Конфігурація безпеки та бездротових мереж зосереджена навколо глобального об'єкта SSID. Команда dot11 ssid <ім'я> створює профіль, який визначає такі параметри, як:

– Асоційований VLAN (vlan 1)
– Метод аутентифікації (authentication open);

– Механізм управління ключами (authentication key-management wpa version 2);

– Попередньо встановлений ключ (wpa-psk);

– Видимість мережі (guest-mode).

Цей профіль є логічним контейнером, який потім явно призначається до одного або обох радіоінтерфейсів через команду ssid <ім'я> в їх конфігурації. На радіоінтерфейсах також налаштовується шифрування (encryption vlan 1 mode ciphers aes-ccm), що є обов'язковим для стандартів WPA2.

Окрім основних інтерфейсів, точка доступу має ряд службових компонентів:

– Консольний (console) та AUX-порти для локального управління та діагностики;

– Веб-сервери HTTP/HTTPS, які надають графічний інтерфейс управління;

– Система облікових записів користувачів, яка використовується для аутентифікації при віддаленому доступі (SSH, веб);

– Системні процеси IOS, такі як CDP, SNMP-агент, NTP-клієнт, які забезпечують взаємодію з іншими мережевими пристроями.

Таким чином, внутрішня архітектура точки доступу являє собою дві логічні площини: площина даних (data plane), зосереджена навколо Bridge Group і відповідальна за прозору передачу кадрів клієнтів, та площина управління (management plane), представлена BVI1 та службовими процесами, яка забезпечує налаштування, моніторинг і обслуговування пристрою. Це розділення дозволяє точці доступу ефективно виконувати свою роль як автономного мережевого пристрою, не вимагаючи додаткової інфраструктури, такої як контролер.

1.4 Принципи роботи бездротового моста в точках доступу

Концепція бездротового моста в точках доступу Cisco відноситься до механізму інтеграції бездротових клієнтів у провідну інфраструктуру через прозоре об’єднання сегментів мережі на канальному рівні OSI. Точка доступу, налаштована як прозорий міст, виконує функцію інтелектуального посередника, який вивчає MAC-адреси пристроїв, приймає рішення про пересилання кадрів та створює єдиний broadcast-домен для провідних і бездротових учасників. Це дозволяє бездротовим клієнтам отримувати IP-адреси від того самого DHCP-сервера та взаємодіяти з мережевими службами без додаткової трансляції адрес.

Принцип роботи базується на алгоритмах навчання та фільтрації IEEE 802.1D. Коли кадр надходить на інтерфейс точки доступу, пристрій аналізує MAC-адресу джерела та додає або оновлює запис у таблиці MAC-адрес, асоціюючи адресу з інтерфейсом. Після цього аналізується адреса призначення: якщо вона асоційована з тим самим інтерфейсом, кадр відкидається (filtering);

якщо з іншим – пересилається тільки туди (forwarding); якщо не знайдена або це broadcast/multicast – реплікується на всі активні інтерфейси (flooding).

У точці доступу Cisco в автономному режимі створюється bridge group – віртуальний комутатор, який об'єднує фізичні та логічні інтерфейси. Типова конфігурація включає Ethernet-інтерфейс (GigabitEthernet0) та радіоінтерфейси (Dot11Radio0 для 2,4 ГГц та Dot11Radio1 для 5 ГГц), кожен може бути розділений на субінтерфейси для VLAN. Команда bridge N protocol ieee ініціалізує протокол IEEE 802.1D з підтримкою Spanning Tree Protocol.

Критична особливість конфігурації радіоінтерфейсів – вимкнення автоматичного навчання MAC-адрес (no bridge-group 1 source-learning) та unicast flooding (no bridge-group 1 unicast-flooding). Це запобігає занесенню в таблицю адрес клієнтів з інших SSID або мереж, усуваючи вразливості безпеки типу MAC spoofing. Вимкнення unicast flooding запобігає надмірному навантаженню на спільне бездротове середовище.

Для управління точкою доступу на мережевому рівні створюється віртуальний інтерфейс BVI (Bridge Virtual Interface), який представляє bridge group як єдиний L3-інтерфейс з IP-адресою, маршрутом за замовчуванням та протоколами управління (SSH, HTTPS, SNMP, NTP). BVI не передає трафік користувачів, а слугує виключно для адміністративного доступу. Команда bridge 1 route ip активує на мосту маршрутизацію IP-пакетів, необхідну для функціонування BVI. Рисунок 7.3 ілюструє архітектуру точки доступу в режимі прозорого моста.

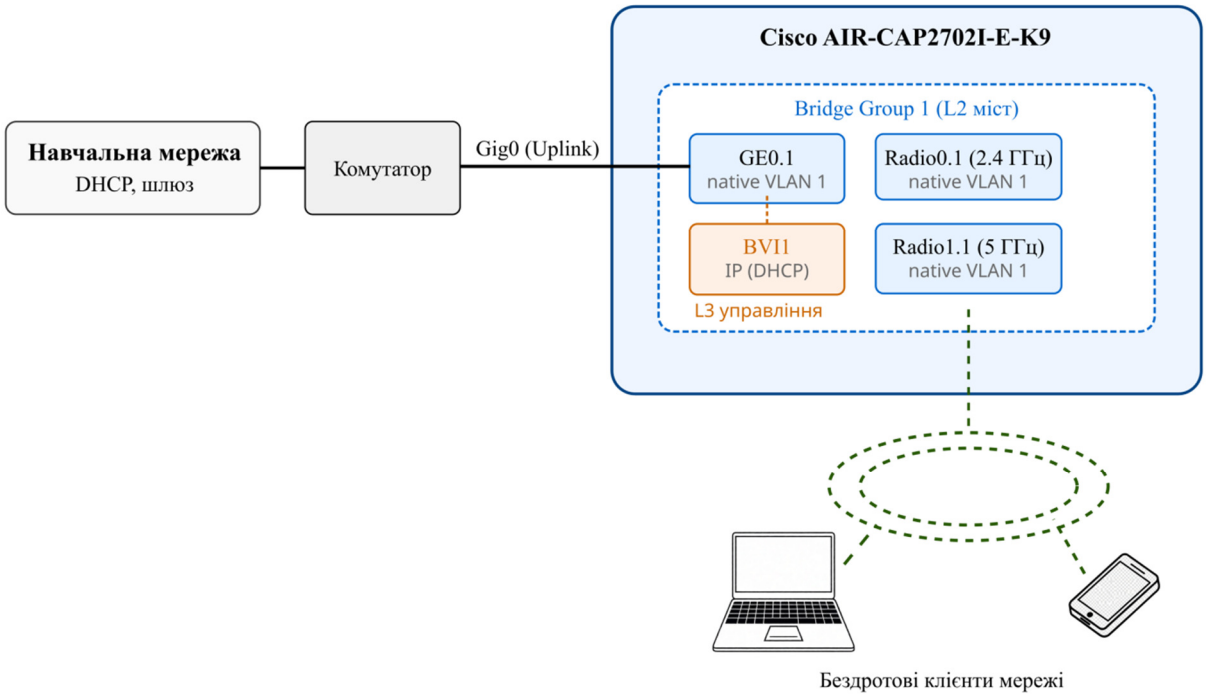

Рисунок 7.3 – Архітектура точки доступу в режимі прозорого моста

У налаштованій конфігурації точка доступу функціонує як прозорий L2-міст. Коли бездротовий клієнт надсилає IP-пакет до провідної мережі, точка розшифровує 802.11-кадр за допомогою WPA2-PSK, витягує Ethernet-кадр,

визначає за таблицею комутації Bridge Group 1, що адреса призначення знаходиться в провідному сегменті, та пересилає кадр через GigabitEthernet0. У зворотному напрямку міст ідентифікує MAC-адресу як бездротового клієнта, визначає відповідний радіоінтерфейс, інкапсулює кадр у 802.11-фрейм, шифрує його AES-CCM та передає по радіоканалу. Весь процес прозорий для клієнта та інших пристроїв, забезпечуючи єдину broadcast-домену та спільну IP-підмережу.

1.5 Особливості налаштування SSID, безпеки та радіоінтерфейсів

Конфігурування автономної точки доступу Cisco AIR-CAP2702I-E-K9 здійснюється через CLI, організований у вигляді ієрархічної структури режимів. Точка доступу підтримує кілька режимів роботи. У рамках роботи використовується автономний режим з функцією прозорого L2-моста між бездротовими клієнтами та провідною інфраструктурою. Основні команди CLI групуються за функціональними блоками (табл. 7.3).

Таблиця 7.3 — Групи основних команд CLI для конфігурування точки доступу

Функціональна група	Команда	Пояснення
Вхід у режими	enable	Переходить у привілейований EXEC-режим (пароль за замовчуванням: Cisco)
	configure terminal	Входить у глобальний режим конфігурації
	interface <ім'я>	Входить у режим конкретного інтерфейсу (Dot11Radio0, BVI1)
	dot11 ssid <ім'я>	Створює або редагує глобальний профіль SSID
Базова ідентифікація	hostname CAP2702I	Задає ім’я пристрою для ідентифікації в мережі
	no service pad	Вимикає застарілий сервіс X.25 PAD
	service timestamps log/debug datetime msec	Додає мілісекундні часові мітки до повідомлень
	no ip domain-lookup	Вимикає DNS-запити при невідомих командах
	ip http serverip http secure-server	Активує веб-інтерфейс через HTTP та HTTPS
Налаштування моста	bridge 1 protocol ieee	Вмикає стандартний протокол мосту IEEE 802.1D
	bridge 1 route ip	Дозволяє мосту передавати IP-трафік (необхідно для BVI)
	interface GigabitEthernet0no shutdown	Активує фізичний провідний інтерфейс (аплінк)
Субінтерфейси	interface <інтерфейс>.1encapsulation dot1Q 1 native	Створює субінтерфейс для нативного VLAN 1
	bridge-group 1	Приєднує інтерфейс до Bridge Group 1
	bridge-group 1 block-unknown-source	Блокує трафік від невідомих MAC-адрес

	no bridge-group 1 source-learning	Вимикає автоматичне навчання MAC-адрес на радіо
	no bridge-group 1 unicast-flooding	Вимикає unicast flooding
Інтерфейс управління	interface BVI1ip address dhcpno shutdown	Налаштовує L3-інтерфейс для управління через DHCP
Профіль SSID	dot11 ssid Cisco_2702I	Визначає ім’я бездротової мережі
	vlan 1	Прив’язує SSID до VLAN 1
	authentication open	Дозволяє клієнтам ініціювати асоціацію
	authentication key-management wpa version 2	Вмикає WPA2 як метод управління ключами
	wpa-psk ascii 0 <пароль>	Встановлює попередньо встановлений ключ у відкритому вигляді
	guest-mode	Транслює SSID у маячкових кадрах
Радіоінтерфейси	interface Dot11Radio0/1no shutdown	Активує радіомодулі 2.4 ГГц або 5 ГГц
	encryption vlan 1 mode ciphers aes-ccm	Вмикає обов’язкове для WPA2 шифрування AES-CCM
	ssid Cisco_2702I	Прив’язує радіо до профілю SSID
	station-role root	Визначає роль як кореневого пристрою
	channel <номер>	Встановлює фіксований канал (наприклад, 6 для 2.4 ГГц)
Управління доступом	username <ім'я> privilege 15 secret <пароль>	Створює локального користувача з повними правами
	line vty 0 4login localtransport input ssh	Налаштовує SSH з локальною аутентифікацією
Збереження	end	Виходить із режиму конфігурації
	write memory абоcopy running-config startup-config	Зберігає конфігурацію у NVRAM
Перевірка роботи	show ip interface brief	Показує IP-адреси всіх інтерфейсів (включаючи BVI1)
	show running-config	Виводить поточну активну конфігурацію
	show dot11 associations	Відображає список асоційованих клієнтів
	show bridge	Показує таблицю MAC-адрес моста та стан Bridge Group
	show controllers dot11radio0/1	Виводить діагностичну інформацію про радіомодуль
	ping <адреса>	Перевіряє зв’язність з іншими хостами

Ключові команди відіграють наступну роль. Команда dot11 ssid <ім'я> створює глобальний профіль бездротової мережі – логічний контейнер для налаштування аутентифікації, шифрування та VLAN-асоціації. Команда authentication open відповідає за початковий етап асоціації клієнта згідно зі стандартом 802.11, а authentication key-management wpa version 2 разом з wpa-psk активує WPA2-Personal з попередньо встановленим ключем. Опція guest-mode забезпечує трансляцію SSID у beacon frames, роблячи мережу видимою для клієнтських пристроїв.

Команда bridge-group 1 у контексті субінтерфейсів формально об’єднує їх у єдину логічну broadcast-домену, забезпечуючи прозору комутацію на канальному рівні. Додаткові параметри (block-unknown-source, no source-learning, no unicast-flooding) підвищують безпеку шляхом обмеження неавторизованого трафіку та зменшення навантаження на радіоінтерфейси. Команда station-role root визначає роль точки доступу як основної базової станції, що є типовим для автономного режиму з підключенням до провідної інфраструктури. Команда interface BVI1 з призначенням IP-адреси дозволяє організувати L3-доступ до пристрою для управління, не втручаючись у трафік клієнтів. Команда write memory є обов’язковою для збереження конфігурації у NVRAM, щоб зміни залишилися після перезавантаження.

2 КЛЮЧОВІ ПИТАННЯ

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?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. 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#
```

3.2. 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
```

3.3. 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
```

3.4. 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-loop-
control
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-loop-
control
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
```

3.5. 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
```

3.6. 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
```

3.7. 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
```

3.8. 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
```

3.9. 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*.

4 ЗМІСТ ПРОТОКОЛУ

Протокол лабораторної роботи оформлюється згідно з загальноприйнятими вимогами до навчальної документації: шрифт Times New Roman, розмір 12 pt, міжрядковий інтервал 1,5. Протокол складається з трьох обов’язкових частин, які розташовуються у наступній послідовності.

1. Вступна частина. У цьому розділі зазначаються тема та мета лабораторної роботи, прізвище, ім’я та по батькові студента, назва академічної групи, а також прізвище, ім’я та по батькові викладача. Мета формулюється у відповідності до навчальних цілей дисципліни та вимог методичних рекомендацій. Також у цьому розділі подаються відповіді на ключові питання, передбачені завданням. Кожна відповідь має бути чіткою, лаконічною, ґрунтуватися на теоретичному матеріалі лабораторної роботи та демонструвати розуміння студентом ключових положень теми.

2. 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 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.

3. Висновкова частина. У цьому розділі студент 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.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

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

2. 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.

3. Азаров О. Д. Комп’ютерні мережі : підручник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін. – Вінниця : ВНТУ, 2020. – 378 с.

4. 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.

5. Блозва А.І. Комп’ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с.

6. Тарбаєв С.І. Проектування інфокомунікаційних мереж. Навчальний посібник. – Київ: ННІТІ ДУТ, 2019. – 186 ст.

7. Задерейко О. В. Комп’ютерні мережі : навчальний посібник [Електронне видання] / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса : Фенікс, 2022. – 249 с.

8. Comer D. E. Computer Networks and Internets. Global Edition : textbook / D. E. Comer. – 6th ed. – Boston : Pearson Education, 2016. – 672 p.

9. Kurose J. F. Computer Networking: A Top-Down Approach : textbook / J. F. Kurose, K. W. Ross. – 8th ed. – Boston : Pearson Education, 2021. – 864 p.

10. Peterson L. L. Computer Networks: A Systems Approach : textbook / L. L. Peterson, B. S. Davie. – 6th ed. – Amsterdam : Morgan Kaufmann, 2021. – 896 p.

11. Goralski W. The Illustrated Network: How TCP/IP Works in a Modern Network : textbook / W. Goralski. – 2nd ed. – Amsterdam : Morgan Kaufmann, 2017. – 936 p.

12. Odom W. CCNA 200-301 Official Cert Guide. Volume 1 / W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 1024 p.

13. Odom W. CCNA 200-301 Official Cert Guide. Volume 2 / W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 992 p.

14. Sequeira A. J. CCNA 200-301 Hands-on Mastery with Packet Tracer : practical guide / A. J. Sequeira, R. Wong. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 704 p.

15. Sanders C. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems : textbook / C. Sanders. – 3rd ed. – San Francisco : No Starch Press, 2021. – 432 p.

16. Limoncelli T. A. The Practice of Network and System Administration : textbook / T. A. Limoncelli, C. J. Hogan, S. R. Chalup. – 2nd ed. – Boston : Addison-Wesley, 2020. – 1040 p.

17. Hucaby D. CCNA 200-301 Portable Command Guide : reference guide / D. Hucaby, W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 352 p.