Педяш В.В., Йона Л.Г., Мазур Г.Д.

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації для практичних та лабораторних занять (частина 2)

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 2)
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 2) [Електронне видання] / Педяш В.В., Йона Л.Г., Мазур Г.Д. — Кафедра комп’ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. — Одеса, 2025. — 142 с.

Методичні рекомендації до практичних та лабораторних занять з дисципліни «Комп'ютерні мережі» (друга частина) розроблено відповідно до навчального плану підготовки здобувачів вищої освіти. Посібник охоплює наступні сім лабораторних робіт (№ 8–14), спрямованих на освоєння сучасних технологій маршрутизації, безпеки та централізованого управління мережею. Матеріали містять детальні інструкції щодо виконання завдань, спрямованих на налаштування, конфігурацію та адміністрування мережевих сервісів і механізмів, а також забезпечення безпеки та моніторингу мережевої інфраструктури.

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 сучасного підприємства неможлива без застосування складних технологій маршрутизації, безпеки та централізованого управління мережею. Розуміння принципів роботи динамічних протоколів маршрутизації, механізмів захисту трафіку, трансляції адрес та систем моніторингу є ключовою компетенцією фахівця з інформаційних технологій та електронних комунікацій, оскільки саме ці технології забезпечують надійність, масштабованість та безпеку корпоративних мереж будь-якого рівня складності. Друга частина курсу «Комп'ютерні мережі», що викладається у другому семестрі навчання, спрямована на формування практичних навичок проектування та адміністрування складних мережевих інфраструктур з використанням сучасних протоколів та механізмів забезпечення безперервності роботи та захисту інформації.

Дані методичні рекомендації призначені для використання під час проведення практичних і лабораторних занять з дисципліни «Комп'ютерні мережі» та охоплюють матеріали другої частини курсу, яка включає наступні сім навчальних робіт. Кожна робота побудована за єдиною логічною структурою, що забезпечує послідовний перехід від опрацювання теоретичних положень до виконання практичних завдань і сприяє глибокому засвоєнню навчального матеріалу. Лабораторні роботи охоплюють такі ключові теми: реалізація відмовостійкої маршрутизації за допомогою резервних статичних маршрутів, конфігурування протоколів динамічної маршрутизації OSPF та EIGRP, механізми трансляції адрес (PAT/NAT) та автоматичного призначення адрес (DHCP), централізована автентифікація за допомогою RADIUS та AAA, побудова захищених міжсайтових з'єднань на основі IPsec VPN, а також централізований моніторинг мережі за допомогою протоколів SNMP та Syslog.

Практичні заняття проводяться на основі розділу «Ключові положення», у якому викладено необхідні теоретичні відомості, подано пояснення принципів роботи складних мережевих технологій і протоколів, а також наведено технічні характеристики обладнання, аналітичні узагальнення та порівняльні характеристики різних підходів до вирішення однієї задачі. Опрацювання цього матеріалу дозволяє студентам сформувати системне розуміння теми, підготуватися до виконання практичних дій і усвідомлено підійти до розв'язання завдань лабораторної роботи з урахуванням реальних обмежень та вимог до безпеки мережевої інфраструктури.

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, доступному в лабораторіях факультету кібербезпеки, програмної інженерії та комп'ютерних наук.

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 складні мережеві сценарії та відпрацьовувати конфігурації без залучення фізичного обладнання, водночас зберігаючи можливість переходу до більш складних і наближених до реальних умов рішень. Сформовані у другому семестрі компетенції створюють основу для подальшого вивчення спеціалізованих дисциплін з інформаційних технологій та управління інформаційною безпекою, а також для підготовки до міжнародних сертифікацій, таких як Cisco Certified Network Associate (CCNA) та вищих рівнів сертифікації в галузі мережевих технологій.

Лабораторна робота № 8

Тема: Відмовостійка маршрутизація з використанням плаваючих статичних маршрутів

Мета роботи: Набути практичних навичок реалізації відмовостійкої маршрутизації шляхом використання плаваючих статичних маршрутів

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Вступ до концепції відмовостійкої маршрутизації

Сучасні комп’ютерні мережі є критичною інфраструктурою для функціонування бізнесу, освіти та державного управління, тому забезпечення їх безперервної роботи є однією з ключових задач мережевих інженерів. Відмовостійкість мережі — це здатність системи автоматично відновлювати зв’язність після виникнення аварійних ситуацій, таких як обрив кабелю, відмова інтерфейсу або вихід з ладу мережевого обладнання, без втручання людини-адміністратора. У реальних умовах мережеві інженери часто стикаються з необхідністю забезпечити резервування шляхів передачі даних навіть у невеликих організаціях, де впровадження складних динамічних протоколів маршрутизації може бути економічно неоправданим або надмірно складним з точки зору адміністрування. Саме для таких сценаріїв механізм резервних статичних маршрутів, відомий як floating static routes, стає ефективним та простим у реалізації рішенням, яке не вимагає додаткових ліцензій або спеціалізованого обладнання. Лабораторна робота №8 спрямована на формування у студентів практичних навичок проектування відмовостійких мереж на основі базових механізмів статичної маршрутизації, що є фундаментальною компетенцією для фахівців у сфері кібербезпеки та мережевих технологій. Під час виконання роботи студенти опановують принципи вибору маршрутів на основі адміністративної відстані, навчаються моделювати аварійні ситуації та аналізувати поведінку мережі під час автоматичного перемикання на резервний шлях, що формує системне розуміння механізмів забезпечення надійності мережевої інфраструктури.

У контексті навчання кібербезпеки важливо розуміти, що відмовостійкість є не лише технічною характеристикою мережі, а й елементом загальної стратегії безпеки інформаційних систем. Атаки типу «відмова в обслуговуванні» (DoS) або фізичне пошкодження мережевої інфраструктури можуть призвести до повної втрати зв’язку між критичними компонентами системи, тому наявність альтернативних шляхів передачі даних є обов’язковою вимогою для захисту від таких загроз. Механізм floating static routes демонструє, як навіть найпростіші інструменти маршрутизації можуть бути ефективно використані для підвищення стійкості мережі до зовнішніх впливів та внутрішніх відмов. Ця лабораторна робота створює основу для подальшого вивчення більш складних механізмів забезпечення відмовостійкості, таких як

протоколи динамічної маршрутизації з вбудованими механізмами швидкого відновлення (наприклад, OSPF з підтримкою BFD) або технології балансування навантаження між кількома шляхами. Таким чином, опанування базових принципів резервування на рівні статичної маршрутизації є необхідним кроком у формуванні професійних компетенцій майбутнього фахівця з кібербезпеки.

1.2 Теоретичні основи статичної маршрутизації та адміністративної відстані

Статична маршрутизація є одним із найпростіших механізмів визначення шляхів передачі даних у комп’ютерних мережах, при якому маршрути до віддалених мереж налаштовуються адміністратором вручну без участі автоматичних протоколів обміну маршрутною інформацією. На відміну від динамічної маршрутизації, де маршрутизатори самостійно обчислюють оптимальні шляхи на основі отриманих від сусідів оголошень, статичні маршрути залишаються незмінними доти, доки їх не змінить адміністратор або не станеться зміна стану інтерфейсу, через який проходить маршрут. Основною перевагою статичної маршрутизації є мінімальне споживання процесорних ресурсів та пропускної здатності каналу, оскільки відсутній постійний обмін службовими пакетами між маршрутизаторами, що робить її ідеальною для невеликих мереж або для налаштування маршрутів за замовчуванням до Інтернету. Однак ключовим обмеженням статичної маршрутизації є відсутність автоматичного адаптування до змін топології мережі, що призводить до втрати зв’язності у разі відмови основного шляху, якщо не передбачено механізмів резервування. Саме для подолання цього обмеження було розроблено концепцію плаваючих статичних маршрутів, яка базується на використанні параметра адміністративної відстані як критерію вибору між кількома маршрутами до однієї і тієї ж мережі.

Адміністративна відстань (Administrative Distance, AD) — це числовий параметр, який маршрутизатор використовує для визначення пріоритету джерела отримання маршруту при наявності кількох маршрутів до однієї мережі з різних джерел. Чим нижче значення адміністративної відстані, тим вища довіра маршрутизатора до цього джерела, і саме маршрут з найнижчим значенням AD буде вибраний для включення в активну таблицю маршрутизації. Для з’єднаних безпосередньо мереж (маршрути, отримані через локальні інтерфейси) значення AD дорівнює 0, для статичних маршрутів за замовчуванням — 1, для протоколу EIGRP — 90, для OSPF — 110, для RIP — 120, а для маршрутів, отриманих через протоколи зовнішньої маршрутизації (наприклад, BGP), — 20 або 200 залежно від типу оголошення. Важливо розуміти, що адміністративна відстань є локальним параметром, який враховується лише на конкретному маршрутизаторі, і не передається між пристроями, на відміну від метрики, яка використовується всередині динамічних протоколів для порівняння маршрутів з одного джерела. При налаштуванні floating static routes адміністратор навмисно встановлює для резервного маршруту значення AD вище за значення основного маршруту

(наприклад, 200 замість 1), що гарантує його неактивність доти, доки основний маршрут залишається доступним. Цей механізм дозволяє створювати прості, але ефективні схеми резервування без необхідності впровадження складних протоколів, що особливо цінно в умовах обмежених ресурсів або при необхідності мінімізації складності конфігурації.

Для кращого розуміння механізму вибору маршрутів на основі адміністративної відстані доцільно розглянути приклад з трьох можливих маршрутів до мережі 192.168.30.0/24 на маршрутизаторі R1 з лабораторної роботи. Припустимо, що на пристрої налаштовано три маршрути: основний статичний маршрут через інтерфейс 10.0.0.2 з AD=1, резервний статичний маршрут через інтерфейс 10.0.0.10 з AD=200, а також маршрут, отриманий через протокол OSPF від сусіднього маршрутизатора, з AD=110. У такій ситуації маршрутизатор порівнює значення AD для всіх трьох маршрутів і вибирає для активної таблиці маршрутизації лише той, що має найнижче значення — основний статичний маршрут з AD=1. Решта маршрутів залишаються в конфігурації, але не впливають на процес маршрутизації доти, доки основний маршрут доступний. Якщо ж основний маршрут стає недоступним (наприклад, через відмову інтерфейсу), маршрутизатор автоматично видаляє його з таблиці та повторно оцінює доступні варіанти, вибираючи тепер маршрут з наступним найнижчим значенням AD — у нашому прикладі це буде маршрут, отриманий через OSPF з AD=110, а не резервний статичний маршрут з AD=200. Цей приклад демонструє важливий нюанс: для ефективної роботи механізму floating static routes необхідно враховувати значення AD інших можливих джерел маршрутів у мережі, щоб гарантувати, що резервний статичний маршрут активується саме тоді, коли це потрібно, а не через конкуренцію з іншими протоколами маршрутизації. Таблиця 8.1 систематизує стандартні значення адміністративної відстані для різних джерел маршрутів у середовищі Cisco IOS, що допомагає адміністратору правильно планувати схеми резервування.

Таблиця 8.1 – Стандартні значення адміністративної відстані в середовищі Cisco IOS

Джерело маршруту	Значення AD	Опис
З’єднана безпосередньо мережа	0	Мережі, підключені до локальних інтерфейсів маршрутизатора
Статичний маршрут	1	Маршрути, налаштовані вручну командою ip route
EIGRP (внутрішній)	90	Маршрути, отримані через внутрішній EIGRP
OSPF	110	Маршрути, отримані через протокол OSPF
RIP	120	Маршрути, отримані через протокол RIP
EIGRP (зовнішній)	170	Маршрути, імпортовані в EIGRP з інших протоколів
Статичний маршрут з вказаною AD	1–255	Маршрути з явно встановленою адміністративною відстанню
Невідоме джерело	255	Маршрут не використовується

Аналізуючи дані таблиці 8.1, можна зробити висновок, що для забезпечення пріоритету резервного статичного маршруту над динамічними протоколами, але нижчого пріоритету за основним статичним маршрутом, оптимальним значенням адміністративної відстані є 200. Це значення вище за AD будь-якого стандартного динамічного протоколу маршрутизації, що гарантує, що резервний маршрут не буде витіснений маршрутами, отриманими через OSPF або EIGRP у складніших топологіях, але при цьому залишається нижчим за максимальне значення 255, яке робить маршрут повністю недійсним. Варто зазначити, що деякі реалізації операційних систем маршрутизаторів дозволяють встановлювати значення AD в діапазоні від 1 до 255, де 255 означає повне ігнорування маршруту, тому вибір значення 200 є компромісом між надійністю та гнучкістю конфігурації. Під час виконання лабораторної роботи студенти мають можливість на власному досвіді переконатися, що зміна значення AD для резервного маршруту безпосередньо впливає на його поведінку під час моделювання відмови основного лінку, що формує практичне розуміння цього абстрактного, але критично важливого параметра мережевої маршрутизації.

1.3 Механізм реалізації резервування за допомогою floating static routes

Механізм floating static routes базується на простому, але елегантному принципі: створення кількох статичних маршрутів до однієї й тієї ж мережі з різними значеннями адміністративної відстані, що дозволяє маршрутизатору автоматично перемикатися між ними залежно від доступності основного шляху. На практиці це реалізується шляхом налаштування двох типів маршрутів: основного маршруту зі стандартним значенням AD=1 та резервного маршруту з явно встановленим вищим значенням AD (наприклад, 200). Основний маршрут вказує на найкоротший або найшвидший шлях до цільової мережі, тоді як резервний маршрут вказує на альтернативний шлях, який може бути довшим за кількістю стрибків або мати нижчу пропускну здатність, але забезпечує збереження зв’язності у разі відмови основного лінку. Ключовою особливістю цього механізму є те, що резервний маршрут залишається в конфігурації маршрутизатора, але не потрапляє до активної таблиці маршрутизації доти, доки основний маршрут доступний, що запобігає зайвому навантаженню на процесор та пам’ять пристрою. При виникненні аварійної ситуації, наприклад, при відключенні інтерфейсу, через який проходить основний маршрут, маршрутизатор автоматично видаляє всі маршрути, пов’язані з цим інтерфейсом, з таблиці маршрутизації, після чого повторно оцінює доступні варіанти та активує резервний маршрут з вищою адміністративною відстанню. Цей процес відбувається повністю автоматично, без участі адміністратора, що забезпечує безперервність роботи мережі навіть у умовах виникнення несподіваних відмов.

Для успішної реалізації механізму floating static routes необхідно дотримуватися кількох важливих принципів проектування мережі. По-перше, топологія мережі повинна передбачати наявність фізично або логічно окремих шляхів між вузлами, що забезпечує справжню незалежність резервного шляху від основного — наприклад, у лабораторній роботі №8 трикутна топологія з трьох маршрутизаторів забезпечує два незалежні шляхи між будь-якими двома точками: прямий лінк та шлях через третій маршрутизатор. По-друге, необхідно забезпечити двонаправленну маршрутизацію, тобто налаштувати резервні маршрути на всіх маршрутизаторах уздовж резервного шляху, оскільки відсутність зворотного маршруту призведе до ситуації, коли пакети можуть дійти до цільової мережі, але відповідь не зможе повернутися до джерела. По-третє, важливо враховувати часові характеристики перемикання: хоча сам процес активації резервного маршруту відбувається миттєво після виявлення недоступності основного шляху, загальний час відновлення зв’язності залежить від таймаутів виявлення відмови на рівні канального шару (наприклад, таймаут визначення стану інтерфейсу в режимі down). У середовищі моделювання Packet Tracer цей час становить кілька секунд, тоді як у реальному обладнанні з використанням механізмів швидкого виявлення відмов (наприклад, протоколу BFD) його можна скоротити до десятків мілісекунд. Рисунок 8.1 умовно зображує топологію мережі з двома можливими шляхами між маршрутизаторами R1 та R3: основним шляхом через маршрутизатор R2 (позначеним суцільною лінією) та резервним шляхом напряму між R1 та R3 (позначеним пунктирною лінією), що наочно демонструє концепцію фізичної незалежності шляхів для забезпечення відмовостійкості.

Для наочності розглянемо конкретний приклад конфігурації маршрутизатора R1 з лабораторної роботи, де реалізовано механізм floating static routes для забезпечення досяжності мережі PC3 (192.168.30.0/24). Основний маршрут налаштовується командою ip route 192.168.30.0 255.255.255.0 10.0.0.2, яка вказує, що для досягнення мережі 192.168.30.0/24 необхідно використовувати шлюз 10.0.0.2 (інтерфейс маршрутизатора R2), при цьому значення адміністративної відстані залишається стандартним — 1. Резервний маршрут налаштовується командою ip route 192.168.30.0 255.255.255.0 10.0.0.10 200, де додатковий параметр 200 явно встановлює адміністративну відстань для цього маршруту. Після виконання обох команд у конфігурації маршрутизатора з’являються два записи для однієї й тієї ж мережі, але в активній таблиці маршрутизації, яку можна переглянути командою show ip route, буде присутній лише основний маршрут з позначкою «S» (static) та метрикою [1/0], де перше число означає значення AD, а друге — метрику (яка для статичних маршрутів завжди дорівнює 0). Резервний маршрут з AD=200 буде відсутній у виведенні цієї команди, але його можна побачити у повній конфігурації пристрою командою show running-config | section ip route. При моделюванні відмови основного лінку шляхом вимкнення інтерфейсу командою shutdown маршрутизатор миттєво видаляє основний маршрут з таблиці, після чого резервний маршрут автоматично активується і з’являється у виведенні show ip route з позначкою «S» та метрикою [200/0], що підтверджує

успішне перемикання на резервний шлях. Цей приклад демонструє простоту та ефективність механізму floating static routes для забезпечення базової відмовостійкості без необхідності впровадження складних протоколів.

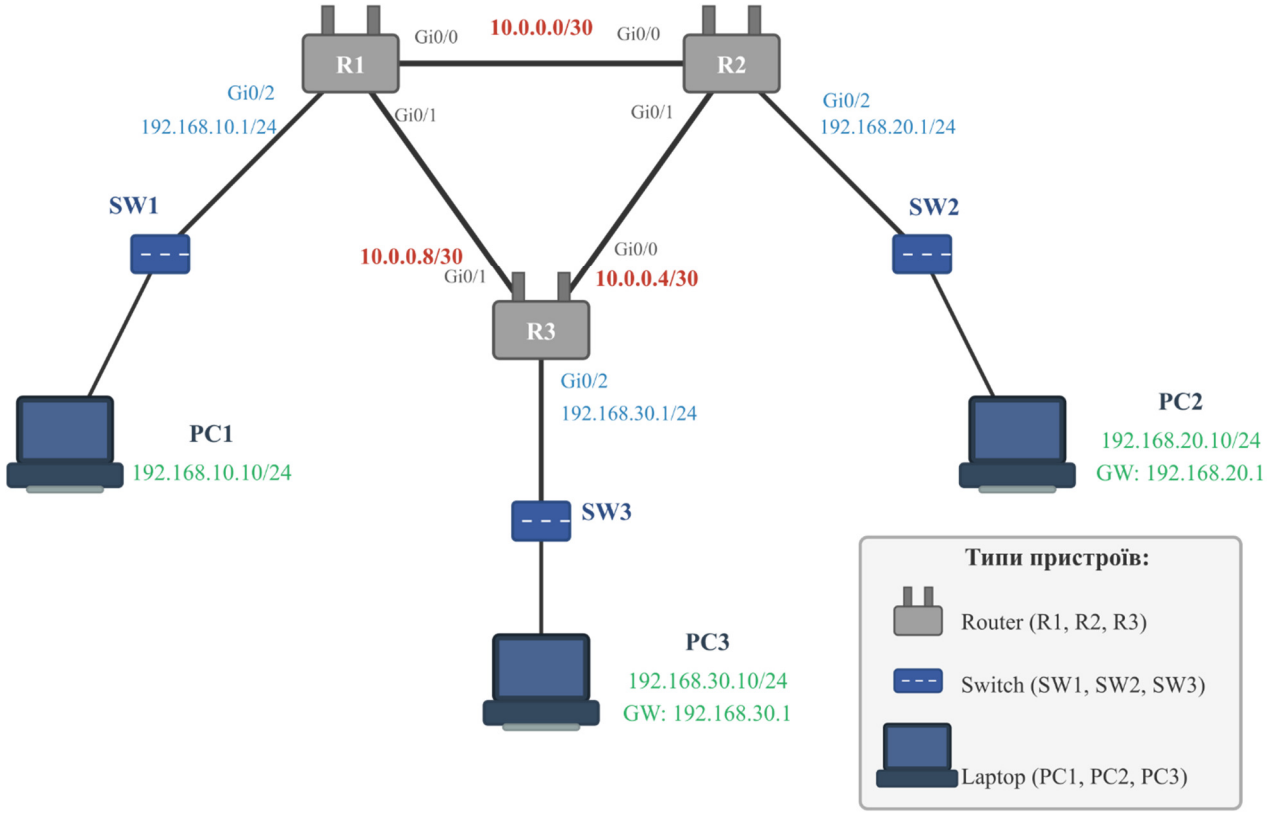

Рисунок 8.1 – Архітектура моделі мережі для дослідження резурвування маршрутів

Таблиця 8.2 — Основні команди Cisco IOS для налаштування та діагностики floating static routes

Команда	Призначення	Приклад використання
ip route <мережа> <маска> <шлюз>	Налаштування статичного маршруту з AD=1	ip route 192.168.30.0 255.255.255.0 10.0.0.2
ip route <мережа> <маска> <шлюз> <AD>	Налаштування резервного статичного маршруту з вказаною AD	ip route 192.168.30.0 255.255.255.0 10.0.0.10 200
show ip route	Перегляд активної таблиці маршрутизації	Виводить усі активні маршрути з їхніми метриками та джерелами
show ip route <мережа>	Перегляд конкретного маршруту	show ip route 192.168.30.0 показує деталі маршруту до цієї мережі
show running-config | section ip route	Перегляд усіх налаштованих статичних маршрутів	Відображає як активні, так і неактивні (резервні) маршрути
traceroute <IP-адреса>	Відстеження шляху до цільового хоста	traceroute 192.168.30.10 показує послідовність маршрутизаторів на шляху
ping <IP-адреса> repeat <кількість>	Тестування зв’язності з повтореннями	ping 192.168.30.10 repeat 100 для перевірки стабільності після перемикання

Аналізуючи команди, наведені в таблиці 8.2, можна виділити кілька ключових моментів, які важливо враховувати під час налаштування та діагностики floating static routes. По-перше, синтаксис команди ip route для резервного маршруту відрізняється від основного лише додаванням четвертого параметра — значення адміністративної відстані, що робить процес конфігурації інтуїтивно зрозумілим навіть для початківців. По-друге, команда show ip route є основним інструментом для перевірки активного стану маршрутів, але вона не показує резервні маршрути, що знаходяться в конфігурації, але не активовані через вищу AD, тому для повної діагностики необхідно використовувати комбінацію команд show ip route та show running-config | section ip route. По-третє, для наочного підтвердження перемикання на резервний шлях під час моделювання відмови найефективнішим є використання команди traceroute, яка візуалізує фактичний шлях проходження пакетів і дозволяє побачити зміну маршруту в реальному часі. Варто також зазначити, що для перевірки стабільності зв’язності після перемикання рекомендується виконувати серію пінгів з великим числом повторень (наприклад, 100), щоб переконатися, що перехід на резервний шлях не супроводжується втратою пакетів або значним збільшенням затримки. Ці практичні рекомендації допомагають студентам не лише правильно налаштувати механізм резервування, але й ефективно перевірити його роботу в умовах, що імітують реальні аварійні ситуації.

1.4 Практичні аспекти впровадження та обмеження механізму резервування

Хоча механізм floating static routes є простим та ефективним рішенням для забезпечення базової відмовостійкості, його впровадження в реальних мережах супроводжується певними обмеженнями та вимагає врахування специфічних практичних аспектів. Одним із ключових обмежень є відсутність механізму швидкого виявлення відмови на рівні мережевого шару: маршрутизатор виявляє недоступність основного шляху лише після того, як інтерфейс переходить у стан down на канальному рівні, що може зайняти від кількох секунд до хвилини залежно від типу з’єднання та налаштувань таймаутів. У випадках, коли фізичне з’єднання залишається активним, але мережевий трафік не проходить (наприклад, при відмові проміжного комутатора або маршрутизатора), статичні маршрути не зможуть виявити таку ситуацію без додаткових механізмів, таких як IP SLA (Service Level Agreement) у реальному обладнанні Cisco, який дозволяє моніторити досяжність віддаленого хоста за допомогою регулярних пінгів та автоматично деактивувати маршрут при втраті відповідей. У середовищі навчального моделювання Packet Tracer такі механізми відсутні, тому студенти мають можливість спостерігати лише найпростіший сценарій виявлення відмови через зміну стану інтерфейсу, що є корисним для розуміння базових принципів, але не відображає всієї складності реальних мережевих середовищ. Це обмеження слід враховувати при плануванні застосування floating static routes у

виробничих умовах, де критичні додатки можуть вимагати часу відновлення менше за 50 мілісекунд, що недосяжно без використання спеціалізованих механізмів швидкого виявлення відмов.

Ще одним важливим практичним аспектом є необхідність ручного управління конфігурацією при зміні топології мережі. На відміну від динамічних протоколів маршрутизації, які автоматично поширюють інформацію про зміни в топології серед усіх учасників мережі, статичні маршрути вимагають ручного оновлення конфігурації на кожному маршрутизаторі при додаванні нових мереж або зміні адресації. Це робить механізм floating static routes придатним лише для невеликих мереж зі стабільною топологією, де кількість змін мінімальна, але непридатним для великих корпоративних мереж або провайдерських інфраструктур, де топологія постійно змінюється. Крім того, при проектуванні схеми резервування необхідно враховувати пропускну здатність резервного шляху: якщо основний шлях забезпечує з’єднання з пропускною здатністю 1 Гбіт/с, а резервний — лише 100 Мбіт/с, то після перемикання на резервний шлях може виникнути перевантаження каналу та зростання затримок, що негативно вплине на якість обслуговування критичних додатків. Тому оптимальним підходом є використання floating static routes як тимчасового рішення або для резервування критично важливих маршрутів у поєднанні з динамічною маршрутизацією для решти мережевого трафіку, що забезпечує баланс між простотою управління та гнучкістю адаптації до змін. Під час виконання лабораторної роботи студенти мають можливість на власному досвіді переконатися в перевагах та обмеженнях цього механізму, що формує практичне розуміння умов його ефективного застосування у реальних мережевих середовищах.

Важливим елементом практичного застосування floating static routes є документування конфігурації та створення чіткого плану аварійного відновлення. Оскільки резервні маршрути не відображаються в активній таблиці маршрутизації за умов нормальної роботи мережі, новий адміністратор, який не знайомий з особливостями конфігурації, може не знати про їх існування та неправильно діяти під час усунення аварії. Тому рекомендується супроводжувати конфігурацію детальними коментарями (у середовищі реального обладнання Cisco це можна зробити за допомогою команди ! для додавання коментарів у конфігураційний файл) та підтримувати актуальний документ з описом топології мережі, включаючи основні та резервні шляхи для кожної мережі. Крім того, для моніторингу стану резервних маршрутів у виробничих умовах доцільно використовувати системи управління мережею (NMS), які можуть регулярно перевіряти наявність резервних маршрутів у конфігурації пристроїв та сповіщати адміністратора про їх відсутність або зміну параметрів. У навчальному середовищі лабораторної роботи ці аспекти моделюються через обов’язкове включення до звіту студентів скріншотів конфігурації з резервними маршрутами та таблиць маршрутизації в різних станах мережі, що формує у майбутніх фахівців звичку до системного документування та аналізу стану мережевої інфраструктури. Таким чином, хоча механізм floating static routes є технічно простим, його ефективне застосування

вимагає від адміністратора не лише технічних знань, але й системного підходу до проектування, документування та моніторингу мережевої інфраструктури, що є важливою професійною компетенцією для фахівців у сфері кібербезпеки та мережевих технологій.

2 КЛЮЧОВІ ПИТАННЯ

1. Поясніть механізм вибору маршруту маршрутизатором на основі адміністративної відстані (AD). Чому резервний маршрут з AD=200 не відображається в активній таблиці маршрутизації за наявності основного маршруту з AD=1, хоча обидва маршрути наявні в конфігурації пристрою?
2. Обґрунтуйте вибір значення адміністративної відстані 200 для резервних статичних маршрутів. Чому це значення є оптимальним для забезпечення пріоритету резервного маршруту над динамічними протоколами, але нижчого пріоритету за основним статичним маршрутом?
3. Опишіть послідовність подій, які відбуваються в маршрутизаторі після вимкнення інтерфейсу основного лінку (команда shutdown). Як маршрутизатор виявляє недоступність шляху та які саме механізми забезпечують автоматичне перемикання на резервний маршрут без участі адміністратора?
4. Поясніть, чому для реалізації ефективного резервування за допомогою floating static routes необхідно забезпечити двонаправленну маршрутизацію (наявність резервних маршрутів на всіх маршрутизаторах уздовж резервного шляху). Які наслідки матиме відсутність зворотного маршруту для досяжності мережі?
5. Які команди необхідно використати для повної діагностики стану резервних маршрутів? Поясніть, чому команда show ip route сама по собі недостатня для перевірки наявності резервних маршрутів у конфігурації, і яку додаткову команду слід застосувати для отримання повної інформації.
6. Проаналізуйте часові характеристики перемикання на резервний шлях у середовищі Packet Tracer порівняно з реальним обладнанням. Від чого залежить час відновлення зв'язності, і які механізми (наприклад, BFD) можуть суттєво скоротити цей час у виробничих умовах?
7. Поясніть, чому трикутна топологія з трьох маршрутизаторів є оптимальною для демонстрації механізму floating static routes. Які принципи проектування мережі (фізична незалежність шляхів, наявність альтернативних маршрутів) забезпечують ефективну роботу механізму резервування?
8. Опишіть обмеження механізму floating static routes у виявленні відмови мережі. Чому статичні маршрути не зможуть виявити ситуацію, коли фізичне з'єднання залишається активним, але мережевий трафік не проходить (наприклад, при відмові проміжного комутатора), і які додаткові механізми (наприклад, IP SLA) необхідні для вирішення цієї проблеми?
9. Поясніть практичну необхідність документування резервних маршрутів у конфігурації мережевих пристроїв. Які ризики виникають для адміністратора, який не знайомий з особливостями конфігурації, при спробі усунення аварії в

мережі з налаштованими floating static routes, і які засоби можуть допомогти уникнути помилок?

10. Проаналізуйте сценарій, коли на маршрутизаторі налаштовано три маршрути до однієї мережі: основний статичний маршрут (AD=1), маршрут через протокол OSPF (AD=110) та резервний статичний маршрут (AD=200). Який маршрут буде активований після відмови основного лінку, і як це вплине на ефективність механізму резервування? Як правильно спланувати значення AD для забезпечення передбачуваної поведінки мережі?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. Архітектура мережі та план адресації. У лабораторній роботі моделюється трикутна топологія (рис. 8.1), що складається з трьох маршрутизаторів Cisco 2911 (R1, R2, R3), трьох комутаторів Cisco 2960 (SW1, SW2, SW3) та трьох персональних комп’ютерів (PC1, PC2, PC3). Маршрутизатори з’єднані між собою у кільце за допомогою точка-точкових лінків з маскою /30, що забезпечує наявність альтернативних шляхів передачі даних. До кожного маршрутизатора підключено комутатор, який обслуговує одну локальну підмережу з кінцевим пристроєм (ПК). Така архітектура дозволяє продемонструвати механізм автоматичного перемикання трафіку на резервний шлях при відмові основного лінку без втручання адміністратора — ключову вимогу до сучасних відмовостійких мереж. Для забезпечення управління комутаторами налаштовано IP-адреси на інтерфейсі VLAN 1 та шлюзи за замовчуванням, що дозволяє виконувати віддалену діагностику обладнання.

Таблиця 8.3 — План адресації мережі прикладу лабораторного завдання

Пристрій	Тип	Інтерфейс	IP-адреса	Маска підмережі	Призначення
R1	Маршрутизатор	Gig0/0	10.0.0.1	255.255.255.252	З’єднання з R2 (основний лінк)
		Gig0/1	10.0.0.9	255.255.255.252	З’єднання з R3 (резервний лінк)
		Gig0/2	192.168.10.1	255.255.255.0	Локальна мережа PC1
R2	Маршрутизатор	Gig0/0	10.0.0.2	255.255.255.252	З’єднання з R1 (основний лінк)
		Gig0/1	10.0.0.5	255.255.255.252	З’єднання з R3
		Gig0/2	192.168.20.1	255.255.255.0	Локальна мережа PC2
R3	Маршрутизатор	Gig0/0	10.0.0.6	255.255.255.252	З’єднання з R2
		Gig0/1	10.0.0.10	255.255.255.252	З’єднання з R1 (резервний лінк)
		Gig0/2	192.168.30.1	255.255.255.0	Локальна мережа PC3
SW1	Комутатор	VLAN 1	192.168.10.2	255.255.255.0	Управління комутатором

		—	Шлюз: 192.168.10.1	—	Шлюз за замовчуванням
SW2	Комутатор	VLAN 1	192.168.20.2	255.255.255.0	Управління комутатором
		—	Шлюз: 192.168.20.1	—	Шлюз за замовчуванням
SW3	Комутатор	VLAN 1	192.168.30.2	255.255.255.0	Управління комутатором
		—	Шлюз: 192.168.30.1	—	Шлюз за замовчуванням
PC1	ПК	NIC	192.168.10.10	255.255.255.0	Клієнтська станція
		—	Шлюз: 192.168.10.1	—	Шлюз за замовчуванням
PC2	ПК	NIC	192.168.20.10	255.255.255.0	Клієнтська станція
		—	Шлюз: 192.168.20.1	—	Шлюз за замовчуванням
PC3	ПК	NIC	192.168.30.10	255.255.255.0	Клієнтська станція
		—	Шлюз: 192.168.30.1	—	Шлюз за замовчуванням

Завдання лабораторної роботи виконується кожним студентом індивідуально згідно з присвоєним варіантом з таблиці 8.4. Варіант визначає унікальну схему адресації мережевих інтерфейсів для всіх пристроїв топології, що забезпечує незалежність виконання завдань та формування практичних навичок роботи з різними адресними просторами. Студент повинен використовувати параметри свого варіанту при налаштуванні інтерфейсів маршрутизаторів, комутаторів та кінцевих пристроїв, а також при конфігурації основних та резервних статичних маршрутів.

Таблиця 8.4 – Варіанти індивідуальних завдань

№ варіанту	Адресація магістральних лінків (/30)	Адресація локальних мереж (/24)
1	R1–R2: 10.1.0.0 (R1: .1, R2: .2) R2–R3: 10.1.0.4 (R2: .5, R3: .6) R3–R1: 10.1.0.8 (R3: .9, R1: .10)	PC1: 192.168.10.0/24 (шлюз: .1) PC2: 192.168.20.0/24 (шлюз: .1) PC3: 192.168.30.0/24 (шлюз: .1)
2	R1–R2: 10.2.0.0 (R1: .1, R2: .2) R2–R3: 10.2.0.4 (R2: .5, R3: .6) R3–R1: 10.2.0.8 (R3: .9, R1: .10)	PC1: 192.168.40.0/24 (шлюз: .1) PC2: 192.168.50.0/24 (шлюз: .1) PC3: 192.168.60.0/24 (шлюз: .1)
3	R1–R2: 10.3.0.0 (R1: .1, R2: .2) R2–R3: 10.3.0.4 (R2: .5, R3: .6) R3–R1: 10.3.0.8 (R3: .9, R1: .10)	PC1: 192.168.70.0/24 (шлюз: .1) PC2: 192.168.80.0/24 (шлюз: .1) PC3: 192.168.90.0/24 (шлюз: .1)
4	R1–R2: 10.4.0.0 (R1: .1, R2: .2) R2–R3: 10.4.0.4 (R2: .5, R3: .6) R3–R1: 10.4.0.8 (R3: .9, R1: .10)	PC1: 192.168.100.0/24 (шлюз: .1) PC2: 192.168.110.0/24 (шлюз: .1) PC3: 192.168.120.0/24 (шлюз: .1)
5	R1–R2: 10.5.0.0 (R1: .1, R2: .2) R2–R3: 10.5.0.4 (R2: .5, R3: .6) R3–R1: 10.5.0.8 (R3: .9, R1: .10)	PC1: 192.168.130.0/24 (шлюз: .1) PC2: 192.168.140.0/24 (шлюз: .1) PC3: 192.168.150.0/24 (шлюз: .1)
6	R1–R2: 10.6.0.0 (R1: .1, R2: .2)	PC1: 192.168.160.0/24 (шлюз: .1)

	R2–R3: 10.6.0.4 (R2: .5, R3: .6) R3–R1: 10.6.0.8 (R3: .9, R1: .10)	PC2: 192.168.170.0/24 (шлюз: .1) PC3: 192.168.180.0/24 (шлюз: .1)
7	R1–R2: 10.7.0.0 (R1: .1, R2: .2) R2–R3: 10.7.0.4 (R2: .5, R3: .6) R3–R1: 10.7.0.8 (R3: .9, R1: .10)	PC1: 192.168.190.0/24 (шлюз: .1) PC2: 192.168.200.0/24 (шлюз: .1) PC3: 192.168.210.0/24 (шлюз: .1)
8	R1–R2: 10.8.0.0 (R1: .1, R2: .2) R2–R3: 10.8.0.4 (R2: .5, R3: .6) R3–R1: 10.8.0.8 (R3: .9, R1: .10)	PC1: 192.168.220.0/24 (шлюз: .1) PC2: 192.168.230.0/24 (шлюз: .1) PC3: 192.168.240.0/24 (шлюз: .1)
9	R1–R2: 10.9.0.0 (R1: .1, R2: .2) R2–R3: 10.9.0.4 (R2: .5, R3: .6) R3–R1: 10.9.0.8 (R3: .9, R1: .10)	PC1: 192.168.11.0/24 (шлюз: .1) PC2: 192.168.21.0/24 (шлюз: .1) PC3: 192.168.31.0/24 (шлюз: .1)
10	R1–R2: 10.10.0.0 (R1: .1, R2: .2) R2–R3: 10.10.0.4 (R2: .5, R3: .6) R3–R1: 10.10.0.8 (R3: .9, R1: .10)	PC1: 192.168.41.0/24 (шлюз: .1) PC2: 192.168.51.0/24 (шлюз: .1) PC3: 192.168.61.0/24 (шлюз: .1)
11	R1–R2: 10.11.0.0 (R1: .1, R2: .2) R2–R3: 10.11.0.4 (R2: .5, R3: .6) R3–R1: 10.11.0.8 (R3: .9, R1: .10)	PC1: 192.168.71.0/24 (шлюз: .1) PC2: 192.168.81.0/24 (шлюз: .1) PC3: 192.168.91.0/24 (шлюз: .1)
12	R1–R2: 10.12.0.0 (R1: .1, R2: .2) R2–R3: 10.12.0.4 (R2: .5, R3: .6) R3–R1: 10.12.0.8 (R3: .9, R1: .10)	PC1: 192.168.101.0/24 (шлюз: .1) PC2: 192.168.111.0/24 (шлюз: .1) PC3: 192.168.121.0/24 (шлюз: .1)
13	R1–R2: 10.13.0.0 (R1: .1, R2: .2) R2–R3: 10.13.0.4 (R2: .5, R3: .6) R3–R1: 10.13.0.8 (R3: .9, R1: .10)	PC1: 192.168.131.0/24 (шлюз: .1) PC2: 192.168.141.0/24 (шлюз: .1) PC3: 192.168.151.0/24 (шлюз: .1)
14	R1–R2: 10.14.0.0 (R1: .1, R2: .2) R2–R3: 10.14.0.4 (R2: .5, R3: .6) R3–R1: 10.14.0.8 (R3: .9, R1: .10)	PC1: 192.168.161.0/24 (шлюз: .1) PC2: 192.168.171.0/24 (шлюз: .1) PC3: 192.168.181.0/24 (шлюз: .1)
15	R1–R2: 10.15.0.0 (R1: .1, R2: .2) R2–R3: 10.15.0.4 (R2: .5, R3: .6) R3–R1: 10.15.0.8 (R3: .9, R1: .10)	PC1: 192.168.191.0/24 (шлюз: .1) PC2: 192.168.201.0/24 (шлюз: .1) PC3: 192.168.211.0/24 (шлюз: .1)
16	R1–R2: 10.16.0.0 (R1: .1, R2: .2) R2–R3: 10.16.0.4 (R2: .5, R3: .6) R3–R1: 10.16.0.8 (R3: .9, R1: .10)	PC1: 192.168.221.0/24 (шлюз: .1) PC2: 192.168.231.0/24 (шлюз: .1) PC3: 192.168.241.0/24 (шлюз: .1)
17	R1–R2: 10.17.0.0 (R1: .1, R2: .2) R2–R3: 10.17.0.4 (R2: .5, R3: .6) R3–R1: 10.17.0.8 (R3: .9, R1: .10)	PC1: 192.168.12.0/24 (шлюз: .1) PC2: 192.168.22.0/24 (шлюз: .1) PC3: 192.168.32.0/24 (шлюз: .1)
18	R1–R2: 10.18.0.0 (R1: .1, R2: .2) R2–R3: 10.18.0.4 (R2: .5, R3: .6) R3–R1: 10.18.0.8 (R3: .9, R1: .10)	PC1: 192.168.42.0/24 (шлюз: .1) PC2: 192.168.52.0/24 (шлюз: .1) PC3: 192.168.62.0/24 (шлюз: .1)
19	R1–R2: 10.19.0.0 (R1: .1, R2: .2) R2–R3: 10.19.0.4 (R2: .5, R3: .6) R3–R1: 10.19.0.8 (R3: .9, R1: .10)	PC1: 192.168.72.0/24 (шлюз: .1) PC2: 192.168.82.0/24 (шлюз: .1) PC3: 192.168.92.0/24 (шлюз: .1)
20	R1–R2: 10.20.0.0 (R1: .1, R2: .2) R2–R3: 10.20.0.4 (R2: .5, R3: .6) R3–R1: 10.20.0.8 (R3: .9, R1: .10)	PC1: 192.168.102.0/24 (шлюз: .1) PC2: 192.168.112.0/24 (шлюз: .1) PC3: 192.168.122.0/24 (шлюз: .1)
21	R1–R2: 10.21.0.0 (R1: .1, R2: .2) R2–R3: 10.21.0.4 (R2: .5, R3: .6) R3–R1: 10.21.0.8 (R3: .9, R1: .10)	PC1: 192.168.132.0/24 (шлюз: .1) PC2: 192.168.142.0/24 (шлюз: .1) PC3: 192.168.152.0/24 (шлюз: .1)
22	R1–R2: 10.22.0.0 (R1: .1, R2: .2) R2–R3: 10.22.0.4 (R2: .5, R3: .6) R3–R1: 10.22.0.8 (R3: .9, R1: .10)	PC1: 192.168.162.0/24 (шлюз: .1) PC2: 192.168.172.0/24 (шлюз: .1) PC3: 192.168.182.0/24 (шлюз: .1)
23	R1–R2: 10.23.0.0 (R1: .1, R2: .2) R2–R3: 10.23.0.4 (R2: .5, R3: .6)	PC1: 192.168.192.0/24 (шлюз: .1) PC2: 192.168.202.0/24 (шлюз: .1)

	R3–R1: 10.23.0.8 (R3: .9, R1: .10)	PC3: 192.168.212.0/24 (шлюз: .1)
24	R1–R2: 10.24.0.0 (R1: .1, R2: .2) R2–R3: 10.24.0.4 (R2: .5, R3: .6) R3–R1: 10.24.0.8 (R3: .9, R1: .10)	PC1: 192.168.222.0/24 (шлюз: .1) PC2: 192.168.232.0/24 (шлюз: .1) PC3: 192.168.242.0/24 (шлюз: .1)
25	R1–R2: 10.25.0.0 (R1: .1, R2: .2) R2–R3: 10.25.0.4 (R2: .5, R3: .6) R3–R1: 10.25.0.8 (R3: .9, R1: .10)	PC1: 192.168.13.0/24 (шлюз: .1) PC2: 192.168.23.0/24 (шлюз: .1) PC3: 192.168.33.0/24 (шлюз: .1)
26	R1–R2: 10.26.0.0 (R1: .1, R2: .2) R2–R3: 10.26.0.4 (R2: .5, R3: .6) R3–R1: 10.26.0.8 (R3: .9, R1: .10)	PC1: 192.168.43.0/24 (шлюз: .1) PC2: 192.168.53.0/24 (шлюз: .1) PC3: 192.168.63.0/24 (шлюз: .1)
27	R1–R2: 10.27.0.0 (R1: .1, R2: .2) R2–R3: 10.27.0.4 (R2: .5, R3: .6) R3–R1: 10.27.0.8 (R3: .9, R1: .10)	PC1: 192.168.73.0/24 (шлюз: .1) PC2: 192.168.83.0/24 (шлюз: .1) PC3: 192.168.93.0/24 (шлюз: .1)
28	R1–R2: 10.28.0.0 (R1: .1, R2: .2) R2–R3: 10.28.0.4 (R2: .5, R3: .6) R3–R1: 10.28.0.8 (R3: .9, R1: .10)	PC1: 192.168.103.0/24 (шлюз: .1) PC2: 192.168.113.0/24 (шлюз: .1) PC3: 192.168.123.0/24 (шлюз: .1)
29	R1–R2: 10.29.0.0 (R1: .1, R2: .2) R2–R3: 10.29.0.4 (R2: .5, R3: .6) R3–R1: 10.29.0.8 (R3: .9, R1: .10)	PC1: 192.168.133.0/24 (шлюз: .1) PC2: 192.168.143.0/24 (шлюз: .1) PC3: 192.168.153.0/24 (шлюз: .1)
30	R1–R2: 10.30.0.0 (R1: .1, R2: .2) R2–R3: 10.30.0.4 (R2: .5, R3: .6) R3–R1: 10.30.0.8 (R3: .9, R1: .10)	PC1: 192.168.163.0/24 (шлюз: .1) PC2: 192.168.173.0/24 (шлюз: .1) PC3: 192.168.183.0/24 (шлюз: .1)

Кожен варіант містить унікальну схему адресації, яка забезпечує незалежність виконання завдань студентами та запобігає копіюванню результатів. Адресація магістральних лінків побудована на основі префікса 10.X.0.0/30, де другий октет (X) відповідає номеру варіанту, що гарантує відсутність перетину адресних просторів між різними варіантами. Для кожної точки-точкової мережі /30 використовуються дві корисні адреси: перша (.1 або .5 або .9) призначається одному маршрутизатору, друга (.2 або .6 або .10) — іншому, що відповідає стандартній практиці конфігурації точка-точкових з’єднань у середовищі Cisco. Адресація локальних мереж ПК використовує діапазон приватних адрес 192.168.0.0/16 з маскою /24, де третій октет унікальний для кожного варіанту та кожної локальної мережі, що забезпечує чітку сегментацію трафіку та спрощує діагностику під час виконання лабораторної роботи.

Для всіх варіантів зберігається єдина топологія «трикутник» з трьох маршрутизаторів, але основний шлях для маршрутизатора R1 завжди проходить через лінк R1–R2 (мережа 10.X.0.0/30), а резервний шлях — через лінк R1–R3 (мережа 10.X.0.8/30). Ця уніфікація дозволяє стандартизувати методичні матеріали та критерії оцінювання, водночас забезпечуючи кожному студенту унікальне завдання з точки зору адресації. Під час виконання роботи студент повинен буде налаштувати основні статичні маршрути через шлюз з найнижчою адресою у відповідній мережі (наприклад, для варіанту 1 шлюз 10.1.0.2 для основного шляху) та резервні маршрути через альтернативний шлюз (наприклад, 10.1.0.10) з адміністративною відстанню 200. Такий підхід до варіативності завдань формує у студентів навички роботи з різними адресними

схемами, що є важливим елементом професійної підготовки фахівців з кібербезпеки та мережевих технологій.

3.2 Базова конфігурація маршрутизаторів. На цьому етапі виконується повна базова конфігурація всіх трьох маршрутизаторів: присвоєння унікальних імен, відключення автоматичного пошуку домену (для уникнення затримок при помилковому введенні команд), налаштування захисту консолі та віддаленого доступу через SSH, а також активація всіх необхідних інтерфейсів з відповідною адресацією. Для забезпечення стабільності ідентифікатора маршрутизатора в майбутніх лабораторних роботах (наприклад, при налаштуванні OSPF) рекомендується також налаштувати loopback-інтерфейс, хоча для цієї роботи він не є обов’язковим. Важливо зазначити, що для точка-точкових з’єднань між маршрутизаторами використовується маска /30 (255.255.255.252), що забезпечує мінімальне споживання адресного простору — лише дві корисні адреси на кожен лінк, що є стандартною практикою для магістральних з’єднань.

Для маршрутизатора R1 виконуємо повну базову конфігурацію, що включає присвоєння імені пристрою, відключення автоматичного пошуку домену, налаштування захисту консолі та віддаленого доступу через SSH, генерацію криптографічних ключів RSA для шифрування сесій, створення локального облікового запису адміністратора з повними привілеями, а також активацію всіх фізичних інтерфейсів з відповідною IP-адресацією згідно з планом мережі:

```
     R1> enable
R1# configure terminal
R1(config)# hostname R1
R1(config)# no ip domain-lookup
R1(config)# enable secret cisco123
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)# transport input ssh
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# ip domain-name km.lab
R1(config)# crypto key generate rsa modulus 1024
R1(config)# username admin privilege 15 secret admin123
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip address 10.0.0.9 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
```

```
R1(config)# interface GigabitEthernet0/2
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# end
R1# copy running-config startup-config
```

Після виконання команди show ip interface brief на R1 ми отримуємо стислий огляд стану всіх інтерфейсів. У виведенні ми бачимо, що всі три інтерфейси (GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/2) мають статус up/up, що свідчить про коректне фізичне та канальне підключення. IP-адреси відповідають плану адресації: 10.0.0.1 для з’єднання з R2, 10.0.0.9 для з’єднання з R3, та 192.168.10.1 для локальної мережі. Команда show running-config | section line підтверджує налаштування захисту консолі та віддаленого доступу, а show ip ssh перевіряє готовність SSH-сервера. Аналогічну конфігурацію необхідно виконати для маршрутизаторів R2 та R3 з відповідною адресацією згідно з Таблицею 8.3.

Для маршрутизатора R2 виконуємо аналогічну базову конфігурацію з урахуванням його ролі в топології: присвоєння імені R2, налаштування захисту консолі та SSH-доступу, генерацію криптографічних ключів, створення локального облікового запису адміністратора, а також активацію інтерфейсів з адресами 10.0.0.2 (з’єднання з R1), 10.0.0.5 (з’єднання з R3) та 192.168.20.1 (локальна мережа PC2):

```
R2> enable
R2# configure terminal
R2(config)# hostname R2
R2(config)# no ip domain-lookup
R2(config)# enable secret cisco123
R2(config)# line console 0
R2(config-line)# password cisco
R2(config-line)# login
R2(config-line)# exit
R2(config)# line vty 0 4
R2(config-line)# transport input ssh
R2(config-line)# password cisco
R2(config-line)# login
R2(config-line)# exit
R2(config)# ip domain-name km.lab
R2(config)# crypto key generate rsa modulus 1024
R2(config)# username admin privilege 15 secret admin123
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip address 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface GigabitEthernet0/1
R2(config-if)# ip address 10.0.0.5 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface GigabitEthernet0/2
```

```
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# end
R2# copy running-config startup-config
```

Для маршрутизатора R3 виконуємо базову конфігурацію, аналогічну до попередніх пристроїв, з присвоєнням імені R3, налаштуванням захисту консолі та віддаленого доступу через SSH, генерацією криптографічних ключів, створенням локального облікового запису адміністратора, а також активацією інтерфейсів з адресами 10.0.0.6 (з’єднання з R2), 10.0.0.10 (з’єднання з R1) та 192.168.30.1 (локальна мережа PC3):

```
R3> enable
R3# configure terminal
R3(config)# hostname R3
R3(config)# no ip domain-lookup
R3(config)# enable secret cisco123
R3(config)# line console 0
R3(config-line)# password cisco
R3(config-line)# login
R3(config-line)# exit
R3(config)# line vty 0 4
R3(config-line)# transport input ssh
R3(config-line)# password cisco
R3(config-line)# login
R3(config-line)# exit
R3(config)# ip domain-name km.lab
R3(config)# crypto key generate rsa modulus 1024
R3(config)# username admin privilege 15 secret admin123
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip address 10.0.0.6 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# interface GigabitEthernet0/1
R3(config-if)# ip address 10.0.0.10 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# interface GigabitEthernet0/2
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# end
R3# copy running-config startup-config
```

3.3 Конфігурація комутаторів. Комутатори в цій топології виконують роль пристроїв рівня доступу, забезпечуючи підключення кінцевих пристроїв (ПК) до локальних мереж. Для можливості віддаленого управління та діагностики на кожному комутаторі налаштовується інтерфейс управління VLAN 1 з відповідною IP-адресою та шлюзом за замовчуванням, що вказує на

інтерфейс підключеного маршрутизатора. Це дозволяє виконувати команди ping та traceroute безпосередньо з комутатора для перевірки зв’язності з іншими сегментами мережі. Важливо зазначити, що в даній лабораторній роботі комутатори працюють у режимі прозорого моста (без налаштування додаткових VLAN), оскільки основна мета — демонстрація механізмів маршрутизації, а не сегментації на канальному рівні.

Для комутатора SW1, який обслуговує локальну мережу PC1, налаштовуємо інтерфейс управління VLAN 1 з адресою 192.168.10.2, встановлюємо шлюз за замовчуванням 192.168.10.1 (інтерфейс R1), а також забезпечуємо базовий захист консольного та віддаленого доступу шляхом налаштування паролів для ліній консолі та VTY:

```
SW1> enable
SW1# configure terminal
SW1(config)# hostname SW1
SW1(config)# no ip domain-lookup
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.10.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# ip default-gateway 192.168.10.1
SW1(config)# line console 0
SW1(config-line)# password cisco
SW1(config-line)# login
SW1(config-line)# exit
SW1(config)# line vty 0 15
SW1(config-line)# password cisco
SW1(config-line)# login
SW1(config-line)# exit
SW1(config)# end
SW1# copy running-config startup-config
```

Для комутатора SW2, який обслуговує локальну мережу PC2, виконуємо аналогічну конфігурацію управління: присвоєння імені SW2, налаштування інтерфейсу VLAN 1 з адресою 192.168.20.2, встановлення шлюза за замовчуванням 192.168.20.1 (інтерфейс R2), а також забезпечення базового захисту консольного та віддаленого доступу:

```
SW2> enable
SW2# configure terminal
SW2(config)# hostname SW2
SW2(config)# no ip domain-lookup
SW2(config)# interface vlan 1
SW2(config-if)# ip address 192.168.20.2 255.255.255.0
SW2(config-if)# no shutdown
SW2(config-if)# exit
SW2(config)# ip default-gateway 192.168.20.1
SW2(config)# line console 0
SW2(config-line)# password cisco
SW2(config-line)# login
```

```
SW2(config-line)# exit
SW2(config)# line vty 0 15
SW2(config-line)# password cisco
SW2(config-line)# login
SW2(config-line)# exit
SW2(config)# end
SW2# copy running-config startup-config
```

Для комутатора SW3, який обслуговує локальну мережу PC3, налаштовуємо інтерфейс управління VLAN 1 з адресою 192.168.30.2, встановлюємо шлюз за замовчуванням 192.168.30.1 (інтерфейс R3), а також забезпечуємо базовий захист консольного та віддаленого доступу аналогічно до попередніх комутаторів:

```
SW3> enable
SW3# configure terminal
SW3(config)# hostname SW3
SW3(config)# no ip domain-lookup
SW3(config)# interface vlan 1
SW3(config-if)# ip address 192.168.30.2 255.255.255.0
SW3(config-if)# no shutdown
SW3(config-if)# exit
SW3(config)# ip default-gateway 192.168.30.1
SW3(config)# line console 0
SW3(config-line)# password cisco
SW3(config-line)# login
SW3(config-line)# exit
SW3(config)# line vty 0 15
SW3(config-line)# password cisco
SW3(config-line)# login
SW3(config-line)# exit
SW3(config)# end
SW3# copy running-config startup-config
```

Після конфігурації комутатора SW1 команда show ip interface brief відображає інтерфейс VLAN1 зі статусом up/up та адресою 192.168.10.2. Команда show running-config | include default-gateway підтверджує наявність шлюза 192.168.10.1. Для перевірки зв’язності з маршрутизатором виконується ping 192.168.10.1 — успішний результат (100% відповідей) свідчить про коректне налаштування управління комутатором. Аналогічні перевірки виконуються для SW2 та SW3.

3.4 Налаштування кінцевих пристроїв (ПК). Кожен персональний комп’ютер налаштовується зі статичною IP-адресою, маскою підмережі та шлюзом за замовчуванням, що вказує на інтерфейс маршрутизатора відповідної локальної мережі. У середовищі Cisco Packet Tracer налаштування виконується через графічний інтерфейс: вкладка Desktop → IP Configuration → вибір режиму Static та введення параметрів згідно з Таблицею 8.3. Також рекомендується перевірити налаштування DNS-сервера (можна залишити

порожнім або вказати 8.8.8.8 для майбутніх лабораторних робіт). Після налаштування всіх ПК виконується базова перевірка зв’язності з власним шлюзом за допомогою інструменту Simple PDU або команди ping у терміналі ПК.

Таблиця 8.5 – Налаштування ПК

Параметр	PC1	PC2	PC3
IP Address	192.168.10.10	192.168.20.10	192.168.30.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.20.1	192.168.30.1

Для перевірки налаштувань на ПК1 відкрийте термінал (Desktop → Command Prompt) та виконайте:

```
ipconfig
ping 192.168.10.1
```

Команда ipconfig відображає поточну конфігурацію мережевого інтерфейсу, що дозволяє переконатися у правильності введених параметрів. Успішний ping до шлюза (192.168.10.1) з мінімальними часовими затримками (0–1 мс у моделі Packet Tracer) підтверджує коректне фізичне підключення та налаштування канального рівня. Аналогічні перевірки виконуються для PC2 та PC3.

3.5. Налаштування основних та резервних статичних маршрутів. На цьому етапі реалізується ключовий механізм лабораторної роботи — конфігурація основних статичних маршрутів для забезпечення повної досяжності між усіма локальними мережами, а також додавання резервних маршрутів з підвищеною адміністративною відстанню (200). Для маршрутизатора R1 основні маршрути до мереж 192.168.20.0/24 (PC2) та 192.168.30.0/24 (PC3) налаштовуються через шлюз 10.0.0.2 (інтерфейс R2), оскільки цей шлях є найкоротшим у штатному режимі. Резервні маршрути до тих самих мереж додаються через альтернативний шлюз 10.0.0.10 (інтерфейс R3) з явним встановленням адміністративної відстані 200. Це значення вище за AD будь-якого стандартного джерела маршрутів (наприклад, з’єднаних маршрутів — 0, статичних — 1), тому такі «плаваючі» маршрути не потрапляють до активної таблиці маршрутизації доти, доки існує маршрут з нижчою AD. Аналогічна логіка застосовується для маршрутизаторів R2 та R3 з урахуванням симетрії топології.

Для маршрутизатора R1 налаштовуємо основні статичні маршрути до мереж PC2 та PC3 через основний шлюз 10.0.0.2 (інтерфейс R2), а також додаємо резервні маршрути через альтернативний шлюз 10.0.0.10 (інтерфейс R3) з підвищеною адміністративною відстанню 200 для забезпечення відмовостійкості:

```
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2
R1(config)# ip route 192.168.30.0 255.255.255.0 10.0.0.2
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.10 200
R1(config)# ip route 192.168.30.0 255.255.255.0 10.0.0.10 200
```

Для маршрутизатора R2 налаштовуємо основні статичні маршрути: до мережі PC1 через шлюз 10.0.0.2 (інтерфейс R1) та до мережі PC3 через шлюз 10.0.0.5 (інтерфейс R3), а також додаємо резервні маршрути через альтернативні шляхи (до PC1 через R3, до PC3 через R1) з адміністративною відстанню 200:

```
R2(config)# ip route 192.168.10.0 255.255.255.0 10.0.0.2
R2(config)# ip route 192.168.30.0 255.255.255.0 10.0.0.5
R2(config)# ip route 192.168.10.0 255.255.255.0 10.0.0.6 200
R2(config)# ip route 192.168.30.0 255.255.255.0 10.0.0.1 200
```

Для маршрутизатора R3 налаштовуємо основні статичні маршрути: до мережі PC1 через шлюз 10.0.0.10 (інтерфейс R1) та до мережі PC2 через шлюз 10.0.0.5 (інтерфейс R2), а також додаємо резервні маршрути через альтернативні шляхи (до PC1 через R2, до PC2 через R1) з адміністративною відстанню 200:

```
R3(config)# ip route 192.168.10.0 255.255.255.0 10.0.0.10
R3(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.5
R3(config)# ip route 192.168.10.0 255.255.255.0 10.0.0.6 200
R3(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.9 200
```

Після виконання команди show ip route на маршрутизаторі R1 ми спостерігаємо, що в таблиці маршрутизації присутні лише основні маршрути з позначкою S (static) та метрикою [1/0] — де 1 означає адміністративну відстань, а 0 — метрику. Наприклад, запис S 192.168.20.0/24 [1/0] via 10.0.0.2 свідчить про те, що трафік до мережі PC2 буде направлятися через інтерфейс з адресою 10.0.0.2 (R2). Резервні маршрути з AD=200 у виведенні відсутні, що підтверджує коректну роботу механізму «плаваючих» маршрутів — вони залишаються в конфігурації, але не активуються доти, доки доступний основний шлях. Це можна додатково перевірити командою show running-config | section ip route, яка відобразить усі налаштовані статичні маршрути, включаючи резервні.

3.6 Перевірка роботи мережі в штатному режимі. Для перевірки коректності роботи мережі в штатному режимі виконується серія тестів зв’язності з кожного ПК до інших кінцевих пристроїв. З ПК1 виконується команда ping 192.168.20.10 (до PC2) та ping 192.168.30.10 (до PC3) — обидва пінги повинні повернути 100% успішних відповідей. Більш інформативною є команда traceroute 192.168.30.10, яка відображає послідовність маршрутизаторів на шляху до PC3. У штатному режимі вивід має містити три

стрибки: перший — шлюз локальної мережі (192.168.10.1, R1), другий — маршрутизатор R2 (10.0.0.2), третій — шлюз мережі PC3 (192.168.30.1, R3). Це підтверджує, що трафік проходить через найкоротший шлях через лінк R1–R2, як і планувалося. Аналогічні перевірки виконуються з ПК2 та ПК3 для забезпечення повної досяжності у всіх напрямках.

З ПК1 виконуємо:

```
C:\> ping 192.168.20.10
C:\> ping 192.168.30.10
C:\> tracert 192.168.30.10
```

У виведенні команди tracert 192.168.30.10 ми бачимо три стрибки: 192.168.10.1 (R1), 10.0.0.2 (R2), 192.168.30.1 (R3). Це підтверджує, що трафік від ПК1 до ПК3 проходить через лінк R1–R2 як основний шлях. Час відгуку для кожного стрибка становить 0–1 мс, що є нормою для моделі Packet Tracer. Для додаткової перевірки можна виконати ping з комутатора SW1 до ПК3 (ping 192.168.30.10) — успішний результат підтверджує коректне налаштування шлюза за замовчуванням на комутаторі та прозорість комутації для керувального трафіку.

3.7 Моделювання відмови лінку та перевірка резервного шляху. Для моделювання аварійної ситуації на маршрутизаторі R1 вимикається основний інтерфейс, що з’єднує його з R2. Це імітує реальну відмову фізичного лінку, обладнання або кабелю. Після вимкнення інтерфейсу маршрутизатор автоматично видаляє всі маршрути, що використовували цей інтерфейс як вихідний шлюз, з таблиці маршрутизації. Оскільки резервні маршрути з адміністративною відстанню 200 тепер стають єдиними доступними шляхами до віддалених мереж, вони негайно активуються та додаються до таблиці маршрутизації. Цей процес відбувається без будь-якого втручання адміністратора, що демонструє ключову перевагу механізму відмовостійкості.

Для імітації відмови основного лінку між маршрутизаторами R1 та R2 вимикаємо інтерфейс GigabitEthernet0/0 на маршрутизаторі R1, що призводить до автоматичного видалення маршрутів, що використовували цей інтерфейс, та активації резервних маршрутів з адміністративною відстанню 200:

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# shutdown
```

Після вимкнення інтерфейсу негайно виконується повторний tracert 192.168.30.10 з ПК1. Тепер вивід демонструє інший шлях: перший стрибок — R1 (192.168.10.1), другий — R3 (10.0.0.10), третій — шлюз мережі PC3 (192.168.30.1). Це підтверджує, що трафік автоматично перемкнувся на резервний шлях через лінк R1–R3 без будь-якого втручання адміністратора. Для підтвердження змін у таблиці маршрутизації виконується команда show ip route на R1: тепер записи для мереж 192.168.20.0/24 та 192.168.30.0/24 мають шлюз 10.0.0.10 (інтерфейс R3) і зберігають позначку S з метрикою [200/0], що

свідчить про активацію резервних маршрутів. Час перемикання в середовищі Packet Tracer становить 2–5 секунд — це пов’язано з таймаутами виявлення відмови інтерфейсу на рівні канального шару. У реальному обладнанні з використанням механізмів типу BFD (Bidirectional Forwarding Detection) цей час може бути скорочений до десятків мілісекунд.

3.8 Відновлення штатного режиму. Для завершення тестування відновлюється штатний режим шляхом активації інтерфейсу, який був вимкнений на попередньому етапі. Після повернення інтерфейсу в робочий стан маршрутизатор автоматично виявляє доступність основного шляху та повторно додає маршрути з нижчою адміністративною відстанню (1) до таблиці маршрутизації. Резервні маршрути з AD=200 автоматично видаляються з активної таблиці, оскільки тепер існують кращі (з точки зору маршрутизації) шляхи до цільових мереж. Це демонструє повну циклічність механізму резервування: автоматичне перемикання на резерв при відмові та автоматичне повернення до основного шляху після його відновлення — без необхідності ручного втручання.

Для відновлення штатного режиму роботи мережі повертаємо інтерфейс GigabitEthernet0/0 маршрутизатора R1 у активний стан, що призводить до автоматичного відновлення основних маршрутів з адміністративною відстанню 1 та видалення резервних маршрутів з таблиці маршрутизації:

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# no shutdown
```

Повторний tracert 192.168.30.10 з ПК1 знову показує шлях через R2 (10.0.0.2), а команда show ip route на R1 підтверджує повернення основних маршрутів з AD=1 до таблиці. Для фінальної перевірки виконується повний цикл тестування зв’язності з усіх ПК до всіх інших ПК — усі пінги повинні бути успішними, що підтверджує повну функціональність мережі після відновлення штатного режиму.

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 № 9

Тема: Динамічна маршрутизація на основі протоколу OSPF

Мета роботи: Вивчити принципи роботи протоколу OSPF та набути практичних навичок його налаштування в маршрутизованій мережі

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1. Призначення маршрутизації в комп'ютерних мережах

Маршрутизація є одним з найважливіших процесів в сучасних комп'ютерних мережах, що забезпечує передачу даних між різними мережними сегментами та визначає оптимальні шляхи доставки пакетів від джерела до призначення. Основне завдання маршрутизації полягає в аналізі мережної топології, визначенні доступних шляхів та виборі найкращого маршруту на основі певних критеріїв, таких як відстань, пропускна здатність, затримка або вартість каналу зв'язку. Маршрутизатори підтримують спеціальні таблиці маршрутизації, які містять інформацію про доступні мережі та наступні переходи (next hop) для досягнення цих мереж. Процес маршрутизації включає в себе два основні компоненти: визначення шляху (path determination) та пересилання пакетів (packet forwarding), які працюють спільно для забезпечення надійної та ефективної доставки даних в мережі.

Ефективна маршрутизація критично важлива для забезпечення якості обслуговування в корпоративних мережах, мережах провайдерів та глобальній мережі Інтернет. Без правильно налаштованої маршрутизації мережа не може функціонувати як єдине ціле, оскільки пакети не зможуть знайти шлях до віддалених мереж. Маршрутизація також відіграє ключову роль в забезпеченні відмовостійкості мережі, дозволяючи автоматично перенаправляти трафік в обхід пошкоджених або перевантажених каналів зв'язку.

Існує два основних підходи до реалізації маршрутизації: статична та динамічна маршрутизація. Статична маршрутизація передбачає ручне налаштування маршрутів адміністратором мережі, що забезпечує повний контроль над процесом, але вимагає значних зусиль для підтримки в складних мережах з великою кількістю вузлів. Динамічна маршрутизація використовує спеціальні протоколи, які автоматично обмінюються інформацією про топологію мережі між маршрутизаторами та розраховують оптимальні маршрути на основі поточного стану мережі. Цей підхід значно спрощує адміністрування великих мереж та забезпечує швидку адаптацію до змін в топології.

1.2 Порівняльна характеристика протоколів маршрутизації

Протоколи динамічної маршрутизації класифікуються за різними критеріями, основними з яких є алгоритм роботи, область застосування та спосіб обміну маршрутною інформацією. За алгоритмом роботи протоколи поділяються на протоколи вектора відстані (distance vector) та протоколи стану каналу (link state), кожен з яких має свої переваги та недоліки в різних мережних сценаріях. Протоколи вектора відстані, такі як RIP та EIGRP, базуються на алгоритмі Беллмана-Форда та обмінюються інформацією про відстань до призначення з сусідніми маршрутизаторами, при цьому кожен маршрутизатор знає лише інформацію про безпосередніх сусідів та відстані до мереж. Протоколи стану каналу, представлені OSPF та IS-IS, використовують алгоритм Дейкстри та підтримують повну топологічну базу даних мережі, що дозволяє кожному маршрутизатору самостійно розраховувати найкращі маршрути до всіх призначень. Різниця в підходах визначає основні характеристики протоколів, такі як швидкість збіжності, споживання ресурсів та стійкість до петель маршрутизації.

Таблиця 9.1 - Порівняльна характеристика основних протоколів маршрутизації

Протокол	Тип алгоритму	Метрика	Час збіжності	Підтримка VLSM	Область застосування
RIP v1/v2	Distance Vector	Hop Count (1-15)	Повільна (90-180 сек)	v2 підтримує	Малі мережі
EIGRP	Hybrid	Composite (BW, Delay)	Швидка (1-3 сек)	Так	Cisco мережі
OSPF	Link State	Cost (100 Mbps/BW)	Швидка (1-10 сек)	Так	Середні/великі мережі
IS-IS	Link State	Cost (налаштовується)	Швидка (1-10 сек)	Так	Провайдерські мережі
BGP	Path Vector	AS Path, атрибути	Повільна (хвилини)	Так	Міжсистемна маршрутизація

Як видно з таблиці 9.1, кожен протокол має свої специфічні характеристики та призначений для вирішення певних завдань в мережній інфраструктурі. Протокол RIP, незважаючи на свою простоту, має обмеження в 15 переходів та повільну збіжність, що робить його непридатним для великих мереж, але корисним для навчальних цілей та простих топологій. EIGRP є пропрієтарним протоколом Cisco, який поєднує переваги обох підходів та забезпечує швидку збіжність з ефективним використанням мережних ресурсів, але його використання обмежене обладнанням одного виробника.

OSPF та IS-IS представляють сучасні протоколи стану каналу, які забезпечують швидку збіжність, підтримку складних топологій та ефективне масштабування в великих мережах. Основна відмінність між ними полягає в тому, що OSPF розроблений спеціально для IP мереж, тоді як IS-IS спочатку був призначений для OSI мереж та пізніше адаптований для IP. BGP займає

особливе місце як протокол міжсистемної маршрутизації, призначений для обміну маршрутною інформацією між різними автономними системами в Інтернеті.

Вибір протоколу маршрутизації залежить від багатьох факторів, включаючи розмір мережі, вимоги до швидкості збіжності, доступне обладнання та рівень кваліфікації адміністраторів. Для корпоративних мереж середнього та великого розміру найбільш поширеним вибором є OSPF завдяки його відкритому стандарту, швидкій збіжності та гнучким можливостям налаштування. Протокол також забезпечує хорошу підтримку різних типів мереж, включаючи Ethernet, Frame Relay та point-to-point з'єднання.

1.3 Детальний опис протоколу маршрутизації OSPF

Open Shortest Path First (OSPF) є протоколом маршрутизації стану каналу, розробленим робочою групою IETF та стандартизованим у RFC 2328 для версії 2, яка широко використовується в IPv4 мережах. Протокол базується на алгоритмі найкоротшого шляху Дейкстри (SPF) та забезпечує швидку збіжність, ефективне використання мережних ресурсів та високу стійкість до збоїв в мережі. OSPF підтримує ієрархічну структуру мережі через концепцію областей (areas), що дозволяє ефективно масштабувати протокол для використання в великих корпоративних мережах та мережах провайдерів послуг. Кожна область представляє логічну групу мереж та маршрутизаторів, які обмінюються детальною топологічною інформацією між собою, тоді як між областями передається лише узагальнена маршрутна інформація. Область 0, відома як backbone area, виконує роль центрального транзитного сегмента, через який проходить весь міжобласний трафік.

Робота OSPF базується на концепції Link State Database (LSDB) - топологічної бази даних, яку підтримує кожен маршрутизатор в області. База даних містить Link State Advertisements (LSA) - повідомлення, які описують стан каналів зв'язку та мережі, підключені до кожного маршрутизатора. Існує кілька типів LSA, кожен з яких несе специфічну інформацію: Router LSA (тип 1) описує канали маршрутизатора, Network LSA (тип 2) генерується призначеним маршрутизатором в багатодоступних мережах, Summary LSA (тип 3) передає інформацію про мережі з інших областей. Процес обміну LSA між маршрутизаторами включає кілька етапів: встановлення сусідських відносин, синхронізацію баз даних та періодичне оновлення інформації для підтримки консистентності.

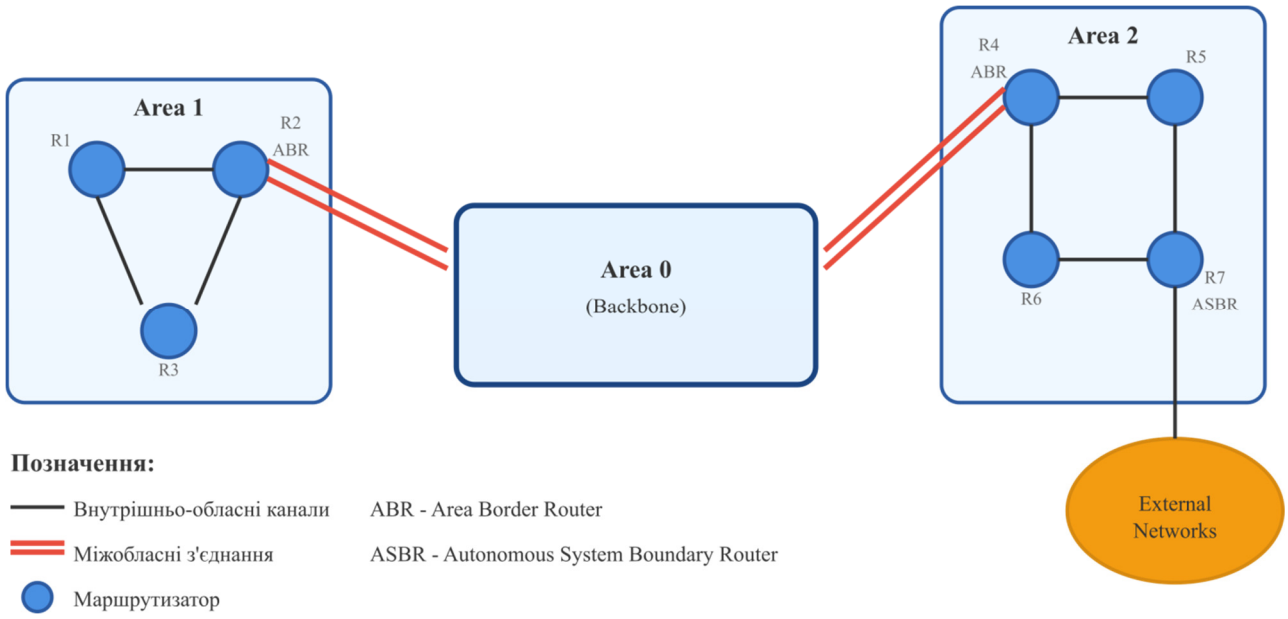

Рисунок 9.1 – Структура OSPF мережі з ієрархією областей

Рисунок 9.1 демонструє типову структуру OSPF мережі з трьома областями: центральна backbone область (Area 0) розташована в центрі схеми та представлена прямокутником з позначкою "Area 0 (Backbone)", від якої відходять з'єднання до двох периферійних областей. Ліва область позначена як "Area 1" та містить три маршрутизатори, з'єднаних між собою, причому один з них має подвійне з'єднання з backbone областю та позначений як Area Border Router (ABR). Права область "Area 2" має аналогічну структуру з чотирма маршрутизаторами, один з яких також є ABR. Всередині кожної області маршрутизатори з'єднані суцільними лініями, що позначають внутрішньо-обласні канали, тоді як з'єднання між областями показані подвійними лініями. Додатково, один з маршрутизаторів в Area 2 має з'єднання з хмарою, позначеною як "External Networks", що вказує на його роль як Autonomous System Boundary Router (ASBR).

Алгоритм SPF виконується кожним маршрутизатором незалежно на основі ідентичної топологічної бази даних, що гарантує консистентність маршрутних рішень в мережі. Процес розрахунку включає побудову дерева найкоротших шляхів з кореневою вершиною в поточному маршрутизаторі та визначення оптимальних маршрутів до всіх доступних призначень. Метрика OSPF, відома як cost, розраховується як відношення еталонної пропускної здатності (за замовчуванням 100 Мбіт/с) до реальної пропускної здатності інтерфейсу, що дозволяє віддавати перевагу каналам з вищою пропускною здатністю. Адміністратори можуть вручну налаштовувати значення cost для окремих інтерфейсів, що забезпечує гнучке управління потоками трафіку в мережі.

OSPF підтримує різні типи мереж, включаючи point-to-point, broadcast, non-broadcast multi-access (NBMA) та point-to-multipoint, кожен з яких має специфічні особливості роботи протоколу. В broadcast мережах, таких як Ethernet, OSPF обирає призначений маршрутизатор (Designated Router, DR) та резервний призначений маршрутизатор (Backup Designated Router, BDR) для

оптимізації обміну LSA та зменшення мережного трафіку. DR виконує роль центрального вузла для обміну топологічною інформацією, тоді як BDR готовий взяти на себе ці функції у випадку відмови DR. В point-to-point мережах такий механізм не потрібен, оскільки існує лише одне з'єднання між двома маршрутизаторами.

Процес встановлення сусідських відносин в OSPF включає обмін Hello пакетами, які передаються періодично для виявлення сусідніх маршрутизаторів та підтримки зв'язку. Hello пакети містають важливу інформацію, таку як Router ID, область, параметри автентифікації та інтервали передачі, які повинні співпадати для успішного встановлення сусідства. Після встановлення сусідських відносин маршрутизатори переходять до процесу синхронізації баз даних через обмін Database Description (DBD) пакетами, Link State Request (LSR) та Link State Update (LSU) повідомленнями. Цей процес забезпечує ідентичність топологічних баз даних у всіх маршрутизаторів області, що є критично важливим для правильної роботи алгоритму SPF.

1.4 Команди та приклади налаштування маршрутизатора Cisco IOS з використанням протоколу OSPF

Конфігурування OSPF на маршрутизаторах Cisco IOS починається з активації процесу OSPF та призначення унікального ідентифікатора процесу, який має локальне значення та не повинен співпадати на різних маршрутизаторах. Команда router ospf [process-id] переводить маршрутизатор в режим конфігурації OSPF, де process-id є числом від 1 до 65535 та використовується для ідентифікації процесу OSPF на локальному маршрутизаторі. Наступним важливим кроком є встановлення Router ID за допомогою команди router-id [ip-address], яка визначає унікальний ідентифікатор маршрутизатора в OSPF домені. Router ID повинен бути унікальним в межах автономної системи та зазвичай встановлюється як IP адреса одного з інтерфейсів маршрутизатора або як спеціально призначена адреса для спрощення ідентифікації. Якщо Router ID не встановлений вручну, система автоматично обирає найвищу IP адресу серед активних інтерфейсів, при цьому пріоритет надається loopback інтерфейсам. Після налаштування основних параметрів необхідно визначити мережі, які будуть оголошені в OSPF, за допомогою команди network [network] [wildcard-mask] area [area-id].

Таблиця 9.2 - Основні команди конфігурації OSPF в Cisco IOS

Команда	Режим конфігурації	Призначення
router ospf [process-id]	Global Config	Активація процесу OSPF
router-id [ip-address]	Router Config	Встановлення Router ID
network [ip] [wildcard] area [area]	Router Config	Оголошення мереж в OSPF
area [area-id] stub	Router Config	Конфігурація stub області
ip ospf cost [value]	Interface Config	Налаштування метрики інтерфейсу
ip ospf hello-interval [seconds]	Interface Config	Інтервал Hello пакетів
ip ospf dead-interval [seconds]	Interface Config	Інтервал dead таймера
ip ospf priority [value]	Interface Config	Пріоритет для вибору DR/BDR

Згідно з таблицею 1.2, процес конфігурації OSPF включає команди різних рівнів, від глобальних налаштувань до специфічних параметрів інтерфейсів. Команда network використовує wildcard маску, яка є інверсією звичайної маски підмережі та визначає, які біти IP адреси повинні точно співпадати для включення інтерфейсу в OSPF процес. Наприклад, для мережі 192.168.1.0/24 wildcard маска буде 0.0.0.255, що означає точне співпадіння перших трьох октетів та ігнорування останнього октету. Область (area) визначає логічну групу мереж, при цьому область 0 завжди є backbone областю та обов'язкова в будь-якій OSPF топології.

Розглянемо практичний приклад базової конфігурації OSPF для маршрутизатора з двома інтерфейсами. Перший інтерфейс FastEthernet0/0 з IP адресою 10.1.1.1/30 з'єднує маршрутизатор з іншим OSPF маршрутизатором, а другий інтерфейс Vlan10 з адресою 192.168.10.1/24 обслуговує локальну мережу. Команди конфігурації будуть наступними: router ospf 1 для активації процесу, router-id 1.1.1.1 для встановлення ідентифікатора, network 10.1.1.0 0.0.0.3 area 0 для включення WAN з'єднання в backbone область та network 192.168.10.0 0.0.0.255 area 0 для оголошення локальної мережі. Ця конфігурація забезпечить участь обох мереж в OSPF процесі та дозволить іншим маршрутизаторам дізнатися про доступність цих мереж.

Налаштування специфічних параметрів інтерфейсів дозволяє точно контролювати поведінку OSPF в різних мережних сегментах. Команда ip ospf cost [value] встановлює метрику інтерфейсу, що може бути корисно для управління вибором маршруту в топологіях з множинними шляхами. Зменшення значення cost робить інтерфейс більш привабливим для OSPF, тоді як збільшення значення знижує його пріоритет. Параметри hello-interval та dead-interval контролюють частоту обміну Hello пакетами та час очікування відповіді від сусіда відповідно, при цьому dead-interval зазвичай встановлюється в чотири рази більшим за hello-interval. Команда ip ospf priority [value] впливає на процес вибору DR та BDR в broadcast мережах, де маршрутизатор з найвищим пріоритетом стає DR, а з другим за величиною - BDR.

Перевірка роботи OSPF здійснюється за допомогою спеціальних команд діагностики, які дозволяють аналізувати стан протоколу та виявляти можливі проблеми конфігурації. Команда show ip ospf neighbor відображає список OSPF сусідів, їх стан, пріоритети та IP адреси, що є першим кроком у діагностиці проблем зв'язності. Стан сусідів повинен бути "Full" для нормальної роботи, інші стани можуть вказувати на проблеми конфігурації або мережні збої. Команда show ip ospf database надає детальну інформацію про Link State Database, включаючи всі LSA та їх характеристики, що дозволяє аналізувати топологію мережі з точки зору OSPF. Для перегляду таблиці маршрутизації використовується команда show ip route ospf, яка показує всі маршрути, вивчені через OSPF, з їх метриками та next-hop адресами.

Таблиця 9.3 – Варіанти індивідуальних завдань

№	LAN			WAN R1 ↔ R2		WAN R1 ↔ R3		WAN R2 ↔ R3	
	R1 (VLAN 10)	R2 (VLAN 20)	R3 (VLAN 30)	R1	R2	R1	R3	R2	R3
1	192.168.1.0/24	192.168.2.0/24	192.168.3.0/24	10.12.0.1	10.12.0.2	10.13.0.1	10.13.0.2	10.23.0.1	10.23.0.2
2	192.168.4.0/24	192.168.5.0/24	192.168.6.0/24	10.12.1.1	10.12.1.2	10.13.1.1	10.13.1.2	10.23.1.1	10.23.1.2
3	192.168.7.0/24	192.168.8.0/24	192.168.9.0/24	10.12.2.1	10.12.2.2	10.13.2.1	10.13.2.2	10.23.2.1	10.23.2.2
4	192.168.10.0/24	192.168.11.0/24	192.168.12.0/24	10.12.3.1	10.12.3.2	10.13.3.1	10.13.3.2	10.23.3.1	10.23.3.2
5	192.168.13.0/24	192.168.14.0/24	192.168.15.0/24	10.12.4.1	10.12.4.2	10.13.4.1	10.13.4.2	10.23.4.1	10.23.4.2
6	192.168.16.0/24	192.168.17.0/24	192.168.18.0/24	10.12.5.1	10.12.5.2	10.13.5.1	10.13.5.2	10.23.5.1	10.23.5.2
7	192.168.19.0/24	192.168.20.0/24	192.168.21.0/24	10.12.6.1	10.12.6.2	10.13.6.1	10.13.6.2	10.23.6.1	10.23.6.2
8	192.168.22.0/24	192.168.23.0/24	192.168.24.0/24	10.12.7.1	10.12.7.2	10.13.7.1	10.13.7.2	10.23.7.1	10.23.7.2
9	192.168.25.0/24	192.168.26.0/24	192.168.27.0/24	10.12.8.1	10.12.8.2	10.13.8.1	10.13.8.2	10.23.8.1	10.23.8.2
10	192.168.28.0/24	192.168.29.0/24	192.168.30.0/24	10.12.9.1	10.12.9.2	10.13.9.1	10.13.9.2	10.23.9.1	10.23.9.2
11	192.168.31.0/24	192.168.32.0/24	192.168.33.0/24	10.12.10.1	10.12.10.2	10.13.10.1	10.13.10.2	10.23.10.1	10.23.10.2
12	192.168.34.0/24	192.168.35.0/24	192.168.36.0/24	10.12.11.1	10.12.11.2	10.13.11.1	10.13.11.2	10.23.11.1	10.23.11.2
13	192.168.37.0/24	192.168.38.0/24	192.168.39.0/24	10.12.12.1	10.12.12.2	10.13.12.1	10.13.12.2	10.23.12.1	10.23.12.2
14	192.168.40.0/24	192.168.41.0/24	192.168.42.0/24	10.12.13.1	10.12.13.2	10.13.13.1	10.13.13.2	10.23.13.1	10.23.13.2
15	192.168.43.0/24	192.168.44.0/24	192.168.45.0/24	10.12.14.1	10.12.14.2	10.13.14.1	10.13.14.2	10.23.14.1	10.23.14.2
16	192.168.46.0/24	192.168.47.0/24	192.168.48.0/24	10.12.15.1	10.12.15.2	10.13.15.1	10.13.15.2	10.23.15.1	10.23.15.2
17	192.168.49.0/24	192.168.50.0/24	192.168.51.0/24	10.12.16.1	10.12.16.2	10.13.16.1	10.13.16.2	10.23.16.1	10.23.16.2
18	192.168.52.0/24	192.168.53.0/24	192.168.54.0/24	10.12.17.1	10.12.17.2	10.13.17.1	10.13.17.2	10.23.17.1	10.23.17.2
19	192.168.55.0/24	192.168.56.0/24	192.168.57.0/24	10.12.18.1	10.12.18.2	10.13.18.1	10.13.18.2	10.23.18.1	10.23.18.2
20	192.168.58.0/24	192.168.59.0/24	192.168.60.0/24	10.12.19.1	10.12.19.2	10.13.19.1	10.13.19.2	10.23.19.1	10.23.19.2
21	192.168.61.0/24	192.168.62.0/24	192.168.63.0/24	10.12.20.1	10.12.20.2	10.13.20.1	10.13.20.2	10.23.20.1	10.23.20.2
22	192.168.64.0/24	192.168.65.0/24	192.168.66.0/24	10.12.21.1	10.12.21.2	10.13.21.1	10.13.21.2	10.23.21.1	10.23.21.2
23	192.168.67.0/24	192.168.68.0/24	192.168.69.0/24	10.12.22.1	10.12.22.2	10.13.22.1	10.13.22.2	10.23.22.1	10.23.22.2
24	192.168.70.0/24	192.168.71.0/24	192.168.72.0/24	10.12.23.1	10.12.23.2	10.13.23.1	10.13.23.2	10.23.23.1	10.23.23.2
25	192.168.73.0/24	192.168.74.0/24	192.168.75.0/24	10.12.24.1	10.12.24.2	10.13.24.1	10.13.24.2	10.23.24.1	10.23.24.2
26	192.168.76.0/24	192.168.77.0/24	192.168.78.0/24	10.12.25.1	10.12.25.2	10.13.25.1	10.13.25.2	10.23.25.1	10.23.25.2
27	192.168.79.0/24	192.168.80.0/24	192.168.81.0/24	10.12.26.1	10.12.26.2	10.13.26.1	10.13.26.2	10.23.26.1	10.23.26.2
28	192.168.82.0/24	192.168.83.0/24	192.168.84.0/24	10.12.27.1	10.12.27.2	10.13.27.1	10.13.27.2	10.23.27.1	10.23.27.2
29	192.168.85.0/24	192.168.86.0/24	192.168.87.0/24	10.12.28.1	10.12.28.2	10.13.28.1	10.13.28.2	10.23.28.1	10.23.28.2
30	192.168.88.0/24	192.168.89.0/24	192.168.90.0/24	10.12.29.1	10.12.29.2	10.13.29.1	10.13.29.2	10.23.29.1	10.23.29.2

2 КЛЮЧОВІ ПИТАННЯ

1. Які основні етапи конфігурації протоколу OSPF на маршрутизаторі Cisco?
2. Навіщо використовується wildcard-маска при оголошенні мереж у OSPF, і як її правильно розрахувати?
3. Яку роль відіграє Router ID у протоколі OSPF, і як його можна налаштувати вручну?
4. Чому в лабораторній роботі всі мережі включено в Area 0, і які переваги це дає в топології з трьох маршрутизаторів?
5. Як налаштувати DHCP-сервер на маршрутизаторі Cisco для автоматичного призначення IP-адрес клієнтам у локальній мережі?
6. Які команди використовуються для перевірки сусідства OSPF та аналізу таблиці маршрутизації?
7. Чому для point-to-point з’єднань між маршрутизаторами використовується маска /30?
8. Як забезпечується відмовостійкість мережі в кільцевій топології за допомогою OSPF?
9. Як налаштовується VLAN та SVI (Switch Virtual Interface) на маршрутизаторі з модулем HWIC-4ESW для підтримки локальної мережі?
10. Як перевірити наскрізну зв’язність між хостами в різних підмережах після налаштування OSPF та DHCP?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. Архітектура мережі та план адресації. Представлена мережна архітектура базується на кільцевій топології з використанням трьох маршрутизаторів Cisco 1841, кожен з яких обладнаний двома вбудованими FastEthernet інтерфейсами та картою розширення HWIC-4ESW для створення додаткових портів комутації. Маршрутизатори R1, R2 та R3 з'єднані між собою у повнозв'язану топологію, де кожен маршрутизатор має пряме з'єднання з двома іншими, що створює три окремі WAN сегменти з підмережами /30 для оптимального використання IP адрес у point-to-point з'єднаннях. Така архітектура забезпечує високу відмовостійкість мережі, оскільки при виході з ладу будь-якого каналу зв'язку між маршрутизаторами трафік може бути автоматично перенаправлений через альтернативний шлях, а протокол OSPF динамічно перерахує найкоротші маршрути та забезпечить безперервність зв'язку. Кожен маршрутизатор обслуговує власний локальний сегмент мережі класу C (192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24) через інтерфейс FastEthernet0/1/0 карти розширення, до якого підключена одна робоча станція, що отримує IP адресу автоматично через DHCP сервіс, налаштований безпосередньо на маршрутизаторі.

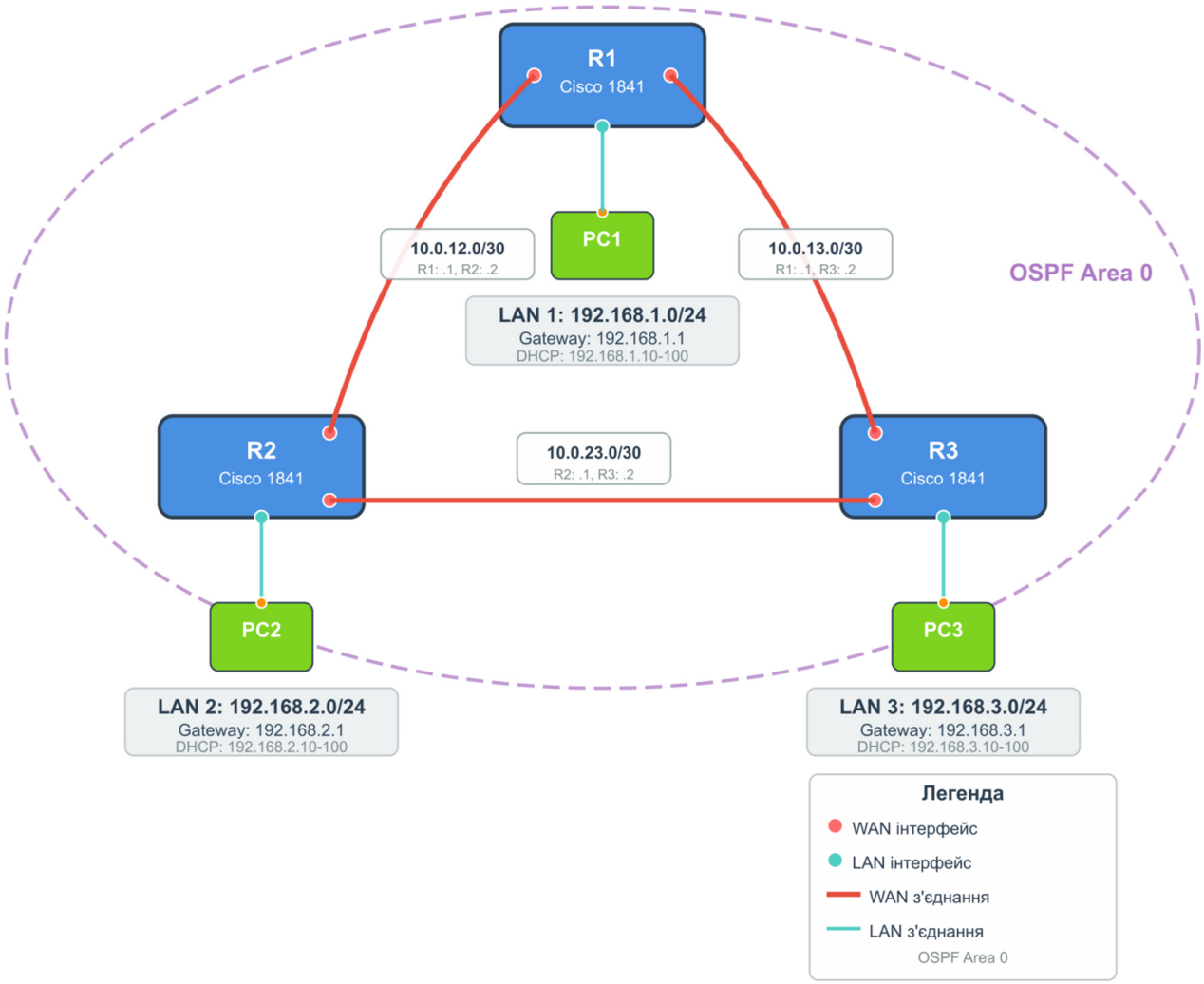

Рисунок 9.2 – Топологія мережі OSPF (кільцева архітектура)

Протокол OSPF Area 0 об'єднує всі мережні сегменти в єдиний домен маршрутизації, де кожен маршрутизатор має унікальний Router ID та підтримує повну топологічну базу даних усієї мережі для розрахунку оптимальних маршрутів за алгоритмом найкоротшого шляху. WAN з'єднання використовують приватні IP адреси з мереж 10.0.12.0/30 (R1-R2), 10.0.13.0/30 (R1-R3) та 10.0.23.0/30 (R2-R3), що дозволяє ефективно сегментувати міжмаршрутизаторський трафік та спростити діагностику мережі. DHCP сервіси на кожному маршрутизаторі працюють незалежно один від одного, призначаючи IP адреси з діапазонів 192.168.x.10-192.168.x.100, залишаючи початкові адреси кожної підмережі для статичного призначення мережному обладнанню та серверам. Така архітектура забезпечує масштабованість рішення, оскільки до кожного маршрутизатора можна підключити додаткові комутатори або точки доступу через вільні порти карти розширення HWIC-4ESW, а кільцева топологія дозволяє легко інтегрувати додаткові маршрутизатори без порушення існуючої структури мережі. Використання єдиної OSPF області спрощує конфігурацію та забезпечує швидку конвергенцію протоколу при змінах топології, що є критично важливим для підтримання стабільної роботи корпоративної мережі.

Таблиця 9.4 – Розподіл IP-адрес мережних пристроїів у прикладів лабораторного завдання

МАРШРУТИЗАТОР	ІНТЕРФЕЙС	ТИП МЕРЕЖІ	IP-АДРЕСА	МЕРЕЖА	ПРИЗНАЧЕННЯ
R1	FastEthernet0/1/0	LAN	192.168.1.1	192.168.1.0/24	Локальна мережа
	FastEthernet0/0	WAN	10.0.12.1	10.0.12.0/30	Підключення до R2
	FastEthernet0/1	WAN	10.0.13.1	10.0.13.0/30	Підключення до R3
R2	FastEthernet0/1/0	LAN	192.168.2.1	192.168.2.0/24	Локальна мережа
	FastEthernet0/0	WAN	10.0.12.2	10.0.12.0/30	Підключення до R1
	FastEthernet0/1	WAN	10.0.23.1	10.0.23.0/30	Підключення до R3
R3	FastEthernet0/1/0	LAN	192.168.3.1	192.168.3.0/24	Локальна мережа
	FastEthernet0/0	WAN	10.0.13.2	10.0.13.0/30	Підключення до R1
	FastEthernet0/1	WAN	10.0.23.2	10.0.23.0/30	Підключення до R2

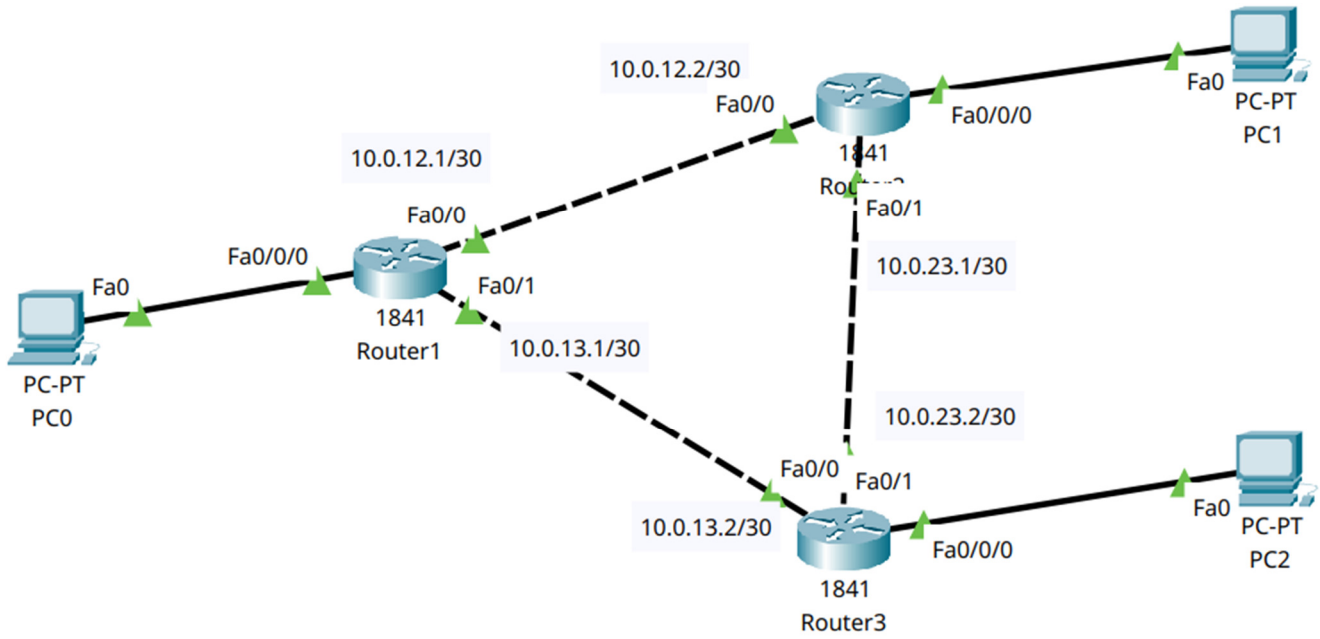

Рисунок 9.3 – Модель мережі в Cisco Packet Tracer

3.2 Базове конфігурування маршрутизатора R1. На першому етапі необхідно виконати базове конфігурування маршрутизатора R1, що включає налаштування імені пристрою, інтерфейсів та їх IP адрес. Маршрутизатор R1 буде виконувати роль центрального вузла в нашій кільцевій топології та обслуговувати локальну мережу 192.168.1.0/24. Для забезпечення зв'язності між маршрутизаторами налаштовуються WAN інтерфейси з адресами підмереж /30, що є оптимальним рішенням для point-to-point з'єднань між маршрутизаторами,

оскільки така маска дозволяє використовувати лише дві корисні IP адреси. Карта розширення HWIC-4ESW працює як Layer 2 комутатор, тому для призначення IP адреси необхідно створити VLAN інтерфейс (SVI) та призначити йому IP адресу, а також налаштувати порти комутатора для роботи в цій VLAN. Важливо переконатись, що всі інтерфейси активовані командою no shutdown та правильно налаштовані IP адреси з відповідними масками підмережі.

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 10.0.12.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface fastethernet0/1
R1(config-if)# ip address 10.0.13.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface vlan 10
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface fastethernet0/0/0
R1(config-if)# switchport mode access
R1(config-if)# switchport access vlan 10
R1(config-if)# exit
```

3.3 Конфігурування DHCP на маршрутизаторі R1. Налаштування DHCP сервісу на маршрутизаторі дозволяє автоматично призначати IP адреси клієнтським пристроям у локальній мережі, що значно спрощує адміністрування та зменшує ймовірність конфліктів адрес. DHCP пул визначає діапазон адрес, які можуть бути призначені клієнтам, а також додаткові параметри мережі, такі як шлюз за замовчуванням та DNS сервери. У нашій конфігурації мережа 192.168.1.0/24 буде обслуговувати клієнтські пристрої з діапазону адрес від 192.168.1.10 до 192.168.1.100, що залишає достатньо адрес для статичного призначення серверам та мережному обладнанню. Шлюзом за замовчуванням для всіх клієнтів буде IP адреса інтерфейсу маршрутизатора 192.168.1.1. Команда ip dhcp excluded-address дозволяє виключити певні адреси з пулу DHCP, щоб зарезервувати їх для статичного призначення критично важливим пристроям.

```
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R1(config)# ip dhcp pool LAN1
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 8.8.8.8
R1(dhcp-config)# exit
R1(config)# service dhcp
```

3.4 Конфігурування OSPF на маршрутизаторі R1

Конфігурування протоколу OSPF на маршрутизаторі є ключовим етапом створення динамічної маршрутизації в мережі. OSPF використовує концепцію областей (areas) для ієрархічної організації мережі, де область 0 завжди є магістральною (backbone area). Процес OSPF ідентифікується унікальним номером (в нашому випадку 1), а Router ID може бути встановлений вручну або автоматично обраний як найвища IP адреса loopback інтерфейсу. Команда network визначає, які мережі будуть оголошені в OSPF та на яких інтерфейсах буде активований протокол. Wildcard маска є інверсією звичайної маски підмережі - для мережі /24 wildcard маска буде 0.0.0.255, а для мережі /30 - 0.0.0.3. При використанні VLAN інтерфейсу для локальної мережі, OSPF оголошує мережу через SVI (Switch Virtual Interface), який працює на Layer 3 рівні та забезпечує маршрутизацію між VLAN та зовнішніми мережами. Всі мережі в нашій топології будуть належати до області 0, що спрощує конфігурацію та забезпечує оптимальну маршрутизацію між всіма сегментами мережі.

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.0.12.0 0.0.0.3 area 0
R1(config-router)# network 10.0.13.0 0.0.0.3 area 0
R1(config-router)# exit
```

3.5 Базове конфігурування та DHCP на маршрутизаторі R2. Конфігурування маршрутизатора R2 виконується за аналогічним принципом до R1, але з використанням відповідних IP адрес для другого сегмента мережі. Маршрутизатор R2 обслуговуватиме локальну мережу 192.168.2.0/24 та матиме WAN з'єднання з маршрутизаторами R1 та R3. Важливо дотримуватись правильної послідовності конфігурування інтерфейсів відповідно до схеми топології, щоб уникнути конфліктів адрес та забезпечити коректну роботу протоколів маршрутизації. Оскільки карта HWIC-4ESW працює як Layer 2 комутатор, необхідно створити окрему VLAN (у нашому випадку VLAN 20) та відповідний SVI інтерфейс для призначення IP адреси локальній мережі. Порт FastEthernet0/1/0 налаштовується як access порт у VLAN 20, що дозволяє підключеним пристроям отримувати доступ до мережі через цей VLAN інтерфейс. DHCP сервіс на R2 буде працювати незалежно від інших маршрутизаторів, обслуговуючи лише локальних клієнтів у мережі 192.168.2.0/24, при цьому шлюзом за замовчуванням буде IP адреса SVI інтерфейсу VLAN 20.

```
Router> enable
Router# configure terminal
Router(config)# hostname R2
```

```
R2(config)# interface fastethernet0/0
R2(config-if)# ip address 10.0.12.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface fastethernet0/1
R2(config-if)# ip address 10.0.23.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface vlan 20
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface fastethernet0/0/0
R2(config-if)# switchport mode access
R2(config-if)# switchport access vlan 20
R2(config-if)# exit
R2(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.9
R2(config)# ip dhcp pool LAN2
R2(dhcp-config)# network 192.168.2.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.2.1
R2(dhcp-config)# dns-server 8.8.8.8
R2(dhcp-config)# exit
R2(config)# service dhcp
```

3.6 Конфігурування OSPF на маршрутизаторі R2. Активація протоколу OSPF на маршрутизаторі R2 завершує налаштування другого вузла нашої мережі та дозволяє йому обмінюватися маршрутною інформацією з іншими OSPF маршрутизаторами. Router ID для R2 встановлюється як 2.2.2.2, що дозволяє легко ідентифікувати цей маршрутизатор в OSPF базі даних та спрощує діагностику мережі. Важливо правильно вказати всі мережі, які повинні бути оголошені через OSPF - це включає локальну мережу 192.168.2.0/24 та WAN підключення до R1 і R3. Використання правильних wildcard масок забезпечує точне визначення мережних сегментів, які будуть включені в OSPF процес. Після активації OSPF на R2, маршрутизатор почне встановлювати сусідські відносини з R1 через мережу 10.0.12.0/30, обмінюватися LSA (Link State Advertisement) повідомленнями та будувати спільну топологічну базу даних мережі для розрахунку найкоротших шляхів до всіх призначень.

```
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
R2(config-router)# network 10.0.12.0 0.0.0.3 area 0
R2(config-router)# network 10.0.23.0 0.0.0.3 area 0
R2(config-router)# exit
```

3.7 Базове конфігурування та DHCP на маршрутизаторі R3. Маршрутизатор R3 завершує нашу кільцеву топологію, встановлюючи з'єднання як з R1, так і з R2, що створює надлишковість шляхів та підвищує

відмовостійкість мережі. Конфігурування R3 включає налаштування двох WAN інтерфейсів для підключення до інших маршрутизаторів та створення VLAN 30 з відповідним SVI інтерфейсом для обслуговування локальної мережі 192.168.3.0/24. Кільцева топологія забезпечує автоматичне перемикання трафіку на альтернативний шлях у випадку виходу з ладу одного з каналів зв'язку, що є важливою перевагою такої архітектури мережі. Карта HWIC-4ESW на R3, як і на інших маршрутизаторах, працює в режимі Layer 2 комутатора, тому порт FastEthernet0/1/0 налаштовується як access порт у VLAN 30, а IP адреса призначається відповідному SVI інтерфейсу. DHCP сервіс на R3 працюватиме незалежно від інших маршрутизаторів, забезпечуючи автоматичне призначення IP адрес локальним клієнтам у третьому сегменті мережі. Правильне налаштування всіх інтерфейсів та DHCP параметрів на R3 є критично важливим для завершення повної конфігурації мережної інфраструктури та забезпечення зв'язності між всіма сегментами мережі.

```
Router> enable
Router# configure terminal
Router(config)# hostname R3
R3(config)# interface fastethernet0/0
R3(config-if)# ip address 10.0.13.2 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# interface fastethernet0/1
R3(config-if)# ip address 10.0.23.2 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# interface vlan 30
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# interface fastethernet0/0/0
R3(config-if)# switchport mode access
R3(config-if)# switchport access vlan 30
R3(config-if)# exit
R3(config)# ip dhcp excluded-address 192.168.3.1 192.168.3.9
R3(config)# ip dhcp pool LAN3
R3(dhcp-config)# network 192.168.3.0 255.255.255.0
R3(dhcp-config)# default-router 192.168.3.1
R3(dhcp-config)# dns-server 8.8.8.8
R3(dhcp-config)# exit
R3(config)# service dhcp
```

3.8 Конфігурування OSPF на маршрутизаторі R3 та завершення налаштування. Активація протоколу OSPF на маршрутизаторі R3 завершує конфігурування динамічної маршрутизації в нашій мережі та дозволяє всім трьом маршрутизаторам обмінюватися повною інформацією про топологію мережі. Router ID 3.3.3.3 для R3 завершує логічну схему ідентифікації маршрутизаторів у OSPF домені. Після активації OSPF на всіх трьох маршрутизаторах, протокол автоматично виявить всі можливі шляхи між

мережними сегментами та обчислить найкоротші маршрути за допомогою алгоритму Дейкстри. Кільцева топологія забезпечить наявність альтернативних шляхів між будь-якими двома точками мережі, що підвищує її надійність та продуктивність. OSPF автоматично адаптуватиметься до змін у топології, швидко переключаючи трафік на резервні шляхи у випадку відмови основних каналів зв'язку. Правильне налаштування всіх мережних сегментів в області 0 забезпечує оптимальну маршрутизацію та мінімізує накладні витрати протоколу на обчислення та обмін маршрутною інформацією.

```
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.0.13.0 0.0.0.3 area 0
R3(config-router)# network 10.0.23.0 0.0.0.3 area 0
R3(config-router)# exit
R3(config)# exit
R3# write memory
```

3.9 Перевірка конфігурації та зв'язності мережі. Після завершення конфігурування всіх маршрутизаторів необхідно провести комплексну перевірку роботи мережі, що включає тестування OSPF сусідських відносин, аналіз таблиці маршрутизації та перевірку зв'язності між різними сегментами мережі. Команда show ip ospf neighbor відображає інформацію про встановлені OSPF сусідства, їх стан та пріоритети, що дозволяє переконатися в правильності роботи протоколу. Таблиця маршрутизації, яку можна переглянути командою show ip route, повинна містити всі мережні сегменти з позначкою "O" (OSPF learned routes), що підтверджує успішне поширення маршрутної інформації між маршрутизаторами. Тестування зв'язності за допомогою команди ping з різних робочих станцій до адрес в інших мережних сегментах дозволяє перевірити наскрізну зв'язність та правильність роботи DHCP сервісів. Важливо також перевірити роботу механізму відмовостійкості, тимчасово відключивши один з каналів зв'язку та переконавшись, що трафік автоматично перемикається на альтернативний шлях без втрати зв'язності.

Таблиця 9.5 – Команди для перевірки на кожному маршрутизаторі

Дія	Команда(и)
Перевірка OSPF сусідства	R1# show ip ospf neighbor
Перевірка таблиці маршрутизації	R1# show ip route
Перевірка інтерфейсів	R1# show ip interface brief
Перевірка OSPF бази даних	R1# show ip ospf database
Перевірка DHCP призначень	R1# show ip dhcp binding
Тестування зв'язності	R1# ping 192.168.2.1 R1# ping 192.168.3.1

Тестування мережі здійснюється з робочих станцій для перевірки її коректної роботи та виявлення можливих проблем. Спочатку необхідно

переконатися, що кожна комп’ютерна станція (PC) успішно отримала IP-адресу від DHCP-сервера, що свідчить про належну функціонування служби динамічного призначення адрес. Після цього слід виконати команду ping з першого комп’ютера (PC1) до другого (PC2) та третього (PC3), щоб перевірити наявність зв’язку між вузлами та виявити можливі проблеми з маршрутизацією або фізичним з’єднанням. Додатково рекомендується використати команду traceroute для детального аналізу шляху, яким проходять пакети між пристроями, що допоможе виявити затримки або точки відмови в мережі. Також важливо протестувати відмовостійкість системи — для цього слід штучно відключити один із мережевих каналів зв’язку та перевірити, чи мережа здатна продовжувати функціонувати без перерв завдяки резервним шляхам або механізмам відновлення.

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 № 10

Тема: Динамічна маршрутизація EIGRP та механізми швидкої збіжності

Мета роботи: Опанувати налаштування протоколу EIGRP та дослідити механізми швидкої збіжності в динамічній маршрутизації

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1. Принципи функціонування протоколу EIGRP

Сучасні комп’ютерні мережі характеризуються постійною зміною топології, виникненням нових сегментів та відмовою окремих ліній зв’язку, що створює потребу в автоматизованих механізмах визначення оптимальних шляхів передачі даних. Протоколи динамічної маршрутизації відіграють ключову роль у забезпеченні надійності та ефективності функціонування мереж, оскільки дозволяють маршрутизаторам автоматично обмінюватися інформацією про доступність мереж та адаптуватися до змін без втручання адміністратора. Серед існуючих протоколів маршрутизації протокол EIGRP (Enhanced Interior Gateway Routing Protocol), розроблений компанією Cisco, займає особливе місце завдяки поєднанню переваг дистанційно-векторних та протоколів стану каналів. На відміну від класичного протоколу RIP, який використовує просту метрику на основі кількості стрибків і має обмеження у 15 хопів, EIGRP застосовує складну композитну метрику, що враховує пропускну здатність, затримку, завантаженість та надійність каналів, що дозволяє обирати дійсно оптимальні шляхи в складних топологіях. Крім того, завдяки алгоритму DUAL (Diffusing Update Algorithm) протокол забезпечує миттєву реакцію на зміни топології за рахунок збереження резервних маршрутів у таблиці топології, що робить його придатним для критично важливих корпоративних середовищ. Хоча EIGRP спочатку був пропрієтарним протоколом Cisco, його часткова відкритість у 2013 році сприяла поширенню в гетерогенних мережах, проте в навчальних лабораторіях він залишається ідеальним інструментом для вивчення сучасних механізмів маршрутизації завдяки інтуїтивно зрозумілій конфігурації та наочній демонстрації ключових концепцій, таких як швидка збіжність та відмовостійкість.

Протокол EIGRP належить до класу гібридних протоколів маршрутизації, що поєднують риси дистанційно-векторних алгоритмів (ефективність обміну інформацією) та протоколів стану каналів (точність топологічної інформації). На відміну від традиційних дистанційно-векторних протоколів, які пересилають повну таблицю маршрутів усім сусідам через фіксовані інтервали, EIGRP використовує інкрементні оновлення та надсилає інформацію лише при змінах у топології, що значно зменшує навантаження на мережу. Ключовим механізмом протоколу є алгоритм DUAL, який забезпечує безпетльову маршрутизацію шляхом математичного аналізу відстаней до мереж та зберігання не лише оптимального маршруту (Successor), але й резервних шляхів

(Feasible Successor), що задовольняють умову можливості (Feasibility Condition). Ця умова визначається як вимога до того, щоб відстань, оголошена сусідом (Reported Distance), була меншою за повну відстань до мережі через поточний оптимальний шлях (Feasible Distance), що гарантує відсутність петель при перемиканні на резервний маршрут. Для обчислення метрики EIGRP використовує композитну формулу, яка за замовчуванням враховує лише два параметри: пропускну здатність (найнижча пропускна здатність на шляху) та затримку (сумарна затримка всіх інтерфейсів на шляху), хоча теоретично можливе врахування завантаженості та надійності каналів через налаштування K-значень. Важливою особливістю протоколу є використання ненадійного транспорту для службових пакетів (наприклад, Hello) та надійного транспорту для критичної інформації (наприклад, оновлень маршрутів), що досягається за рахунок механізму підтверджень (Acknowledgements) без використання повноцінного TCP. Такий підхід забезпечує баланс між надійністю передачі службової інформації та мінімізацією накладних витрат на встановлення з’єднань.

Таблиця 10.1 — Основні типи пакетів протоколу EIGRP та їх призначення

Тип пакета	Призначення	Надійна доставка	Періодичність
Hello	Встановлення та підтримка сусідства	Ні	Кожні 5 сек (широкосмугові лінки)
Update	Передача інформації про доступні мережі	Так	При змінах топології
Query	Запит про недоступну мережу під час перерахунку	Так	При втраті всіх маршрутів до мережі
Reply	Відповідь на запит Query	Так	Після отримання Query
ACK	Підтвердження отримання надійного пакета	Ні	Після отримання надійного пакета

Передача службових пакетів у мережі EIGRP здійснюється за допомогою мультикастової адреси 224.0.0.10 для пакетів типу Hello та унікастової адресації для надійних пакетів (Update, Query, Reply). Пакети типу Hello надсилаються періодично кожним маршрутизатором для підтримки сусідства, і якщо протягом часу, вказаного в таймері Hold (зазвичай утричі більше за інтервал Hello), не отримано жодного пакета від сусіда, він вважається недоступним, і запускається процес перерахунку маршрутів. Пакети Update використовуються для початкового обміну інформацією про мережі після встановлення сусідства та для інкрементних оновлень при змінах топології, причому вони надсилаються лише тим сусідам, які потребують цієї інформації, що значно ефективніше за повний обмін таблицями, як у протоколі RIP. У разі втрати всіх маршрутів до певної мережі маршрутизатор надсилає пакети Query своїм сусідам для пошуку альтернативних шляхів, що може ініціювати лавиноподібний процес запитів у мережі, однак алгоритм DUAL мінімізує його тривалість завдяки наявності резервних маршрутів. Пакети Reply надсилаються

у відповідь на Query і містять інформацію про доступність мережі або підтвердження її недоступності. Механізм підтверджень (ACK) реалізований у вигляді спеціальних пакетів з нульовою корисною інформацією, які підтверджують отримання надійних пакетів, що дозволяє уникнути повторної передачі при втраті пакетів. Така структура пакетів забезпечує ефективний баланс між надійністю обміну інформацією та мінімізацією службового трафіку в мережі.

1.2 Структура таблиць протоколу EIGRP

Робота протоколу EIGRP ґрунтується на трьох ключових таблицях, кожна з яких відіграє визначену роль у процесі маршрутизації та забезпечує механізми швидкої адаптації до змін топології. Таблиця сусідства (Neighbor Table) містить інформацію про всіх активних сусідів, з якими встановлено двонаправлений зв’язок, включаючи їх IP-адреси, інтерфейси підключення, інтервали Hello та значення таймерів Hold, що дозволяє оперативно виявляти відмови лінків. Таблиця топології (Topology Table) є центральним елементом протоколу, оскільки зберігає повну інформацію про всі відомі маршрути до кожної мережі, включаючи метрики, оголошені сусідами (Reported Distance), повні метрики через кожного сусіда (Feasible Distance), а також статус кожного маршруту (пасивний або активний). Саме в цій таблиці зберігаються резервні маршрути (Feasible Successor), які задовольняють умову можливості, що дозволяє миттєво перемикати трафік при відмові основного шляху без запуску повного алгоритму DUAL. Таблиця маршрутизації (Routing Table) містить лише ті маршрути, які фактично використовуються для пересилання трафіку, тобто оптимальні шляхи (Successor) з таблиці топології, позначені літерою «D» (EIGRP) або «D EX» (зовнішні маршрути) у виводі команди show ip route. Важливо розуміти, що таблиця маршрутизації є підмножиною таблиці топології, і не всі маршрути з таблиці топології потрапляють до таблиці маршрутизації — лише ті, що мають найнижчу метрику та задовольняють умову можливості для резервних шляхів. Процес вибору маршрутів відбувається наступним чином: після отримання інформації від сусідів маршрутизатор обчислює Feasible Distance для кожного шляху, вибирає маршрут з найнижчою метрикою як Successor, а серед решти маршрутів шукає ті, що задовольняють умову RD < FD_successor, які стають Feasible Successor. У разі відмови основного шляху маршрутизатор негайно перемикається на перший доступний Feasible Successor, що займає менше секунди, на відміну від протоколів без механізму резервування маршрутів, де час відновлення може становити десятки секунд.

Таблиця 10.2 — Команди для налаштування та верифікації протоколу EIGRP

Категорія	Команда	Призначення
Налаштування	router eigrp <AS-number>	Активація процесу EIGRP з вказаним номером автономної системи
Налаштування	network <network> <wildcard-mask>	Оголошення мережі для участі в процесі EIGRP
Налаштування	no auto-summary	Вимкнення автоматичного підсумування маршрутів на межах класових мереж
Налаштування	passive-interface <interface>	Запобігання надсиланню Hello-пакетів через вказаний інтерфейс
Верифікація	show ip eigrp neighbors	Перегляд таблиці сусідства з інформацією про активних сусідів
Верифікація	show ip eigrp topology	Перегляд таблиці топології з усіма відомими маршрутами та їх метриками
Верифікація	show ip eigrp topology <network>	Детальний аналіз маршрутів до конкретної мережі
Верифікація	show ip route eigrp	Перегляд маршрутів EIGRP у загальній таблиці маршрутизації
Верифікація	show ip protocols	Перегляд параметрів усіх активних протоколів маршрутизації

Команди налаштування протоколу EIGRP відрізняються своєю лаконічністю та інтуїтивною зрозумілістю, що робить їх доступними для навчання. Ключовим параметром при активації процесу є номер автономної системи (AS), який повинен бути ідентичним на всіх маршрутизаторах, що беруть участь у обміні маршрутною інформацією, оскільки маршрутизатори з різними номерами AS не встановлюють сусідство навіть при фізичній досяжності. Команда network використовує маску-підказку (wildcard mask), яка є інверсією стандартної маски підмережі, що дозволяє гнучко вказувати, які інтерфейси повинні брати участь у процесі маршрутизації — наприклад, маска 0.0.0.3 для підмережі /30 дозволяє активувати протокол лише на конкретному точка-точка інтерфейсі без ризику неочікуваного оголошення суміжних мереж. Вимкнення автоматичного підсумування (no auto-summary) є обов’язковим кроком у сучасних мережах з безкласовою адресацією (CIDR), оскільки за замовчуванням EIGRP підсумовує маршрути на межах класових мереж (наприклад, 192.168.1.0/24 та 192.168.2.0/24 будуть оголошені як 192.168.0.0/16), що призводить до некоректної маршрутизації. Для верифікації роботи протоколу найбільш інформативними є команди show ip eigrp neighbors, яка підтверджує встановлення сусідства, та show ip eigrp topology, яка дозволяє проаналізувати наявність резервних маршрутів та перевірити виконання умови можливості. Команда show ip route eigrp надає стислу інформацію про маршрути, що фактично використовуються для пересилання трафіку, з вказівкою метрики та наступного стрибка.

1.3 Механізми швидкої збіжності та відмовостійкості

Однією з ключових переваг протоколу EIGRP є його здатність до миттєвої реакції на зміни топології мережі завдяки механізму збереження резервних маршрутів у таблиці топології. На відміну від протоколу RIP, який при втраті основного шляху повинен очікувати закінчення таймера втрати маршруту (180 секунд) та отримати оновлення від сусідів, або протоколу OSPF, який потребує повторного обчислення дерева найкоротших шляхів (алгоритм Дейкстри), EIGRP використовує попередньо обчислені резервні шляхи (Feasible Successor), що дозволяє перемикати трафік за час, що не перевищує 1 секунди. Цей механізм базується на математичній властивості алгоритму DUAL, яка гарантує, що будь-який маршрут, що задовольняє умову можливості (RD < FD_successor), не утворює петлі навіть при одночасній відмові основного шляху.

У трикутній топології, яка використовується в лабораторній роботі (рис. 10.1), цей механізм проявляється особливо наочно: при наявності двох можливих шляхів між двома маршрутизаторами (наприклад, через прямий гігабітний лінк та через два послідовні фаст-етернет лінки) протокол обирає основний шлях з нижчою метрикою, але зберігає другий шлях як резервний, якщо він задовольняє умову можливості. При імітації відмови основного лінку маршрутизатор негайно активує резервний шлях без необхідності запуску запитів Query до сусідів, що виключає період невизначеності та втрату пакетів понад мінімальний рівень. Для успішного формування резервного шляху критичним є забезпечення різниці в метриках основного та альтернативного шляхів, що досягається в лабораторній роботі шляхом використання інтерфейсів різної пропускної здатності (100 Мбіт/с та 1000 Мбіт/с), оскільки метрика EIGRP обернено пропорційна пропускній здатності каналу. Якщо ж обидва шляхи мають ідентичну метрику, EIGRP виконує балансування навантаження (load balancing) між ними, але не формує резервного шляху у класичному розумінні, що ускладнює демонстрацію механізму швидкої збіжності.

Уявімо три маршрутизатори R1, R2 та R3, з’єднані у трикутник, де лінк між R1 та R3 має пропускну здатність 1000 Мбіт/с, а лінки між R1–R2 та R2–R3 — по 100 Мбіт/с. Мережа ПК3 (192.168.3.0/24) підключена до R3. З точки зору R1 існують два шляхи до цієї мережі: прямий через R3 (один гігабітний лінк) та непрямий через R2 (два фаст-етернет лінки). Метрика прямого шляху обчислюється на основі пропускної здатності 1000 Мбіт/с та затримки одного інтерфейсу, тоді як метрика шляху через R2 базується на найнижчій пропускній здатності 100 Мбіт/с та сумарній затримці двох інтерфейсів, що робить її значно вищою. При цьому метрика, оголошена R2 для мережі 192.168.3.0/24 (Reported Distance), враховує лише один фаст-етернет лінк між R2 та R3, тому вона може бути нижчою за повну метрику прямого шляху від R1 до R3 (Feasible Distance), що задовольняє умову можливості. У результаті прямий шлях стає основним (Successor), а шлях через R2 — резервним (Feasible Successor). При відмові лінку між R1 та R3 маршрутизатор R1 негайно перемикає трафік на

шлях через R2 без запуску запитів Query, оскільки резервний маршрут уже перевірений на відсутність петель під час початкового обчислення. Така поведінка забезпечує практично непомітне для кінцевих користувачів відновлення зв’язку, що є критичним для додатків реального часу, таких як VoIP або відеоконференції.

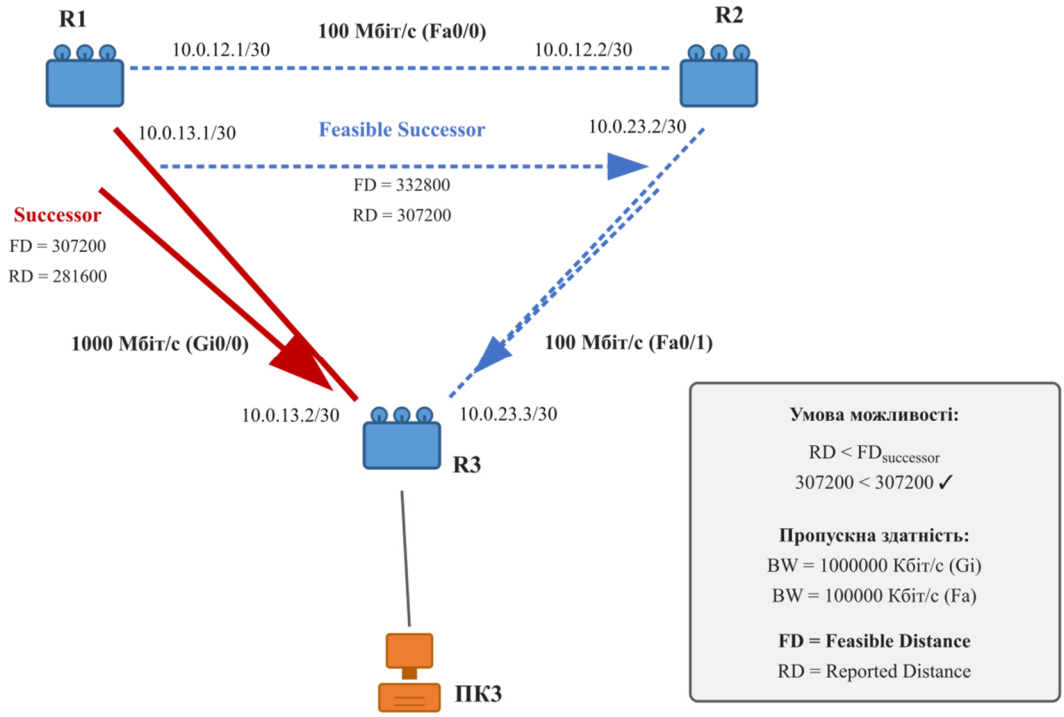

Рисунок 10.1 — Механізм вибору основного та резервного шляхів у трикутній топології EIGRP

1.4 Порівняльний аналіз протоколів маршрутизації

Для повного розуміння переваг протоколу EIGRP необхідно розглянути його у контексті інших популярних протоколів внутрішньої маршрутизації, зокрема RIP та OSPF, що дозволяє оцінити його місце в сучасній мережевій архітектурі. Протокол RIP версії 2, будучи класичним дистанційно-векторним протоколом, використовує надзвичайно просту метрику — кількість стрибків, що робить його легким у налаштуванні, але абсолютно непридатним для складних топологій через обмеження у 15 хопів та ігнорування реальної пропускної здатності каналів. Наприклад, у трикутній топології лабораторної роботи RIP обирав би шлях з меншою кількістю стрибків навіть за умови значно нижчої пропускної здатності, що призводило б до неефективного використання мережевих ресурсів. Крім того, час збіжності RIP у разі відмови лінку становить десятки секунд через необхідність очікування таймерів втрати маршрутів та отримання повних оновлень від сусідів. Протокол OSPF, що належить до класу протоколів стану каналів, забезпечує значно кращу масштабованість та точність маршрутизації завдяки побудові повної карти топології мережі та застосуванню алгоритму Дейкстри для обчислення найкоротших шляхів. Однак ця перевага досягається за рахунок збільшення

навантаження на процесор маршрутизатора під час перерахунку маршрутів та більш складної конфігурації, що включає розбиття мережі на області (areas) для великих топологій. У той час як OSPF гарантує найкоротший шлях у термінах вартості лінків, він не зберігає резервних маршрутів у пасивному стані, тому час реакції на відмову лінку залежить від швидкості виявлення відмови та виконання алгоритму Дейкстри. Протокол EIGRP займає проміжне положення, поєднуючи простоту конфігурації дистанційно-векторних протоколів з ефективністю та швидкістю реакції протоколів стану каналів, що робить його оптимальним вибором для середніх корпоративних мереж, де важливі як надійність, так і простота адміністрування.

Таблиця 10.3 — Порівняльна характеристика протоколів внутрішньої маршрутизації

Параметр	RIP v2	EIGRP	OSPF
Тип протоколу	Дистанційно-векторний	Гібридний	Стану каналів
Метрика	Кількість стрибків (макс. 15)	Композитна (пропускна здатність, затримка)	Вартість лінка (зазвичай обернено пропорційна пропускній здатності)
Час збіжності	30–180 секунд	< 1 секунда (при наявності Feasible Successor)	1–10 секунд
Масштабованість	Низька (до 15 хопів)	Середня–висока	Висока (підтримка ієрархії областей)
Навантаження на ЦП	Низьке	Середнє	Високе під час перерахунку
Складність конфігурації	Низька	Середня	Висока
Підтримка безкласової маршрутизації	Так (RIPv2)	Так	Так
Пропрієтарність	Відкритий стандарт	Спочатку пропрієтарний (частково відкритий з 2013 р.)	Відкритий стандарт (RFC 2328)

Вибір протоколу маршрутизації для конкретної мережі залежить від ряду факторів, включаючи розмір топології, вимоги до часу відновлення після відмов, доступність обладнання різних виробників та кваліфікація адміністраторів. Для невеликих мереж з однорідним обладнанням від одного виробника протокол EIGRP часто є оптимальним вибором завдяки своєму балансу між продуктивністю, надійністю та простотою налаштування. У гетерогенних середовищах з обладнанням різних виробників перевагу слід віддавати відкритим стандартам, таким як OSPF або протоколи на основі відстані до межі (BGP для міжавтономної маршрутизації). Проте навіть у таких випадках знання принципів роботи EIGRP залишається важливим для розуміння сучасних механізмів маршрутизації, оскільки багато концепцій, таких як композитна метрика та механізми швидкої збіжності, були вперше

реалізовані саме в цьому протоколі та пізніше адаптовані в інших стандартах. У навчальному процесі лабораторні роботи з налаштування EIGRP дозволяють студентам на практиці зрозуміти фундаментальні принципи динамічної маршрутизації, які застосовуються в усіх сучасних протоколах, незалежно від їхньої конкретної реалізації.

1.5 Практичні аспекти налаштування EIGRP у навчальному середовищі

При виконанні лабораторної роботи з налаштування EIGRP важливо звернути увагу на ряд практичних аспектів, які часто стають джерелом помилок для студентів, особливо на початкових етапах вивчення мережевої маршрутизації. Однією з найпоширеніших помилок є неузгодженість номерів автономних систем на різних маршрутизаторах, що повністю блокує встановлення сусідства, оскільки EIGRP розглядає маршрутизатори з різними номерами AS як належні до різних адміністративних доменів. Іншою типовою помилкою є відсутність команди no auto-summary у середовищах з безкласовою адресацією, що призводить до некоректного підсумування маршрутів та втрати зв’язку з окремими підмережами, особливо коли вони належать до однієї класової мережі, але мають різні маски підмереж. Неправильне використання маски-підказки у команді network також часто стає причиною проблем — замість інверсії стандартної маски підмережі студенти намагаються використовувати звичайну маску, що призводить до неочікуваної активізації протоколу на небажаних інтерфейсах або, навпаки, до відсутності оголошення необхідних мереж. Для уникнення цих помилок рекомендується після налаштування кожного маршрутизатора виконувати перевірку командою show ip protocols, яка відображає всі активні процеси маршрутизації, їхні параметри та оголошені мережі, що дозволяє оперативно виявити неузгодженості. Крім того, перед активацією EIGRP необхідно переконатися в наявності базової зв’язності між інтерфейсами маршрутизаторів за допомогою команди ping, оскільки відсутність фізичної або канальної досяжності також блокує встановлення сусідства незалежно від коректності конфігурації протоколу. При роботі в симуляторі Packet Tracer слід пам’ятати про необхідність явного встановлення швидкості інтерфейсів командами speed та duplex, оскільки за замовчуванням усі інтерфейси можуть мати однакові характеристики, що унеможливлює демонстрацію впливу пропускної здатності на вибір оптимального шляху та формування резервного маршруту. Нарешті, для успішного тестування механізму швидкої збіжності важливо переконатися в наявності двох шляхів до однієї мережі з різною метрикою, але з виконанням умови можливості для резервного шляху, що можна перевірити детальним аналізом виводу команди show ip eigrp topology <network> перед імітацією відмови лінку.

2 КЛЮЧОВІ ПИТАННЯ

1. Чому при налаштуванні протоколу EIGRP обов'язково використовується команда `no auto-summary` у сучасних мережах з безкласовою адресацією (CIDR), і які наслідки матиме її відсутність?

2. Поясніть механізм умови можливості (Feasibility Condition) у протоколі EIGRP: чому виконання умови RD < FD є гарантією відсутності маршрутних петель при перемиканні на резервний шлях?

3. Як пропускна здатність інтерфейсів впливає на обчислення метрики EIGRP за замовчуванням, і чому в лабораторній роботі використовуються лінки різної швидкості (100 Мбіт/с та 1000 Мбіт/с) для демонстрації роботи протоколу?

4. Опишіть відмінності між таблицею сусідства, таблицею топології та таблицею маршрутизації в контексті протоколу EIGRP, та поясніть, чому не всі маршрути з таблиці топології потрапляють до таблиці маршрутизації.

5. Чому час відновлення зв'язку при відмові лінку в EIGRP становить менше 1 секунди за наявності Feasible Successor, тоді як у протоколі RIP цей процес займає десятки секунд?

6. Які параметри визначають успішне встановлення сусідства між маршрутизаторами EIGRP, і які три найпоширеніші причини відсутності записів у виводі команди `show ip eigrp neighbors` при наявності фізичної досяжності?

7. Поясніть призначення маски-підказки (wildcard mask) у команді `network` при налаштуванні EIGRP, і наведіть приклад перетворення маски підмережі 255.255.255.252 у відповідну маску-підказку для мережі /30.

8. Чим відрізняється поведінка протоколу EIGRP при відмові лінку у випадку наявності Feasible Successor порівняно з ситуацією, коли такий маршрут відсутній, і які службові пакети генеруються в кожному з цих випадків?

9. Які переваги та обмеження має протокол EIGRP у порівнянні з протоколами RIP та OSPF з точки зору масштабованості, швидкості збіжності та складності адміністрування?

10. Чому в трикутній топології лабораторної роботи шлях через два послідовні лінки 100 Мбіт/с може стати Feasible Successor для прямого лінку 1000 Мбіт/с, незважаючи на вищу сумарну метрику, і як це пов'язано з концепцією Reported Distance?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1 Архітектура мережі та повна адресація. Лабораторна робота реалізується в середовищі симулятора мережевого обладнання (Cisco Packet Tracer або GNS3) із трикутною топологією, що складається з трьох маршрутизаторів Cisco 2911 (R1, R2, R3), трьох комутаторів Cisco 2960 (SW1, SW2, SW3) та трьох персональних комп’ютерів (ПК1, ПК2, ПК3). Кожен маршрутизатор підключений до власного комутатора, до якого, у свою чергу,

приєднано один ПК. Маршрутизатори з’єднані між собою трьома лінками різної пропускної здатності: з’єднання R1–R2 та R2–R3 реалізовано через інтерфейси FastEthernet (100 Mbps), а безпосереднє з’єднання R1–R3 — через інтерфейс GigabitEthernet (1000 Mbps). Така асиметрія дозволяє наочно продемонструвати вплив пропускної здатності на обчислення метрики EIGRP та вибір оптимального шляху. Для точного контролю над процесом маршрутизації використовується безкласова адресація (CIDR) з підмережами /30 для точка-точка з’єднань між маршрутизаторами та /24 для локальних сегментів ПК. Повну таблицю адресації всіх пристроїв мережі наведено в таблиці 10.4.

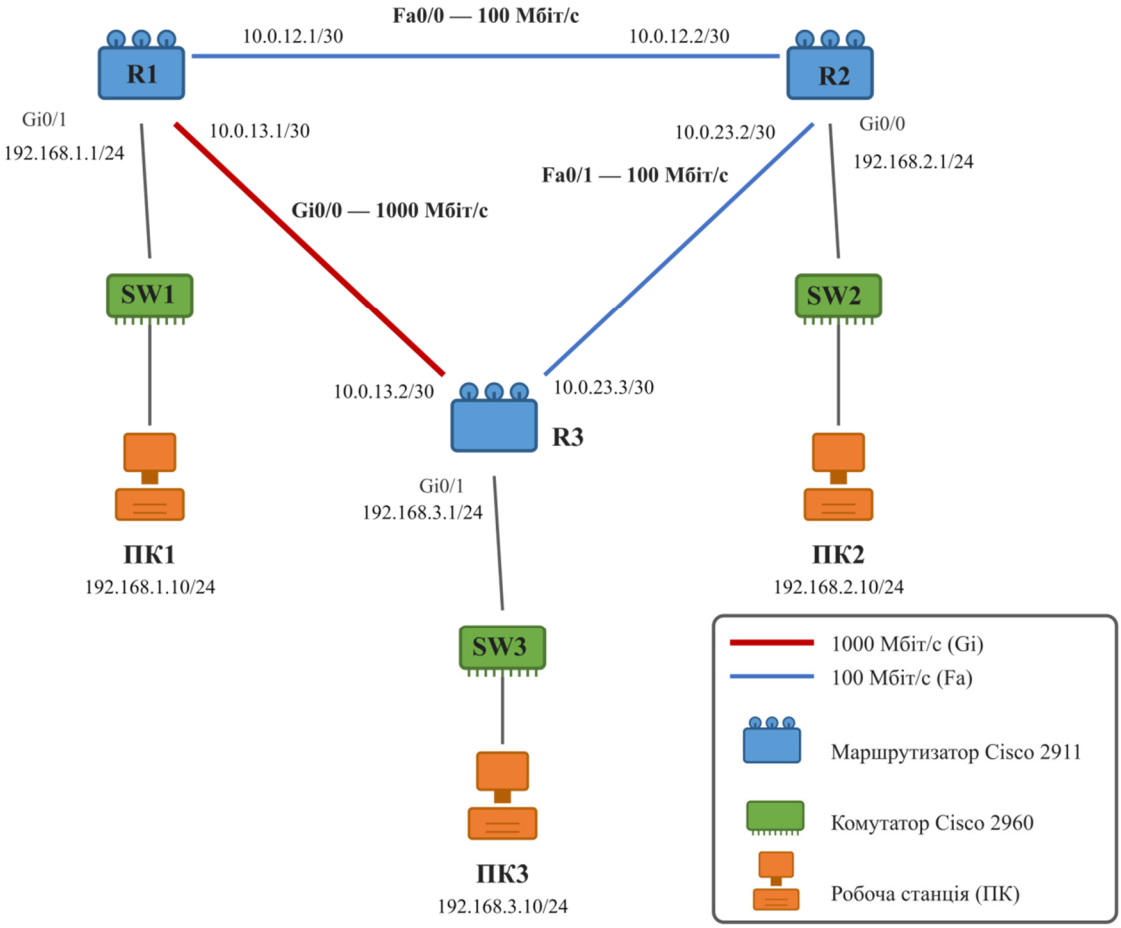

Рисунок 10.2 – Топологія мережі з протоколом EIGRP

Таблиця 10.4 – Налаштування мережевих пристроїв прикладу лабораторного завдання

Пристрій	Тип інтерфейсу	Назва інтерфейсу	IP-адреса	Маска підмережі
R1	Маршрутизатор	Gig0/0	10.0.13.1	255.255.255.252
		Fast0/0	10.0.12.1	255.255.255.252
		Gig0/1	192.168.1.1	255.255.255.0
R2	Маршрутизатор	Fast0/0	10.0.12.2	255.255.255.252
		Fast0/1	10.0.23.2	255.255.255.252
		Gig0/0	192.168.2.1	255.255.255.0
R3	Маршрутизатор	Fast0/1	10.0.23.3	255.255.255.252

		Gig0/0	10.0.13.2	255.255.255.252
		Gig0/1	192.168.3.1	255.255.255.0
SW1	Комутатор	VLAN 1	192.168.1.2	255.255.255.0
		Fa0/1	—	—
		Fa0/2	—	—
SW2	Комутатор	VLAN 1	192.168.2.2	255.255.255.0
		Fa0/1	—	—
		Fa0/2	—	—
SW3	Комутатор	VLAN 1	192.168.3.2	255.255.255.0
		Fa0/1	—	—
		Fa0/2	—	—
ПК1	Робоча станція	NIC	192.168.1.10	255.255.255.0
ПК2	Робоча станція	NIC	192.168.2.10	255.255.255.0
ПК3	Робоча станція	NIC	192.168.3.10	255.255.255.0

Примітка. Для наочності різниці в метриці EIGRP рекомендується вручну встановити швидкість інтерфейсів між маршрутизаторами: на лінках FastEthernet використовувати speed 100, на лінку GigabitEthernet — speed 1000. Це гарантує, що EIGRP обиратиме шлях через R1–R3 як основний (нижча метрика) навіть за умови однакової затримки.

Таблиця 10.5 – Варіанти індивідуальних завдань

№ варіанту	Адресація точка-точка з’єднань (мережі /30)	Адресація локальних сегментів (мережі /24)	Номер автономної системи
1	R1–R2: 10.0.0.0 R2–R3: 10.0.4.0 R1–R3: 10.0.8.0	ПК1: 192.168.10.0 ПК2: 192.168.20.0 ПК3: 192.168.30.0	100
2	R1–R2: 10.0.12.0 R2–R3: 10.0.16.0 R1–R3: 10.0.20.0	ПК1: 192.168.40.0 ПК2: 192.168.50.0 ПК3: 192.168.60.0	101
3	R1–R2: 10.0.24.0 R2–R3: 10.0.28.0 R1–R3: 10.0.32.0	ПК1: 192.168.70.0 ПК2: 192.168.80.0 ПК3: 192.168.90.0	102
4	R1–R2: 10.0.36.0 R2–R3: 10.0.40.0 R1–R3: 10.0.44.0	ПК1: 192.168.100.0 ПК2: 192.168.110.0 ПК3: 192.168.120.0	103
5	R1–R2: 10.0.48.0 R2–R3: 10.0.52.0 R1–R3: 10.0.56.0	ПК1: 192.168.130.0 ПК2: 192.168.140.0 ПК3: 192.168.150.0	104
6	R1–R2: 10.0.60.0 R2–R3: 10.0.64.0 R1–R3: 10.0.68.0	ПК1: 192.168.160.0 ПК2: 192.168.170.0 ПК3: 192.168.180.0	105
7	R1–R2: 10.0.72.0 R2–R3: 10.0.76.0 R1–R3: 10.0.80.0	ПК1: 192.168.190.0 ПК2: 192.168.200.0 ПК3: 192.168.210.0	106
8	R1–R2: 10.0.84.0 R2–R3: 10.0.88.0 R1–R3: 10.0.92.0	ПК1: 192.168.220.0 ПК2: 192.168.230.0 ПК3: 192.168.240.0	107
9	R1–R2: 10.0.96.0 R2–R3: 10.0.100.0 R1–R3: 10.0.104.0	ПК1: 10.10.1.0 ПК2: 10.10.2.0 ПК3: 10.10.3.0	108

10	R1–R2: 10.0.108.0 R2–R3: 10.0.112.0 R1–R3: 10.0.116.0	ПК1: 10.10.4.0 ПК2: 10.10.5.0 ПК3: 10.10.6.0	109
11	R1–R2: 172.16.0.0 R2–R3: 172.16.0.4 R1–R3: 172.16.0.8	ПК1: 10.10.7.0 ПК2: 10.10.8.0 ПК3: 10.10.9.0	110
12	R1–R2: 172.16.0.12 R2–R3: 172.16.0.16 R1–R3: 172.16.0.20	ПК1: 10.10.10.0 ПК2: 10.10.11.0 ПК3: 10.10.12.0	111
13	R1–R2: 172.16.0.24 R2–R3: 172.16.0.28 R1–R3: 172.16.0.32	ПК1: 10.10.13.0 ПК2: 10.10.14.0 ПК3: 10.10.15.0	112
14	R1–R2: 172.16.0.36 R2–R3: 172.16.0.40 R1–R3: 172.16.0.44	ПК1: 10.10.16.0 ПК2: 10.10.17.0 ПК3: 10.10.18.0	113
15	R1–R2: 172.16.0.48 R2–R3: 172.16.0.52 R1–R3: 172.16.0.56	ПК1: 10.10.19.0 ПК2: 10.10.20.0 ПК3: 10.10.21.0	114
16	R1–R2: 172.16.0.60 R2–R3: 172.16.0.64 R1–R3: 172.16.0.68	ПК1: 10.10.22.0 ПК2: 10.10.23.0 ПК3: 10.10.24.0	115
17	R1–R2: 172.16.0.72 R2–R3: 172.16.0.76 R1–R3: 172.16.0.80	ПК1: 10.10.25.0 ПК2: 10.10.26.0 ПК3: 10.10.27.0	116
18	R1–R2: 172.16.0.84 R2–R3: 172.16.0.88 R1–R3: 172.16.0.92	ПК1: 10.10.28.0 ПК2: 10.10.29.0 ПК3: 10.10.30.0	117
19	R1–R2: 172.16.0.96 R2–R3: 172.16.0.100 R1–R3: 172.16.0.104	ПК1: 10.20.1.0 ПК2: 10.20.2.0 ПК3: 10.20.3.0	118
20	R1–R2: 172.16.0.108 R2–R3: 172.16.0.112 R1–R3: 172.16.0.116	ПК1: 10.20.4.0 ПК2: 10.20.5.0 ПК3: 10.20.6.0	119
21	R1–R2: 172.16.0.120 R2–R3: 172.16.0.124 R1–R3: 172.16.0.128	ПК1: 10.20.7.0 ПК2: 10.20.8.0 ПК3: 10.20.9.0	120
22	R1–R2: 172.16.0.132 R2–R3: 172.16.0.136 R1–R3: 172.16.0.140	ПК1: 10.20.10.0 ПК2: 10.20.11.0 ПК3: 10.20.12.0	121
23	R1–R2: 172.16.0.144 R2–R3: 172.16.0.148 R1–R3: 172.16.0.152	ПК1: 10.20.13.0 ПК2: 10.20.14.0 ПК3: 10.20.15.0	122
24	R1–R2: 172.16.0.156 R2–R3: 172.16.0.160 R1–R3: 172.16.0.164	ПК1: 10.20.16.0 ПК2: 10.20.17.0 ПК3: 10.20.18.0	123
25	R1–R2: 172.16.0.168 R2–R3: 172.16.0.172 R1–R3: 172.16.0.176	ПК1: 10.20.19.0 ПК2: 10.20.20.0 ПК3: 10.20.21.0	124
26	R1–R2: 172.16.0.180 R2–R3: 172.16.0.184 R1–R3: 172.16.0.188	ПК1: 10.20.22.0 ПК2: 10.20.23.0 ПК3: 10.20.24.0	125
27	R1–R2: 172.16.0.192	ПК1: 10.20.25.0	126

	R2–R3: 172.16.0.196 R1–R3: 172.16.0.200	ПК2: 10.20.26.0 ПК3: 10.20.27.0	
28	R1–R2: 172.16.0.204 R2–R3: 172.16.0.208 R1–R3: 172.16.0.212	ПК1: 10.20.28.0 ПК2: 10.20.29.0 ПК3: 10.20.30.0	127
29	R1–R2: 172.16.0.216 R2–R3: 172.16.0.220 R1–R3: 172.16.0.224	ПК1: 10.30.1.0 ПК2: 10.30.2.0 ПК3: 10.30.3.0	128
30	R1–R2: 172.16.0.228 R2–R3: 172.16.0.232 R1–R3: 172.16.0.236	ПК1: 10.30.4.0 ПК2: 10.30.5.0 ПК3: 10.30.6.0	129

У кожному варіанті студент повинен призначити IP-адреси інтерфейсам маршрутизаторів згідно з вказаною адресацією. Для точка-точка з’єднань (/30) перший хост у підмережі призначається маршрутизатору з меншим номером (наприклад, для мережі 10.0.0.0/30: R1 отримує 10.0.0.1, R2 — 10.0.0.2). Для локальних сегментів ПК шлюзом за замовчуванням є перший хост у підмережі (наприклад, для 192.168.10.0/24 шлюз — 192.168.10.1), а ПК отримує адресу .10 (наприклад, 192.168.10.10). Номер автономної системи вказується у команді router eigrp <номер> під час налаштування протоколу. Варіанти 1–10 використовують діапазон 10.0.x.0/30 для лінків та 192.168.x.0/24 або 10.10.x.0/24 для локальних сегментів; варіанти 11–30 — діапазон 172.16.0.x/30 для лінків та 10.20.x.0/24 або 10.30.x.0/24 для локальних сегментів. Такий підхід забезпечує унікальність завдань для кожного студента та дозволяє перевірити розуміння принципів безкласової адресації (CIDR).

3.2. Базові налаштування маршрутизаторів та комутаторів. Перед налаштуванням маршрутизації необхідно виконати базову конфігурацію кожного мережевого пристрою: встановити унікальне ім’я (hostname), вимкнути автоматичний пошук доменних імен (no ip domain-lookup), щоб уникнути затримок при введенні помилкових команд, та налаштувати банер входу для інформування користувачів про обмежений доступ.

Для комутаторів додатково налаштовується інтерфейс управління VLAN 1 з IP-адресою та шлюзом за замовчуванням для можливості віддаленого управління (хоча для цієї лабораторної роботи віддалений доступ не використовується, це є стандартною практикою у корпоративних мережах). Важливо переконатися, що всі інтерфейси фізично активовані (no shutdown) і мають коректні описи (description), що значно спрощує подальшу діагностику та інтерпретацію виводу верифікаційних команд.

Нижче наведено послідовність команд для налаштування базових параметрів маршрутизатора R1, включаючи встановлення імені пристрою, вимкнення пошуку доменних імен, налаштування банеру повідомлення та активацію синхронізації виводу для консольного підключення:

```
     R1> enable
R1# configure terminal
R1(config)# hostname R1
```

```
R1(config)# no ip domain-lookup
R1(config)# banner motd # Unauthorized access prohibited #
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)# exit
```

Наступним кроком виконується базова конфігурація комутатора SW1, яка включає встановлення імені пристрою, вимкнення пошуку доменних імен, налаштування інтерфейсу управління VLAN 1 з IP-адресою 192.168.1.2 та шлюзом за замовчуванням 192.168.1.1, а також активацію синхронізації виводу для консолі:

```
     Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
Switch(config)# no ip domain-lookup
Switch(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# ip default-gateway 192.168.1.1
SW1(config)# line console 0
SW1(config-line)# logging synchronous
SW1(config-line)# exit
SW1(config)# exit
```

Після завершення конфігурації перевірте коректність імен пристроїв командою show running-config | include hostname. На маршрутизаторі R1 у виводі має з’явитися рядок hostname R1. Якщо замість нього відображається hostname Router або ім’я відсутнє, повторіть налаштування. Для комутатора SW1 виконайте show ip interface brief — інтерфейс VLAN 1 повинен мати стан «up/up» та IP-адресу 192.168.1.2. Відсутність повідомлень типу «Translating “команда”…» під час введення невірних команд у CLI підтверджує успішне виконання no ip domain-lookup. Базові налаштування для R2, R3, SW2 та SW3 виконуються аналогічно з відповідними іменами пристроїв та параметрами згідно з таблицею 10.1.

3.3 Налаштування інтерфейсів маршрутизаторів. На цьому етапі виконується конфігурація фізичних інтерфейсів маршрутизатора R1: призначаються IP-адреси для трьох інтерфейсів (два для з’єднання з іншими маршрутизаторами та один для локального сегменту), встановлюються описи призначень, явно задається швидкість 1000 Mbps та повний дуплекс для гігабітного лінку до R3, швидкість 100 Mbps для фаст-етернет лінку до R2, а також активуються всі інтерфейси командою no shutdown:

```
     R1# configure terminal
R1(config)# interface GigabitEthernet0/0
```

```
R1(config-if)# description Link_to_R3_Gigabit
R1(config-if)# ip address 10.0.13.1 255.255.255.252
R1(config-if)# speed 1000
R1(config-if)# duplex full
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# interface FastEthernet0/0
R1(config-if)# description Link_to_R2_Fast
R1(config-if)# ip address 10.0.12.1 255.255.255.252
R1(config-if)# speed 100
R1(config-if)# duplex full
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# interface GigabitEthernet0/1
R1(config-if)# description LAN_to_SW1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
```

Далі виконується аналогічна конфігурація інтерфейсів маршрутизатора R2, де налаштовуються два фаст-етернет інтерфейси для з’єднання з R1 та R3 (швидкість 100 Mbps) та один гігабітний інтерфейс для підключення локального сегменту з ПК2:

```
R2# configure terminal
R2(config)# interface FastEthernet0/0
R2(config-if)# description Link_to_R1_Fast
R2(config-if)# ip address 10.0.12.2 255.255.255.252
R2(config-if)# speed 100
R2(config-if)# duplex full
R2(config-if)# no shutdown
R2(config-if)# exit

R2(config)# interface FastEthernet0/1
R2(config-if)# description Link_to_R3_Fast
R2(config-if)# ip address 10.0.23.2 255.255.255.252
R2(config-if)# speed 100
R2(config-if)# duplex full
R2(config-if)# no shutdown
R2(config-if)# exit

R2(config)# interface GigabitEthernet0/0
R2(config-if)# description LAN_to_SW2
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# exit
```

Завершується налаштування інтерфейсів конфігурацією маршрутизатора R3, де налаштовується фаст-етернет інтерфейс для з’єднання з R2 (100 Mbps), гігабітний інтерфейс для з’єднання з R1 (1000 Mbps) та гігабітний інтерфейс для локального сегменту з ПК3:

```
R3# configure terminal
R3(config)# interface FastEthernet0/1
R3(config-if)# description Link_to_R2_Fast
R3(config-if)# ip address 10.0.23.3 255.255.255.252
R3(config-if)# speed 100
R3(config-if)# duplex full
R3(config-if)# no shutdown
R3(config-if)# exit

R3(config)# interface GigabitEthernet0/0
R3(config-if)# description Link_to_R1_Gigabit
R3(config-if)# ip address 10.0.13.2 255.255.255.252
R3(config-if)# speed 1000
R3(config-if)# duplex full
R3(config-if)# no shutdown
R3(config-if)# exit

R3(config)# interface GigabitEthernet0/1
R3(config-if)# description LAN_to_SW3
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# exit
```

Для перевірки стану інтерфейсів виконайте команду show ip interface brief на маршрутизаторі R1. У колонках «Status» та «Protocol» для всіх трьох інтерфейсів має відображатися значення «up». Якщо інтерфейс має стан «administratively down», це означає, що не була виконана команда no shutdown. Стан «down/down» при активованому інтерфейсі вказує на фізичну проблему з’єднання або помилку на суміжному пристрої (неправильна маска підмережі, неактивований інтерфейс). У колонці «IP-Address» переконайтеся, що адреси відповідають даним таблиці 1. Для детального аналізу швидкості інтерфейсу виконайте show interface GigabitEthernet0/0 | include BW — у виводі має бути рядок «BW 1000000 Kbit/sec», що підтверджує роботу на 1000 Mbps. На цьому етапі виконайте базову перевірку зв’язності: з ПК1 виконайте ping 192.168.1.1 (шлюз) та ping 10.0.12.2 (інтерфейс R2). Останній пінг має бути успішним, оскільки пристрої знаходяться в одній мережі /30. Пінг до віддалених підмереж (наприклад, 192.168.3.10) ще не працюватиме, оскільки маршрутизація не налаштована.

3.4 Налаштування комутаторів. Комутатори у цій топології виконують роль пасивних пристроїв комутації рівня 2, тому їх конфігурація мінімальна: налаштовуються лише інтерфейси підключення та базові параметри

управління. Всі порти за замовчуванням знаходяться в режимі access VLAN 1, що достатньо для підключення ПК та маршрутизаторів. Для забезпечення стабільності рекомендується встановити описи портів та переконатися, що порти активовані. Головне завдання комутаторів — забезпечити прозору комутацію кадрів між ПК та маршрутизатором у межах однієї підмережі без участі в процесі маршрутизації.

Нижче наведено конфігурацію комутатора SW1, яка включає налаштування порту Fa0/1 для підключення до маршрутизатора R1 та порту Fa0/2 для підключення робочої станції ПК1, з встановленням режиму доступу та активацією обох портів:

```
SW1# configure terminal
SW1(config)# interface FastEthernet0/1
SW1(config-if)# description Uplink_to_R1_Gig0/1
SW1(config-if)# switchport mode access
SW1(config-if)# no shutdown
SW1(config-if)# exit

SW1(config)# interface FastEthernet0/2
SW1(config-if)# description Connection_to_PC1
SW1(config-if)# switchport mode access
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# exit
```

Аналогічним чином виконується налаштування комутатора SW2 для підключення до маршрутизатора R2 та робочої станції ПК2:

```
SW2# configure terminal
SW2(config)# interface FastEthernet0/1
SW2(config-if)# description Uplink_to_R2_Gig0/0
SW2(config-if)# switchport mode access
SW2(config-if)# no shutdown
SW2(config-if)# exit

SW2(config)# interface FastEthernet0/2
SW2(config-if)# description Connection_to_PC2
SW2(config-if)# switchport mode access
SW2(config-if)# no shutdown
SW2(config-if)# exit
SW2(config)# exit
```

Завершується конфігурація комутаторів налаштуванням комутатора SW3 для підключення до маршрутизатора R3 та робочої станції ПК3:

```
SW3# configure terminal
SW3(config)# interface FastEthernet0/1
SW3(config-if)# description Uplink_to_R3_Gig0/1
SW3(config-if)# switchport mode access
SW3(config-if)# no shutdown
```

```
SW3(config-if)# exit

SW3(config)# interface FastEthernet0/2
SW3(config-if)# description Connection_to_PC3
SW3(config-if)# switchport mode access
SW3(config-if)# no shutdown
SW3(config-if)# exit
SW3(config)# exit
```

Перевірте стан портів комутатора SW1 командою show interfaces status. У колонці «Status» для портів Fa0/1 та Fa0/2 має відображатися значення «connected», а в колонці «VLAN» — «1». Якщо замість «connected» відображається «notconnect», перевірте фізичне підключення кабелів та стан інтерфейсів на суміжних пристроях. Стан «disabled» вказує на відсутність команди no shutdown на відповідному інтерфейсі. Успішний стан портів є необхідною умовою для подальшої комутації трафіку між ПК та маршрутизатором. Аналогічну перевірку виконайте для SW2 та SW3.

3.5 Налаштування робочих станцій. Налаштування робочих станцій (ПК1, ПК2, ПК3) виконується через графічний інтерфейс симулятора Packet Tracer або через командний рядок операційної системи у випадку використання GNS3 з реальними образами ОС. Для кожної станції необхідно призначити статичну IP-адресу, маску підмережі та шлюз за замовчуванням згідно з таблицею 1. Шлюзом за замовчуванням для кожної станції є IP-адреса інтерфейсу маршрутизатора, що належить до відповідної локальної підмережі. Це забезпечує можливість пересилання трафіку до віддалених мереж через маршрутизатор після налаштування протоколу EIGRP. DNS-сервер для цієї лабораторної роботи не налаштовується, оскільки всі перевірки виконуються за IP-адресами.

Таблиця 10.2 – Налаштування параметрів мережі робочих станцій

Робоча станція	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Інтерфейс підключення
ПК1	192.168.1.10	255.255.255.0	192.168.1.1	до SW1 (Fa0/2)
ПК2	192.168.2.10	255.255.255.0	192.168.2.1	до SW2 (Fa0/2)
ПК3	192.168.3.10	255.255.255.0	192.168.3.1	до SW3 (Fa0/2)

Для налаштування ПК1 у середовищі Packet Tracer виконайте такі дії: двічі клацніть на іконці ПК1, перейдіть на вкладку «Desktop» → «IP Configuration», виберіть режим «Static» та введіть параметри згідно з таблицею 2 (IP Address: 192.168.1.10, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1). Аналогічні дії виконайте для ПК2 та ПК3 з відповідними параметрами.

Після налаштування перевірте коректність параметрів командою ipconfig на ПК1 через вкладку «Command Prompt». У розділі «Ethernet adapter Local Area Connection» мають відображатися наступні значення: IPv4 Address — 192.168.1.10, Subnet Mask — 255.255.255.0, Default Gateway — 192.168.1.1.

Якщо замість цих даних відображається «Media disconnected», перевірте фізичне підключення до комутатора SW1. Адреса, що починається з 169.254.x.x, свідчить про активацію APIPA через відсутність статичної конфігурації — повторіть налаштування через вкладку «IP Configuration». Після підтвердження параметрів виконайте локальний пінг до шлюза: ping 192.168.1.1. Успішний результат (4 з 4 пакетів отримано) підтверджує базову зв’язність на рівні 3 у локальній підмережі. Аналогічну перевірку виконайте для ПК2 та ПК3.

3.6 Налаштування протоколу EIGRP на маршрутизаторах. Активація протоколу EIGRP на маршрутизаторі R1 виконується шляхом створення процесу маршрутизації з автономною системою AS 100, вимкнення автоматичного підсумування маршрутів для підтримки безкласової адресації, та оголошення трьох мереж: двох точка-точка з’єднань з іншими маршрутизаторами (/30) та локальної підмережі ПК1 (/24) за допомогою команд network з відповідними масками-підказками:

```
R1# configure terminal
R1(config)# router eigrp 100
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.12.0 0.0.0.3
R1(config-router)# network 10.0.13.0 0.0.0.3
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# exit
R1(config)# exit
```

Наступним кроком виконується аналогічна конфігурація протоколу EIGRP на маршрутизаторі R2, де оголошуються мережі з’єднань з R1 та R3 (/30) та локальна підмережа ПК2 (/24) в межах тієї самої автономної системи AS 100:

```
R2# configure terminal
R2(config)# router eigrp 100
R2(config-router)# no auto-summary
R2(config-router)# network 10.0.12.0 0.0.0.3
R2(config-router)# network 10.0.23.0 0.0.0.3
R2(config-router)# network 192.168.2.0 0.0.0.255
R2(config-router)# exit
R2(config)# exit
```

Завершується налаштування маршрутизації активацією процесу EIGRP на маршрутизаторі R3 з оголошенням мереж з’єднань з R1 та R2 (/30) та локальної підмережі ПК3 (/24), що забезпечує повну видимість топології для всіх маршрутизаторів:

```
R3# configure terminal
R3(config)# router eigrp 100
R3(config-router)# no auto-summary
```

```
R3(config-router)# network 10.0.13.0 0.0.0.3
R3(config-router)# network 10.0.23.0 0.0.0.3
R3(config-router)# network 192.168.3.0 0.0.0.255
R3(config-router)# exit
R3(config)# exit
```

Через 10–15 секунд після завершення конфігурації перевірте встановлення сусідства командою show ip eigrp neighbors на маршрутизаторі R1. У таблиці мають відображатися два записи: сусід 10.0.12.2 (R2) через інтерфейс FastEthernet0/0 та сусід 10.0.13.2 (R3) через інтерфейс GigabitEthernet0/0. Колонка «Hold» показує час у секундах до наступного очікуваного Hello-пакета (зазвичай 12–15 секунд для швидких лінків). Якщо сусід відсутній, перевірте три ключові умови: ідентичність номера AS на всіх маршрутизаторах (show ip protocols | include EIGRP), належність суміжних інтерфейсів до однієї підмережі /30 (show ip interface brief), та відсутність помилок на інтерфейсах (show interfaces | include errors). Найчастішою причиною відсутності сусідства при наявності базової зв’язності є помилка в команді network або відсутність no auto-summary.

3.7 Верифікація роботи EIGRP та аналіз таблиць. Верифікація роботи протоколу EIGRP включає чотири ключові етапи: перевірка таблиці сусідства, аналіз таблиці топології, перегляд таблиці маршрутів та функціональне тестування зв’язності. Таблиця сусідства (show ip eigrp neighbors) підтверджує встановлення двонаправлених зв’язків. Таблиця топології (show ip eigrp topology) відображає всі відомі маршрути з їх метриками: Feasible Distance (FD) — повна метрика до мережі, та Reported Distance (RD) — метрика, оголошена сусідом. Наявність двох шляхів до однієї мережі з позначкою «P» (Passive) та виконання умови Feasibility Condition (RD_feasible_successor < FD_successor) свідчить про наявність резервного шляху (Feasible Successor). Таблиця маршрутів (show ip route eigrp) показує маршрути, що використовуються для пересилання трафіку (позначка «D»). Функціональне тестування виконується командою ping між ПК у різних підмережах.

Для детального аналізу маршрутизації до мережі ПК3 виконайте команду перегляду таблиці топології EIGRP на маршрутизаторі R1 з фільтрацією за конкретною мережею 192.168.3.0/24:

```
R1# show ip eigrp topology 192.168.3.0 255.255.255.0
```

У виводі для мережі 192.168.3.0/24 має відображатися запис із позначкою «P» (Passive) та двома рядками «via». Перший рядок (з нижчою метрикою, наприклад, 307200) вказує на основний маршрут (Successor) через 10.0.13.2 (R3). Другий рядок вказує на резервний маршрут (Feasible Successor) через 10.0.12.2 (R2) з вищою метрикою (наприклад, 332800), але з Reported Distance меншою за FD основного маршруту (наприклад, RD = 307200 < FD = 307200). Саме ця умова (RD < FD) гарантує можливість миттєвого перемикання при відмові основного лінку. Якщо другий шлях відсутній або має позначку

«active», перевірте налаштування швидкості інтерфейсів (show interface | include BW) — лінк R1–R3 повинен працювати на 1000 Mbps (BW 1000000), а лінки через R2 — на 100 Mbps (BW 100000).

Для функціонального тестування зв’язності між віддаленими робочими станціями виконайте команду пінг з ПК1 до ПК3:

```
C:\> ping 192.168.3.10
```

Усі чотири пакети мають успішно повертатися з часом відгуку 1–50 мс. Якщо пінг не проходить, перевірте таблицю маршрутів на R1 командою show ip route 192.168.3.0 — запис має мати позначку «D» (EIGRP) та шлюз 10.0.13.2. Відсутність маршруту вказує на проблему з оголошенням мережі на R3 (show run | section router eigrp) або на порушення сусідства між R1 та R3 (show ip eigrp neighbors). Якщо маршрут присутній, але пінг не проходить, перевірте налаштування шлюза на ПК3 та базову зв’язність у підмережі 192.168.3.0/24 (ping 192.168.3.1 з ПК3). Успішний пінг підтверджує коректну роботу EIGRP та можливість маршрутизації трафіку між віддаленими підмережами.

3.8 Тестування відмовостійкості мережі. Останнім етапом є імітація відмови лінку для перевірки механізму швидкої збіжності EIGRP. Вимкніть основний інтерфейс на R1 (GigabitEthernet0/0), що з’єднує його з R3, і негайно виконайте ping з ПК1 до ПК3. Завдяки наявності Feasible Successor у таблиці топології, EIGRP миттєво перемикає трафік на резервний шлях через R2 без запуску повного алгоритму DUAL. Це забезпечує відмовостійкість мережі з мінімальними затримками, що є ключовою перевагою EIGRP перед протоколами типу RIP.

Для імітації відмови основного гігабітного лінку між R1 та R3 виконайте деактивацію інтерфейсу GigabitEthernet0/0 на маршрутизаторі R1:

```
R1# configure terminal
R1(config)# interface GigabitEthernet0/0
R1(config-if)# shutdown
R1(config-if)# exit
R1(config)# exit
```

Негайно після деактивації інтерфейсу виконайте розширений пінг з ПК1 до ПК3 для оцінки часу відновлення зв’язку:

```
C:\> ping 192.168.3.10 -n 20
```

Перші 1–2 пакети можуть бути втрачені (позначка «Request timed out»), але подальші 18–19 пакетів мають успішно повертатися. Це свідчить про миттєве перемикання на резервний шлях (час відновлення < 1 секунди). Для порівняння: при використанні протоколу RIP час відновлення становив би 30–60 секунд через необхідність очікування таймера втрати маршруту та

повторного обчислення таблиці. Після тестування перевірте таблицю топології на R1 командою show ip eigrp topology 192.168.3.0 255.255.255.0 — колишній Feasible Successor (через R2) тепер відображається як єдиний маршрут із позначкою «Successor», а шлях через R3 відсутній. Для відновлення первинної топології виконайте активацію інтерфейсу:

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# no shutdown
```

Через 15–20 секунд після повторного встановлення сусідства трафік автоматично повернеться на основний шлях через R3 (GigabitEthernet) через нижчу метрику. Цей експеримент наочно демонструє ключову перевагу EIGRP — відмовостійкість без затримок завдяки збереженню резервних маршрутів у таблиці топології, що робить його придатним для критично важливих корпоративних мереж.

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 № 11

Тема: Трансляція мережевих адрес NAT/PAT та автоматичне призначення IP-адрес DHCP

Мета роботи: Набути практичних навичок налаштування механізмів NAT/PAT та автоматичного призначення IP-адрес за допомогою DHCP

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Створення та розвиток технології NAT

Протокол IPv4, розроблений у 1981 році, передбачав використання 32-бітних адрес, що теоретично дозволяло адресувати близько 4,3 мільярда пристроїв. На момент створення протоколу це здавалося достатнім ресурсом, проте стрімке зростання кількості комп’ютерів та мережевих пристроїв у 1990-х роках продемонструвало обмеженість цього адресного простору. Особливо гостро проблема виявилася з появою масового доступу до Інтернету, розвитком мобільних пристроїв та концепції Інтернету речей, коли кількість підключених до мережі пристроїв почала зростати експоненційно.

Вичерпання адресного простору IPv4 стало реальною загрозою для подальшого розвитку глобальної мережі вже наприкінці 1980-х років. Це призвело до активного пошуку технічних рішень, які б дозволили ефективніше використовувати наявний адресний простір та забезпечити можливість підключення до мережі нових пристроїв без необхідності виділення для кожного з них унікальної публічної IP-адреси.

Технологія трансляції мережевих адрес (Network Address Translation, NAT) була запропонована як одне з проміжних рішень проблеми вичерпання IPv4-адрес. Концепція NAT вперше офіційно задокументована в RFC 1631, опублікованому в травні 1994 року. Автором документа став Кевін Ейтчісон з компанії Cray Research, який описав механізм перекладу приватних IP-адрес у публічні на межі локальної та глобальної мережі. Ідея полягала в тому, що багато пристроїв усередині організації можуть використовувати приватні адреси з зарезервованих діапазонів, визначених у RFC 1918, а при виході в Інтернет їхні адреси динамічно перекладатимуться в одну або кілька публічних адрес.

Первісна реалізація NAT передбачала простий переклад адрес один до одного або багато до одного, проте швидко стало зрозуміло, що для ефективного використання обмеженої кількості публічних адрес необхідний більш досконалий механізм. Це призвело до розробки технології PAT (Port Address Translation), також відомої як NAT Overload або NAPT (Network Address and Port Translation). PAT дозволяє використовувати не лише IP-адреси, але й номери портів TCP та UDP для розрізнення з’єднань різних внутрішніх пристроїв, що виходять у зовнішню мережу через одну публічну адресу.

Для розуміння роботи технології NAT необхідно чітко визначити ключові терміни. Внутрішня локальна адреса (Inside Local Address) являє собою приватну IP-адресу пристрою у внутрішній мережі, яка використовується для комунікації всередині локальної мережі організації. Це адреси з діапазонів, визначених RFC 1918, таких як 192.168.0.0/16, 172.16.0.0/12 або 10.0.0.0/8, які не маршрутизуються в глобальному Інтернеті. Внутрішня глобальна адреса (Inside Global Address) - це публічна IP-адреса або адреса з публічного діапазону, яка представляє один або кілька внутрішніх пристроїв назовні і використовується для виходу в зовнішню мережу.

Зовнішня локальна адреса (Outside Local Address) визначається як IP-адреса зовнішнього хоста так, як вона видна з внутрішньої мережі. Зовнішня глобальна адреса (Outside Global Address) являє собою IP-адресу пристрою у зовнішній мережі, присвоєну власником цього хоста, яка є публічно маршрутизованою адресою в Інтернеті. Розуміння цих термінів критично важливе для налаштування та діагностики роботи NAT, оскільки маршрутизатор оперує саме цими категоріями адрес при виконанні трансляції.

Статичний NAT (Static NAT) здійснює постійне відображення однієї приватної IP-адреси на одну публічну IP-адресу. Цей тип трансляції використовується, коли необхідно забезпечити постійну доступність внутрішнього ресурсу з зовнішньої мережі, наприклад, для веб-серверів або поштових серверів. Динамічний NAT (Dynamic NAT) створює тимчасове відображення приватних адрес на публічні адреси з визначеного пулу доступних адрес. Коли внутрішній хост ініціює з’єднання із зовнішньою мережею, йому динамічно призначається вільна публічна адреса з пулу на час існування цього з’єднання.

PAT (Port Address Translation), або NAT Overload, являє собою найбільш ефективний та широко використовуваний тип трансляції адрес. PAT дозволяє відображати багато приватних адрес на одну або кілька публічних адрес, використовуючи різні номери портів для розрізнення з’єднань. Коли внутрішній пристрій відправляє пакет назовні, маршрутизатор змінює не лише вихідну IP-адресу на публічну, але й модифікує номер порту джерела, створюючи унікальну комбінацію адреса-порт для кожного з’єднання.

1.2 Механізм роботи PAT на рівні пакетів

Розглянемо конкретний приклад роботи PAT на основі мережевої топології з лабораторної роботи. У нашій конфігурації внутрішня мережа використовує адресний простір 192.168.3.0/24, робочі станції PC1, PC2 та PC3 мають адреси 192.168.3.10, 192.168.3.11 та 192.168.3.12 відповідно. Маршрутизатор Router0 має внутрішній інтерфейс FastEthernet0/1 з адресою 192.168.3.1 та зовнішній інтерфейс FastEthernet0/0 з адресою 203.0.113.9. Сервер Server0 розташований у зовнішній мережі та має адресу 203.0.113.10.

Коли користувач на робочій станції PC2 з адресою 192.168.3.11 намагається відкрити веб-сторінку сервера, його комп’ютер створює HTTP-запит до адреси 203.0.113.10 на порт 80. Операційна система PC2 призначає

цьому з’єднанню динамічний порт джерела, наприклад 52341, тому вихідний TCP-пакет має адресу джерела 192.168.3.11:52341 та адресу призначення 203.0.113.10:80. Цей пакет надходить через комутатор 2960-24TT на внутрішній інтерфейс Fa0/1 маршрутизатора, який налаштовано як inside interface для NAT.

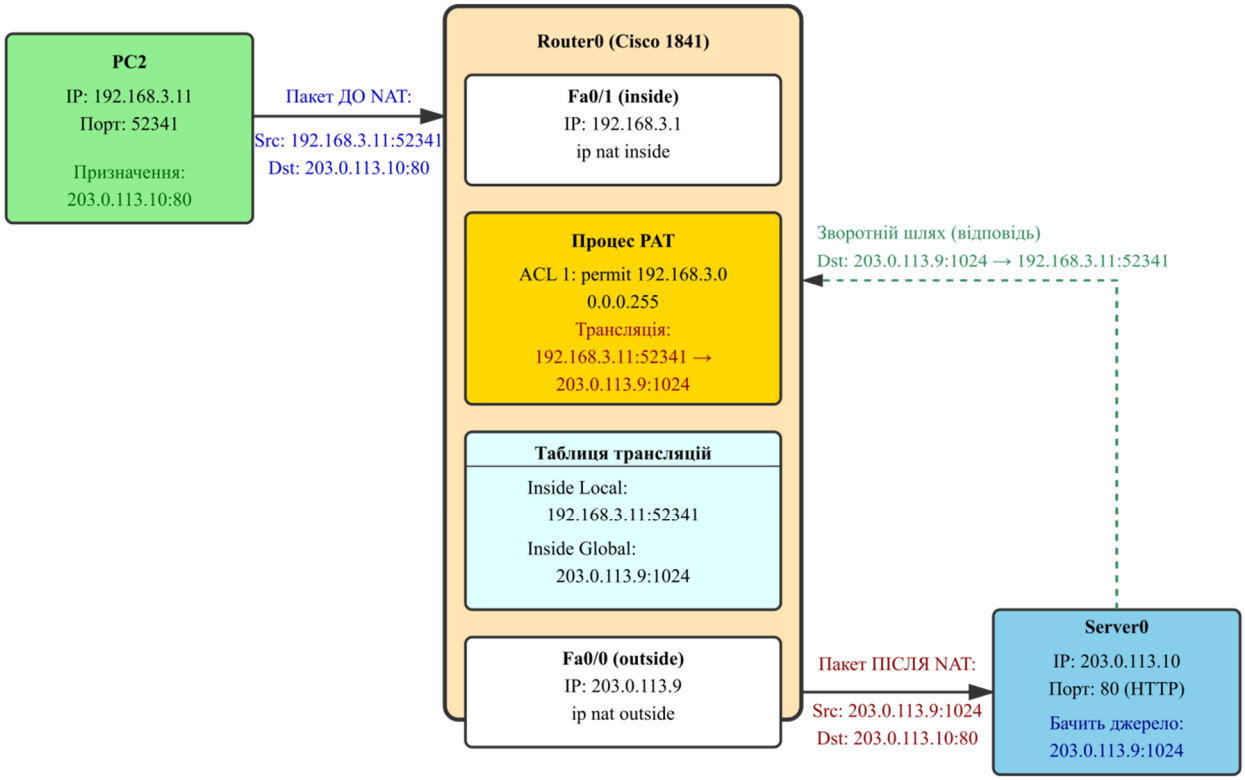

Рисунок 11.1 – Приклад роботи технлогії PAT

Маршрутизатор Router0 аналізує пакет та виявляє, що вихідна адреса 192.168.3.11 належить до діапазону, визначеного в списку доступу для NAT (192.168.3.0 з wildcard-маскою 0.0.0.255). Він створює новий запис у таблиці трансляцій PAT, де внутрішня локальна адреса 192.168.3.11 з портом 52341 відображається на зовнішню глобальну адресу зовнішнього інтерфейсу 203.0.113.9 з новим унікальним портом, наприклад 1024. Маршрутизатор модифікує заголовок IP-пакета, змінюючи вихідну адресу з 192.168.3.11 на 203.0.113.9, а також модифікує TCP-заголовок, замінюючи порт джерела з 52341 на 1024. Після перерахунку контрольних сум IP та TCP заголовків модифікований пакет відправляється через зовнішній інтерфейс Fa0/0 до сервера.

Сервер Server0 отримує пакет з вихідною адресою 203.0.113.9:1024 та адресою призначення 203.0.113.10:80. З точки зору сервера, запит надійшов від маршрутизатора за адресою 203.0.113.9, він не має інформації про реальну внутрішню адресу PC2. Сервер обробляє HTTP-запит та формує відповідь, яка адресується до 203.0.113.9:1024. Коли відповідь надходить на зовнішній інтерфейс маршрутизатора, він шукає у своїй таблиці трансляцій PAT запис, що

відповідає комбінації 203.0.113.9:1024, та знаходить відповідність з внутрішньою адресою 192.168.3.11:52341.

Маршрутизатор виконує зворотну трансляцію, замінюючи адресу призначення з 203.0.113.9:1024 на 192.168.3.11:52341, перераховує контрольні суми та відправляє пакет через внутрішній інтерфейс Fa0/1 до комутатора, який передає його на PC2. Таким чином, робоча станція PC2 отримує відповідь від сервера, не маючи уявлення про те, що її адреса була перекладена маршрутизатором. Аналогічним чином працює PAT для будь-яких інших з’єднань від PC1 або PC3, при цьому маршрутизатор використовує різні номери портів для розрізнення одночасних сеансів від різних внутрішніх хостів.

1.3 Конфігурація NAT/PAT на маршрутизаторах Cisco

Налаштування технології NAT/PAT на маршрутизаторах Cisco передбачає виконання послідовності конфігураційних команд. Перший крок полягає у визначенні того, який інтерфейс маршрутизатора буде внутрішнім (inside), а який - зовнішнім (outside). Для позначення інтерфейсів використовуються команди ip nat inside та ip nat outside в режимі конфігурації інтерфейсу. На внутрішньому інтерфейсі FastEthernet0/1, підключеному до локальної мережі через комутатор, налаштовується IP-адреса з діапазону локальної мережі та команда ip nat inside. На зовнішньому інтерфейсі FastEthernet0/0, підключеному безпосередньо до сервера, налаштовується публічна IP-адреса з підмережі /30 та команда ip nat outside.

Наступним кроком є створення списку доступу (Access Control List, ACL), який визначає, які внутрішні адреси підлягають трансляції. Стандартний ACL створюється командою access-list з номером від 1 до 99, після якої вказується дозвіл (permit) та діапазон адрес у форматі мережа з wildcard-маскою. Наприклад, команда access-list 1 permit 192.168.3.0 0.0.0.255 дозволяє трансляцію для всіх адрес у діапазоні від 192.168.3.0 до 192.168.3.255. Wildcard-маска 0.0.0.255 є інверсією звичайної маски підмережі 255.255.255.0 і вказує, що перші три октети мають співпадати, а четвертий може бути будь-яким.

Після створення ACL налаштовується власне правило NAT/PAT за допомогою команди ip nat inside source list, яка зв’язує список доступу з параметрами трансляції. Для налаштування PAT використовується команда ip nat inside source list 1 interface FastEthernet0/0 overload, де параметр overload вказує на використання перевантаження портів. Ця команда означає, що всі адреси, які відповідають ACL номер 1, будуть перекладатися в адресу зовнішнього інтерфейсу FastEthernet0/0 з використанням різних номерів портів для розрізнення з’єднань.

Важливим елементом конфігурації є налаштування маршрутизації, зокрема створення маршруту за замовчуванням (default route), який вказує маршрутизатору, куди відправляти пакети, призначені для адрес, що не належать до безпосередньо підключених мереж. Команда ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 створює такий маршрут. Без маршруту за замовчуванням

маршрутизатор не зможе коректно передавати пакети до зовнішньої мережі, навіть якщо NAT налаштовано правильно.

1.4 Діагностика та перевірка роботи NAT/PAT

Після завершення конфігурації необхідно переконатися в коректності налаштувань та працездатності технології трансляції адрес. Команда show ip interface brief виводить короткий список усіх інтерфейсів маршрутизатора з їх IP-адресами та поточним статусом. Статус кожного інтерфейсу відображається двома значеннями: перше вказує на фізичний стан з’єднання, друге - на логічний стан протоколу. Обидва інтерфейси FastEthernet0/0 та FastEthernet0/1 мають бути у стані up/up.

Команда show running-config виводить поточну активну конфігурацію маршрутизатора, включаючи всі налаштування інтерфейсів, списків доступу та правил NAT. Аналіз цього виводу дозволяє переконатися, що всі необхідні команди були введені правильно. Особливу увагу слід приділити секціям конфігурації інтерфейсів, де мають бути присутні команди ip nat inside або ip nat outside. Команда show access-lists відображає всі налаштовані списки доступу з їх номерами, правилами та лічильниками збігів.

Команда show ip route виводить таблицю маршрутизації маршрутизатора, яка містить інформацію про всі відомі мережі та шляхи до них. У виводі використовуються коди для позначення джерела маршруту: C означає безпосередньо підключену мережу (connected), S позначає статичний маршрут, а S* вказує на статичний маршрут за замовчуванням. Таблиця маршрутизації повинна містити записи для обох безпосередньо підключених мереж (192.168.3.0/24 на Fa0/1 та 203.0.113.8/30 на Fa0/0), а також маршрут за замовчуванням S* 0.0.0.0/0, який вказує на інтерфейс FastEthernet0/0.

Найбільш інформативною командою для діагностики NAT є show ip nat translations, яка відображає поточну таблицю активних трансляцій адрес. Кожен запис у таблиці містить інформацію про протокол (TCP, UDP, ICMP), внутрішню глобальну адресу з портом (Inside global), внутрішню локальну адресу з портом (Inside local), зовнішню локальну адресу з портом (Outside local) та зовнішню глобальну адресу з портом (Outside global). Наприклад, після виконання команди ping з PC2 до сервера, у таблиці з’являться записи типу: icmp 203.0.113.9:1024 192.168.3.11:1 203.0.113.10:1 203.0.113.10:1024, що показує трансляцію ICMP-пакету від внутрішньої адреси 192.168.3.11 у зовнішню адресу 203.0.113.9 при комунікації із сервером 203.0.113.10.

Команда show ip nat statistics надає загальну статистичну інформацію про роботу NAT, включаючи загальну кількість активних трансляцій, кількість створених та видалених записів, інформацію про налаштовані інтерфейси inside та outside, а також інформацію про налаштовані ACL для NAT. Ця команда корисна для оцінки загального завантаження системи NAT та виявлення потенційних проблем.

Таблиця 11.1 – Таблиця команд для роботи з NAT/PAT

Команда	Режим виконання	Призначення
enable	User EXEC	Перехід у привілейований режим EXEC
configure terminal	Privileged EXEC	Вхід у режим глобальної конфігурації
interface [тип] [номер]	Global Config	Вхід у режим конфігурації інтерфейсу
ip address [адреса] [маска]	Interface Config	Призначення IP-адреси інтерфейсу
ip nat inside	Interface Config	Позначення інтерфейсу як внутрішнього для NAT
ip nat outside	Interface Config	Позначення інтерфейсу як зовнішнього для NAT
no shutdown	Interface Config	Активація інтерфейсу
access-list [номер] permit [мережа] [wildcard]	Global Config	Створення стандартного списку доступу для NAT
ip nat inside source list [номер_ACL] interface [інтерфейс] overload	Global Config	Налаштування PAT з використанням адреси інтерфейсу
ip route 0.0.0.0 0.0.0.0 [інтерфейс]	Global Config	Створення маршруту за замовчуванням
show ip interface brief	Privileged EXEC	Перегляд статусу всіх інтерфейсів
show running-config	Privileged EXEC	Відображення поточної конфігурації
show access-lists	Privileged EXEC	Перегляд налаштованих списків доступу
show ip route	Privileged EXEC	Відображення таблиці маршрутизації
show ip nat translations	Privileged EXEC	Перегляд активних трансляцій NAT
show ip nat statistics	Privileged EXEC	Відображення статистики роботи NAT

1.5 Типові помилки при налаштуванні NAT/PAT

При налаштуванні NAT/PAT студенти часто стикаються з типовими помилками, які призводять до некоректної роботи мережі. Неправильне позначення інтерфейсів як inside або outside призводить до того, що маршрутизатор намагається виконувати трансляцію в неправильному напрямку. Перевірити правильність позначень можна командою show running-config, аналізуючи секції конфігурації інтерфейсів.

Помилки в синтаксисі wildcard-маски в списку доступу також є частою проблемою. На відміну від звичайної маски підмережі, wildcard-маска використовує інверсну логіку, де 0 означає “мусить співпадати”, а 1 означає “може бути будь-яким”. Для підмережі 192.168.3.0/24 правильна wildcard-маска буде 0.0.0.255, а не 255.255.255.0. Відсутність маршруту за замовчуванням є

критичною помилкою, яка унеможливлює передачу пакетів до зовнішньої мережі.

Неузгодженість адрес у підмережі /30 для з'єднання маршрутизатора з сервером також часто призводить до проблем. Підмережа /30 містить лише чотири адреси, з яких лише дві можуть використовуватися для пристроїв. Якщо підмережа визначена як 203.0.113.8/30, то доступні адреси - 203.0.113.9 та 203.0.113.10. Призначення маршрутизатору адреси 203.0.113.9, а серверу - 203.0.113.10 із маскою 255.255.255.252 забезпечує їх знаходження в одній підмережі. Помилки в налаштуванні шлюзу за замовчуванням на кінцевих пристроях також є джерелом проблем - робочі станції повинні мати шлюзом адресу внутрішнього інтерфейсу маршрутизатора (192.168.3.1), а сервер - адресу зовнішнього інтерфейсу (203.0.113.9).

2 КЛЮЧОВІ ПИТАННЯ

1. Що таке NAT і яка головна причина його виникнення в мережах IPv4?
2. Які основні типи NAT існують, і чим відрізняється PAT (NAT Overload) від Static і Dynamic NAT?
3. Поясніть значення термінів: Inside Local Address, Inside Global Address, Outside Local Address, Outside Global Address.
4. Як PAT забезпечує одночасний вихід у Інтернет кількох пристроїв через одну публічну IP-адресу?
5. Які команди використовуються в Cisco IOS для позначення інтерфейсів як inside і outside при налаштуванні NAT?
6. Як правильно скласти стандартний ACL для визначення діапазону приватних IP-адрес, що підлягають трансляції? Наведіть приклад з wildcard-маскою.
7. Яка роль маршруту за замовчуванням (ip route 0.0.0.0 0.0.0.0) у коректній роботі NAT/PAT?
8. Які команди діагностики використовуються для перевірки коректності конфігурації NAT на маршрутизаторі Cisco?
9. Як у Packet Tracer перевірити, що трансляція адрес відбувається під час ICMP- або HTTP-запитів у Simulation Mode?
10. Які типові помилки можуть виникнути під час налаштування NAT/PAT, і як їх уникнути?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1. Створення моделі мережі. Відкрити симулятор мереж Cisco Packet Tracer. Побудувати схему мережі згідно рисунку 11.2, що включає: три робочі станції (PC1, PC2, PC3), комутатор типу 2960-24TT, маршрутизатор Cisco 1841 та сервер Server-PT. Робочі станції підключаються до комутатора, який у свою чергу з'єднується з маршрутизатором через інтерфейс FastEthernet0/1. Маршрутизатор з'єднаний з сервером напряму через інтерфейс FastEthernet0/0. Ця конфігурація дозволяє реалізувати технологію NAT для забезпечення

доступу приватних комп’ютерів до ресурсів сервера, розташованого у зовнішній мережі.

IP-адреси для приватної LAN-мережі та публічного сервера визначаються згідно з індивідуальним варіантом студента (номером у журналі). Для визначення адрес використовується таблиця 5.4, де кожен варіант відповідає номеру студента і визначає діапазон приватних адрес для внутрішньої мережі та публічну адресу сервера з урахуванням підмережі /30. У даному випадку сервер має маску 255.255.255.252 (/30), тому шлюз повинен бути в тій самій підмережі.

Оскільки маршрутизатор Cisco 1841 має два вбудовані інтерфейси FastEthernet, які достатні для підключення до LAN (Fa0/1) та до сервера (Fa0/0), додаткові модулі розширення не потрібні.

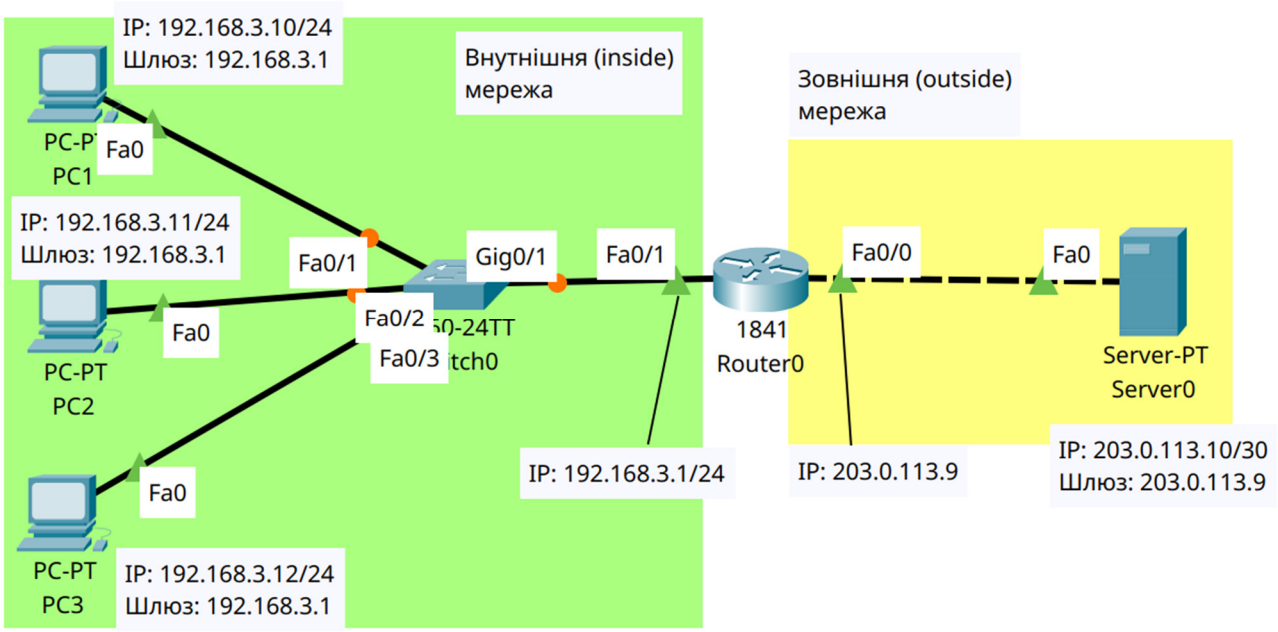

Рисунок 11.2 – Схема мережі для виконання лабораторної роботи з використанням NAT

Таблиця 11.2 – Варіанти індивідуальних завдань

Номер варіанта (N)	IP адреса LAN внутрішньої підмережі	IP адреси зовнішньої підмережі			
		Шлюз	Сервер	Маска	Підмережа
1	192.168.1.0	203.0.113.1	203.0.113.2	255.255.255.252	203.0.113.0/30
2	192.168.2.0	203.0.113.5	203.0.113.6	255.255.255.252	203.0.113.4/30
3	192.168.3.0	203.0.113.9	203.0.113.10	255.255.255.252	203.0.113.8/30
4	192.168.4.0	203.0.113.13	203.0.113.14	255.255.255.252	203.0.113.12/30
5	192.168.5.0	203.0.113.17	203.0.113.18	255.255.255.252	203.0.113.16/30
6	192.168.6.0	203.0.113.21	203.0.113.22	255.255.255.252	203.0.113.20/30
7	192.168.7.0	203.0.113.25	203.0.113.26	255.255.255.252	203.0.113.24/30
8	192.168.8.0	203.0.113.29	203.0.113.30	255.255.255.252	203.0.113.28/30
9	192.168.9.0	203.0.113.33	203.0.113.34	255.255.255.252	203.0.113.32/30
10	192.168.10.0	203.0.113.37	203.0.113.38	255.255.255.252	203.0.113.36/30

11	192.168.11.0	203.0.113.41	203.0.113.42	255.255.255.252	203.0.113.40/30
12	192.168.12.0	203.0.113.45	203.0.113.46	255.255.255.252	203.0.113.44/30
13	192.168.13.0	203.0.113.49	203.0.113.50	255.255.255.252	203.0.113.48/30
14	192.168.14.0	203.0.113.53	203.0.113.54	255.255.255.252	203.0.113.52/30
15	192.168.15.0	203.0.113.57	203.0.113.58	255.255.255.252	203.0.113.56/30
16	192.168.16.0	203.0.113.61	203.0.113.62	255.255.255.252	203.0.113.60/30
17	192.168.17.0	203.0.113.65	203.0.113.66	255.255.255.252	203.0.113.64/30
18	192.168.18.0	203.0.113.69	203.0.113.70	255.255.255.252	203.0.113.68/30
19	192.168.19.0	203.0.113.73	203.0.113.74	255.255.255.252	203.0.113.72/30
20	192.168.20.0	203.0.113.77	203.0.113.78	255.255.255.252	203.0.113.76/30
21	192.168.21.0	203.0.113.81	203.0.113.82	255.255.255.252	203.0.113.80/30
22	192.168.22.0	203.0.113.85	203.0.113.86	255.255.255.252	203.0.113.84/30
23	192.168.23.0	203.0.113.89	203.0.113.90	255.255.255.252	203.0.113.88/30
24	192.168.24.0	203.0.113.93	203.0.113.94	255.255.255.252	203.0.113.92/30
25	192.168.25.0	203.0.113.97	203.0.113.98	255.255.255.252	203.0.113.96/30
26	192.168.26.0	203.0.113.101	203.0.113.102	255.255.255.252	203.0.113.100/30
27	192.168.27.0	203.0.113.105	203.0.113.106	255.255.255.252	203.0.113.104/30
28	192.168.28.0	203.0.113.109	203.0.113.110	255.255.255.252	203.0.113.108/30
29	192.168.29.0	203.0.113.113	203.0.113.114	255.255.255.252	203.0.113.112/30
30	192.168.30.0	203.0.113.117	203.0.113.118	255.255.255.252	203.0.113.116/30

3.2. Налаштування мережевих інтерфейсів маршрутизатора та обладнання

3.2.1. Налаштовуємо маршрутизатор Router0 для реалізації функції перекладу адрес. Для цього вводимо команди у режимі конфігурації. У нашому прикладі використовується варіант 3, тому налаштування виконуються для мережі 192.168.3.0/24:

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

Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 203.0.113.9 255.255.255.252
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# access-list 1 permit 192.168.3.0 0.0.0.255
Router(config)#   ip   nat   inside   source   list   1   interface
FastEthernet0/0 overload
```

```
Router(config)# ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
Router(config)# exit
```

Увага: інтерфейс Fa0/0 отримує статичну адресу з підмережі сервера (203.0.113.9/30), бо сервер має адресу 203.0.113.10. Таким чином, маршрутизатор і сервер знаходяться в одній підмережі.

3.2.2. Налаштовуємо робочі станції. Кожна з них повинна мати статичну IP-адресу з діапазону відповідної LAN-підмережі, маску підмережі 255.255.255.0 та шлюз за замовчуванням – адресу внутрішнього інтерфейсу маршрутизатора (192.168.N.1).

У нашому прикладі (варіант 3) для PC1 встановлюємо: IP-адреса — 192.168.3.10, Subnet Mask — 255.255.255.0, Default Gateway — 192.168.3.1. Аналогічно налаштовуємо PC2 і PC3 з адресами 192.168.3.11 та 192.168.3.12. Для цього клікаємо подвійним клацанням на робочу станцію, переходимо до вкладки Desktop → IP Configuration → Static, вводимо параметри та натискаємо OK.

3.2.3. Налаштовуємо сервер. Клікаємо подвійним клацанням на сервер, переходимо до вкладки Desktop → IP Configuration → Static. Вводимо IP-адресу сервера, вказану в таблиці вихідних даних для відповідного варіанта. У нашому прикладі (варіант 3) це: IP-адреса — 203.0.113.10, Subnet Mask — 255.255.255.252, Default Gateway — 203.0.113.9. Після введення даних натискаємо кнопку OK. Далі переходимо до вкладки Config → Services і включаємо HTTP-сервіс, натиснувши кнопку ON. Це дозволить серверу відповідати на веб-запити.

3.3. Перевірка роботи мережі

3.3.1 Перевірка у режимі реального часу. Після завершення налаштування всіх пристроїв необхідно перевірити коректність роботи мережі, використовуючи два режими: реальний час (Realtime) та покроковий режим (Simulation Mode). Переконайтеся, що всі інтерфейси пристроїв активовані (показані як зелені). У режимі Realtime відкрийте командний рядок (Command Prompt) на одній із робочих станцій (PC1, PC2 або PC3). Виконайте команду

```
ping 203.0.113.10
```

де 203.0.113.10 — це IP-адреса сервера, вказану в таблиці вихідних даних для вашого варіанта. Якщо мережа налаштована правильно, має бути отримано відповіді від сервера. Додатково відкрийте веб-браузер на одній із робочих станцій і введіть адресу http:// 203.0.113.10. У разі успішного підключення відображається веб-сторінка сервера, що підтверджує роботу HTTP-запитів через NAT.

Після успішного пінгування сервера та відкриття його веб-сторінки з робочої станції, необхідно перейти до консолі маршрутизатора Router0 для

детальної перевірки конфігурації та роботи технології NAT/PAT. Це дозволить підтвердити, що всі компоненти налаштовані коректно і працюють як очікувалося. Для цього виконайте наступні кроки.

Перший крок — перевірка статусу інтерфейсів. Виконайте команду `show ip interface brief`. Ця команда показує список усіх інтерфейсів маршрутизатора разом з їх IP-адресами та поточним статусом. У нашому випадку (варіант 3) важливо переконатися, що обидва ключові інтерфейси, FastEthernet0/0 (зовнішній) та FastEthernet0/1 (внутрішній), мають статус up/up, що означає, що вони фізично підключені та логічно активовані. Нижче наведено приклад коректного виводу цієї команди.

```
Interface          IP-Address   OK?  MethodStatus              Protocol
FastEthernet0/0    203.0.113.9  YES  manualup                  up
FastEthernet0/1    192.168.3.1  YES  manualup                  up
```

Другий крок — перевірка позначень NAT-зон. Виконайте команду `show running-config` або скорочену версію `show run`. Проаналізуйте вивід, зосередившись на секціях конфігурації для інтерфейсів FastEthernet0/0 та FastEthernet0/1. Переконайтеся, що на інтерфейсі FastEthernet0/1 (що з’єднується з внутрішньою мережею) встановлено команду ip nat inside, а на інтерфейсі FastEthernet0/0 (що з’єднується з зовнішньою мережею) — команду ip nat outside. Це критично важливо для того, щоб маршрутизатор правильно визначав, який трафік потрібно перекладати.

Третій крок — перевірка списку доступу (ACL) для NAT. Виконайте команду `show access-lists`. Ця команда виведе всі налаштовані списки доступу. Знайдіть ACL з номером 1 (який був створений для NAT) і переконайтеся, що він містить рядок permit 192.168.3.0 0.0.0.255. Цей запис дозволяє трафіку з усієї внутрішньої мережі (192.168.3.0/24) проходити через процес перекладу адрес. Приклад виводу наведено нижче:

```
Standard IP access list 1
10 permit 192.168.3.0 0.0.0.255
```

Четвертий крок — перевірка наявності маршруту за замовчуванням. Виконайте команду `show ip route`. Ця команда показує таблицю маршрутів маршрутизатора. У ній має бути запис про маршрут за замовчуванням (S* 0.0.0.0/0), який вказує на інтерфейс FastEthernet0/0. Цей маршрут необхідний для того, щоб маршрутизатор знав, куди відправляти всі пакети, призначені для адрес, які не входять до його безпосередніх мереж (тобто для всіх зовнішніх адрес, таких як 203.0.113.10). Приклад виводу:

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS
inter area
* – candidate default, U – per-user static route, o – ODR
P – periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C 192.168.3.0/24 is directly connected, FastEthernet0/1
203.0.113.0/30 is subnetted, 1 subnets
C 203.0.113.8 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 is directly connected, FastEthernet0/0
```

П’ятий крок — перевірка активних перекладів адрес (NAT translations). Виконайте команду `show ip nat translations`. Після того, як ви зробили ping або відкрили сторінку в браузері, у виводі цієї команди має з’явитися один або кілька записів. Ці записи показують, як внутрішня приватна IP-адреса (наприклад, 192.168.3.10) була динамічно перекладена в публічну IP-адресу інтерфейсу FastEthernet0/0 (203.0.113.9). Це пряме підтвердження того, що технологія PAT (Port Address Translation) працює коректно, оскільки вона використовує порти для розрізнення сеансів різних хостів, що виходять у зовнішню мережу. Приклад виводу:

```
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 203.0.113.9:1024 192.168.3.11:1 203.0.113.10:1
203.0.113.10:1024
icmp 203.0.113.9:1025 192.168.3.11:2 203.0.113.10:2
203.0.113.10:1025
icmp 203.0.113.9:1026 192.168.3.11:3 203.0.113.10:3
203.0.113.10:1026
icmp 203.0.113.9:1027 192.168.3.11:4 203.0.113.10:4
203.0.113.10:1027
icmp 203.0.113.9:1 192.168.3.10:1 203.0.113.10:1 203.0.113.10:1
icmp 203.0.113.9:2 192.168.3.10:2 203.0.113.10:2 203.0.113.10:2
icmp 203.0.113.9:3 192.168.3.10:3 203.0.113.10:3 203.0.113.10:3
icmp 203.0.113.9:4 192.168.3.10:4 203.0.113.10:4 203.0.113.10:4
```

Виконання цих п’яти кроків дозволяє повністю підтвердити, що мережа налаштована правильно, а технологія NAT/PAT працює як очікувалося, забезпечуючи доступ приватних хостів до публічного сервера.

3.3.2 Перевірка у покроковому режимі. Перейдіть до режиму Simulation Mode, натиснувши вкладку Simulation у нижній частині вікна Packet Tracer. У панелі Event List натисніть кнопку Edit Filters і залиште ввімкненими протоколи ICMP (для ping) та TCP (для HTTP). Знову відкрийте командний рядок на

робочій станції і виконайте команду ping 203.0.113.10. У режимі симуляції ви побачите анімацію пакетів, що проходять через мережу. Клацніть на пакет у списку подій, щоб переглянути його деталі. У вікні PDU Information спостерігайте, як при вході в маршрутизатор пакет має внутрішню IP-адресу (наприклад, 192.168.3.10), а при виході — публічну IP-адресу інтерфейсу Fa0/0 маршрутизатора. Це свідчить про те, що технологія NAT/PAT працює правильно. Для перевірки HTTP-запитів відкрийте браузер на PC і перейдіть за адресою http://203.0.113.50. У режимі Simulation ви побачите TCP-запити, які також проходять через NAT. Таким чином, ви можете візуалізувати процес перекладу адрес і зрозуміти механізм роботи NAT крок за кроком.

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 № 12

Тема: Централізована автентифікація мережевого обладнання з використанням AAA та RADIUS

Мета роботи: Набути практичних навичок налаштування централізованої автентифікації мережевого обладнання з використанням AAA та RADIUS

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Вступ до централізованої автентифікації мережевого обладнання

Централізована автентифікація мережевого обладнання є критично важливим елементом забезпечення безпеки сучасних корпоративних мереж, оскільки вона дозволяє організувати єдину точку контролю доступу до всіх активних компонентів інфраструктури. У традиційних підходах до управління мережею кожен окремий пристрій, будь то маршрутизатор, комутатор чи бездротова точка доступу, зберігає власну локальну базу облікових записів користувачів, що призводить до значних адміністративних труднощів у великих організаціях. Адміністратор вимушений синхронізувати облікові дані на десятках або сотнях пристроїв, що не тільки збільшує ймовірність помилок конфігурації, але й ускладнює процеси аудиту безпеки та дотримання регуляторних вимог. Крім того, локальне зберігання паролів на кожному пристрої створює додаткові вразливості, оскільки компрометація одного пристрою може призвести до витоку облікових даних, які потенційно використовуються на інших елементах мережі. Централізовані системи автентифікації вирішують ці проблеми шляхом делегування функцій верифікації облікових даних спеціалізованому серверу, який виступає єдиним джерелом істини щодо автентичності користувачів.

Модель Authentication, Authorization, and Accounting, відома як AAA, представляє собою архітектурну основу для організації централізованого управління доступом до мережевих ресурсів. Ця модель складається з трьох функціонально незалежних, але тісно інтегрованих компонентів, кожен з яких відповідає за певний аспект безпеки. Компонент Authentication відповідає за верифікацію ідентичності користувача шляхом перевірки облікових даних, таких як комбінація логіна та пароля, цифрових сертифікатів або інших факторів автентифікації. Після успішної автентифікації активується компонент Authorization, який визначає, до яких саме ресурсів та команд має доступ верифікований користувач, базуючись на його ролі в організації та налаштованих політиках доступу. Нарешті, компонент Accounting забезпечує детальну реєстрацію всіх дій користувача, включаючи час підключення, виконані команди та обсяг переданих даних, що є критично важливим для проведення аудиту безпеки, розслідування інцидентів та виконання вимог комплаєнсу.

Протокол RADIUS, що розшифровується як Remote Authentication Dial-In User Service, є де-факто промисловим стандартом для реалізації централізованої AAA-функціональності в мережевому обладнанні. Розроблений компанією Livingston Enterprises у середині 1990-х років для автентифікації користувачів комутованого доступу, RADIUS згодом еволюціонував у універсальний протокол, що широко підтримується практично всіма виробниками мережевого обладнання. Протокол визначений у RFC 2865 для функцій автентифікації та авторизації, а також у RFC 2866 для функцій обліку. RADIUS функціонує за клієнт-серверною архітектурою, де мережеві пристрої виступають як RADIUS-клієнти, а спеціалізовані сервери виконують роль централізованих точок верифікації. Важливою особливістю протоколу є використання транспортного протоколу UDP, що забезпечує ефективну роботу навіть у умовах високого навантаження та можливих втрат пакетів у мережі.

1.2 Архітектура та принципи роботи протоколу RADIUS

Функціонування протоколу RADIUS базується на обміні повідомленнями між мережевим пристроєм, що виступає як RADIUS-клієнт, та RADIUS-сервером, який зберігає базу даних облікових записів користувачів. Коли користувач намагається отримати доступ до мережевого пристрою, наприклад, ініціюючи Telnet або SSH з’єднання, пристрій не перевіряє облікові дані локально, а формує спеціальне повідомлення Access-Request та надсилає його на RADIUS-сервер. Це повідомлення містить набір атрибутів, які описують запит на автентифікацію, зокрема ім’я користувача у відкритому вигляді, пароль у захищеному форматі, IP-адресу пристрою, тип підключення та інші параметри контексту. Критично важливим елементом безпеки є механізм захисту атрибута User-Password, який не передається у відкритому вигляді навіть у зашифрованому каналі. Замість цього RADIUS використовує спеціальний алгоритм, що комбінує пароль користувача зі спільним секретним ключем та випадковим значенням, що міститься у повідомленні, після чого результат хешується за допомогою алгоритму MD5. Цей підхід забезпечує конфіденційність паролів навіть у разі перехоплення мережевого трафіку, оскільки без знання спільного секретного ключа зловмисник не може відновити оригінальний пароль.

Після отримання повідомлення Access-Request сервер виконує низку перевірок для валідації запиту та автентифікації користувача. Спочатку сервер перевіряє, чи зареєстрований пристрій, що надіслав запит, у базі даних дозволених RADIUS-клієнтів, порівнюючи його IP-адресу з налаштованим списком. Якщо пристрій не авторизований для використання сервера, запит відхиляється без подальшої обробки. Далі сервер перевіряє цілісність повідомлення, використовуючи спільний секретний ключ для обчислення контрольної суми та порівняння її з отриманим значенням. Цей механізм захищає від атак типу man-in-the-middle та спроб підробки запитів. Після успішної валідації запиту сервер витягує ім’я користувача та захищений пароль, виконує дешифрування паролю з використанням спільного ключа,

після чого порівнює отримані дані з базою облікових записів. У разі співпадіння облікових даних сервер формує відповідь Access-Accept, яка може містити додаткові атрибути авторизації, такі як призначений IP-адреса, рівень привілеїв або параметри сесії.

У таблиці 12.1 наведено основні типи RADIUS-повідомлень та їх призначення в процесі взаємодії між клієнтом та сервером.

Таблиця 12.1 – Типи повідомлень протоколу RADIUS

Тип повідомлення	Код	Напрямок передачі	Призначення
Access-Request	1	Клієнт → Сервер	Запит на автентифікацію користувача з передачею облікових даних та контексту підключення
Access-Accept	2	Сервер → Клієнт	Підтвердження успішної автентифікації з можливістю передачі атрибутів авторизації
Access-Reject	3	Сервер → Клієнт	Відмова в автентифікації через неправильні облікові дані або порушення політик безпеки
Access-Challenge	11	Сервер → Клієнт	Запит додаткової інформації для багатофакторної автентифікації або інтерактивного діалогу
Accounting-Request	4	Клієнт → Сервер	Передача інформації про події обліку (початок сесії, завершення, проміжні дані)
Accounting-Response	5	Сервер → Клієнт	Підтвердження отримання інформації про подію обліку

Процес взаємодії RADIUS-клієнта та сервера характеризується певними особливостями, які необхідно враховувати при проектуванні мережевої інфраструктури. По-перше, протокол використовує механізм таймаутів та повторних спроб для забезпечення надійності доставки повідомлень, оскільки UDP не гарантує доставку пакетів. Якщо клієнт не отримує відповіді від сервера протягом налаштованого інтервалу часу, він повторює передачу запиту, збільшуючи лічильник спроб. По-друге, кожне повідомлення містить унікальний ідентифікатор транзакції, який дозволяє коректно співставляти запити та відповіді навіть у разі затримок або неупорядкованої доставки пакетів. По-третє, стандартні порти UDP для RADIUS становлять 1812 для автентифікації та 1813 для обліку, хоча історично також використовувалися порти 1645 та 1646 відповідно. У навчальному середовищі Cisco Packet Tracer зазвичай використовується порт 1645 для сумісності з реалізацією емулятора. По-четверте, RADIUS підтримує концепцію проксі-серверів, що дозволяє організовувати ієрархічні структури автентифікації для великих розподілених мереж.

Механізм авторизації в RADIUS реалізується через передачу атрибутів у повідомленні Access-Accept, які інформують мережевий пристрій про дозволені дії та ресурси для автентифікованого користувача. Одним з найбільш важливих атрибутів є Service-Type, який визначає тип сервісу, доступний користувачу,

наприклад Login (інтерактивний доступ до командного рядка) або Framed (підключення до мережі з отриманням IP-адреси). Для обладнання Cisco критично важливим є атрибут cisco-avpair, який може передавати специфічні для Cisco команди авторизації, зокрема рівень привілеїв користувача через значення shell:priv-lvl=15 для адміністраторського доступу. Атрибути Filter-Id та Reply-Message дозволяють застосовувати політики фільтрації трафіку та передавати текстові повідомлення користувачу відповідно. Важливо розуміти, що остаточне рішення про надання доступу приймає мережевий пристрій на основі отриманих атрибутів та локальних політик безпеки, тому некоректна конфігурація пристрою може нівелювати рішення сервера.

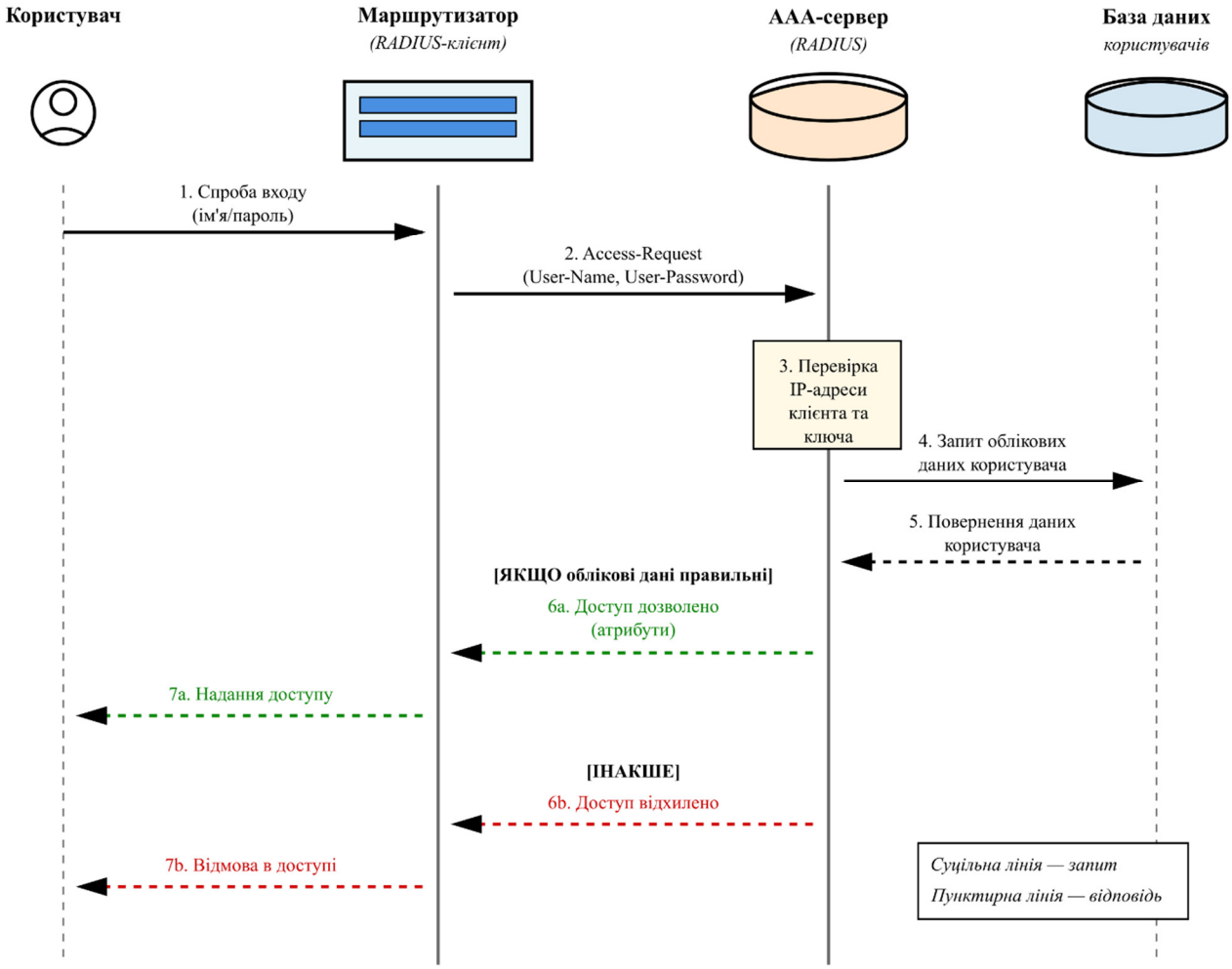

Рисунок 12.1 – Послідовність взаємодії компонентів при RADIUS-автентифікації

На рисунку 12.1 зображена діаграма послідовності взаємодії між чотирма ключовими учасниками процесу автентифікації. Зліва направо розташовані вертикальні лінії життя для таких об’єктів: користувач (зображений як піктограма людини), мережевий пристрій або RADIUS-клієнт (зображений як прямокутник з підписом "Router"), RADIUS-сервер (зображений як циліндр бази даних з підписом "AAA Server"), та база даних користувачів (зображений як циліндр з підписом "User DB"). Послідовність починається з горизонтальної

стрілки від користувача до маршрутизатора з підписом "1. Спроба входу (логін/пароль)", що символізує спробу підключення. Далі від маршрутизатора до сервера йде стрілка "2. Запит на автентифікацію (User-Name, User-Password)", що представляє передачу запиту на автентифікацію. Сервер виконує внутрішню операцію, показану петлею на лінії життя з підписом "3. Перевірка IP-адреси клієнта та ключа", після чого відбувається взаємодія з базою даних через стрілки "4. Запит облікових даних" від сервера до бази та "5. Повернення даних користувача" у зворотному напрямку. Залежно від результату перевірки, сервер надсилає маршрутизатору або "6а. Доступ дозволено (атрибути)" або "6б. Доступ відхилено", що показано двома альтернативними стрілками. Нарешті, маршрутизатор інформує користувача про результат через стрілки "7а. Надання доступу" або "7б. Відмова в доступі" відповідно. Всі стрілки мають суцільні лінії для запитів та пунктирні для відповідей, що відповідає нотації UML для діаграм послідовності, про що також зазначено в легенді рисунка: "Суцільна лінія — запит, Пунктирна лінія — відповідь".

1.3 Реалізація моделі AAA на мережевому обладнанні Cisco

Впровадження централізованої автентифікації на обладнанні Cisco вимагає виконання послідовності конфігураційних кроків, які активують модель AAA та інтегрують пристрій з RADIUS-сервером. Фундаментальною командою, яка перемикає операційну систему Cisco IOS у режим централізованого управління доступом, є команда глобальної конфігурації aaa new-model, виконання якої є обов’язковою передумовою для всіх наступних налаштувань AAA. До активації цієї команди маршрутизатор або комутатор використовує традиційні методи автентифікації через локальну базу користувачів та конфігурацію ліній доступу, а після активації всі механізми безпеки починають керуватися через централізовані політики AAA. Важливо розуміти, що команда aaa new-model змінює поведінку консольного доступу, тому рекомендується попередньо налаштувати принаймні один метод автентифікації, щоб уникнути блокування доступу до пристрою. Після активації моделі AAA необхідно визначити параметри підключення до RADIUS-сервера за допомогою команди radius-server host, яка специфікує IP-адресу сервера, порт автентифікації та спільний секретний ключ. Саме цей ключ використовується для криптографічного захисту обміну даними між пристроєм та сервером, тому його конфіденційність має критичне значення для безпеки всієї системи.

Конфігурація методів автентифікації в Cisco IOS базується на концепції списків методів, які визначають послідовність джерел верифікації облікових даних та поведінку системи у разі недоступності певного джерела. Команда aaa authentication login створює іменований або стандартний список методів автентифікації для входу в систему, де кожен метод представляє певний спосіб перевірки облікових даних. Найпоширенішими методами є group radius для використання RADIUS-серверів, local для локальної бази користувачів, line для

паролів на лініях доступу, enable для пароля привілейованого режиму, та none для доступу без автентифікації. Порядок перерахування методів визначає послідовність їх використання: система спочатку намагається автентифікувати користувача через перший метод у списку, і лише у разі його недоступності або технічної помилки переходить до наступного. Критично важливо розуміти різницю між недоступністю методу та невдалою автентифікацією: якщо RADIUS-сервер відповів повідомленням Access-Reject, це вважається остаточним рішенням про відмову в доступі, і система не переходить до наступних методів, натомість якщо сервер взагалі не відповідає через мережеві проблеми, система автоматично використовує наступний метод у списку.

У таблиці 12.2 наведено основні команди конфігурації AAA на обладнанні Cisco з детальним описом їх синтаксису та призначення.

Таблиця 12.2 — Команди конфігурації моделі AAA в Cisco IOS

Команда	Режим конфігурації	Опис та приклад використання
aaa new-model	Global Config	Активує модель AAA на пристрої. Після виконання всі механізми доступу керуються через AAA-політики. Приклад: Router(config)# aaa new-model
radius-server host {ip} auth-port {port} key {secret}	Global Config	Визначає параметри RADIUS-сервера: IP-адресу, порт автентифікації та спільний секретний ключ. Приклад: Router(config)# radius-server host 192.168.1.100 auth-port 1645 key radius_key
aaa authentication login {default|list-name} method1 [method2…]	Global Config	Створює список методів автентифікації для входу. Список default застосовується до всіх ліній без явного списку. Приклад: Router(config)# aaa authentication login default group radius local
aaa authorization exec {default|list-name} method1 [method2…]	Global Config	Визначає методи авторизації для виконавчого режиму (EXEC). Контролює привілеї після успішного входу. Приклад: Router(config)# aaa authorization exec default group radius if-authenticated
login authentication {list-name}	Line Config	Застосовує іменований список методів автентифікації до конкретної лінії доступу. Приклад: Router(config-line)# login authentication default
username {name} privilege {level} secret {password}	Global Config	Створює локальний обліковий запис з рівнем привілеїв та захищеним паролем для резервного доступу. Приклад: Router(config)# username backup privilege 15 secret emergency_pass

Застосування списків методів автентифікації до конкретних ліній доступу здійснюється через конфігурацію відповідних інтерфейсів командного рядка, зокрема консолі (con 0), допоміжного порту (aux 0) та віртуальних терміналів (vty 0 4 або vty 0 15 залежно від моделі пристрою). Для активації централізованої автентифікації на віртуальних терміналах, які

використовуються для віддаленого доступу через Telnet або SSH, необхідно увійти в режим конфігурації ліній командою line vty 0 4 та виконати команду login authentication з посиланням на відповідний список методів. Якщо використовується стандартний список default, він автоматично застосовується до всіх ліній, що не мають явно визначеного альтернативного списку. Важливою особливістю конфігурації віртуальних терміналів є те, що без явної команди login authentication або login local доступ через ці лінії буде заблокований навіть за наявності правильних облікових даних, оскільки система не знає, який метод автентифікації застосувати. Додатково рекомендується налаштувати параметр transport input на лініях vty для обмеження дозволених протоколів доступу, зокрема transport input telnet ssh для обмеження доступу тільки через Telnet та SSH з блокуванням інших протоколів.

Механізм відмовостійкості в системах централізованої автентифікації реалізується через створення резервних методів доступу, які дозволяють адміністратору отримати доступ до пристрою навіть у разі повної недоступності RADIUS-серверів. Найпростішим підходом є включення методу local як другого або третього в списку методів автентифікації, що дозволяє системі автоматично перемикатися на локальну базу користувачів у разі проблем з мережею або сервером. Для цього необхідно створити принаймні один локальний обліковий запис з високим рівнем привілеїв командою username, наприклад username admin privilege 15 secret strong_password, де рівень привілеїв 15 надає повний адміністративний доступ до всіх команд конфігурації. Альтернативним підходом є збереження консольного доступу поза системою AAA шляхом використання команди login local безпосередньо на консольній лінії без застосування AAA-списків, що гарантує можливість локального відновлення конфігурації навіть при катастрофічних збоях централізованої системи. Проте цей підхід знижує рівень централізації та ускладнює аудит, тому має використовуватися виключно як механізм надзвичайного відновлення.

Компонент авторизації моделі AAA відповідає за контроль дій користувача після успішної автентифікації, визначаючи, які саме команди та ресурси доступні конкретному користувачу на основі його ролі та налаштованих політик безпеки. На обладнанні Cisco авторизація налаштовується окремо для різних типів сервісів командою aaa authorization, яка приймає параметри типу сервісу (exec для виконавчого режиму, commands для окремих команд, network для мережевих сервісів) та списку методів авторизації аналогічно до автентифікації. Найпоширенішою конфігурацією є команда aaa authorization exec default group radius if-authenticated, яка делегує визначення привілеїв виконавчого режиму RADIUS-серверу, використовуючи локальні налаштування як резерв через метод if-authenticated. Метод if-authenticated є спеціальним методом авторизації, який автоматично надає доступ користувачам, що успішно пройшли автентифікацію, навіть якщо сервер не надіслав явних атрибутів авторизації, що забезпечує працездатність системи при базовій конфігурації RADIUS-сервера. Для детального контролю доступу

до окремих команд можна використовувати команду aaa authorization commands з вказанням рівня привілеїв, наприклад aaa authorization commands 15 default group radius local для авторизації команд рівня 15 через RADIUS з локальним резервом.

Компонент обліку (Accounting) забезпечує детальну реєстрацію всіх подій, пов’язаних з доступом користувачів до мережевого обладнання, включаючи час початку та завершення сесій, виконані команди, обсяг переданих даних та результати операцій. Облік налаштовується командою aaa accounting, яка визначає тип подій для реєстрації (exec для сесій командного рядка, commands для окремих команд, connection для вихідних з’єднань, network для мережевих сесій) та методи передачі інформації на сервер. Типова конфігурація aaa accounting exec default start-stop group radius реєструє початок та завершення кожної виконавчої сесії на RADIUS-сервері, передаючи інформацію через Accounting-Request повідомлення. Параметр start-stop вказує, що сервер отримає повідомлення як на початку сесії, так і після її завершення, що дозволяє точно розрахувати тривалість підключення та відстежувати активні сесії в реальному часі. Альтернативним параметром є stop-only, який надсилає інформацію тільки після завершення сесії, знижуючи навантаження на мережу та сервер за рахунок втрати можливості моніторингу активних підключень. Важливо розуміти, що повна функціональність обліку вимагає відповідної підтримки з боку RADIUS-сервера, зокрема наявності бази даних для зберігання записів та механізмів їх обробки, що може бути обмежено в навчальних середовищах на кшталт Cisco Packet Tracer.

1.4 Практичні аспекти налагодження та верифікації

Процес налагодження централізованої автентифікації вимагає систематичного підходу до перевірки кожного етапу взаємодії між компонентами системи, починаючи від базової мережевої зв’язності та закінчуючи детальним аналізом обміну RADIUS-повідомленнями. Першим кроком завжди має бути перевірка IP-зв’язку між мережевим пристроєм та RADIUS-сервером за допомогою команди ping з консолі пристрою, оскільки будь-які проблеми на мережевому рівні унеможливлюють коректну роботу протоколу. Успішний результат команди ping з показниками 100% доставки пакетів та мінімальними затримками підтверджує працездатність фізичної інфраструктури, правильність адресації та наявність маршрутів між пристроями. У разі проблем зі зв’язком необхідно послідовно перевірити стан інтерфейсів командою show ip interface brief, правильність налаштування IP-адрес, масок підмережі та шлюзів за замовчуванням, а також відсутність блокуючих правил на проміжних міжмережевих екранах або списках доступу. Після підтвердження мережевої зв’язності наступним етапом є верифікація конфігурації RADIUS-сервера, зокрема перевірка активності сервісу, правильності налаштування параметрів клієнтів (IP-адреса та секретний ключ мають точно збігатися з конфігурацією на мережевому пристрої) та наявності облікових записів користувачів у базі даних сервера.

Для детального аналізу процесу автентифікації на обладнанні Cisco використовується механізм відлагодження, який дозволяє спостерігати за внутрішніми операціями системи в реальному часі через консольне підключення або термінальну сесію. Команда debug radius активує виведення детальних повідомлень про всі етапи взаємодії з RADIUS-сервером, включаючи формування запитів, передачу повідомлень, отримання відповідей та інтерпретацію результатів. У виводі команди відображаються ключові параметри кожної транзакції: IP-адреса та порт сервера, унікальний ідентифікатор запиту, довжина повідомлення, перелік переданих атрибутів та отриманий результат автентифікації. Типовий успішний обмін виглядає як послідовність рядків “Send to server_ip:1645” з переліком атрибутів User-Name, User-Password, NAS-IP-Address, після чого йде рядок “Received from server_ip:1645” з результатом Authentication successful або Authentication failed. Аналіз цього виводу дозволяє ідентифікувати конкретне місце збою: якщо повідомлення надіслано, але відповідь не отримана, проблема полягає в мережевій зв’язності або недоступності сервера; якщо отримано Access-Reject, причина в неправильних облікових даних або конфігурації сервера; якщо виникає помилка перевірки секретного ключа, необхідно синхронізувати налаштування ключів на обох сторонах.

У таблиці 12.3 наведено основні команди діагностики та моніторингу стану системи AAA на обладнанні Cisco.

Таблиця 12.3 – Команди верифікації та діагностики системи AAA

Команда	Призначення та інформація у виводі
show aaa servers	Відображає стан усіх налаштованих AAA-серверів, включаючи IP-адреси, порти, поточний статус (UP/DOWN), статистику запитів (успішних та невдалих), час останньої відповіді та кількість таймаутів. Дозволяє оперативно виявити проблеми зі зв’язком із серверами.
show aaa sessions	Показує інформацію про всі активні AAA-сесії на пристрої, включаючи ідентифікатор сесії, ім’я користувача, IP-адресу джерела підключення та тривалість сесії. Корисно для моніторингу активних підключень та виявлення несанкціонованого доступу.
show users	Відображає список усіх користувачів, підключених до пристрою через будь-які інтерфейси (консоль, vty, aux), з інформацією про тип лінії, ім’я користувача, час бездіяльності та IP-адресу джерела. Дозволяє контролювати поточні сесії управління.
debug radius	Активує детальне виведення інформації про всі RADIUS-транзакції, включаючи відправлені та отримані повідомлення, атрибути, результати автентифікації. Критично важливо для налагодження проблем інтеграції з RADIUS-сервером.
debug aaa authentication	Виводить детальну інформацію про процес автентифікації на пристрої, включаючи застосування списків методів, спроби використання різних методів, результати перевірки облікових даних. Допомагає діагностувати проблеми з конфігурацією AAA-політик.
debug aaa authorization	Показує процес авторизації користувачів після успішної автентифікації, включаючи отримані атрибути авторизації від серверів, застосування локальних політик та остаточне рішення про надання привілеїв.
test aaa group	Дозволяє протестувати RADIUS-автентифікацію без реального

radius {username} {password} new-code	підключення користувача, надсилаючи тестовий запит на сервер з вказаними обліковими даними. Корисно для перевірки працездатності системи без ризику блокування доступу.

Розв’язання типових проблем централізованої автентифікації вимагає розуміння найпоширеніших сценаріїв збоїв та систематичного підходу до їх усунення. Найчастішою проблемою є невідповідність спільного секретного ключа між мережевим пристроєм та RADIUS-сервером, що призводить до відхилення всіх запитів навіть при правильних облікових даних користувачів, оскільки сервер не може перевірити цілісність повідомлень та дешифрувати пароль. Симптомами цієї проблеми є систематичне отримання Access-Reject від сервера або взагалі відсутність відповідей при активному debug radius. Вирішення полягає в ретельній перевірці налаштувань ключа на обох сторонах з увагою до регістру символів, наявності пробілів та спеціальних символів, після чого необхідно видалити та повторно створити конфігурацію сервера для гарантованого застосування змін. Другою поширеною проблемою є блокування власного доступу адміністратора через некоректну конфігурацію AAA без налаштованих резервних методів, що вимагає фізичного доступу до пристрою для виконання процедури відновлення паролів або використання консольного підключення з локальною автентифікацією.

Проблеми з мережевою зв’язністю між RADIUS-клієнтом та сервером можуть виникати через неправильну конфігурацію мережевих параметрів, наявність міжмережевих екранів або списків доступу, що блокують UDP-трафік на портах 1812-1813 або 1645-1646, а також через проблеми з маршрутизацією в складних топологіях. Діагностика цих проблем починається з команди ping для підтвердження базової IP-зв’язності, після чого виконується аналіз маршрутів командою show ip route для перевірки наявності шляху до мережі сервера. Якщо ping проходить успішно, але RADIUS-запити не досягають сервера, необхідно перевірити списки доступу на всіх проміжних пристроях командою show access-lists та за потреби додати правила дозволу для UDP-портів RADIUS. У середовищі з трансляцією мережевих адрес необхідно переконатися, що RADIUS-сервер коректно ідентифікує IP-адресу пристрою після трансляції та ця адреса зареєстрована в базі клієнтів на сервері. Особливу увагу слід приділити налаштуванням міжмережевих екранів, оскільки деякі з них можуть блокувати UDP-трафік за замовчуванням або встановлювати агресивні таймаути для UDP-сесій, що призводить до втрати RADIUS-відповідей.

Моніторинг та аналіз логів системи AAA є критично важливим для забезпечення безпеки та виявлення потенційних інцидентів безпеки, таких як спроби підбору паролів або несанкціонованого доступу. На RADIUS-сервері необхідно активувати детальне логування всіх спроб автентифікації з фіксацією імені користувача, IP-адреси пристрою, часу події та результату перевірки. Регулярний аналіз цих логів дозволяє виявити підозрілу активність, зокрема множинні невдалі спроби входу з одного джерела, спроби використання неіснуючих облікових записів або підключення з нетипових локацій. На

мережевих пристроях рекомендується налаштувати передачу системних повідомлень на централізований syslog-сервер командою logging host, що забезпечує збереження інформації про всі події доступу навіть у разі компрометації або перезавантаження пристрою. Додатково корисно налаштувати оповіщення адміністратора про критичні події, такі як множинні невдалі спроби автентифікації або зміни конфігурації безпеки, що дозволяє оперативно реагувати на потенційні інциденти до їх ескалації.

2 КЛЮЧОВІ ПИТАННЯ

1. Що означають три компоненти моделі AAA та яку конкретну функцію виконує кожен з них у процесі управління доступом до мережевого обладнання?
2. Чому у середовищі Packet Tracer для RADIUS-автентифікації використовується порт 1645 замість стандартного промислового порту 1812, і як ця особливість впливає на конфігурацію маршрутизатора?
3. Як реалізується захист пароля користувача в протоколі RADIUS згідно зі специфікацією RFC 2865, і яку роль відіграє спільний секретний ключ у цьому механізмі?
4. Чому консольний доступ до маршрутизатора (лінія 0) має налаштовуватися виключно через локальну автентифікацію (login local), а не через централізований RADIUS-сервер?
5. Яка різниця між отриманням відповіді *Access-Reject* від RADIUS-сервера та повною недоступністю сервера, і як маршрутизатор поводиться в кожному з цих випадків при налаштуванні group radius local?
6. Які три ключові атрибути обов'язково передаються у повідомленні *Access-Request* від маршрутизатора до RADIUS-сервера, і яке призначення має кожен з них?
7. Які дві основні команди використовуються для верифікації стану зв'язку з RADIUS-сервером після завершення конфігурації, і яку інформацію надає кожна з них адміністратору?
8. Що відображається у виводі команди debug radius під час успішної автентифікації, і як за цим виводом можна визначити, що проблема полягає саме в неправильному секретному ключі?
9. Чому в лабораторній роботі для тестування використовується протокол Telnet замість більш безпечного SSH, і як це спрощення впливає на навчальну цінність роботи?
10. Які два обов'язкові елементи необхідно налаштувати на RADIUS-сервері у Packet Tracer (окрім активування сервісу), щоб маршрутизатор міг успішно взаємодіяти з ним для автентифікації користувачів?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1 Архітектура мережі та параметри налаштування пристроїв

Для моделювання механізму централізованої автентифікації використовується спрощена топологія, що включає чотири ключові компоненти: клієнтську станцію для тестування віддаленого доступу, комутатор шару 2 для організації локального сегменту, маршрутизатор як об’єкт управління, та спеціалізований сервер типу AAA/RADIUS Server, який виступає централізованою точкою верифікації облікових даних. Всі пристрої розміщені в єдиній IPv4-мережі 192.168.1.0/24 для мінімізації складності маршрутизації та концентрації уваги на механізмах безпеки. Маршрутизатор виступає шлюзом за замовчуванням для клієнта та сервера, забезпечуючи міжмережеву взаємодію на рівні 3. Для забезпечення цілісності обміну між маршрутизатором і RADIUS-сервером використовується спільний секретний ключ radius_key, який застосовується для захисту атрибуту User-Password у RADIUS-повідомленнях згідно зі специфікацією протоколу (RFC 2865). Така архітектура відображає реальну практику організації безпечного управління мережевою інфраструктурою в організаціях середнього масштабу, де адміністративний доступ до всіх пристроїв контролюється єдиним сервером політик.

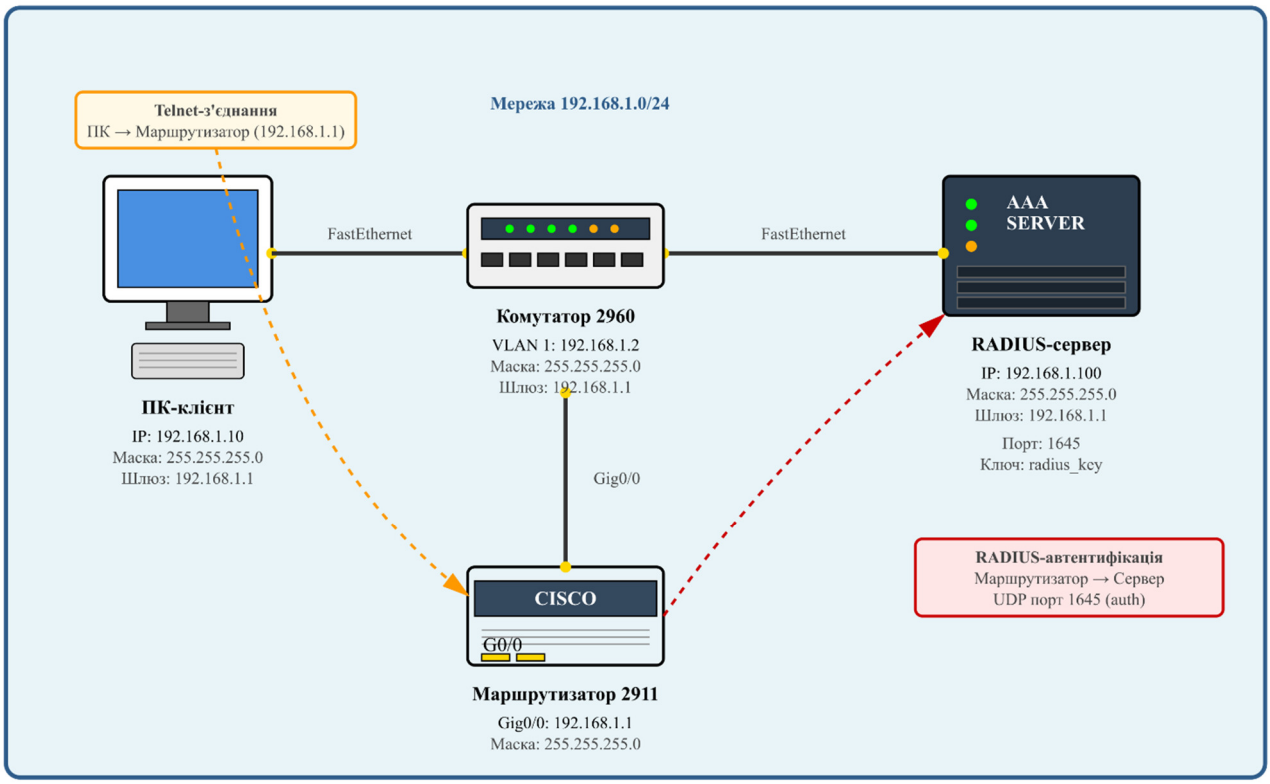

Рисунок 12.2 – Архітектура мережі

Таблиця 12.4 – Параметри конфігурації пристроїв мережі

Пристрій	Тип пристрою (Packet Tracer)	Інтерфейс	IP-адреса (Шлюз за замовч.)	Додаткові параметри
ПК-клієнт	PC	FastEthernet0	192.168.1.10 (192.168.1.1)	Telnet-клієнт активовано
Комутатор	2960	VLAN 1 (management)	192.168.1.2 (192.168.1.1)	Базова конфігурація управління
Маршрутизатор	2911	Gig0/0	192.168.1.1	AAA/RADIUS інтеграція, Telnet-доступ
RADIUS-сервер	AAA/ RADIUS Server	FastEthernet0	192.168.1.100 (192.168.1.1)	Порт 1645, ключ radius_key, 2 користувачі

Для виконання лабораторної роботи кожному студенту необхідно обрати варіант згідно зі своїм порядковим номером у журналі групи та використати наведені в таблиці параметри для налаштування мережі. Варіанти відрізняються ключовими параметрами безпеки — секретним ключем для захисту обміну між маршрутизатором і сервером, а також обліковими даними користувачів, що запобігає копіюванню конфігурацій між студентами та формує індивідуальні навички роботи з механізмами автентифікації. При виконанні завдання слід зберегти базову топологію мережі (192.168.1.0/24) та типи пристроїв згідно з основним завданням, але замінити всі параметри безпеки відповідно до обраного варіанту, зокрема: секретний ключ у конфігурації radius-server host, імена та паролі користувачів у секції User Setup RADIUS-сервера, ім’я локального резервного користувача на маршрутизаторі, а також ім’я пристрою командою hostname. Після завершення налаштувань обов’язково перевірити роботу системи шляхом тестування автентифікації обох користувачів через Telnet з ПК-клієнта та фіксувати результати у звіті з вказівкою номера виконаного варіанту.

Таблиця 12.5 – Варіанти індивідуальних завдань

№ варіанту	Секретний ключ	Адміністратор (логін / пароль)	Користувач (логін / пароль)	Ім’я маршрутизатора
1	net1	adm1 / adm@1234	usr1 / usr#5678	R1
2	key2	adm2 / adm@2345	usr2 / usr#6789	R2
3	sec3	adm3 / adm@3456	usr3 / usr#7890	R3
4	rad4	adm4 / adm@4567	usr4 / usr#8901	R4
5	aaa5	adm5 / adm@5678	usr5 / usr#9012	R5
6	cisco6	adm6 / adm@6789	usr6 / usr#0123	R6
7	pt7	adm7 / adm@7890	usr7 / usr#1234	R7
8	lab8	adm8 / adm@8901	usr8 / usr#2345	R8
9	net9	adm9 / adm@9012	usr9 / usr#3456	R9
10	key10	adm10 / adm@0123	usr10 / usr#4567	R10
11	sec11	sup1 / sup@1234	gst1 / gst#5678	RT1
12	rad12	sup2 / sup@2345	gst2 / gst#6789	RT2
13	aaa13	sup3 / sup@3456	gst3 / gst#7890	RT3

14	cisco14	sup4 / sup@4567	gst4 / gst#8901	RT4
15	pt15	sup5 / sup@5678	gst5 / gst#9012	RT5
16	lab16	sup6 / sup@6789	gst6 / gst#0123	RT6
17	net17	sup7 / sup@7890	gst7 / gst#1234	RT7
18	key18	sup8 / sup@8901	gst8 / gst#2345	RT8
19	sec19	sup9 / sup@9012	gst9 / gst#3456	RT9
20	rad20	sup10 / sup@0123	gst10 / gst#4567	RT10
21	aaa21	rt1 / rt@1234	std1 / std#5678	GW1
22	cisco22	rt2 / rt@2345	std2 / std#6789	GW2
23	pt23	rt3 / rt@3456	std3 / std#7890	GW3
24	lab24	rt4 / rt@4567	std4 / std#8901	GW4
25	net25	rt5 / rt@5678	std5 / std#9012	GW5
26	key26	rt6 / rt@6789	std6 / std#0123	GW6
27	sec27	rt7 / rt@7890	std7 / std#1234	GW7
28	rad28	rt8 / rt@8901	std8 / std#2345	GW8
29	aaa29	rt9 / rt@9012	std9 / std#3456	GW9
30	cisco30	rt10 / rt@0123	std10 / std#4567	GW10

3.2 Початкова ініціалізація пристроїв мережі

3.2.1 Побудова фізичної топології та базова адресація. Перед активацією механізмів безпеки необхідно забезпечити базову працездатність мережі на рівні 2 та 3, оскільки протокол RADIUS функціонує поверх транспортного рівня (UDP) і вимагає безперебійного IP-зв’язку між маршрутизатором і сервером. На цьому етапі виконується повна ініціалізація всіх пристроїв мережі з нуля, включаючи розміщення обладнання у середовищі Packet Tracer, фізичне з’єднання кабелями, налаштування інтерфейсів та перевірку зв’язності. Цей підхід гарантує, що студенти зможуть відтворити топологію повністю самостійно, не звертаючись до додаткових джерел для базових налаштувань.

3.2.2 Розміщення пристроїв та фізичне з’єднання. Розмістіть у робочій області Packet Tracer чотири пристрої: ПК (з категорії End Devices), комутатор 2960 (з категорії Switches), маршрутизатор 2911 (з категорії Routers) та сервер типу AAA/RADIUS Server (з категорії End Devices → Servers). З’єднайте пристрої кабелями типу Copper Straight-Through: ПК (порт FastEthernet0) → комутатор (порт FastEthernet0/1), комутатор (порт FastEthernet0/2) → маршрутизатор (порт GigabitEthernet0/0), комутатор (порт FastEthernet0/3) → сервер (порт FastEthernet0). Після з’єднання всі інтерфейси повинні відображати зелений індикатор стану, що свідчить про встановлення фізичного зв’язку на рівні 1.

3.2.3 Налаштування маршрутизатора 2911. Виконайте наступну послідовність команд для базової конфігурації маршрутизатора, включаючи присвоєння імені, активацію інтерфейсу управління, налаштування параметрів консолі та збереження конфігурації:

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# no ip domain-lookup
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# transport input telnet
R1(config-line)# exit
R1(config)# end
R1# copy running-config startup-config
```

Аналізуючи виконані команди, можна виділити кілька ключових етапів: присвоєння імені пристрою (hostname R1) полегшує ідентифікацію в мережі під час налагодження; активація інтерфейсу Gig0/0 з присвоєнням IP-адреси 192.168.1.1/24 створює точку маршрутизації для всієї мережі; команда no ip domain-lookup вимикає автоматичний DNS-пошук при помилковому введенні команд, що прискорює роботу з консоллю; налаштування logging synchronous запобігає перериванню введення команд системними повідомленнями; попереднє визначення transport input telnet на лініях VTY спрощує подальшу конфігурацію віддаленого доступу. Збереження конфігурації командою copy running-config startup-config гарантує збереження налаштувань після перезавантаження пристрою.

3.2.4 Налаштування комутатора 2960. Для забезпечення управління комутатором через мережу необхідно налаштувати IP-адресу на інтерфейсі управління VLAN 1 та вказати шлюз за замовчуванням:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# ip default-gateway 192.168.1.1
SW1(config)# no ip domain-lookup
SW1(config)# line console 0
SW1(config-line)# logging synchronous
SW1(config-line)# exit
SW1(config)# end
SW1# copy running-config startup-config
```

Аналізуючи конфігурацію комутатора, слід зазначити, що інтерфейс vlan 1 є віртуальним інтерфейсом управління для комутаторів шару 2, який дозволяє віддалений доступ до пристрою через мережу; команда ip default-gateway 192.168.1.1 визначає шлюз за замовчуванням, необхідний для маршрутизації трафіку поза локальну підмережу (хоча в даній лабораторній роботі всі пристрої знаходяться в одній підмережі, це налаштування є гарною практикою); решта команд аналогічні до налаштувань маршрутизатора і забезпечують зручність роботи з консоллю та збереження конфігурації.

3.2.5 Налаштування ПК-клієнта та RADIUS-сервера. Налаштуйте ПК-клієнт: клацніть двічі на ПК → вкладка Desktop → IP Configuration → встановіть Static IP: IP Address 192.168.1.10, Subnet Mask 255.255.255.0, Default Gateway 192.168.1.1. Для RADIUS-сервера: клацніть двічі на сервер → вкладка Config → INTERFACE → FastEthernet0 → встановіть IP Address 192.168.1.100, Subnet Mask 255.255.255.0, Default Gateway 192.168.1.1. На цьому етапі сервіс RADIUS ще не активований — це буде зроблено пізніше після підтвердження базової зв’язності.

3.2.6 Перевірка базової зв’язності. Після завершення фізичного з’єднання та адресації обов’язково перевірте зв’язність між усіма пристроями за допомогою команди ping:

```
R1# ping 192.168.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1
ms

R1# 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 = 1/1/1
ms
```

Аналізуючи результати перевірки зв’язку, можна констатувати успішну ініціалізацію мережевого рівня: п’ять пакетів ICMP Echo Request були надіслані між усіма парами пристроїв, і на кожен отримано підтвердження Echo Reply (символи !!!!!), що свідчить про відсутність проблем з фізичним з’єднанням, коректну роботу комутатора на рівні 2, правильну адресацію інтерфейсів та наявність маршруту за замовчуванням. Середній час затримки 1 мс вказує на локальний характер мережі без проміжних маршрутизаторів. Цей етап є критично важливим — будь-яка помилка на ньому (неправильна маска, відсутній шлюз, неактивний інтерфейс) призведе до невдачі на етапі інтеграції з

RADIUS-сервером, оскільки запити автентифікації просто не досягнуть сервера.

3.3 Налаштування механізмів централізованої автентифікації

3.3.1 Конфігурація RADIUS-сервера. Конфігурація сервера є фундаментом усієї системи AAA, оскільки саме він зберігає облікові дані користувачів та приймає рішення щодо їхньої автентичності. У середовищі Packet Tracer для цього використовується спеціалізований пристрій AAA/RADIUS Server, який імітує поведінку промислових рішень на кшталт Cisco ISE або відкритого сервера FreeRADIUS. Налаштування починається з активації сервісу RADIUS на вкладці SERVICES → AAA, де необхідно встановити перемикач у положення On. Важливо зазначити, що у Packet Tracer використовується порт 1645 замість стандартного 1812 для RADIUS (як видно на інтерфейсі сервера). Далі в секції Network Configuration додається маршрутизатор як клієнт RADIUS-сервера, де необхідно вказати його ім’я R1, IP-адресу 192.168.1.1 та секретний ключ radius_key, який має точно збігатися з ключем, налаштованим на маршрутизаторі. У секції User Setup створюються два тестових облікових записів: admin з паролем cisco123 (для моделювання адміністратора) та student з паролем lab456 (для моделювання звичайного користувача). Кожен запис має тип RADIUS, що вказує на належність до бази даних сервера. Після введення даних обов’язково натискається кнопка Save, оскільки без збереження конфігурація не активується навіть при видимому наявності записів у інтерфейсі.

```
Параметри сервера (візуальна перевірка у ПТ):
- Статус сервісу: [On]
- Radius Port: 1645
- Network Configuration:
    ✓ Client Name: R1
    ✓ Client IP: 192.168.1.1
    ✓ Key: radius_key
- User Setup:
    ✓ admin / cisco123
    ✓ student / lab456
```

Аналізуючи стан сервера після збереження, слід звернути увагу на індикатор статусу сервісу — зелений маркер підтверджує готовність приймати запити на порту 1645. Наявність двох користувачів у списку User Setup гарантує можливість тестування як успішної, так і неуспішної автентифікації. Критично важливою є перевірка точності секретного ключа та використання порту 1645 замість 1812, оскільки будь-яка розбіжність (наприклад, додатковий пробіл або регістр літер) призведе до відхилення всіх запитів, оскільки сервер і маршрутизатор не зможуть перевірити цілісність атрибуту User-Password. У реальних умовах такий ключ генерується як довільний рядок з високою

ентропією, але для навчальних цілей використовується простий ключ для зручності налагодження.

3.3.2. Активація моделі AAA на маршрутизаторі. Активація глобальної моделі AAA є обов'язковим першим кроком перед будь-якими налаштуваннями автентифікації, оскільки без цієї команди решта параметрів ігноруються операційною системою Cisco IOS. Команда aaa new-model перемикає маршрутизатор у режим, де всі методи автентифікації, авторизації та обліку керуються централізовано через групи серверів, а не через локальні механізми. Після активації моделі налаштовується зв'язок із зовнішнім сервером за допомогою команди radius-server host, яка визначає IP-адресу сервера, порт автентифікації (1645) та спільний секретний ключ. Для забезпечення відмовостійкості системи рекомендується додатково налаштувати локального користувача backup з високим рівнем привілеїв (15), який дозволить отримати доступ до пристрою в разі тимчасової недоступності RADIUS-сервера — це критично важливо для уникнення ситуації "заблокованого" пристрою, коли адміністратор втрачає можливість управління через помилку в конфігурації або відмову сервера.

```
R1> enable
R1# configure terminal
R1(config)# aaa new-model
R1(config)# radius-server host 192.168.1.100 auth-port 1645 key
radius_key
R1(config)# username backup privilege 15 secret emergency_access
R1(config)# aaa authentication login default group radius local
R1(config)# line vty 0 4
R1(config-line)# login authentication default
R1(config-line)# exit
R1(config)# end
```

Аналізуючи вивід команд, слід зазначити, що після виконання aaa new-model маршрутизатор не виводить підтвердження — успішність операції перевіряється командою show aaa servers, яка має відобразити статус сервера UP. Команда aaa authentication login default group radius local встановлює послідовність методів: спочатку пробується група серверів RADIUS, а при її недоступності — локальна база (користувач backup). Це забезпечує баланс між безпекою (перевага централізованої автентифікації) та надійністю (резервний механізм доступу). Налаштування login authentication default на лініях VTY застосовує стандартний список методів до віддалених з'єднань, що дозволяє використовувати централізовану автентифікацію для всіх вхідних підключень через віртуальні термінали.

3.3.3. Захист консольного доступу та резервний механізм. Для запобігання повної втрати доступу до пристрою в разі помилки в конфігурації або відмови мережі, консольний інтерфейс (лінія 0) налаштовується виключно з

використанням локальної бази користувачів, без залучення зовнішнього RADIUS-сервера. Це гарантує, що навіть при повній ізоляції маршрутизатора від мережі (наприклад, через помилку в кабелі або відключення комутатора) адміністратор зможе підключитися напряму через консольний порт і виправити конфігурацію. Такий підхід є стандартом безпеки в промисловій практиці — централізована автентифікація застосовується лише для віддалених методів доступу (Telnet, SSH), тоді як локальний фізичний доступ залишається під контролем локальних механізмів. Крім того, налаштовується пароль привілеїв enable для захисту переходу в привілейований режим, що додає додатковий рівень безпеки навіть після успішної автентифікації користувача.

```
R1# configure terminal
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# enable secret cisco_enable
R1(config)# service password-encryption
R1(config)# end
```

Аналізуючи цю частину конфігурації, варто підкреслити стратегічну важливість резервного механізму: метод login local для консолі гарантує, що доступ до пристрою залишається можливим навіть при повній відмові мережі або помилці в налаштуваннях RADIUS. Це критично важливо для навчальних лабораторних робіт, де студенти можуть допустити помилки в конфігурації. Команда enable secret шифрує пароль привілеїв за допомогою алгоритму MD5 (на відміну від небезпечного enable password, який зберігає пароль у відкритому вигляді), а service password-encryption додає базове шифрування для всіх інших паролів у конфігурації (хоча це шифрування є слабким і легко зламується, воно запобігає випадковому перегляду паролів при візуальному огляді конфігурації).

3.4 Перевірка роботи механізму централізованої автентифікації

3.4.1 Тестування віддаленого доступу через Telnet. Перевірка функціональності системи виконується шляхом моделювання реального сценарію адміністративного доступу: з клієнтської станції ініціюється Telnet-з’єднання з маршрутизатором, після чого система запитує облікові дані та делегує їхню перевірку RADIUS-серверу. Для повноцінного тестування виконуються три сценарії: успішна автентифікація користувача admin, неуспішна спроба з неправильним паролем, та успішна автентифікація обмеженого користувача student. Кожен сценарій дозволяє перевірити різні аспекти роботи системи — коректність обміну даними з сервером, обробку помилок, та механізм резервування через локальну базу. Для глибшого аналізу активується режим відлагодження debug radius на маршрутизаторі, який відображає деталі кожного запиту та відповіді між пристроями.

Сценарій 1. Успішна автентифікація (ПК → маршрутизатор):

```
C:\> telnet 192.168.1.1
Trying 192.168.1.1 ... Open
User Access Verification
Username: admin
Password: ********
R1>
```

Сценарій 2. Аналіз відлагоджувальних повідомлень (маршрутизатор):

```
R1# debug radius
RADIUS: Initialising radius library
RADIUS: Send to 192.168.1.100:1645, id 5, length 78
RADIUS: User-Name = "admin"
RADIUS: User-Password = 16 bytes
RADIUS: NAS-IP-Address = 192.168.1.1
RADIUS: Received from 192.168.1.100:1645, id 5, length 20
RADIUS: Authentication successful
R1# undebug all
```

Аналізуючи результати тестування, можна зробити кілька ключових висновків. У Сценарії 1 після введення правильних облікових даних користувач отримує доступ до користувацького режиму маршрутизатора (R1>), що підтверджує успішну інтеграцію з сервером. У Сценарії 2 відлагоджувальні повідомлення детально відображають процес обміну: маршрутизатор формує запит із захищеним атрибутом User-Password (16 байт), надсилає його на сервер, який після перевірки бази даних повертає позитивну відповідь Authentication successful. Критично важливим є аналіз помилкових сценаріїв — при неправильному паролі сервер повертає код відмови, а маршрутизатор відображає повідомлення % Authentication failed, не надаючи додаткової інформації про причину відмови (що є елементом безпеки проти перебору паролів). Для перевірки резервного механізму можна тимчасово вимкнути сервер у ПТ та спробувати підключитися з обліковими даними backup / emergency_access — система автоматично перейде до локальної автентифікації через метод local у послідовності group radius local.

3.4.2. Верифікація стану сервісів. Остаточна перевірка включає аналіз стану сервісів за допомогою команд show aaa servers та show users, які надають інформацію про доступність сервера та активні сесії відповідно. Команда show aaa servers відображає статус кожного налаштованого сервера (UP/DOWN), кількість успішних/невдалих запитів, та час останньої відповіді — це дозволяє оперативно виявити проблеми зі зв’язком із сервером. Команда show users відображає всі активні термінальні сесії, включаючи ім’я користувача, тип лінії (VTY), IP-джерело підключення, та час бездіяльності.

```
R1# show aaa servers
RADIUS: id 1, priority 1, host 192.168.1.100, auth-port 1645,
acct-port 1646
     State: UP
     Response Timeouts: 0
     Retransmits: 0
     Transaction ID: 0x4A3B2C1D

R1# show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
   2 vty 0    admin      idle                 00:02:15
192.168.1.10
```

Аналізуючи вивід команди show aaa servers, можна констатувати, що сервер знаходиться в стані UP з нульовою кількістю повторних спроб (Retransmits: 0) та таймаутів (Response Timeouts: 0), що свідчить про стабільний зв’язок без переривань. У виводі show users видно активну сесію користувача admin на лінії vty 0 з джерелом 192.168.1.10, що точно відповідає IP-адресі клієнтської станції — це підтверджує успішну ідентифікацію користувача та прив’язку сесії до реального джерела підключення. Зірочка (*) біля лінії con 0 позначає поточну консольну сесію, з якої виконуються команди, що дозволяє адміністратору одночасно керувати пристроєм локально та моніторити віддалені підключення.

У даній лабораторній роботі реалізується лише механізм автентифікації (Authentication) та базова авторизація (Authorization). Механізм обліку (Accounting) у повному обсязі (з фіксацією подій у зовнішній базі даних) вимагає додаткової конфігурації aaa accounting та підтримки сервером відповідних атрибутів. У середовищі Packet Tracer цей функціонал обмежений, тому в роботі розглядається лише теоретична основа компонента Accounting моделі AAA.

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 № 13

Тема: Побудова захищеного міжсайтового IPsec VPN

Мета роботи: Опанувати принципи побудови захищеного міжсайтового VPN-з'єднання на основі протоколу IPsec

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Загальні відомості про технологію IPsec VPN

Технологія IPsec (Internet Protocol Security) являє собою комплексний набір стандартів і протоколів, призначених для забезпечення конфіденційності, цілісності та автентичності даних під час їх передачі через незахищені публічні мережі, зокрема мережу Інтернет. На відміну від протоколів прикладного рівня, таких як SSL/TLS, які забезпечують захист окремих додатків, IPsec функціонує на мережевому рівні моделі OSI, що дозволяє створювати універсальні захищені канали для будь-яких типів трафіку незалежно від протоколів вищих рівнів. Головною перевагою IPsec є можливість побудови віртуальних приватних мереж (VPN), які логічно об'єднують географічно розподілені сегменти корпоративної інфраструктури через спільну публічну мережу, створюючи ілюзію прямого фізичного з'єднання. У контексті даної лабораторної роботи розглядається архітектура site-to-site VPN, яка забезпечує постійне шифроване з'єднання між двома локальними мережами через спеціально налаштовані пограничні маршрутизатори.

Архітектура site-to-site IPsec VPN передбачає використання двох основних компонентів: пограничних маршрутизаторів, які виконують функції VPN-шлюзів, та транзитної мережі, яка забезпечує фізичне з'єднання між ними. Кожен пограничний маршрутизатор має два мережеві інтерфейси з різними функціональними призначеннями. Внутрішній інтерфейс підключений до локальної мережі офісу і використовує приватну адресацію згідно зі стандартом RFC 1918, типово з діапазонів 192.168.0.0/16 або 10.0.0.0/8. Зовнішній інтерфейс, підключений до публічної мережі Інтернет, отримує глобально маршрутизовану IP-адресу, яка забезпечує досяжність між VPN-пірами. Транзитна мережа, представлена в лабораторній топології маршрутизатором R-INTERNET, виконує виключно функції маршрутизації пакетів між публічними інтерфейсами пограничних маршрутизаторів і не бере участі в криптографічних операціях. Такий підхід моделює реальну ситуацію, коли корпоративний трафік проходить через інфраструктуру інтернет-провайдера або магістральні мережі.

Принцип роботи IPsec базується на концепції криптографічного інкапсулювання, при якому оригінальний IP-пакет з приватними адресами джерела та призначення повністю або частково шифрується та вміщується всередину нового зовнішнього пакета з публічними адресами VPN-шлюзів. Існують два основні режими інкапсулювання: транспортний (transport mode) та тунельний (tunnel mode). У транспортному режимі шифрується лише корисне

навантаження оригінального пакета, тоді як заголовок IP залишається незмінним, що робить цей режим придатним лише для з'єднань типу “хост-хост”. Тунельний режим, який використовується в архітектурі site-to-site VPN, забезпечує повне інкапсулювання оригінального пакета разом із його IP-заголовком у новий зовнішній пакет. Зовнішній IP-заголовок містить адреси VPN-шлюзів як джерело та призначення, що дозволяє маршрутизаторам транзитної мережі обробляти такі пакети як звичайний IP-трафік, не маючи доступу до інформації про справжні адреси відправника та одержувача. Для кінцевих хостів усередині приватних мереж процес шифрування є повністю прозорим, оскільки криптографічні операції виконуються виключно на пограничних маршрутизаторах.

1.2 Структура протоколу IPsec та двофазовий механізм встановлення з'єднання

Протокольний стек IPsec складається з кількох взаємопов'язаних компонентів, кожен з яких виконує специфічні функції в процесі забезпечення безпеки. Центральними елементами є протокол автентифікації заголовка AH (Authentication Header) та протокол інкапсуляції корисного навантаження ESP (Encapsulating Security Payload). Протокол AH забезпечує автентифікацію джерела даних та перевірку цілісності пакетів, але не надає можливості шифрування. Його використання обмежене сценаріями, де конфіденційність не є критичною вимогою, але необхідно гарантувати, що дані не були модифіковані під час передачі. Протокол ESP, навпаки, забезпечує повний набір сервісів безпеки: шифрування корисного навантаження для конфіденційності, автентифікацію для підтвердження джерела та перевірку цілісності для виявлення модифікацій. У сучасних реалізаціях IPsec протокол ESP практично повністю витіснив AH завдяки своїй універсальності та можливості одночасного забезпечення всіх необхідних функцій безпеки. Комбінація алгоритмів шифрування та автентифікації, які використовуються протоколом ESP, визначається параметрами transform set.

Процес встановлення IPsec з'єднання реалізований у вигляді двофазового механізму, де кожна фаза вирішує специфічні завдання безпеки. Фаза 1, відома як IKE (Internet Key Exchange) або ISAKMP (Internet Security Association and Key Management Protocol), призначена для встановлення захищеного каналу управління між VPN-пірами. Цей канал використовується виключно для обміну службовою інформацією та узгодження параметрів фази 2, але не для передачі користувацького трафіку. Під час фази 1 піри автентифікують один одного, узгоджують криптографічні параметри для захисту службового каналу та генерують симетричні ключі шифрування за допомогою алгоритму Діффі-Геллмана. Протокол ISAKMP підтримує два режими роботи: основний режим (main mode) та агресивний режим (aggressive mode). Основний режим передбачає шість послідовних повідомлень між пірами, забезпечуючи максимальний рівень захисту ідентифікаційної інформації, оскільки ідентичність сторін передається в зашифрованому вигляді. Агресивний режим

скорочує процес до трьох повідомлень за рахунок зниження конфіденційності ідентифікаторів, але забезпечує швидше встановлення з'єднання.

Після успішного завершення фази 1 ініціюється фаза 2, також відома як швидкий режим (quick mode). Головним завданням фази 2 є створення асоціацій безпеки (Security Associations, SA) для захисту користувацького трафіку між приватними мережами. На відміну від фази 1, яка встановлює єдиний двосторонній захищений канал управління, фаза 2 створює однонаправлені SA окремо для кожного напрямку передачі даних. Кожна асоціація безпеки характеризується унікальним індексом параметрів безпеки (Security Parameter Index, SPI), який дозволяє отримувачу ідентифікувати набір криптографічних параметрів для декапсулювання та розшифрування вхідних пакетів. Механізм визначення “цікавого трафіку”, який повинен проходити через IPsec тунель, реалізується за допомогою розширених списків контролю доступу (Access Control Lists, ACL). Адміністратор створює ACL, що специфікує діапазони адрес джерела та призначення, для яких необхідне шифрування. Коли маршрутизатор отримує пакет, що відповідає умовам ACL, він автоматично ініціює процес встановлення тунелю фази 2, якщо асоціація безпеки ще не існує, або використовує існуючу SA для інкапсулювання та шифрування пакета.

Таблиця 13.1 систематизує основні параметри, які налаштовуються під час кожної з двох фаз протоколу IPsec, та пояснює їхнє призначення у контексті забезпечення безпеки VPN-з'єднання.

Таблиця 13.1 — Порівняння параметрів фази 1 та фази 2 протоколу IPsec

Параметр	Фаза 1 (IKE/ISAKMP)	Фаза 2 (Quick Mode)
Призначення	Створення захищеного каналу управління для узгодження параметрів фази 2	Створення асоціацій безпеки для захисту користувацького трафіку
Алгоритм шифрування	AES-128, AES-256, 3DES (для службових повідомлень)	ESP-AES, ESP-3DES (для користувацьких даних)
Хеш-функція	SHA-256, SHA-1, MD5 (для перевірки цілісності ISAKMP-повідомлень)	ESP-SHA-HMAC, ESP-MD5-HMAC (для автентифікації даних)
Група Діффі-Геллмана	Group 2 (1024 біт), Group 14 (2048 біт), Group 19 (256-bit ECC)	Опційно: PFS (Perfect Forward Secrecy) з додатковим DH-обміном
Метод автентифікації	Pre-shared key, цифрові сертифікати RSA, ECDSA	Успадковується від фази 1, додаткова автентифікація не потрібна
Час життя (lifetime)	Типово 86400 секунд (24 години), після чого канал перегенеровується	Типово 3600 секунд (1 година) або після передачі певного обсягу даних

Важливим аспектом безпеки є концепція ідеальної прямої секретності (Perfect Forward Secrecy, PFS), яка може бути активована під час фази 2. Механізм PFS передбачає виконання додаткового обміну за алгоритмом Діффі-Геллмана на етапі створення кожної нової асоціації безпеки фази 2. Це гарантує, що компрометація довготривалих ключів фази 1 не призведе до можливості розшифрування раніше перехопленого трафіку фази 2, оскільки кожна сесія використовує унікальні, незалежно згенеровані ключі. Хоча PFS вносить додаткове обчислювальне навантаження через необхідність виконання криптографічних операцій на основі складних математичних обчислень, його використання є рекомендованою практикою для критичних корпоративних застосувань. У лабораторній конфігурації параметр PFS активується командою set pfs group14 у контексті crypto map, що вказує на використання групи Діффі-Геллмана 14 з довжиною ключа 2048 біт для додаткового обміну під час встановлення фази 2.

1.3 Криптографічні алгоритми та механізми безпеки

Надійність IPsec VPN безпосередньо залежить від криптографічних алгоритмів, які використовуються для шифрування даних та забезпечення їхньої автентифікації. Алгоритм шифрування AES (Advanced Encryption Standard) є сучасним стандартом симетричного блокового шифрування, схваленим Національним інститутом стандартів та технологій США (NIST) у 2001 році. AES підтримує три варіанти довжини ключа: 128, 192 та 256 біт, де більша довжина ключа забезпечує вищий рівень криптографічної стійкості за рахунок збільшення обчислювальної складності злому методом повного перебору. Алгоритм працює з блоками даних розміром 128 біт і застосовує серію раундів підстановок та перестановок, кількість яких залежить від довжини ключа: 10 раундів для 128-бітного ключа, 12 раундів для 192-бітного та 14 раундів для 256-бітного. У контексті IPsec найчастіше використовується варіант AES-128, оскільки він забезпечує оптимальний баланс між рівнем безпеки та продуктивністю, а криптоаналітичні дослідження не виявили практично можливих атак навіть на цей найкоротший варіант ключа.

Паралельно з шифруванням IPsec використовує криптографічні хеш-функції для забезпечення цілісності даних та автентифікації відправника. Хеш-функція SHA-256 (Secure Hash Algorithm 256-bit) генерує унікальний 256-бітний відбиток (хеш) для довільного блоку даних, причому будь-яка навіть мінімальна зміна вхідних даних призводить до кардинально іншого значення хешу через властивість лавинного ефекту. Для реалізації механізму автентифікації повідомлень у протоколі IPsec використовується конструкція HMAC (Hash-based Message Authentication Code), яка комбінує хеш-функцію з секретним ключем. Під час відправлення пакета відправник обчислює HMAC на основі вмісту пакета та спільного секретного ключа, потім додає отриманий код автентифікації до пакета. Отримувач, маючи той самий секретний ключ, незалежно обчислює HMAC для отриманих даних і порівнює його з переданим значенням. Збіг підтверджує як автентичність джерела, так і відсутність

модифікацій під час передачі. Використання SHA-256 у складі HMAC надає захист від атак на основі колізій хеш-функцій, оскільки навіть теоретична можливість знайти два різні повідомлення з однаковим хешем не дозволяє зловмиснику підробити HMAC без знання секретного ключа.

Алгоритм Діффі-Геллмана (DH) є фундаментальним механізмом для безпечного встановлення спільного секретного ключа через незахищений канал зв'язку без попереднього обміну секретною інформацією. Математична основа алгоритму базується на складності обчислення дискретного логарифма в кінцевих полях або на еліптичних кривих. Група Діффі-Геллмана визначає математичну структуру та розмір простого числа або параметри еліптичної кривої, які використовуються під час обміну. Група 14, рекомендована в лабораторній роботі, використовує 2048-бітне просте число, що забезпечує криптографічну стійкість, порівнянну з 112-бітними симетричними ключами згідно з рекомендаціями NIST. Процес обміну DH відбувається публічно: кожна сторона генерує приватне випадкове число, обчислює відповідне публічне значення та передає його партнеру. На основі отриманого публічного значення партнера та власного приватного числа кожна сторона незалежно обчислює ідентичний спільний секрет. Навіть маючи доступ до обох публічних значень, зловмисник не може ефективно обчислити спільний секрет без знання принаймні одного з приватних чисел через обчислювальну складність задачі дискретного логарифмування.

Таблиця 13.2 наводить основні команди операційної системи Cisco IOS, які використовуються для конфігурації IPsec VPN на пограничних маршрутизаторах, разом із поясненням їхнього призначення та синтаксису.

Таблиця 13.2 — Основні команди конфігурації IPsec VPN у Cisco IOS

Команда	Призначення та опис
`crypto isakmp policy` *`priority`*	Створює політику ISAKMP фази 1 з вказаним пріоритетом (1-10000). При узгодженні з віддаленим піром використовується політика з найнижчим номером, параметри якої збігаються на обох сторонах.
`encryption {aes | 3des}`	Визначає алгоритм шифрування для захисту службового каналу ISAKMP. Опції: AES-128, AES-192, AES-256 або 3DES. У Packet Tracer підтримується лише базовий AES (128 біт).
`hash {sha256 | sha | md5}`	Вказує хеш-функцію для забезпечення цілісності ISAKMP-повідомлень. Рекомендується SHA-256 для нових інсталяцій. SHA-1 та MD5 вважаються застарілими через виявлені вразливості.
`authentication pre-share`	Встановлює метод автентифікації пірів через попередньо узгоджений ключ (pre-shared key). Альтернативними методами є цифрові сертифікати RSA або ECDSA.

`group {2 | 14 | 19 | ...}`	Визначає групу Діффі-Геллмана для обміну ключами. Group 2 (1024 біт) - мінімально прийнятна, Group 14 (2048 біт) - рекомендована, Group 19 (256-bit ECC) - для високої продуктивності.
`crypto isakmp key` *`key address peer-ip`*	Налаштовує попередньо узгоджений ключ для автентифікації конкретного віддаленого піра за його публічною IP-адресою. Ключ повинен бути ідентичним на обох маршрутизаторах.
`crypto ipsec transform-set` *`name transforms`*	Створює набір криптографічних перетворень для фази 2. Приклад: esp-aes esp-sha-hmac означає використання AES для шифрування та SHA-HMAC для автентифікації в рамках протоколу ESP.
`access-list` *`num permit ip src dst`*	Визначає “цікавий трафік” для шифрування. Використовується розширений ACL (100-199) з wildcard масками. Трафік, що відповідає умовам, автоматично ініціює створення IPsec тунелю.
`crypto map` *`name seq ipsec-isakmp`*	Створює crypto map запис з унікальним номером послідовності. Об'єднує всі параметри IPsec: піра, ACL, transform set. Може містити кілька записів для різних VPN-з'єднань.
`set peer` *`ip-address`*	Вказує публічну IP-адресу віддаленого VPN-шлюза, з яким встановлюється IPsec тунель. Використовується в контексті конфігурації crypto map.
`match address` *`acl-num`*	Прив'язує ACL до crypto map для визначення трафіку, який підлягає шифруванню. Номер ACL має відповідати раніше створеному розширеному списку доступу.
`set transform-set` *`name`*	Вказує, який transform set використовувати для шифрування та автентифікації трафіку фази 2. Назва повинна відповідати раніше створеному набору перетворень.
`set pfs group14`	Активує Perfect Forward Secrecy з групою DH 14 для додаткового обміну ключами під час фази 2. Забезпечує незалежність ключів сесій від ключів фази 1.
`crypto map` *`name`* (на інтерфейсі)	Прив'язує crypto map до зовнішнього інтерфейсу маршрутизатора. Критично важливо застосувати до WAN-інтерфейсу, а не LAN, оскільки перевірка ACL виконується на інтерфейсі з crypto map.

Діагностика стану IPsec VPN здійснюється за допомогою спеціалізованих команд show, які відображають поточний стан асоціацій безпеки, лічильники трафіку та параметри активних тунелів. Команда show crypto isakmp sa виводить інформацію про стан фази 1, включаючи адреси пірів, стан з'єднання

(QM_IDLE означає успішно встановлений канал управління) та ідентифікатори з'єднань. Команда show crypto ipsec sa надає детальну інформацію про асоціації безпеки фази 2: лічильники інкапсульованих та декапсульованих пакетів, використовувані криптографічні алгоритми, час життя поточної SA та SPI-індекси. Ненульові значення лічильників свідчать про активну передачу даних через тунель. Для глибшої діагностики проблем можна тимчасово активувати режим налагодження командами debug crypto isakmp та debug crypto ipsec, які виводять детальну інформацію про процес узгодження параметрів, обмін повідомленнями та причини можливих помилок. Після завершення діагностики налагодження необхідно вимкнути командою no debug all для уникнення надмірного навантаження на процесор маршрутизатора.

1.4 Топологія мережі та організація адресного простору

Топологія лабораторної роботи моделює типовий корпоративний сценарій з'єднання двох географічно віддалених офісів через публічну мережу Інтернет. Кожен офіс представлений окремим сегментом локальної мережі, що включає робочу станцію, комутатор другого рівня моделі Catalyst 2960 та пограничний маршрутизатор Cisco 2911, який виконує функції VPN-шлюза. Робоча станція підключається до комутатора за допомогою медного прямого кабелю (Copper Straight-Through), оскільки з'єднання відбувається між пристроями різних типів: кінцевий хост та комутатор. Комутатор, у свою чергу, з'єднується з внутрішнім інтерфейсом маршрутизатора також прямим кабелем, оскільки порти комутатора автоматично визначають тип з'єднання через механізм Auto-MDIX. Зовнішні інтерфейси обох пограничних маршрутизаторів підключені до центрального маршрутизатора R-INTERNET за допомогою кабелів Cross-Over, які необхідні для прямого з'єднання двох маршрутизаторів без проміжного комутаційного обладнання. Маршрутизатор R-INTERNET не бере участі в операціях IPsec і служить виключно для імітації транзитної мережі провайдера.

Рисунок 13.1 відображає повну топологію мережі з усіма пристроями та їхніми взаємозв'язками. У лівій частині схеми розташований Site A, який складається з персонального комп'ютера PC-A з IP-адресою 192.168.1.10/24, комутатора SW-A з адресою управління 192.168.1.2/24 у VLAN 1 та пограничного маршрутизатора R-A. Маршрутизатор R-A має два інтерфейси: внутрішній GigabitEthernet0/0 з адресою 192.168.1.1/24, який служить шлюзом за замовчуванням для локальної мережі, та зовнішній GigabitEthernet0/1 з публічною адресою 203.0.113.1/30. У правій частині схеми симетрично розташований Site B з комп'ютером PC-B (192.168.2.10/24), комутатором SW-B (192.168.2.2/24) та маршрутизатором R-B, внутрішній інтерфейс якого має адресу 192.168.2.1/24, а зовнішній — 198.51.100.2/30. У центрі схеми зображений маршрутизатор R-INTERNET у вигляді хмари, що символізує публічну мережу Інтернет. Цей маршрутизатор має два інтерфейси: GigabitEthernet0/0 з адресою 203.0.113.2/30 для з'єднання з Site A та GigabitEthernet0/1 з адресою 198.51.100.1/30 для з'єднання з Site B.

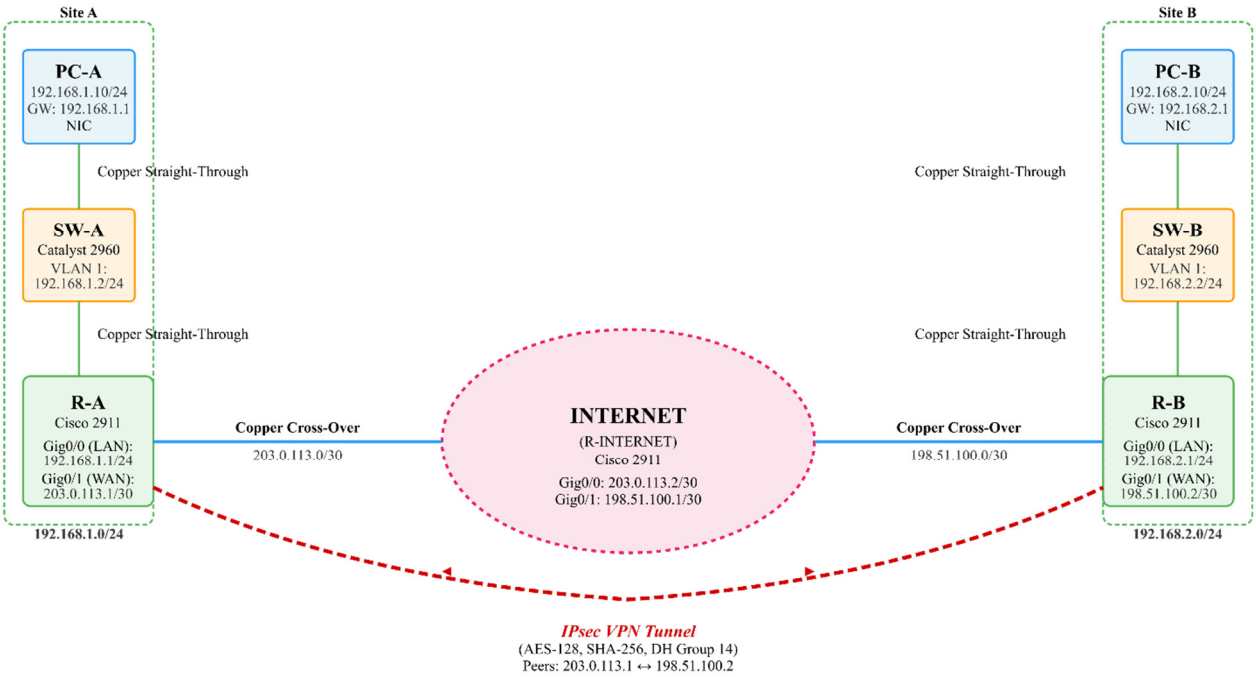

Рисунок 13.1 — Топологія site-to-site IPsec VPN мережі

Організація адресного простору в топології відповідає найкращим практикам розділення приватних та публічних мереж. Локальні сегменти використовують приватні адреси з діапазону 192.168.0.0/16, зарезервованого RFC 1918 для внутрішнього використання в корпоративних мережах. Мережа Site A отримала підмережу 192.168.1.0/24, що надає 254 придатні адреси для хостів, з яких використано лише три: шлюз маршрутизатора, адреса управління комутатора та робоча станція. Аналогічно мережа Site B використовує підмережу 192.168.2.0/24 з ідентичним розподілом адрес. Публічні з'єднання між маршрутизаторами використовують адреси з діапазонів, спеціально зарезервованих RFC 5737 для документації та прикладів: 203.0.113.0/24 та 198.51.100.0/24. Ці діапазони гарантовано не конфліктують з реальними адресами в Інтернеті. Для з'єднань типу “точка-точка” між маршрутизаторами застосовується маска /30, яка надає лише дві придатні адреси на кожне з'єднання, що є оптимальним використанням адресного простору. Наприклад, підмережа 203.0.113.0/30 містить адреси від 203.0.113.0 до 203.0.113.3, де .0 — адреса мережі, .1 та .2 — придатні адреси для інтерфейсів, .3 — широкомовна адреса.

Статична маршрутизація в топології налаштована таким чином, щоб забезпечити повну досяжність між усіма мережевими сегментами. На маршрутизаторі R-A налаштований статичний маршрут до віддаленої мережі 192.168.2.0/24 через наступний крок 203.0.113.2, що є адресою інтерфейсу R-INTERNET. Це означає, що весь трафік від хостів Site A, призначений для Site B, спрямовується через зовнішній інтерфейс до транзитного маршрутизатора. Симетрично на R-B налаштований маршрут до 192.168.1.0/24 через 198.51.100.1. Маршрутизатор R-INTERNET має два статичні маршрути: до 192.168.1.0/24 через 203.0.113.1 та до 192.168.2.0/24 через 198.51.100.2, що

дозволяє йому коректно переспрямовувати пакети між публічними інтерфейсами пограничних маршрутизаторів. Важливо розуміти, що на рівні транзитної мережі весь IPsec-трафік є звичайними IP-пакетами з публічними адресами джерела та призначення, тому R-INTERNET маршрутизує їх без будь-якої спеціальної обробки. Фактичне шифрування та дешифрування відбувається виключно на пограничних маршрутизаторах R-A та R-B, які мають повну конфігурацію IPsec.

2 КЛЮЧОВІ ПИТАННЯ

1. Яка фундаментальна відмінність між моделями комунікації протоколів Syslog та базового SNMP, і як ця різниця впливає на реакцію системи моніторингу на критичні події?
2. Поясніть призначення рівня важливості «informational» (6) у конфігурації logging trap informational на маршрутизаторі та чому саме цей рівень рекомендується для повноцінного моніторингу.
3. Чому для ефективного аудиту безпеки необхідно активувати команду service timestamps log datetime msec, і як відсутність мілісекундної точності ускладнює аналіз інцидентів після перезавантаження обладнання?
4. Опишіть структуру ідентифікатора об'єкта OID 1.3.6.1.2.1.1.1.0 та поясніть, яку конкретну змінну MIB він представляє та для яких завдань моніторингу використовується.
5. Яка ключова відмінність між операціями GET та TRAP у протоколі SNMP, і чому трапи забезпечують миттєве сповіщення про події, на відміну від регулярного опитування?
6. Чому в навчальному середовищі використовується версія SNMPv2c з незахищеною спільнотою public, і які конкретні ризики безпеки це створює в реальних експлуатаційних мережах?
7. Поясніть механізм роботи команди snmp-server enable traps snmp linkdown linkup та як вона забезпечує автоматичне сповіщення про зміну стану інтерфейсу без участі адміністратора.
8. Які три ключові відмінності між текстовими повідомленнями Syslog та структурованими даними SNMP з точки зору автоматизованої обробки та побудови аналітичних графіків?
9. Чому в топології лабораторної роботи критично важливо прив'язувати crypto map до зовнішнього (публічного) інтерфейсу маршрутизатора, а не до внутрішнього, і як ця помилка впливає на роботу механізму визначення «цікавого трафіку»?
10. Як лічильник snmpOutTraps у виводі команди show snmp mib підтверджує фактичну генерацію трапів маршрутизатором навіть у середовищі Packet Tracer, де візуалізація трапів на сервері обмежена?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1 Топологія та адресація

Топологія моделює класичний сценарій підключення двох віддалених офісів (Site A та Site B) через публічну мережу Інтернет. Кожен офіс представлений локальним сегментом, що складається з персонального комп’ютера (ПК) та комутатора управління Catalyst 2960. ПК підключається до комутатора за допомогою медного прямого кабелю (модель «Copper Straight-Through»), а комутатор — до внутрішнього інтерфейсу пограничного маршрутизатора Cisco 2911. Зовнішні інтерфейси обох пограничних маршрутизаторів (R-A та R-B) з’єднані з центральним маршрутизатором R-INTERNET, який імітує інфраструктуру провайдера або глобальну мережу Інтернет. R-INTERNET не бере участі в криптографічних операціях — він лише маршрутизує пакети між публічними інтерфейсами R-A та R-B. Усі з’єднання між маршрутизаторами реалізовані за допомогою медних кабелів «Copper Cross-Over» на інтерфейсах GigabitEthernet. Приватні мережі (192.168.1.0/24 та 192.168.2.0/24) використовують адреси з діапазону RFC 1918, а публічні інтерфейси отримали адреси з діапазонів, зарезервованих для документації (RFC 5737): 203.0.113.0/24 для з’єднання Site A з «Інтернетом» та 198.51.100.0/24 для з’єднання Site B. Такий підхід забезпечує методичну коректність та уникнення конфліктів з реальними мережами.

Таблиця 13.1 — Адресація пристроїв

Пристрій	Інтерфейс	IP-адреса/маска	Призначення
PC-A	NIC	192.168.1.10/24	Клієнтська станція Site A
SW-A	VLAN 1	192.168.1.2/24	Управління комутатором Site A
R-A	Gig0/0	192.168.1.1/24	Внутрішній інтерфейс (LAN)
	Gig0/1	203.0.113.1/30	Зовнішній інтерфейс (WAN)
R-INTERNET	Gig0/0	203.0.113.2/30	Підключення до Site A
	Gig0/1	198.51.100.1/30	Підключення до Site B
R-B	Gig0/0	192.168.2.1/24	Внутрішній інтерфейс (LAN)
	Gig0/1	198.51.100.2/30	Зовнішній інтерфейс (WAN)
SW-B	VLAN 1	192.168.2.2/24	Управління комутатором Site B
PC-B	NIC	192.168.2.10/24	Клієнтська станція Site B

Маска /30 (255.255.255.252) на з’єднаннях «точка-точка» між маршрутизаторами дозволяє ефективно використовувати адресний простір, оскільки таке з’єднання потребує лише двох придатних IP-адрес.

Для закріплення навичок налаштування site-to-site IPsec VPN кожен студент виконує лабораторну роботу з унікальними параметрами згідно з призначеним варіантом. Студент повинен виконати лабораторну роботу з унікальними параметрами свого варіанту: використовувати вказані в таблиці 13.2 IP-адреси персональних комп'ютерів та шлюзів за замовчуванням для кожного сайту, призначити публічні адреси з'єднань «точка-точка» згідно з даними таблиці (при цьому адреса інтерфейсу маршрутизатора R-INTERNET

розраховується як наступна придатна адреса в /30 підмережі), а також застосувати вказаний у варіанті pre-shared ключ замість стандартного ключа P@ssw0rd123.

Наприклад, для варіанту 1 публічний інтерфейс R-A отримує адресу 203.0.113.5/30, отже інтерфейс R-INTERNET на цьому з'єднанні повинен бути налаштований на адресу 203.0.113.6/30 (друга придатна адреса в підмережі 203.0.113.4/30), аналогічно визначається пара адрес для з'єднання між R-B та R-INTERNET у діапазоні 198.51.100.0/30.

Таблиця 13.2 — Варіанти індивідуальних завдань

Варіант	Site A (ПК; шлюз; публ. інтерфейс R-A)	Site B (ПК; шлюз; публ. інтерфейс R-B)	Pre-shared key
1	10.15.30.10; 10.15.30.1; 203.0.113.5/30	10.25.40.10; 10.25.40.1; 198.51.100.5/30	Ip$ec@2024!A
2	172.16.50.10; 172.16.50.1; 203.0.113.9/30	172.16.60.10; 172.16.60.1; 198.51.100.9/30	N3t_S3cur!ty#1
3	192.168.10.10; 192.168.10.1; 203.0.113.13/30	192.168.20.10; 192.168.20.1; 198.51.100.13/30	VpnTunn3l$2025
4	10.45.100.10; 10.45.100.1; 203.0.113.17/30	10.45.110.10; 10.45.110.1; 198.51.100.17/30	$3cur3_C0nn3ct
5	172.18.10.10; 172.18.10.1; 203.0.113.21/30	172.18.20.10; 172.18.20.1; 198.51.100.21/30	K3y!P@ss#2026
6	192.168.55.10; 192.168.55.1; 203.0.113.25/30	192.168.65.10; 192.168.65.1; 198.51.100.25/30	Crypt0_G@teway
7	10.77.88.10; 10.77.88.1; 203.0.113.29/30	10.77.99.10; 10.77.99.1; 198.51.100.29/30	Tunn3l!Secur3#
8	172.20.33.10; 172.20.33.1; 203.0.113.33/30	172.20.44.10; 172.20.44.1; 198.51.100.33/30	P@cket_Tr@c3r
9	192.168.111.10; 192.168.111.1; 203.0.113.37/30	192.168.222.10; 192.168.222.1; 198.51.100.37/30	1p53c_Vpn$Key
10	10.100.200.10; 10.100.200.1; 203.0.113.41/30	10.100.201.10; 10.100.201.1; 198.51.100.41/30	N3tw0rk$2024!
11	172.22.55.10; 172.22.55.1; 203.0.113.45/30	172.22.66.10; 172.22.66.1; 198.51.100.45/30	$h@redK3y!2025
12	192.168.77.10; 192.168.77.1; 203.0.113.49/30	192.168.88.10; 192.168.88.1; 198.51.100.49/30	VPN_Tunn3l@UA
13	10.123.45.10; 10.123.45.1; 203.0.113.53/30	10.123.67.10; 10.123.67.1; 198.51.100.53/30	Crypt0!2026#UA
14	172.24.80.10; 172.24.80.1; 203.0.113.57/30	172.24.90.10; 172.24.90.1; 198.51.100.57/30	S3cur3!P@ssw0rd
15	192.168.150.10; 192.168.150.1; 203.0.113.61/30	192.168.160.10; 192.168.160.1; 198.51.100.61/30	1nt3rn3t$G@t3
16	10.200.100.10; 10.200.100.1; 203.0.113.65/30	10.200.101.10; 10.200.101.1; 198.51.100.65/30	K3y$Exch@nge!
17	172.26.111.10; 172.26.111.1; 203.0.113.69/30	172.26.222.10; 172.26.222.1; 198.51.100.69/30	D1ff13_H3llm@n
18	192.168.201.10; 192.168.201.1;	192.168.202.10; 192.168.202.1;	AES_256!Sh@256

	203.0.113.73/30	198.51.100.73/30	
19	10.55.66.10; 10.55.66.1; 203.0.113.77/30	10.55.77.10; 10.55.77.1; 198.51.100.77/30	Gr0up14$PFS!Key
20	172.28.40.10; 172.28.40.1; 203.0.113.81/30	172.28.50.10; 172.28.50.1; 198.51.100.81/30	Tunn3l_L!f3t!m3
21	192.168.220.10; 192.168.220.1; 203.0.113.85/30	192.168.230.10; 192.168.230.1; 198.51.100.85/30	Crypto_Map#10!
22	10.111.222.10; 10.111.222.1; 203.0.113.89/30	10.111.223.10; 10.111.223.1; 198.51.100.89/30	ESP_AES!HMAC_SHA
23	172.30.70.10; 172.30.70.1; 203.0.113.93/30	172.30.80.10; 172.30.80.1; 198.51.100.93/30	QM_IDLE$State_OK
24	192.168.240.10; 192.168.240.1; 203.0.113.97/30	192.168.250.10; 192.168.250.1; 198.51.100.97/30	ACL_101$Tr@ff1c
25	10.145.145.10; 10.145.145.1; 203.0.113.101/30	10.145.146.10; 10.145.146.1; 198.51.100.101/30	Transform$Set_Key
26	172.31.99.10; 172.31.99.1; 203.0.113.105/30	172.31.100.10; 172.31.100.1; 198.51.100.105/30	P@cket_Tr@c3r_VPN
27	192.168.254.10; 192.168.254.1; 203.0.113.109/30	192.168.253.10; 192.168.253.1; 198.51.100.109/30	Cisco$PT_IPsec!
28	10.222.111.10; 10.222.111.1; 203.0.113.113/30	10.222.112.10; 10.222.112.1; 198.51.100.113/30	Main_M0d3$Auth
29	172.16.200.10; 172.16.200.1; 203.0.113.117/30	172.16.201.10; 172.16.201.1; 198.51.100.117/30	Site2Site$VPN_UA
30	192.168.99.10; 192.168.99.1; 203.0.113.121/30	192.168.100.10; 192.168.100.1; 198.51.100.121/30	F1n@l_T3st!2026

3.2 Базова конфігурація всіх пристроїв

Перед налаштуванням IPsec необхідно забезпечити базову функціональність усіх пристроїв: коректну адресацію, активацію інтерфейсів та статичну маршрутизацію. Цей етап є критично важливим — якщо базова маршрутизація не працює, фаза 1 протоколу IKE не зможе ініціюватися, оскільки піри повинні обмінюватися службовими пакетами через публічну мережу. Особливу увагу слід приділити маршрутизатору R-INTERNET, який виступає як транзитний вузол і не бере участі в криптографічних операціях, але забезпечує досяжність між публічними інтерфейсами пограничних маршрутизаторів.

3.2.1 Налаштування робочих станцій (ПК). Робочі станції виступають як кінцеві точки для генерації «цікавого трафіку», що ініціює встановлення IPsec-тунелю. Ключовим елементом їхньої конфігурації є правильне налаштування шлюза за замовчуванням — саме через нього весь трафік, призначений для віддаленої мережі, спрямовується до пограничного маршрутизатора. У середовищі Packet Tracer налаштування виконується через

графічний інтерфейс: на вкладці «Desktop» обираємо пункт «IP Configuration», де вказуємо статичну IP-адресу, маску підмережі та шлюз за замовчуванням згідно з таблицею 1. Автоматичне отримання адреси через DHCP не застосовується, оскільки в лабораторній топології відсутній DHCP-сервер.

Налаштування PC-A:

1. Відкриваємо пристрій PC-A → вкладка «Desktop» → «IP Configuration»
2. Обираємо режим «Static»
3. Вводимо: - IP Address: 192.168.1.10 - Subnet Mask: 255.255.255.0 - Default Gateway: 192.168.1.1

Налаштування PC-B:

1. Відкриваємо пристрій PC-B → вкладка «Desktop» → «IP Configuration»
2. Обираємо режим «Static»
3. Вводимо: - IP Address: 192.168.2.10 - Subnet Mask: 255.255.255.0 - Default Gateway: 192.168.2.1

Після завершення налаштувань рекомендується перевірити конфігурацію за допомогою команди ipconfig /all у вікні командного рядка (вкладка «Command Prompt»). У виводі має відображатися коректна IP-адреса, маска 255.255.255.0 та шлюз за замовчуванням, що відповідає внутрішньому інтерфейсу відповідного пограничного маршрутизатора. Наявність цих параметрів гарантує, що ПК зможе надсилати пакети до власної мережі напряму, а до віддалених мереж — через маршрутизатор.

3.2.2 Налаштування комутаторів управління. Комутатори Catalyst 2960 виступають як прозорі комутаційні елементи на канальному рівні, забезпечуючи з’єднання між ПК та маршрутизаторами. Хоча для базової роботи тунелю їхня IP-конфігурація не є обов’язковою, налаштування інтерфейсу VLAN 1 та шлюза за замовчуванням дозволяє виконувати діагностику з самого комутатора (наприклад, перевірку зв’язку з маршрутизатором за допомогою ping). Це спрощує виявлення проблем на рівні локального сегмента. Обидва комутатори налаштовуються ідентично, з урахуванням специфіки своєї мережі.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.2 255.255.255.0   ! для
SW-A
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.1.1
Switch(config)# exit
Switch# copy running-config startup-config
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.2.2 255.255.255.0   ! для
SW-B
```

```
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.2.1
Switch(config)# exit
Switch# copy running-config startup-config
```

Після застосування конфігурації команда show ip interface brief на будь-якому комутаторі має показати інтерфейс VLAN 1 у стані «up/up» з призначеною IP-адресою. Перевірка зв’язку з маршрутизатором за допомогою ping 192.168.1.1 (для SW-A) або ping 192.168.2.1 (для SW-B) має повернути п’ять знаків оклику («!!!!!»), що підтверджує коректну роботу локального сегмента. Якщо пінг не проходить, слід перевірити фізичне підключення кабелів та стан портів за допомогою show interfaces status.

3.2.3 Налаштування пограничного маршрутизатора R-A. Конфігурація R-A включає активацію внутрішнього (LAN) та зовнішнього (WAN) інтерфейсів, призначення відповідних IP-адрес та створення статичного маршруту до віддаленої мережі 192.168.2.0/24 через шлюз 203.0.113.2 (інтерфейс R-INTERNET). Описи інтерфейсів (`description`) додаються для покращення читабельності конфігурації та спрощення технічної підтримки. Вимкнення CDP на зовнішньому інтерфейсі моделює реальну практику безпеки — у публічних мережах рекомендується обмежувати поширення інформації про обладнання.

```
R-A> enable
R-A# configure terminal
R-A(config)# hostname R-A
R-A(config)# interface GigabitEthernet0/0
R-A(config-if)# ip address 192.168.1.1 255.255.255.0
R-A(config-if)# description LAN_Site_A
R-A(config-if)# no shutdown
R-A(config-if)# exit
R-A(config)# interface GigabitEthernet0/1
R-A(config-if)# ip address 203.0.113.1 255.255.255.252
R-A(config-if)# description WAN_to_Internet
R-A(config-if)# no cdp enable
R-A(config-if)# no shutdown
R-A(config-if)# exit
R-A(config)# ip route 192.168.2.0 255.255.255.0 203.0.113.2
```

Команда show ip interface brief має показати обидва інтерфейси у стані «up/up», що підтверджує фізичне та канальне підключення. Статичний маршрут до мережі Site B з’явиться у таблиці маршрутизації з позначкою «S» (static) після виконання show ip route — це гарантія того, що пакети, призначені для 192.168.2.0/24, будуть спрямовані через інтерфейс Gig0/1 до R-INTERNET.

3.2.4 Налаштування пограничного маршрутизатора R-B. Конфігурація R-B є симетричною до R-A: внутрішній інтерфейс отримує адресу

192.168.2.1/24, зовнішній — 198.51.100.2/30, а статичний маршрут вказує на шлюз 198.51.100.1 для досяжності мережі Site A. Зверніть увагу на дзеркальну структуру маршрутів — це забезпечує двосторонню маршрутизацію, необхідну для роботи тунелю.

```
R-B> enable
R-B# configure terminal
R-B(config)# hostname R-B
R-B(config)# interface GigabitEthernet0/0
R-B(config-if)# ip address 192.168.2.1 255.255.255.0
R-B(config-if)# description LAN_Site_B
R-B(config-if)# no shutdown
R-B(config-if)# exit
R-B(config)# interface GigabitEthernet0/1
R-B(config-if)# ip address 198.51.100.2 255.255.255.252
R-B(config-if)# description WAN_to_Internet
R-B(config-if)# no cdp enable
R-B(config-if)# no shutdown
R-B(config-if)# exit
R-B(config)# ip route 192.168.1.0 255.255.255.0 198.51.100.1
```

Перевірка з’єднання між публічними інтерфейсами за допомогою ping 203.0.113.1 source 198.51.100.2 з контексту R-B має повернути п’ять знаків оклику («!!!!!»), що свідчить про повну досяжність на рівні мережі. Якщо пінг не проходить, необхідно негайно перевірити конфігурацію R-INTERNET — саме він є критичною точкою для базової маршрутизації.

3.2.5 Налаштування транзитного маршрутизатора R-INTERNET. Маршрутизатор R-INTERNET виконує роль публічної мережі та не потребує складних налаштувань. Його завдання — маршрутизувати пакети між двома підмережами «Інтернету» (203.0.113.0/30 та 198.51.100.0/30) та забезпечити досяжність приватних мереж через статичні маршрути. Оскільки цей маршрутизатор не бере участі в криптографічних операціях, на ньому не налаштовуються жодні елементи IPsec. Для реалістичності можна вимкнути непотрібні служби, такі як HTTP-сервер.

```
R-INTERNET> enable
R-INTERNET# configure terminal
R-INTERNET(config)# hostname R-INTERNET
R-INTERNET(config)# no ip http server
R-INTERNET(config)# interface GigabitEthernet0/0
R-INTERNET(config-if)# ip address 203.0.113.2 255.255.255.252
R-INTERNET(config-if)# description Link_to_R-A
R-INTERNET(config-if)# no shutdown
R-INTERNET(config-if)# exit
R-INTERNET(config)# interface GigabitEthernet0/1
R-INTERNET(config-if)# ip address 198.51.100.1 255.255.255.252
R-INTERNET(config-if)# description Link_to_R-B
R-INTERNET(config-if)# no shutdown
```

```
R-INTERNET(config-if)# exit
R-INTERNET(config)# ip route 192.168.1.0 255.255.255.0 203.0.113.1
R-INTERNET(config)# ip route 192.168.2.0 255.255.255.0
198.51.100.2
```

Команда show ip route на R-INTERNET має відобразити дві статичні маршрути до приватних мереж з позначкою «S». Критичною перевіркою є виконання пінгу між публічними інтерфейсами обох пограничних маршрутизаторів: з R-A команда ping 198.51.100.2 має успішно завершитися. Якщо цей тест пройдено, можна переходити до налаштування криптографічних елементів — базова інфраструктура готова.

3.3 Налаштування фази 1 (IKE/ISAKMP)

Фаза 1 протоколу IKE (Internet Key Exchange), реалізована в Cisco через ISAKMP (Internet Security Association and Key Management Protocol), встановлює захищений канал управління між пірами для обміну ключами та параметрами безпеки фази 2. Цей канал захищається за допомогою заздалегідь узгодженої політики, що включає алгоритм шифрування, хеш-функцію, метод автентифікації, групу Діффі-Геллмана (DH) та час життя асоціації безпеки (SA). У середовищі Packet Tracer рекомендується використовувати алгоритм шифрування AES-128 (команда encr aes), оскільки версії з 192/256 бітами можуть не підтримуватися; групу Діффі-Геллмана 14 (2048 біт) для кращої сумісності з сучасними стандартами. Ключовим моментом є використання попередньо узгодженого ключа (pre-shared key), який має бути ідентичним на обох маршрутизаторах і прив’язаним до публічної IP-адреси віддаленого піра.

3.3.1 Створення ISAKMP policy на R-A. Політика з ідентифікатором 10 визначає параметри захисту каналу управління: шифрування AES-128 забезпечує конфіденційність, хеш SHA-256 — цілісність даних, група Діффі-Геллмана 14 дозволяє безпечний обмін ключами, а автентифікація за попередньо узгодженим ключем є найпростішим методом для навчального середовища. Час життя 86400 секунд (24 години) визначає період, після якого асоціація безпеки буде перегенерована.

```
R-A(config)# crypto isakmp policy 10
R-A(config-isakmp)# encryption aes
R-A(config-isakmp)# hash sha256
R-A(config-isakmp)# authentication pre-share
R-A(config-isakmp)# group 14
R-A(config-isakmp)# lifetime 86400
R-A(config-isakmp)# exit
R-A(config)# crypto isakmp key P@ssw0rd123 address 198.51.100.2
```

Після виходу з контексту політики команда show crypto isakmp policy відобразить деталі активної конфігурації. У колонці «Encryption» має бути

вказано «aes», «Hash» — «sha256», «Authentication» — «pre-share», а «Group» — «14 (2048 bit)». Якщо замість цього відображається «des» або «md5», це означає, що попередні команди не були застосовані — можливо, через вихід з контексту без збереження параметрів. Ключова команда crypto isakmp key не має виводу підтвердження, тому для перевірки слід використати show run | section isakmp, де має з’явитися рядок з ключем та адресою піра.

3.3.2 Створення симетричної ISAKMP policy на R-B. Конфігурація на R-B повинна бути дзеркальною: ті самі параметри політики (ідентифікатор може відрізнятися, але параметри — ідентичні) та ключ, прив’язаний до публічної адреси R-A (203.0.113.1). Критично важливо, щоб ключ P@ssw0rd123 збігався символ у символ — будь-яка розбіжність призведе до невдачі фази 1, оскільки процес автентифікації завершиться помилкою.

```
R-B(config)# crypto isakmp policy 10
R-B(config-isakmp)# encryption aes
R-B(config-isakmp)# hash sha256
R-B(config-isakmp)# authentication pre-share
R-B(config-isakmp)# group 14
R-B(config-isakmp)# lifetime 86400
R-B(config-isakmp)# exit
R-B(config)# crypto isakmp key P@ssw0rd123 address 203.0.113.1
```

Для діагностики можна тимчасово активувати налагоджувальний режим за допомогою debug crypto isakmp на обох маршрутизаторах. Під час ініціації тунелю (через пінг з ПК) у консолі з’являться повідомлення про обмін повідомленнями Main Mode. Успішне завершення фази 1 підтверджується станом QM_IDLE у виводі show crypto isakmp sa: запис з адресою піра 198.51.100.2 (для R-A) або 203.0.113.1 (для R-B) зі статусом ACTIVE. Якщо замість цього відображається MM_NO_STATE, це вказує на розбіжність у політиках або ключах — найчастіша причина помилки для початківців.

3.4 Налаштування фази 2 (IPsec transform set та ACL)

Фаза 2 встановлює асоціації безпеки (SA) для захисту корисного трафіку між приватними мережами. На відміну від фази 1, яка захищає службовий канал, фаза 2 визначає параметри шифрування та автентифікації для самого корисного навантаження. Ключовим елементом є механізм визначення «цікавого трафіку» через розширений ACL: лише трафік, що відповідає умовам списку, ініціює встановлення тунелю фази 2. Це дозволяє ефективно використовувати ресурси, шифруючи лише необхідні потоки. Transform set об’єднує алгоритми шифрування (наприклад, ESP-AES) та автентифікації (наприклад, ESP-SHA-HMAC) у єдиний профіль захисту.

3.4.1 Створення розширеного ACL та transform set на R-A. Розширений ACL 101 дозволяє IP-трафік з мережі Site A (192.168.1.0/24) до

мережі Site B (192.168.2.0/24). Важливо використовувати розширений ACL (номери 100–199), оскільки стандартний ACL не дозволяє фільтрувати за адресою призначення. Transform set MY_TRANSFORM_SET визначає захист через ESP з шифруванням AES-128 та автентифікацією HMAC-SHA1. У Packet Tracer HMAC-SHA256 може не підтримуватися, тому використовуємо перевірений варіант. Режим tunnel вказує на інкапсуляцію повного оригінального IP-пакета у новий зовнішній пакет з публічними адресами — саме цей режим використовується для site-to-site VPN.

```
R-A(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
R-A(config)# crypto ipsec transform-set MY_TRANSFORM_SET esp-aes
esp-sha-hmac
R-A(cfg-crypto-trans)# mode tunnel
R-A(cfg-crypto-trans)# exit
```

Команда show access-lists 101 має відобразити один запис: «permit ip host 192.168.1.0 0.0.0.255 host 192.168.2.0 0.0.0.255». Зверніть увагу на маску з інверсією (wildcard mask) 0.0.0.255 — саме вона визначає діапазон адрес. Якщо замість неї використати звичайну маску підмережі (255.255.255.0), ACL буде некоректним і не спрацює. Для перевірки transform set команда show crypto ipsec transform-set відобразить параметри: «Transform set MY_TRANSFORM_SET: { esp-aes esp-sha-hmac }» та режим «tunnel» — це підтвердить готовність профілю захисту для фази 2.

3.4.2 Створення симетричних елементів на R-B. Конфігурація на R-B є дзеркальною: ACL 101 дозволяє трафік у зворотному напрямку (з 192.168.2.0/24 до 192.168.1.0/24), а transform set має ідентичні параметри. Ця симетрія критична — розбіжність у алгоритмах шифрування або автентифікації призведе до невдачі фази 2, оскільки піри не зможуть узгодити параметри захисту.

```
R-B(config)# access-list 101 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
R-B(config)# crypto ipsec transform-set MY_TRANSFORM_SET esp-aes
esp-sha-hmac
R-B(cfg-crypto-trans)# mode tunnel
R-B(cfg-crypto-trans)# exit
```

Порівняння виводу show crypto ipsec transform-set на обох маршрутизаторах має показати ідентичні параметри. Якщо на одному пристрої вказано, наприклад, esp-3des, а на іншому — esp-aes, узгодження фази 2 буде неможливим. Це проявиться у відсутності записів у виводі show crypto ipsec sa після спроби передачі трафіку, хоча фаза 1 може бути успішною (стан QM_IDLE у show crypto isakmp sa).

3.5 Створення crypto map та активація тунелю

Crypto map є центральним елементом конфігурації IPsec, що об’єднує всі компоненти: визначає піра за публічною IP-адресою, посилається на ACL для визначення «цікавого трафіку», вказує transform set для фази 2 та встановлює параметри часу життя фази 2. Після створення crypto map його необхідно прив’язати до зовнішнього (публічного) інтерфейсу маршрутизатора — саме через цей інтерфейс буде проходити шифрований трафік. Критичною помилкою студентів часто є прив’язка crypto map до внутрішнього інтерфейсу (наприклад, Gig0/0), що робить тунель нефункціональним, оскільки «цікавий трафік» перевіряється лише на тому інтерфейсі, де застосований crypto map.

3.5.1 Створення та застосування crypto map на R-A. Crypto map MY_CRYPTO_MAP з послідовністю 10 визначає піра 198.51.100.2 (публічний інтерфейс R-B), посилається на ACL 101 для фільтрації трафіку, використовує створений раніше transform set та встановлює час життя фази 2 у 3600 секунд. Параметр set pfs group14 увімкнює ідеальну прямою секретність (Perfect Forward Secrecy), що забезпечує додатковий рівень безпеки через генерацію нових ключів для кожної сесії фази 2. Прив’язка до інтерфейсу Gig0/1 (зовнішнього) активує механізм перевірки вхідного/вихідного трафіку на відповідність ACL.

```
R-A(config)# crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
R-A(config-crypto-map)# set peer 198.51.100.2
R-A(config-crypto-map)# match address 101
R-A(config-crypto-map)# set transform-set MY_TRANSFORM_SET
R-A(config-crypto-map)# set pfs group14
R-A(config-crypto-map)# set security-association lifetime seconds
3600
R-A(config-crypto-map)# exit
R-A(config)# interface GigabitEthernet0/1
R-A(config-if)# crypto map MY_CRYPTO_MAP
R-A(config-if)# exit
```

Команда show crypto map відобразить повну структуру криптографічної політики. У секції «Crypto Map “MY_CRYPTO_MAP” 10» мають бути присутні всі налаштовані параметри: peer address, access list, transform set та lifetime. Для підтвердження прив’язки до інтерфейсу достатньо виконати show run interface Gig0/1 — у виводі обов’язково має бути рядок crypto map MY_CRYPTO_MAP. Якщо його немає, тунель не активуватиметься навіть за наявності коректного «цікавого трафіку».

3.5.2 Створення симетричного crypto map на R-B. Конфігурація на R-B дзеркальна: пір вказує на 203.0.113.1 (публічний інтерфейс R-A), ACL 101 фільтрує трафік у зворотному напрямку, решта параметрів ідентична. Прив’язка до інтерфейсу Gig0/1 (зовнішнього) є обов’язковою — саме через нього проходить трафік до «Інтернету».

```
R-B(config)# crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
R-B(config-crypto-map)# set peer 203.0.113.1
R-B(config-crypto-map)# match address 101
R-B(config-crypto-map)# set transform-set MY_TRANSFORM_SET
R-B(config-crypto-map)# set pfs group14
R-B(config-crypto-map)# set security-association lifetime seconds
3600
R-B(config-crypto-map)# exit
R-B(config)# interface GigabitEthernet0/1
R-B(config-if)# crypto map MY_CRYPTO_MAP
R-B(config-if)# exit
```

Після завершення цього кроку конфігурація IPsec завершена. Тунель активується автоматично при появі «цікавого трафіку» — тобто при спробі ПК з однієї мережі зв’язатися з ПК з іншої мережі. До цього моменту асоціації безпеки не створюються, що є нормальною поведінкою для IPsec у режимі «за запитом» (on-demand).

3.6 Перевірка роботи тунелю та аналіз стану

Перевірка роботи IPsec VPN ґрунтується на трьох рівнях: досяжність кінцевих хостів (пінг), стан асоціацій безпеки фази 1 (ISAKMP SA) та фази 2 (IPsec SA). Важливо розуміти, що в середовищі Packet Tracer пакети між публічними інтерфейсами передаються без реального шифрування — це обмеження симулятора. Тому аналіз вмісту пакетів у режимі симуляції не покаже шифрованих даних, але команди show crypto нададуть достовірну інформацію про стан тунелю.

3.6.1 Ініціація трафіку та перевірка досяжності. З комп’ютера PC-A виконайте команду ping 192.168.2.10. Перший пакет часто втрачається через час, необхідний для встановлення тунелю (фаза 1 + фаза 2 займає кілька секунд). Подальші пакети мають проходити успішно з відповіддю «Reply from 192.168.2.10: bytes=32 time<1ms TTL=126». Аналогічно перевірте зворотний напрямок з PC-B до PC-A. Якщо пінг не проходить, але базова маршрутизація працює (пінг між публічними інтерфейсами 203.0.113.1 та 198.51.100.2 успішний), проблема полягає в конфігурації IPsec — необхідно перевірити стан асоціацій безпеки.

```
C:\> ping 192.168.2.10
```

Успішний пінг після першої спроби підтверджує, що механізм визначення «цікавого трафіку» працює коректно: пакети відповідають умовам ACL 101, що ініціює процес встановлення тунелю. Якщо пінг не проходить взагалі, перевірте шлюзи за замовчуванням на ПК та статичні маршрути на маршрутизаторах — найчастіша причина помилки на цьому етапі.

3.6.2 Аналіз стану фази 1 (ISAKMP SA). Виконайте команду на маршрутизаторі R-A для перевірки стану асоціації фази 1.

```
R-A# show crypto isakmp sa
```

У виводі з’явиться таблиця з колонками «dst», «src», «state», «conn-id» та «status». Ключовим індикатором успіху є стан QM_IDLE (Quick Mode Idle) у колонці «state» — це означає, що фаза 1 завершена успішно та канал управління готовий до узгодження параметрів фази 2. Приклад коректного запису: `198.51.100.2 203.0.113.1 QM_IDLE 1001 ACTIVE` Якщо замість QM_IDLE відображається MM_NO_STATE або запис відсутній, це свідчить про невдачу фази 1. Найпоширеніші причини: розбіжність у ключах (crypto isakmp key), несумісність політик ISAKMP або відсутність базової досяжності між публічними інтерфейсами.

3.6.3 Аналіз стану фази 2 (IPsec SA). Виконайте команду для перевірки асоціацій фази 2 після успішного пінгу.

```
R-A# show crypto ipsec sa
```

Вивід містить детальну інформацію про тунель, включаючи лічильники інкапсуляції (#pkts encaps) та декапсуляції (#pkts decaps). Ненульові значення (наприклад, #pkts encaps: 4, #pkts decaps: 4) підтверджують, що трафік проходить через тунель. Також перевірте параметри тунелю: рядок transform: esp-aes esp-sha-hmac має точно відповідати налаштованому transform set. Якщо лічильники залишаються нульовими, але фаза 1 активна (QM_IDLE), проблема полягає в ACL — трафік не відповідає умовам «цікавого трафіку» або crypto map прив’язаний до неправильного інтерфейсу.

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 № 14

Тема: Централізований моніторинг і керування мережею з використанням SNMP та Syslog

Мета роботи: Набути практичних навичок централізованого моніторингу стану мережі та збору подій за допомогою SNMP і Syslog

1 КЛЮЧОВІ ПОЛОЖЕННЯ

1.1 Вступ

Моніторинг мережевого обладнання є критично важливим компонентом сучасного управління інформаційними системами, оскільки забезпечує безперервний контроль за станом мережевих пристроїв, своєчасне виявлення аномалій та швидку реакцію на інциденти. У професійних середовищах, де відмова мережевих вузлів призводить до значних фінансових втрат або порушення критичних бізнес-процесів, застосування надійних протоколів моніторингу стає обов'язковою вимогою. Два провідні стандарти в цій області — протокол простого управління мережею SNMP (Simple Network Management Protocol) та протокол системного логування Syslog — хоча й призначені для схожих цілей, реалізують фундаментально різні підходи до збору та обробки інформації про стан мережевої інфраструктури. Розуміння концептуальних відмінностей між цими механізмами дозволяє інженерам вибирати оптимальні інструменти для конкретних завдань моніторингу.

Протокол SNMP функціонує за моделлю активного опитування, де централізована система управління (менеджер) періодично запитує стан керованих пристроїв (агентів), отримуючи у відповідь структуровані дані з управлінської інформаційної бази MIB. Цей підхід забезпечує регулярний збір метрик продуктивності та дозволяє виявляти тенденції зміни параметрів мережі, що є незамінним для довгострокового планування ресурсів. На противагу цьому, протокол Syslog працює в асинхронному режимі, коли мережеві пристрої самостійно відправляють текстові повідомлення про події на централізований сервер без попереднього запиту, що робить цей механізм особливо ефективним для реєстрації несподіваних інцидентів та аудиту безпеки.

Паралельно з механізмами опитування та логування, сучасні системи моніторингу використовують SNMP-трапи — спеціальний тип повідомлень, які мережеві пристрої надсилають самостійно при настанні критичних подій без очікування запиту від менеджера. Трапи займають проміжну позицію між активним опитуванням та асинхронним логуванням, оскільки ініціюються агентом, але передають структуровані дані в форматі SNMP замість текстових повідомлень Syslog. Поєднання всіх трьох підходів у єдиній системі моніторингу забезпечує комплексний контроль за мережею, де регулярні SNMP-опитування надають статистику продуктивності, Syslog накопичує

детальні логи всіх операцій, а SNMP-трапи миттєво сповіщають про критичні зміни стану обладнання. Така багаторівнева архітектура моніторингу є стандартом де-факто в корпоративних мережах та центрах обробки даних.

Мета даного лабораторного заняття полягає у набутті практичних навичок конфігурування всіх трьох механізмів моніторингу на реальному мережевому обладнанні та глибокому розумінні їхніх функціональних відмінностей. Студенти навчаться налаштовувати маршрутизатори як джерела подій Syslog, активувати SNMP-агентів для відповіді на запити менеджера, конфігурувати генерацію SNMP-трапів при зміні стану інтерфейсів, а також розгортати централізований сервер для збору та аналізу отриманої інформації. Практичне виконання завдання передбачає не лише технічну реалізацію конфігурацій, але й експериментальну перевірку роботи кожного механізму шляхом штучного генерування подій та спостереження за реакцією системи моніторингу, що дозволяє закріпити теоретичні знання через безпосередню взаємодію з протоколами.

1.2 Архітектура та принципи функціонування протоколу Syslog

Протокол Syslog, стандартизований у RFC 5424, реалізує клієнт-серверну архітектуру для централізованого збору системних подій від розподілених мережевих пристроїв. Кожен пристрій у мережі виступає клієнтом (відправником), який генерує повідомлення про різноманітні події операційної системи та мережевих служб, відправляючи їх на віддалений сервер через транспортний протокол UDP на стандартний порт 514. Використання UDP замість TCP обумовлене необхідністю мінімізувати накладні витрати на встановлення з'єднання та підтвердження доставки, що є критично важливим для високонавантажених систем, де пристрої генерують тисячі повідомлень за секунду. Однак така архітектура передбачає можливість втрати пакетів у перевантажених мережах, тому для критичних систем існують реалізації Syslog поверх TCP із гарантованою доставкою, хоча вони менш поширені в типових корпоративних мережах.

Кожне Syslog-повідомлення складається з трьох основних компонентів: пріоритету, заголовка та текстового вмісту. Пріоритет визначається комбінацією двох параметрів — категорії (facility), яка вказує на підсистему, що згенерувала подію, та рівня важливості (severity), який відображає критичність інциденту. Категорія може набувати значень від kern (повідомлення ядра операційної системи) до local0–local7 (користувацькі категорії для спеціалізованих додатків), а рівень важливості варіюється від 0 (emergency — система непрацездатна) до 7 (debug — налагоджувальна інформація). Така класифікація дозволяє адміністраторам фільтрувати повідомлення на сервері, зберігаючи критичні події в окремих файлах для швидкого доступу, а менш важливі — в архівних сховищах для довгострокового аудиту. Заголовок повідомлення містить позначку часу з точністю до мілісекунди та ідентифікатор пристрою-джерела, що є

обов'язковим для кореляції подій у розподілених системах, де синхронізація часу між пристроями здійснюється через протокол NTP.

Конфігурація Syslog на мережевих пристроях Cisco здійснюється через режим глобальної конфігурації та включає кілька обов'язкових параметрів. Команда logging host вказує IP-адресу централізованого сервера, куди мають надсилатися всі згенеровані повідомлення, що дозволяє організувати єдину точку збору логів для всієї мережевої інфраструктури. Параметр logging trap визначає мінімальний рівень важливості повідомлень, які будуть відправлятися на сервер — наприклад, значення informational (рівень 6) означає, що передаватимуться всі події від рівня 0 до рівня 6 включно, тобто всі крім налагоджувальних повідомлень. Для забезпечення точної кореляції подій у часі необхідно активувати позначки часу командою service timestamps log datetime msec, що додає до кожного повідомлення дату, час та мілісекунди, оскільки без цієї опції багато пристроїв Cisco використовують лише лічильник часу роботи з моменту завантаження, що ускладнює аналіз логів після перезавантаження обладнання.

На практиці Syslog-сервери зберігають отримані повідомлення у текстових файлах з ротацією за датою або розміром, що дозволяє управляти обсягом дискового простору та організовувати архівування старих записів. Сучасні реалізації серверів, такі як rsyslog або syslog-ng, підтримують додаткові можливості: фільтрацію повідомлень за ключовими словами, пересилання подій на інші сервери для резервування, інтеграцію з системами централізованого моніторингу через REST API та шифрування каналу зв'язку через TLS для захисту конфіденційної інформації. Особливо важливим є механізм буферизації на стороні клієнта, який дозволяє тимчасово зберігати повідомлення в оперативній пам'яті пристрою у випадку недоступності сервера та відправляти їх після відновлення зв'язку, що запобігає втраті критичних записів аудиту під час мережевих збоїв. Для перевірки коректності налаштування використовується команда show logging, яка відображає налаштований сервер, рівень важливості, статистику відправлених повідомлень та наявність помилок доставки.

У таблиці 14.1 наведено повну класифікацію рівнів важливості Syslog-повідомлень відповідно до стандарту RFC 5424, що є обов'язковим для розуміння при налаштуванні фільтрації подій на сервері та інтерпретації отриманих логів під час діагностики інцидентів.

Таблиця 14.1 – Рівні важливості повідомлень протоколу Syslog

Рівень	Назва	Опис
0	Emergency	Система повністю непрацездатна, критична аварія
1	Alert	Необхідна негайна дія адміністратора
2	Critical	Критична помилка компонента системи
3	Error	Помилка, що не впливає на загальну працездатність

4	Warning	Попередження про потенційну проблему
5	Notification	Нормальна подія, що заслуговує на увагу
6	Informational	Інформаційне повідомлення про роботу системи
7	Debug	Налагоджувальна інформація для розробників

Наведена класифікація застосовується не лише в протоколі Syslog, але й у багатьох інших системах логування та моніторингу, що робить її універсальним стандартом для категоризації серйозності подій у розподілених інформаційних системах. Правильний вибір порогового рівня важливості при налаштуванні відправлення логів дозволяє збалансувати повноту моніторингу та обсяг збережених даних, оскільки включення налагоджувального рівня може генерувати сотні мегабайт записів щоденно навіть для невеликої мережі.

1.3 Протокол SNMP: структура управлінської інформації

Протокол простого управління мережею SNMP є стандартом прикладного рівня моделі OSI, призначеним для централізованого управління та моніторингу мережевого обладнання через опитування структурованих параметрів, що зберігаються в управлінській інформаційній базі кожного пристрою. На відміну від текстово-орієнтованого Syslog, SNMP оперує числовими ідентифікаторами об'єктів OID (Object Identifier), організованими у вигляді ієрархічного дерева MIB (Management Information Base), що дозволяє стандартизувати доступ до параметрів різних виробників обладнання та автоматизувати збір метрик продуктивності. Архітектура SNMP базується на моделі менеджер-агент, де програмне забезпечення менеджера (системи моніторингу) надсилає запити до агентів (демонів SNMP на мережевих пристроях), які відповідають поточними значеннями запитуваних змінних або підтверджують зміну конфігураційних параметрів.

Управлінська інформаційна база MIB представляє собою формальний опис усіх параметрів, доступних для читання або запису через SNMP, організованих у деревоподібну структуру з числовою адресацією. Кожен вузол дерева має унікальний OID, що складається з послідовності цілих чисел, розділених крапками, наприклад 1.3.6.1.2.1.1.1.0 відповідає змінній sysDescr, яка містить текстовий опис пристрою. Перші кілька чисел OID завжди однакові для всіх пристроїв: 1.3.6.1 позначає інтернет-підгілку дерева ідентифікаторів ISO, 2 вказує на управлінську категорію, 1 — на стандартну MIB-II, а наступні числа специфікують конкретні групи параметрів та окремі змінні. Така структура дозволяє виробникам обладнання розширювати стандартну MIB власними параметрами в приватних гілках (зазвичай починаються з 1.3.6.1.4.1), зберігаючи сумісність із загальноприйнятими інструментами моніторингу через підтримку базового набору змінних MIB-II.

Сучасні реалізації SNMP представлені трьома основними версіями протоколу, що мають суттєві відмінності в функціональності та рівні безпеки.

SNMPv1, стандартизована у 1988 році, забезпечує базові операції читання та запису змінних, використовуючи спільноти (community strings) як примітивний механізм автентифікації, де правильне знання паролю дає повний доступ до всіх дозволених змінних без шифрування трафіку. SNMPv2c, створена як покращена версія у 1993 році, додала підтримку масових операцій (отримання кількох змінних одним запитом) та покращила обробку помилок, але залишила незмінним механізм безпеки на основі незахищених спільнот. SNMPv3, стандартизована у 2002 році, кардинально змінила підхід до безпеки, запровадивши автентифікацію користувачів через хеш-функції MD5 або SHA, шифрування даних алгоритмами DES або AES та контроль цілісності повідомлень, що зробило її придатною для використання в продуктивних мережах з високими вимогами до конфіденційності.

Основні операції SNMP реалізуються через п'ять типів повідомлень протоколу, кожне з яких виконує специфічну функцію в процесі управління мережею. Операція GET дозволяє менеджеру запитати значення однієї змінної від агента, що використовується для отримання точкових параметрів, таких як поточне завантаження процесора або кількість помилок на інтерфейсі. Операція GET-NEXT служить для послідовного обходу дерева MIB, запитуючи наступну змінну після вказаної, що дозволяє виявляти доступні параметри без попереднього знання їхніх OID. Операція GET-BULK, доступна з SNMPv2c, оптимізує збір великих обсягів даних, дозволяючи отримати кілька послідовних змінних одним запитом замість серії окремих GET-NEXT. Операція SET використовується для зміни конфігураційних параметрів агента, наприклад встановлення адміністративного опису інтерфейсу або активації певної функції протоколу маршрутизації, але потребує спеціальних прав доступу (спільнота з правами read-write). Найважливішою є операція TRAP, яка відрізняється від інших тим, що ініціюється агентом без запиту менеджера при настанні певної події, такої як перезавантаження пристрою або зміна стану лінка, забезпечуючи асинхронне сповіщення про критичні зміни.

У таблиці 14.2 систематизовано основні команди конфігурування SNMP-агента на обладнанні Cisco IOS, що є необхідним для практичного розгортання системи моніторингу в корпоративних мережах.

Таблиця 14.2 – Основні команди конфігурування протоколу SNMP на обладнанні Cisco

Команда	Призначення
`snmp-server community`	Визначає спільноту та рівень доступу (RO – лише читання, RW – читання та запис)
`snmp-server location`	Встановлює фізичне розташування пристрою (змінна sysLocation)
`snmp-server contact`	Встановлює контактну особу для пристрою (змінна sysContact)
`snmp-server enable`	Активує генерацію трапів для вказаних типів подій

`traps`	
`snmp-server host`	Визначає IP-адресу менеджера для отримання трапів та версію протоколу
`show snmp`	Відображає загальну інформацію про стан служби SNMP
`show snmp host`	Відображає налаштовані хости-приймачі трапів
`show snmp community`	Відображає налаштовані спільноти та рівні доступу

Правильна конфігурація SNMP-агента передбачає послідовне виконання всіх перерахованих команд у режимі глобальної конфігурації, причому спільнота та системні атрибути є обов'язковими параметрами, тоді як налаштування трапів необхідне лише для реалізації асинхронних сповіщень про події. Важливо розуміти, що використання SNMPv2c із незахищеними спільнотами створює ризик перехоплення чутливої інформації про мережеву інфраструктуру, тому в продуктивних середовищах рекомендується застосовувати SNMPv3 із механізмами автентифікації та шифрування, навіть незважаючи на більшу складність початкового налаштування.

1.4 Порівняльний аналіз механізмів моніторингу

Протоколи Syslog та SNMP, хоча й використовуються в одній екосистемі мережевого моніторингу, базуються на фундаментально різних підходах до збору та обробки інформації про стан обладнання. Розуміння цих відмінностей є критично важливим для архітекторів мережевих систем, оскільки дозволяє оптимально поєднувати обидва протоколи для досягнення комплексної видимості мережевої інфраструктури. Ключова концептуальна відмінність полягає в ініціаторі комунікації: Syslog реалізує модель push, де пристрої самостійно відправляють повідомлення про події на сервер без будь-якого запиту, тоді як базовий SNMP використовує модель pull, коли система моніторингу активно опитує пристрої для отримання поточних значень змінних. Це призводить до принципово різних характеристик навантаження на мережу та реакції на події.

З точки зору структури даних протоколи також демонструють контрастні підходи. Syslog оперує текстовими повідомленнями довільного формату, що робить їх зручними для читання людиною та швидкого аналізу адміністратором через звичайні текстові редактори або команди grep і awk у Unix-системах. Однак ця гнучкість ускладнює автоматизовану обробку, оскільки різні виробники використовують власні формати повідомлень, і для їхнього розбору необхідні складні регулярні вирази або спеціалізовані парсери. Натомість SNMP використовує жорстко структуровані дані відповідно до схем MIB, де кожна змінна має чітко визначений тип (цілі числа, рядки, IP-адреси, лічильники), що спрощує автоматичну агрегацію метрик, побудову графіків продуктивності та встановлення порогових значень для тригерів сповіщень. Крім того, стандартизація MIB-II забезпечує однакову семантику базових

змінних для обладнання різних виробників, що неможливо у випадку вільноформатних Syslog-повідомлень.

Транспортні характеристики протоколів також суттєво різняться. Syslog традиційно використовує UDP порт 514 для мінімізації накладних витрат, що дозволяє пристроям відправляти логи навіть в умовах високого навантаження або часткової недоступності мережі, хоча це призводить до можливості втрати повідомлень у випадку перевантаження каналів або відмови сервера. SNMP також використовує UDP порти 161 (для запитів агента) та 162 (для трапів менеджера), але реалізує механізм повторної передачі у випадку відсутності відповіді від агента, що підвищує надійність доставки критичних метрик. Версія SNMPv3 додатково забезпечує шифрування трафіку та автентифікацію користувачів, тоді як стандартний Syslog передає дані у відкритому вигляді, хоча існують реалізації Syslog over TLS для захищеного транспорту логів у середовищах з високими вимогами до конфіденційності.

Частота оновлення інформації є ще одним важливим критерієм порівняння. Syslog забезпечує майже миттєве (в межах секунд) сповіщення про події, оскільки повідомлення генерується та відправляється одразу після настання інциденту, що робить цей протокол ідеальним для систем реагування на інциденти безпеки або критичні відмови обладнання. SNMP-опитування виконується з інтервалом, встановленим адміністратором системи моніторингу (зазвичай від 1 до 5 хвилин для рутинних метрик), що створює затримку між фактичною зміною параметра та її виявленням системою. Для компенсації цього недоліку SNMP підтримує трапи — асинхронні сповіщення, схожі за принципом дії на Syslog, але передають структуровані дані замість текстових повідомлень, поєднуючи переваги обох підходів.

У реальних корпоративних середовищах обидва протоколи застосовуються комплементарно: Syslog збирає детальні текстові логи всіх операцій для аудиту та післяінцидентного аналізу, SNMP-опитування надає регулярні метрики продуктивності для побудови історичних трендів та прогнозування потреб у ресурсах, а SNMP-трапи забезпечують негайне сповіщення про критичні події з передачею структурованих даних для автоматизованої класифікації та маршрутизації сповіщень. Така багатошарова архітектура моніторингу дозволяє одночасно досягти повноти логування, оперативності реагування та ефективності аналітичної обробки, що є необхідним для підтримання високого рівня доступності та безпеки складних розподілених систем.

2 КЛЮЧОВІ ПИТАННЯ

1. Як відрізняється модель комунікації протоколу Syslog (push) від базового механізму SNMP (pull), і чому ця різниця визначає швидкість реакції системи моніторингу на критичні події?
2. Чому для ефективного аудиту безпеки необхідно активувати команду service timestamps log datetime msec замість стандартних позначок часу, і як

відсутність мілісекундної точності ускладнює аналіз ланцюжка подій після перезавантаження обладнання?

3. Яку роль відіграє рівень важливості «informational» (6) у конфігурації logging trap informational, і чому саме цей рівень забезпечує повноцінний моніторинг без надмірного навантаження на сервер?

4. Як ідентифікатор об'єкта OID 1.3.6.1.2.1.1.3.0 пов'язаний із змінною sysUpTime, і для яких практичних завдань моніторингу використовується цей параметр?

5. Чому в навчальному середовищі використовується версія SNMPv2c з незахищеною спільнотою public, і які конкретні ризики безпеки це створює в реальних експлуатаційних мережах?

6. Як механізм роботи команди snmp-server enable traps snmp linkdown linkup забезпечує автоматичне сповіщення про зміну стану інтерфейсу без участі адміністратора?

7. Яка ключова відмінність між текстовими повідомленнями Syslog та структурованими даними SNMP з точки зору автоматизованої обробки та побудови аналітичних графіків продуктивності?

8. Чому в топології лабораторної роботи критично важливо прив'язувати crypto map до зовнішнього (публічного) інтерфейсу маршрутизатора, а не до внутрішнього, і як ця помилка впливає на роботу механізму визначення «цікавого трафіку»?

9. Як лічильник snmpOutTraps у виводі команди show snmp mib підтверджує фактичну генерацію трапів маршрутизатором навіть у середовищі Packet Tracer, де візуалізація трапів на сервері обмежена?

10. Які три ключові переваги поєднання механізмів активного опитування (SNMP GET), пасивних сповіщень (трапи) та асинхронного логування (Syslog) у єдиній системі моніторингу для забезпечення комплексного контролю за станом мережі?

3 ЛАБОРАТОРНЕ ЗАВДАННЯ

3.1 Топологія мережі та базові налаштування

Топологія лабораторної роботи охоплює чотири ключові пристрої, об’єднані в єдину локальну мережу 192.168.1.0/24 за допомогою комутатора Cisco 2960: маршрутизатор Cisco 2911 (R1) з IP-адресою 192.168.1.1 на інтерфейсі FastEthernet0/0, комутатор Cisco 2960 (SW1) з управлінським інтерфейсом VLAN 1, налаштованим на адресу 192.168.1.2, клієнтську робочу станцію (PC1) з адресою 192.168.1.10 для перевірки базової зв’язності, та універсальний сервер (Server1) з адресою 192.168.1.100, який виконує роль централізованої точки збору подій. Усі пристрої фізично з’єднані прямими мідними кабелями (Copper Straight-Through) через вільні порти комутатора, що забезпечує просту, але функціональну топологію «зірка», характерну для багатьох реальних мережевих середовищ. Така архітектура дозволяє зосередитися на налаштуванні протоколів моніторингу без ускладнення

додатковою маршрутизацією або сегментацією, що є доцільним для навчального середовища.

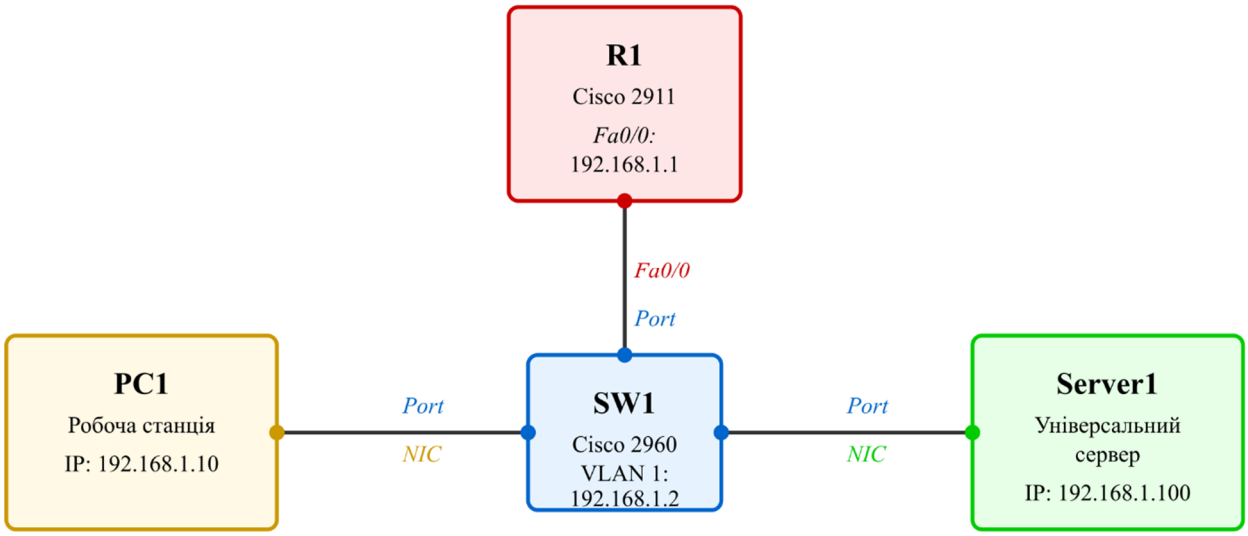

Рисунок 14.1 – Топологія мережі лабораторної роботи

3.2 Базові налаштування мережевої інфраструктури

Перед активацією служб моніторингу необхідно забезпечити стабільну IP-з’єднаність між усіма елементами топології, оскільки як протокол Syslog, так і SNMP покладаються на транспортний рівень моделі OSI та використовують протокол UDP для передачі даних. Без коректно налаштованих інтерфейсів та перевіреної маршрутизації механізми доставки подій не зможуть функціонувати, навіть якщо самі служби налаштовані правильно.

3.2.1 Налаштування інтерфейсу маршрутизатора R1. Маршрутизатор виступає основним джерелом системних подій у мережі, оскільки саме він генерує критичні повідомлення про зміну стану інтерфейсів, перезавантаження або помилки безпеки. Для активації інтерфейсу необхідно перевести його зі стану administratively down (стан за замовчуванням у симуляторі Packet Tracer) у робочий стан, призначивши коректну IP-адресу та маску підмережі. Цей процес виконується через режим глобальної конфігурації з подальшим переходом у контекст інтерфейсу.

```
R1> enable
R1# configure terminal
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
```

Після виконання команди no shutdown інтерфейс повинен перейти у стан up/up, що підтверджується за допомогою команди show ip interface brief. У

виводі цієї команди колонка «Status» відображає фізичний стан інтерфейсу (має бути up), а колонка «Protocol» — стан канального рівня (також up). Якщо хоча б одна з цих колонок містить значення down, це вказує на проблему: відсутність фізичного з’єднання, помилку конфігурації на сусідньому пристрої або неправильний тип кабелю. Успішна активація інтерфейсу є необхідною передумовою для подальшого налаштування служб моніторингу.

3.2.2 Налаштування комутатора SW1 та сервера моніторингу. Комутатор рівня 2, хоча й не виконує маршрутизації між підмережами, потребує IP-адреси на віртуальному інтерфейсі VLAN 1 для управління та участі в мережевій взаємодії як керованого пристрою. Крім призначення адреси 192.168.1.2/24, важливо налаштувати шлюз за замовчуванням 192.168.1.1, що дозволить комутатору надсилати пакети поза локальну мережу VLAN 1 у випадках, коли це знадобиться в більш складних топологіях. На сервері Server1 IP-адреса 192.168.1.100/24 та шлюз 192.168.1.1 налаштовуються через графічний інтерфейс у вкладці Desktop → IP Configuration, оскільки цей пристрій виступатиме приймачем подій від маршрутизатора.

```
SW1> enable
SW1# configure terminal
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# ip default-gateway 192.168.1.1
SW1(config)# exit
```

Для підтвердження готовності інфраструктури виконується перевірка зв’язності з маршрутизатора R1 до сервера командою ping 192.168.1.100. Успішний результат у вигляді п’яти отриманих відповідей (5/5 пакетів) свідчить про те, що мережева основа функціонує коректно, і можна переходити до налаштування спеціалізованих служб моніторингу. Цей етап є критичним, оскільки будь-яка помилка на рівні базової зв’язності унеможливить роботу механізмів доставки подій незалежно від правильності їхньої конфігурації.

3.3 Налаштування централізованого збору подій через Syslog

Протокол Syslog забезпечує асинхронний механізм збору текстових повідомлень про події різних рівнів важливості — від налагоджувальних записів до критичних аварійних сповіщень. На відміну від SNMP, який оперує структурованими змінними у форматі MIB, Syslog передає людино-читабельні повідомлення з точною позначкою часу, що робить його незамінним інструментом для аудиту безпеки та діагностики інцидентів. У симуляторі Packet Tracer окремого пристрою «Syslog Server» не передбачено, тому для цієї ролі використовується універсальний сервер з активованим сервісом SYSLOG у вкладці Services.

3.3.1. Активація сервісу Syslog на сервері Server1. Сервер моніторингу потребує попередньої активації відповідного сервісу перед тим, як зможе приймати повідомлення. У графічному інтерфейсі сервера необхідно перейти до вкладки Services, знайти сервіс SYSLOG та перемкнути його стан у положення On. Після активації сервіс автоматично починає прослуховувати стандартний порт UDP 514, готовий до прийому повідомлень від будь-якого джерела у мережі. Важливо зауважити, що в реальних умовах для захисту конфіденційності та цілісності логів рекомендується використовувати шифровані транспорти (наприклад, TLS через rsyslog або syslog-ng), але в навчальному середовищі достатньо базової реалізації без шифрування.

3.3.2 Налаштування маршрутизатора R1 як джерела Syslog-подій. Маршрутизатор налаштовується на відправлення подій на централізований сервер шляхом вказання його IP-адреси командою logging host. Для забезпечення повноцінного моніторингу встановлюється рівень важливості informational, що дозволяє передавати не лише критичні помилки, а й інформаційні події, такі як зміна стану інтерфейсу. Додатково активується позначка часу з мілісекундною точністю (service timestamps log datetime msec), що є обов’язковим для точного відстеження послідовності подій під час розслідування інцидентів.

```
R1# configure terminal
R1(config)# service timestamps log datetime msec
R1(config)# logging host 192.168.1.100
R1(config)# logging trap informational
R1(config)# exit
```

Верифікація конфігурації виконується командою show logging, яка відображає поточний стан системи логування. У виводі слід звернути увагу на рядок Logging to 192.168.1.100, що підтверджує налаштування віддаленого сервера, а також на значення (0 messages dropped), яке свідчить про відсутність втрат повідомлень через переповнення буфера або мережеві проблеми. Після генерації події (наприклад, вимкнення інтерфейсу) на вкладці SYSLOG сервера миттєво з’явиться запис із точною датою, часом, ім’ям пристрою та текстом події, що наочно демонструє ефективність централізованого збору логів.

3.4 Налаштування агента SNMP на маршрутизаторі. Протокол SNMP реалізує модель взаємодії «менеджер-агент», де агент (маршрутизатор) зберігає управлінську інформацію у вигляді ієрархічної бази даних MIB, а менеджер (сервер) отримує доступ до неї через запити або отримує асинхронні сповіщення про події. У лабораторній роботі використовується версія SNMPv2c, яка, хоча й не забезпечує шифрування даних, є широко поширеною в навчальних та тестових середовищах завдяки простоті налаштування. Важливо розуміти, що в реальних експлуатаційних мережах рекомендується SNMPv3 з підтримкою автентифікації та шифрування.

3.4.1 Базова конфігурація SNMP-агента. Налаштування починається з визначення спільноти (community string) public з правами лише для читання (RO), що дозволяє менеджеру отримувати інформацію з агента, але не змінювати її. Також задаються системні атрибути — контактна особа та фізичне розташування пристрою — які відображаються у відповідних MIB-змінних sysContact та sysLocation і є обов’язковими для професійного управління інфраструктурою.

```
R1# configure terminal
R1(config)# snmp-server community public RO
R1(config)# snmp-server location "Lab Room 305, Building A"
R1(config)# snmp-server contact "admin@university.edu.ua"
R1(config)# exit
```

Команда show snmp надає повну картину стану служби: відображається ідентифікатор обладнання (Chassis: CISCO2911/K9), контактна інформація, фізичне розташування, налаштовані спільноти та стан логування трапів. Відсутність помилок у виводі підтверджує коректність базової конфігурації. Для перевірки доступності MIB-змінних використовується вкладка Services → SNMP на сервері Server1: після введення адреси агента 192.168.1.1 та спільноти public можна отримати значення sysName (ім’я пристрою), sysUpTime (час роботи з останнього перезавантаження) та sysDescr (опис пристрою), що наочно демонструє механізм активного опитування.

3.4.2 Налаштування генерації трапів. Трапи є асинхронними сповіщеннями, які агент надсилає менеджеру без запиту при настанні певних подій, таких як зміна стану інтерфейсу або перезавантаження пристрою. Для активації цього механізму необхідно увімкнути генерацію трапів загалом командою snmp-server enable traps, а потім конкретизувати типи подій (наприклад, linkdown та linkup для зміни стану інтерфейсу) та вказати адресу менеджера для отримання сповіщень. Варто зазначити, що функціональність трапів у Packet Tracer обмежена: хоча агент генерує трапи, вони не відображаються візуально на сервері через спрощену реалізацію протоколу в симуляторі. Тому акцент робиться на перевірці конфігурації та теоретичному розумінні механізму.

```
R1# configure terminal
R1(config)# snmp-server enable traps snmp linkdown linkup
R1(config)# snmp-server host 192.168.1.100 version 2c public
R1(config)# exit
```

Для підтвердження налаштування використовується команда show snmp host, яка відображає адресу менеджера 192.168.1.100, версію протоколу v2c, спільноту public та тип повідомлення trap. Додатково команда show snmp mib дозволяє переглянути лічильник snmpOutTraps, який збільшується після кожної

генерації трапа. Цей лічильник слугує непрямим підтвердженням фактичної відправки трапа, навіть якщо він не відображається на сервері через обмеження симулятора.

3.5 Генерація подій та верифікація роботи механізмів моніторингу

Для експериментального підтвердження функціонування механізмів моніторингу необхідно згенерувати подію, яка спричинить реакцію усіх трьох систем: асинхронного логування (Syslog), активного опитування (SNMP GET) та пасивних сповіщень (SNMP traps). Найбільш наочним сценарієм є штучне вимкнення інтерфейсу маршрутизатора, яке моделює реальну ситуацію відмови лінка або планового технічного обслуговування. Важливо виконувати вимкнення через CLI, а не через графічний інтерфейс Packet Tracer, щоб гарантувати генерацію системних повідомлень.

3.5.1 Генерація події шляхом вимкнення інтерфейсу. Вимкнення інтерфейсу виконується командою shutdown у контексті інтерфейсу FastEthernet0/0. Ця дія миттєво переводить інтерфейс у стан administratively down і спричиняє генерацію каскаду пов’язаних подій у різних підсистемах маршрутизатора.

```
R1# configure terminal
R1(config)# interface FastEthernet0/0
R1(config-if)# shutdown
R1(config-if)# exit
R1(config)# exit
```

Після виконання команди система генерує повідомлення для служби Syslog: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down, яке миттєво надсилається на сервер 192.168.1.100 і з’являється у вікні сервісу SYSLOG з точною позначкою часу. Одночасно генерується SNMP-трап linkDown, що підтверджується збільшенням лічильника snmpOutTraps у виводі команди show snmp mib. Крім того, змінюється значення MIB-змінної ifOperStatus для цього інтерфейсу з up(1) на down(2), що може бути перевірено через активний SNMP GET-запит. Для повного циклу спостереження рекомендується повторно активувати інтерфейс командою no shutdown та спостерігати за генерацією подій linkUp у всіх трьох системах.

3.5.2 Перевірка активного опитування через SNMP GET. Механізм активного опитування відрізняється від трапів тим, що ініціатива запиту належить менеджеру, а не агенту. Для демонстрації цього підходу на сервері Server1 відкривається вкладка Services → SNMP, де вводиться IP-адреса агента 192.168.1.1, спільнота public та OID або назва змінної, наприклад sysUpTime.0. Після натискання кнопки «Get» сервер надсилає запит до маршрутизатора та

отримує у відповідь поточне значення часу роботи пристрою у сотих долях секунди.

Результат запиту відображається у вікні відповіді як числове значення (наприклад, 4321500), що відповідає 12 годинам 0 хвилинам 15 секундам роботи маршрутизатора. Це значення динамічно змінюється при кожному запиті, що підтверджує актуальність отриманих даних. На відміну від трапів, які надсилаються лише при настанні подій, активне опитування дозволяє регулярно збирати метрики продуктивності (завантаження CPU, використання пам’яті, статистику інтерфейсів) для побудови трендів та прогнозування навантаження, що робить його незамінним для довгострокового моніторингу.

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.