ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Кафедра інформаційних систем та технологій

Сергій ПАЛІЙ
Мирослава ГЛАДКА
Ірина БОРИСЕНКО
Ганна ТЕРЕЩУК

МЕТОДИЧНІ ВКАЗІВКИ З ВИВЧЕННЯ ДИСЦИПЛІНИ
ВСТУП ДО МЕРЕЖ

для здобувачів освітнього ступеня «бакалавр»
спеціальності F6 «Інформаційні системи і технології»
освітня програма «Програмні технології інтернет речей»

Київ 2026

Рецензенти:
д.т.н., професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка Сергій ТОЛЮПА
д.т.н., професор, декан факультету автоматизації та інформаційних технологій Київського національного університету будівництва та архітектури Олександр ТЕРЕНТЬЄВ

Рекомендовано до публікації кафедрою інформаційних систем та технологій, протокол №08_25/26 від 26.12.2025 року. Затверджено Вченою радою факультету інформаційних технологій, протокол №__ від __.01.2026 року.

ПАЛІЙ Сергій Володимирович
ГЛАДКА Мирослава Вікторівна
БОРИСЕНКО Ірина Ігорівна
ТЕРЕЩУК Ганна Михайлівна

Методичні вказівки до вивчення дисципліни **Вступ до мереж** [Електронний ресурс]: для здобувачів освітнього ступеня «бакалавр» спеціальності F6 «Інформаційні системи і технології», освітня програма «Програмні технології інтернет речей» / уклад. Палій С.В., Гладка М.В., Борисенко І.І., Терещук Г.М. – К.: КНУ імені Тараса Шевченка, 2026. – 91 с.

Метою вивчення дисципліни «Вступ до мереж» є набуття студентами спеціальності F6 «Інформаційні системи і технології» теоретичних знань та практичних навичок, що необхідні для проєктування, побудови та підтримки комп'ютерних мереж і вміння користуватись мережними технологіями. Дисципліна відповідає курсу «CCNA: Introduction to Network» мережної академії Cisco. При вивченні дисципліни у студентів мають сформуватись здатності проєктування, побудови та тестування локальних комп'ютерних мереж; здійснення моніторингу роботи окремих систем комп'ютерної мережі та перевірки їх працездатності.

Публікується в авторській редакції.

Електронна версія цього видання опублікована на сайті кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка. URL: https://www.ist.fit.knu.ua/

(дата публікації «___» січня 2026 року)

ЗМІСТ

ВСТУП

Під час вивчення дисципліни «Вступ до мереж» студенти опановують ефективне застосування мережних інформаційних технологій з використанням сучасних методів побудови комп'ютерних мереж. Розглядаються базові поняття та принципи побудови сучасних комп'ютерних мереж; новітні та перспективні розробки мережних технологій; сучасний стан розвитку технологій каналів зв'язку для комп'ютерних мереж; нові телекомунікаційні протоколи; мережні технології обробки інформації; сучасні засоби керування комп'ютерними мережами; управління мережним обладнанням та інформаційними ресурсами мереж. Дисципліна відповідає курсу «CCNA: Introduction to Networks» мережної академії Cisco [1].

Мета дисципліни – набуття студентами теоретичних знань та практичних навичок, що необхідні для проєктування, побудови та підтримки комп'ютерних мереж і вміння користуватись мережними технологіями.

Завдання (навчальні цілі): формування у студентів здатностей проєктування, побудови та тестування локальних комп'ютерних мереж; застосування глобальних зв'язків, здійснення моніторингу роботи окремих елементів комп'ютерної мережі та перевірки їх працездатності.

Методичні вказівки містять теоретичні відомості, практичні завдання, лабораторні роботи та питання для самоперевірки. Оскільки дисципліна носить прикладний характер, саме лабораторним роботам приділяється особлива увага. Під час вивчення дисципліни студенти мають здобути навички безпечної роботи в комп'ютерних мережах, системного аналізу об'єктів проєктування та обґрунтування вибору способів передачі інформації в мережах, організовувати взаємодію між апаратними і програмними засобами з використанням комунікаційних протоколів, використовувати можливості мережних систем.

Використання методичних вказівок пропонується разом з електронним курсом «CCNA: Introduction to Networks» мережної академії Cisco. В них детально розглядаються обрані найскладніші теми та лабораторні роботи, які є обов'язковими до виконання відповідно до робочої програми навчальної дисципліни, що полегшить студентам як засвоєння дисципліни так і підготовку до сертифікації.

1 ЦІЛІ І ЗАДАЧІ МЕТОДИЧНИХ ВКАЗІВОК

Теоретичний матеріал та лабораторні роботи дисципліни «Вступ до мереж» є ключовим елементом навчання, вони дозволяють студентам застосовувати отримані теоретичні знання на практиці. До основних цілей виконання лабораторних робіт відноситься розвиток практичних навичок, розуміння ключових технологій, підготовка до вирішення реальних завдань, а також підготовка до сертифікації CCNA.

При виконанні лабораторних робіт студенти можуть використовувати як реальні комутатори та маршрутизатори, так і симулятор комп'ютерних мереж Cisco Packet Tracer.

Серед задач виконання лабораторних робіт можна виділити опанування студентами навичок працювати з реальними або віртуальними мережевими пристроями (комутаторами, маршрутизаторами та кінцевими пристроями), вміння налаштовувати мережеві пристрої через інтерфейс командного рядку (CLI, Command-Line Interface), поглиблене розуміння принципів Ethernet, IPv4, IPv6, ARP, Neighbor Discovery, ICMP та інших мережевих протоколів, їх налаштування та оптимізацію.

Для підготовки студентів до вирішення реальних завдань застосовуються реалістичні сценарії налаштування та усунення несправностей у мережах, що дозволяє сформувати навички аналізу вимог до мережі, формування технічного завдання, проєктування та налаштування комп'ютерних мереж невеликого розміру. Також використання лабораторних завдань важливе для глибшого розуміння питань, які зустрічаються на сертифікаційному іспиті за програмою 200-301 Cisco Certified Network Associate.

Виконання лабораторних робіт допомагає сформувати комплексний підхід до створення, налаштування та управління мережами, що є важливою складовою професійної підготовки майбутніх фахівців.

2 ОФОРМЛЕННЯ ЗВІТІВ З ЛАБОРАТОРНИХ РОБІТ

Звіт з виконання лабораторних робіт оформлюється відповідно до ДСТУ 3008:1995 [3]. Друкується на одному боці аркуша офісного паперу формату А4 (210 х 297 мм) книжкової орієнтації. Текст форматується шрифтом Times New Roman, 14 кеглем. Інтервал перед та після абзацу 0 пт, міжрядковий інтервал 1,5 рядка, відступ першого рядку абзаців ліворуч 1,25 см, вирівнювання рівномірне (по ширині). Поля: ліве 2,5 см, праве 1,5 см, верхнє та нижнє по 2 см. До звіту додається титульний лист, оформлений відповідно до додатку А.

2.1 Заголовки

Заголовки підрозділів, пунктів та підпунктів друкуються в нижньому регістрі (крім першої літери), вирівнювання рівномірне без відступів. Такі заголовки на нову сторінку не переносяться, перед ними встановлюється інтервал 18 пт.

Всі заголовки форматуються напівжирним шрифтом, після них встановлюється інтервал 12 пт.

2.2 Нумерація

Нумерацію сторінок, розділів, підрозділів, пунктів, підпунктів, рисунків, таблиць та формул здійснюють за допомогою арабських цифр без використання знаку «№». Першою сторінкою звіту є титульна сторінка, яка включається до загальної нумерації сторінок, але номер на ній не зазначається. Номер другої та всіх наступних сторінок проставляється у нижньому правому куті.

Номер зазначається за допомогою арабських цифр, починаючи з цифри «1». Підрозділи, пункти та підпункти нумеруються у межах кожного розділу, використовуючи номер розділу і порядковий номер підрозділу, між якими ставиться крапка. Наприклад, «2.3 Третій підрозділ другого розділу» або «3.5.1» (перший пункт п’ятого підрозділу третього розділу). Назва розділів зазначається великими літерами, а підрозділів, пунктів та підпунктів маленькими літерами починаючи з великої через пробіл після номера.

2.3 Ілюстрації

Ілюстрації (схеми, графіки, скріншоти тощо) розміщуються в роботі безпосередньо після абзацу, де міститься перше посилання на них. Якщо їх так неможливо розмістити, тоді вони переносяться на початок наступної сторінки. Ілюстрації, що займають більше 2/3 сторінки, розміщують у додатках. На всі ілюстрації в тексті мають міститись посилання.

Пояснювальний текст, номер ілюстрації, та її назва розміщуються безпосередньо під самою ілюстрацією з вирівнюванням по центру. Ілюстрації позначають словом «Рисинок» і нумерують послідовно в межах розділу. Номер ілюстрації має складатися з номера розділу і порядкового номера ілюстрації, між якими ставиться крапка, після номера крапка не ставиться. Після номер через дефіс з великої літери пишуться назва ілюстрації. Наприклад, «Рисунок 1.2 – Приклад ілюстрації» (другий рисунок першого розділу).

Ілюстрації, що розміщуються в додатках, позначають за допомогою арабських цифр з додаванням перед цифрою позначення додатка, наприклад, «Рисунок А.1» (перший рисунок додатку А).

2.4 Таблиці

Таблиці, як і рисунки, розміщуються в роботі безпосередньо після абзацу, де міститься перше посилання на них. Якщо їх так неможливо розмістити, тоді вони переносяться на початок наступної сторінки. Таблиці, що займають більше 2/3 сторінки, розміщують у додатках. На всі таблиці в тексті мають міститись посилання.

Таблиці нумерують послідовно у межах розділу. Безпосередньо над таблицею розміщують слово «Таблиця ___» із зазначенням її номера, який складається з номера розділу і порядкового номера таблиці, між якими ставиться крапка, наприклад: «Таблиця 2.3» (третя таблиця другого розділу). Вирівнювання здійснюється по лівому краю. В цьому ж рядку через дефіс зазначається назва таблиці.

Якщо таблицю неможливо розмістити на одній сторінці, її ділять на частини, які розміщують на сусідніх сторінках, при цьому в кожній частині таблиці повторюють її заголовок («шапку»). Над першою частиною таблиці пишуть слово «Таблиця» із зазначенням відповідного номера та назви, а над наступними частинами «Продовження таблиці ___» або «Кінець таблиці ___» із зазначенням її номера але без повторення назви.

Таблиці, що розміщують у додатках, позначають арабськими цифрами з додаванням перед цифрою позначення додатка, наприклад, «Таблиця А.1».

Заголовки стовпців і рядків таблиці слід друкувати з великої літери, підзаголовки – з малої, якщо вони є продовженням заголовку, або з великої, якщо вони мають самостійне значення. У кінці заголовків і підзаголовків таблиць крапки не ставляться.

2.5 Формули

Рівняння та формули розміщуються безпосередньо після згадування їх у тексті. Вони розміщуються посередині рядка та нумеруються арабськими цифрами. Між текстом і формулою зверху та знизу слід зробити відступи 12 пунктів.

Літери та знаки повинні бути такого розміру: великі літери та цифри – 16, малі – 14, показники степенів та індексів над літерами та під літерами – 8. Номер формули наводиться праворуч від самої формули в круглих дужках та складається з номеру розділу та порядкового номеру самої формули у цьому розділі, розділеного крапкою. При посиланні в тексті на формулу необхідно вказати її повний номер в дужках, наприклад, «у формулі (3.1)». Після формули пишуть слово «де» і розшифровують позначення словами в такій послідовності, в якій вони подані у формулі. Після слова «де» двокрапка не ставиться.

Наприклад: Кількість вузлів в підмережі розраховується за формулою (2.5.1).

$$i = 2^n - 2 \qquad (2.5.1)$$

де i – максимальна кількість вузлів в підмережі, n – кількість бітів, що залишилась у вузловій частині IP-адреси.

2.6 Інформаційні джерела

Список використаних джерел згідно з наказом Міністерства освіти і науки України від 12 січня 2017 року № 40 оформлюється відповідно до Національного стандарту України 8302:2015 [4] або одного зі стилів, віднесених до рекомендованого переліку стилів оформлення списку наукових публікацій, які є загальновживаними в зарубіжній практиці оформлення наукових робіт. Джерела в списку упорядковується, як правило, або за абеткою, або відповідно до черговості першого згадування джерел у тексті роботи.

Посилання на джерела інформації у тексті роботи слід зазначати в квадратних дужках у вигляді порядкового номера інформаційного джерела у списку використаних джерел, наведеному в кінці роботи, а також номера сторінки в самому джерелі. Наприклад: [8, с. 12–14].

Посилання на нормативні акти слід вказувати із зазначенням повної назви акту, відповідного розділу або статті. Якщо в тексті роботи наведено всі реквізити нормативного акту, а саме: назву, вид, номер та дату прийняття, то посилання в квадратних дужках на нормативний акт можна не наводити, але у переліку використаних джерел його все рівно необхідно зазначити. Забороняється дослівне списування тексту з літературного джерела. Якщо за текстом необхідно навести цитату, вона береться в лапки з подальшим посиланням на відповідне джерело.

2.7 Додатки

Додатки включаються до звіту як доповнення або роз’яснення основного тексту, їх розміщують у порядку появи посилань на них в основному тексті звіту. Додатки можуть містити допоміжні матеріали, таблиці, рисунки, розрахунки, вміст файлів конфігурації. Посилання на додатки є обов’язковим у текстовій частині звіту. Перед додатками наводиться чистий аркуш зі словом «ДОДАТКИ»

у верхньому регістрі посередині сторінки. Кожен додаток починається з нової сторінки. Заголовок додатку друкується малими літерами з першою великою літерою, вирівнювання по центру. Додатки нумеруються великими літерами української абетки, починаючи з літери А, за винятком літер Ґ, Є, З, І, Ї, Й, О, Ч, Ь. Наприклад, «Додаток А». В наступному рядку вказується назва додатку, вирівнювання також по центру.

Додатки можуть наводитись як в книжковій, так і в альбомній орієнтації.

3 РЕКОМЕНДАЦІЇ ДО ПІДГОТОВКИ ЗВІТІВ ТА ЗАХИСТУ ЛАБОРАТОРНИХ РОБІТ

3.1 Підготовка звітів

При підготовці звіту з виконання лабораторної роботи студент повинен дотримуватися певних вимог:

- звіт має бути написаний державною мовою;
- кожен студент виконує ЛР самостійно та індивідуально;
- оформлення звіту з ЛР має відповідати вимогам, що ставляться до робіт, поданих до друку [3];
- при написанні звіту з ЛР студент повинен посилатися на автора та джерело, у випадку запозичення матеріалів.

Неодмінною умовою якісного виконання ЛР є ґрунтовне ознайомлення з інформаційними джерелами за визначеною темою. Після ґрунтовного опрацювання літературних джерел і з'ясування теоретичної бази дослідження студент приступає до виконання лабораторної роботи за допомогою програми моделювання Cisco Packet Tracer.

3.2 Підготовка до захисту

Роздрукований звіт з виконання лабораторної роботи разом із додатками зшивають за допомогою швидкозшивачу або в інший спосіб. Оформлений належним чином звіт підписується автором.

Відсутність звіту з виконання лабораторної роботи, невідповідність оформлення вимогам тягне за собою недопуск студента до захисту лабораторної роботи.

3.3 Захист лабораторних робіт

Захист лабораторних робіт студентами відбувається згідно з розкладом занять. Під час захисту студентові задаються як теоретичні питання та і практичні завдання з усіх розділів, які входять до відповідного модуля.

3.4 Оцінювання лабораторних робіт

Лабораторна робота оцінюється за стобальною системою. Оцінка за лабораторну роботу входить до загальної оцінки за дисципліну з ваговим коефіцієнтом відповідно до робочої програми. Критерії оцінювання лабораторної роботи представлені в таблицях 3.4.1 та 3.4.2:

Таблиця 3.4.1 – Розподіл балів

Назва елемента роботи	Максимальна кількість балів
Теоретичні питання	40
Практичні завдання	50
Загальне оформлення звіту	10
Всього:	100

Таблиця 3.4.2 – Шкала оцінювання кожного елемента роботи

% від максимальної кількості балів	Опис
100	бездоганно
90-99	з незначним зауваження
80-89	з незначними зауваженнями
75-79	із зауваженням
65-74	із суттєвим зауваженням
60-64	із суттєвими зауваженнями

4 ЛАБОРАТОРНІ РОБОТИ

Лабораторна робота 1

Взаємодія з операційною системою Cisco IOS

Мета: Навчитись здійснювати навігацію по операційній системі Cisco IOS за допомогою командного рядку, переходити між різними режимами та використовувати довідку.

Завдання:
1. Отримання доступ до командного рядку.
2. Дослідження переходу між різними режимами.
3. Отримання контекстної довідки.
4. Зміна назви комутатора.

Необхідні ресурси: комп'ютер, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель та будь-який з комутаторів Cisco: Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо.

Теоретичні відомості

Для отримання доступу до командного рядку (command line interface, CLI) операційної системи комутатора Cisco IOS може використовуватись підключення через консольний порт або один з протоколів віддаленого доступу – SSH або Telnet. Протокол Telnet пересилає дані через мережу без шифрування у відкритому вигляді, тому він вважається застарілим і його використання допускається виключно в навчальному середовищі. Також потрібна програма емуляції терміналу. Для початкового налаштування або для аварійного відновлення роботи комутатора використовується виключно консольне підключення.

Одразу після отримання доступу до CLI на екран виведеться запрошення командного рядку. Наприклад, воно може мати такий вигляд: «**Switch>**», де «Switch» це назва комутатора, а символ «>» вказує на користувацький режим, який ще називають режимом «Read only». В цьому режимі неможливо змінювати налаштування комутатора, а для перегляду доступна обмежена кількість

параметрів. Наступний режим, в який можна перейти з користувацького режиму, носить назву привілейований режим. Його ознакою є символ «#» в кінці запрошення командного рядку. Для переходу в цей режим застосовується команда **enable**. Відповідно до найменування цієї команди привілейований режим також іноді називають режимом enable. В режимі enable можна переглядати будь-які параметри роботи комутатора, а також працювати з файловими системами – файлами конфігурації, операційної системи, бази даних VLAN тощо. Можна переглядати файли та папки, копіювати, перейменовувати та видаляти їх. Щоб повернутись в користувацький режим застосовується команда **disable**. Також з привілейованого режиму можна перейти в режим глобальної конфігурації. Це робиться за допомогою команди **configure terminal**. Ознакою режиму глобальної конфігурації є слово «config» яке додається в дужках після назви комутатора. Таким чином запрошення командного рядка в режимі глобальної конфігурації може виглядати так: «**Switch(config)#**». В режимі глобальної конфігурації можна вносити зміни в конфігурацію комутатора, які глобально впливають на його роботу: налаштувати назву пристрою, системний час, банер тощо. З режиму глобальної конфігурації можна перейти в один з режимів налаштування конкретної складової комутатора – інтерфейсу, лінії зв'язку, протоколу, віртуальної локальної мережі тощо. Для повернення в режим глобальної конфігурації застосовується команда **exit**. Повторне введення команди **exit** призведе до виходу в привілейований режим. Також для цього можна застосувати комбінацію клавіш «Ctrl»+«Z». Приклад перемикання між режимами наведено на рисунку 4.1.1.

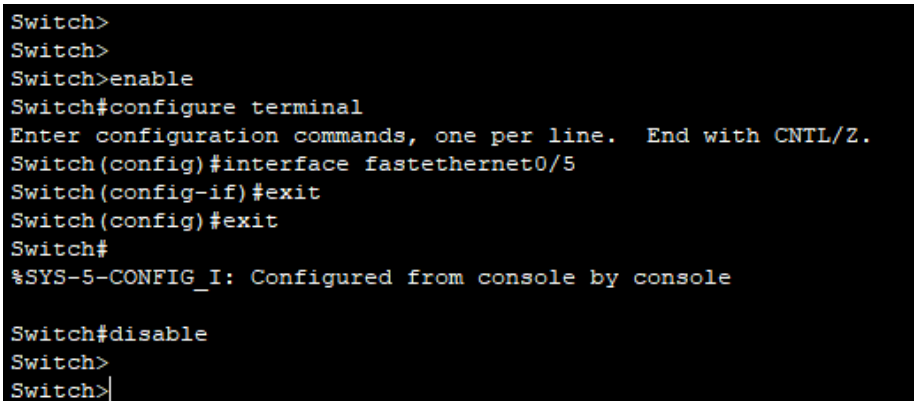

Рисунок 4.1.1 – Перехід між режимам Cisco IOS.

Налаштовувати мережний пристрій за допомогою командного рядку може бути складною задачею, оскільки необхідно знати велику кількість команд та їх синтаксис. Для полегшення цієї задачі в операційній системі Cisco IOS є вбудована контекстна довідка. Довідка називається контекстною, оскільки її вміст залежить від того, при яких умовах її викликали, тобто від контексту. Отримати довідку можна за допомогою натискання клавіші «?» на клавіатурі, при цьому довідка виводиться одразу після натискання, «Enter» натискати не потрібно. Якщо на екрані виведено запрошення командного рядку і жодного символу не було введено з клавіатури, контекстна довідка виведе перелік команд, доступних в поточному режимі. Якщо ввести один або декілька символів, а потім натиснути клавішу «?», контекстна довідка покаже перелік команд, що починаються на введені символи. Якщо ввести команду, пробіл, а потім клавішу «?», контекстна довідка виведе на екран можливі параметри для введеної команди. Якщо параметри не передбачені синтаксисом введеної команди, довідка відобразить текст «<cr>», що означає необхідність завершити введення команди натискання клавіші «Enter». Використання контекстної довідки наведено на рисунку 4.1.2.

```
Switch>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Switch>p?
ping
Switch>ping ?
  WORD  Ping destination address or hostname
Switch>ping 172.17.57.23 ?
  <cr>
Switch>ping 172.17.57.23
```

Рисунок 4.1.2 – Використання контекстної довідки.

Будь-яка інформація про комутатор та його стан виводиться на екран за допомогою команди **show** та відповідних параметрів або ключових слів. Команду show необхідно виконувати в привілейованому режимі. За замовченням, інформація виводиться на екран порціями по 24 рядки, після яких виводиться рядок с текстом «--More--» і виведення призупиняється (рис. 4.1.3).

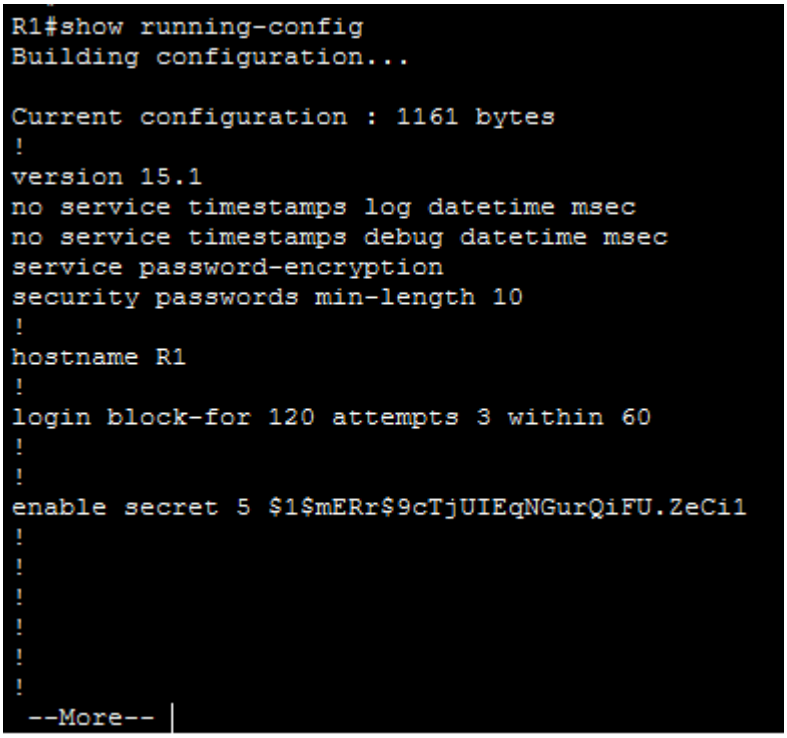

Рисунок 4.1.3 – Призупинення виведення після заповнення екрану.

Цей рядок вказує на те, що у команди show є ще текст для виводу на екран. В такій ситуації можна натиснути на клавіатурі клавішу «Space bar» для виведення ще однієї порції з 24 рядків, «Enter» для виведення ще одного рядка або будь-яку іншу клавішу для переривання виведення інформації на екран. Якщо на екран не було виведено текст «--More--», це означає, що вся інформація вже відображена на екрані. Є можливість змінити кількість рядків, що виводиться до призупинення. Це можна зробити за допомогою команди **terminal length *number***, де number – число в діапазоні від 0 до 512, яке вказує кількість рядків. Якщо параметр number дорівнює нулю, відбуватиметься безперервне виведення інформації на екран.

Хід роботи

Завдання 1. Отримайте доступ до командного рядку.

Для підключення через консольний порт в першу чергу необхідно забезпечити фізичне з’єднання мережного пристрою з комп’ютером. Для цього використовується консольний кабель, зображений на рисунку 4.1.4.

Рисунок 4.1.4 – Консольний кабель Cisco.

З одного кінця кабелю знаходиться конектор RJ-45 8P8C, який необхідно приєднати до консольного порту мережного пристрою, з іншого кінця конектор DB-9, призначений для з’єднання з COM (RS232) портом комп’ютера. Якщо комп’ютер не обладнаний COM портом, необхідно використати конвертер USB to RS232.

ВАЖЛИВО! Пам’ятайте, стандарт RS232 НЕ ПІДТРИМУЄ «гаряче» під’єднання пристроїв. Тому завжди вимикайте як комп’ютер, так і комутатор перед підключенням або від’єднанням кабелю. Це запобігає появі електричних імпульсів, які можуть пошкодити порт комп’ютера та мережного пристрою. Ніколи не підключайте та не від’єднуйте пристрій, коли порт активний, оскільки це може призвести до пошкодження обладнання! Перед підключенням торкніться металевої поверхні або використовуйте заземлений браслет, щоб

уникнути пошкодження портів через статичну електрику. Також ніколи не під’єднуйте кінець консольного кабелю з конектором RJ-45 8P8C в Ethernet порт мережного пристрою або комп’ютера.

Запустіть програму емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal) та встановіть такі параметри підключення:

– Швидкість: 9600 bps.

– Біт даних: 8.

– Парність: None.

– Стоп-біти: 1.

– Контроль потоку: None.

Ввімкніть комутатор та дочекайтеся завантаження операційної системи Cisco IOS. У терміналі з’явиться повідомлення «Press RETURN to get started!» (рис. 4.1.5).

```
cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 65536K bytes of memory.
Processor board ID FOC1010X104
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:90:0C:88:1E:E5
Motherboard assembly number     : 73-10390-03
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC10093R12
Power supply serial number      : AZS1007032H
Model revision number           : B0
Motherboard revision number     : B0
Model number                    : WS-C2960-24TT-L
System serial number            : FOC1010X104
Top Assembly Part Number        : 800-27221-02
Top Assembly Revision Number    : A0
Version ID                      : V02
CLEI Code Number                : COM3L00BRA
Hardware Board Revision Number  : 0x01

Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!
```

Рисунок 4.1.5 – Операційна система Cisco IOS завантажилась та готова до взаємодії із користувачем.

Завдання 2. Дослідження переходу між різними режимами.

Після під'єднання до командного рядку ви побачите запрошення, що складається зі слова «Switch», яке є ім'ям комутатора за замовченням, та символу «>» (закрита трикутна дужка), який говорить про те, що ви перебуваєте в користувацькому режимі.

В користувацькому режимі доступна незначна кількість команд для моніторингу роботи комутатора та перевірки зв'язку. Будь-які зміни в налаштування в цьому режимі робити неможливо.

З користувацького режиму можна перейти до привілейованого режиму. Це робиться за допомогою команди **enable.** Введення будь-якої команди закінчується натисканням клавіші «Enter» на клавіатурі. Відповідно до цієї команди привілейований режим іноді також називають «режимом enable». Ознака привілейованого режиму – символ «#», що стоїть в запрошенні командного рядку після назви комутатора. Повернутись з привілейованого режиму до користувацького можна виконавши команду **disable** (рис. 4.1.6). В привілейованому режимі доступні усі команди для моніторингу роботи комутатора, перевірки зв'язку, а також роботи з файловою системою. Найчастіше в привілейованому режимі застосовують команду **show** для перегляду різних аспектів роботи комутатора та команди для перегляду, копіювання та видалення файлів конфігурації.

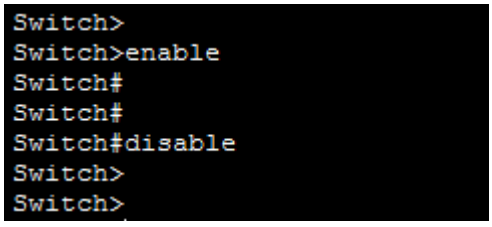

Рисунок 4.1.6 – Перехід між користувацьким та привілейованим режимами.

Для будь-яких змін в конфігурації комутатора необхідно перейти в режим глобальної конфігурації командою **configure terminal**. Після зміни режиму в запрошенні командного рядку після назви пристрою в круглих дужках буде зазначено слово «(config)». В режимі глобальної конфігурації можна робити зміни, що впливають на роботу усього пристрою в цілому. Також з режиму

глобальної конфігурації можна перейти в якійсь зі спеціалізованих підрежимів налаштування певного інтерфейсу, лінії зв'язку, функції чи протоколу. Для повернення зі спеціалізованого підрежиму в режим глобальної конфігурації потрібно ввести команду **exit**. Повторне введення цієї команди призведе до повернення в привілейований режим (рис. 4.1.7).

```
Switch>
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
Switch>
Switch>
```

Рисунок 4.1.7 – Перехід між режимами глобальної конфігурації та спеціалізованими підрежимами.

Здійснити перехід з спеціалізованого режиму конфігурації одразу в привілейований режим можна командою **end**. Також для цього можна скористатись комбінацією клавіш «Ctrl» + «Z» (рис. 4.1.8).

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
Switch>
```

Рисунок 4.1.8 – Перехід з режиму конфігурації інтерфейсу до привілейованого режиму.

В операційній системі Cisco IOS реалізована можливість вводити команди в скороченій формі. Наприклад, команду **enable** можна скоротити до **enabl**, **enab**, **ena** або навіть **en**. Натомість, її не можна скоротити до **e**. На скільки ж можна скорочувати команди? Скорочувати команди можна до такої мінімальної кількості літер, яка дозволить командному інтерпретатору унікально

ідентифікувати цю команду. Зокрема, в користувацькому режимі є дві команди, що починаються на літеру «е»: **enable** та **exit**. При спробі скоротити команду **enable** до однієї літери операційна система «не зрозуміє» яку саме команду ви намагаєтесь ввести. Натомість, скорочення **en** дозволить однозначно ідентифікувати тільки одну команду – **enable**. Приклад використання скорочених команд ви можете побачити на рисунку 4.1.9. Ці скорочення є повним відповідником команд в повному форматі, наведених на рисунку 4.1.8.

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#li c 0
Switch(config-line)#exi
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disa
Switch>
```

Рисунок 4.1.9 – Приклад використання команд в скороченому вигляді.

Завдання 3. Отримання контекстної довідки.

Робота з інтерфейсом командного рядку може видатись доволі складною, особливо на початковому етапі знайомства з операційною системою Cisco IOS. Насправді, тримати в пам’яті велику кількість команд немає потреби, оскільки в командному рядку є контекстна довідка, яка завжди може підказати, які команди доступні в тому чи іншому режимі, а також які параметри та ключові слова необхідно застосувати з тією чи іншою командою. Довідка називається «контекстною», оскільки інформація, що виводиться на екран залежить від контексту, тобто, від поточного режиму та того тексту, який ви ввели в поточній команді до моменту виклику довідки. Для отримання довідки необхідно натиснути клавішу «?» на клавіатурі, при цьому «Enter» натискати не потрібно.

Спробуйте, перебуваючи в користувацькому режимі отримати контекстну довідку. На екран буде виведено близько п’ятнадцяти команд, доступних в цьому режимі. Введіть букву «t» та ще раз натисніть знак питання на клавіатурі. Цього

разу на екран буде виведено тільки команди, що починаються на відповідну літеру. Скільки таких команд?

Тепер введіть в командному рядку «telnet», поставити пробіл та натисніть знак питання. На екран виведеться інформація про параметри команди telnet (рис. 4.1.10).

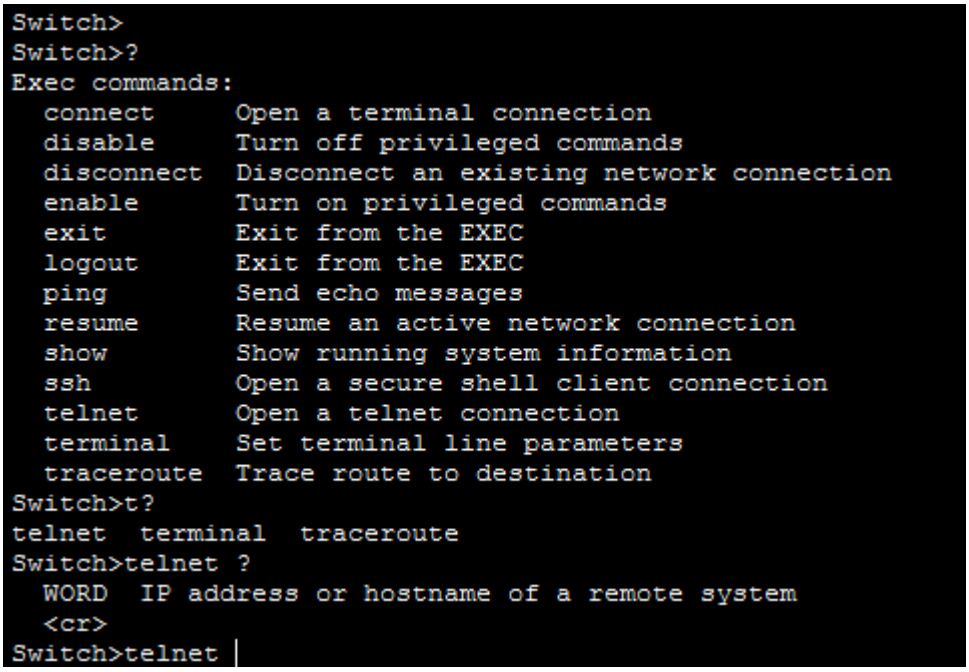

Рисунок 4.1.10 – Приклад використання контекстної довідки.

Завдання 4. Зміна назви комутатора.

Для зміни назви пристрою використовується команда **hostname** *ім'я_пристрою*. Команда вводиться в режимі глобальної конфігурації. Для скасування будь-якої команди необхідно повторно ввести цю команду з приставкою **no**. Зокрема, введення команди **no hostname** повертає комутатору назву за замовченням «Switch» (рис. 4.1.11).

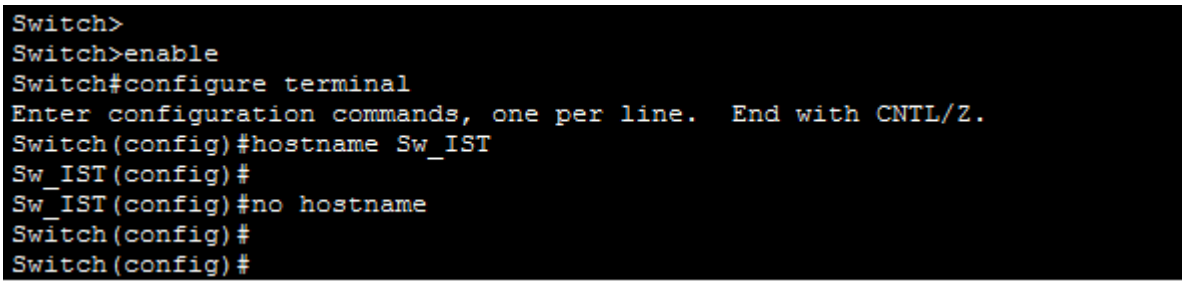

Рисунок 4.1.11 – Налаштування назви пристрою.

Питання для самоперевірки

1. Який вигляд має запрошення командного рядку в користувацькому режимі?
2. Яка команда використовується для переходу з користувацького режиму до привілейованого?
3. Який вигляд має запрошення командного рядку в привілейованому режимі?
4. Яка команда використовується для повернення з привілейованого режиму до користувацького?
5. Як перейти з режиму глобальної конфігурації до режиму налаштування інтерфейсу?
6. За допомогою якої команди можна вийти на один рівень з поточного підрежиму конфігурації?
7. Якою командою можна вийти з будь-якого підрежиму конфігурації одразу до привілейованого режиму?
8. Яка команда використовується для зміни назви пристрою?
9. В якому режимі потрібно перебувати для використання команди зміни назви пристрою?
10. Який результат ви отримаєте після виконання команди «hostname Sw1»?
11. Як отримати перелік усіх доступних команд у поточному режимі?
12. Як дізнатися про синтаксис конкретної команди, наприклад команди «show»?
13. Чим відрізняється довідка в привілейованому режимі від довідки у режимі конфігурації інтерфейсу?
14. Яку команду потрібно виконати, щоб перейти до режиму налаштування інтерфейсу GigabitEthernet0/0?
15. Як зміниться вигляд запрошення командного рядку після виконання команди «hostname IST-11»?
16. В чому різниця між командами «exit» та «end».

Лабораторна робота 2

Початкове налаштування комутатора та кінцевого пристрою

Мета: Навчитись здійснювати налаштування за допомогою командного рядку базових параметрів комутатора та кінцевого пристрою.

Завдання: 1. Отримання доступ до командного рядку.

2. Налаштування базових параметрів комутатора.

3. Перевірка параметрів комутатора.

Необхідні ресурси: комп'ютер з програмою емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель, Ethernet кабель та будь-який з комутаторів Cisco: Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо.

Теоретичні відомості

Налаштування базових параметрів комутатора здійснюється після першого запуску нового пристрою або після очищення конфігурації. Мета початкового налаштування – уможливлення віддаленого керування та забезпечення захисту.

До базових відносяться наступні параметри комутатора: ім'я пристрою, пароль для доступу до привілейованого режиму, пароль для консольного доступу, пароль для віддаленого доступу, банерне повідомлення, IP-адреса керування на інтерфейсі VLAN 1, IP-адреса шлюзу за замовчуванням. Також опціонально може бути налаштований час та часово зона. Налаштування IP-адреси керування на інтерфейсі VLAN 1, пароль для консольного доступу, а також пароль для віддаленого доступу здійснюються в спеціалізованих підрежимах, налаштування часу в привілейованому режимі, усі інші налаштування в режимі глобальною конфігурації.

Для встановлення імені пристрою застосовується команда **hostname** *name*, де *name* – нове ім'я пристрою. Одразу після введення команди hostname змінеться запрошення командного рядку, оскільки ім'я пристрою – одна з його

складових. Для того щоб повернутись до імені пристрою за замовченням, необхідно ввести команду **no hostname**.

Для встановлення пароля для доступу до привілейованого режиму використовується команда **enable secret** *password*, де *password* – пароль. Надійний пароль має складатись з великих і маленьких літер, цифр та спеціальних знаків та мати довжину не менше 10 символів. В лабораторних умовах допускається використання паролів **cisco** та **class**.

Для налаштування банерного повідомлення застосовується команда **banner motd #** *message #,* де *message* – текст повідомлення, що виводитиметься на екран при спробі доєднатись до комутатора. Перед початком та після закінчення тексту повідомлення мають бути однакові символи-обмежувачі. В якості символу-обмежувача може бути будь-який символ, що не міститься в тексті самого повідомлення. Повідомлення може складатись з одного або декількох рядків тексту.

Налаштування шлюзу за замовчуванням здійснюється для уможливлення керування комутатором з віддаленої мережі. Для цього застосовується команда **ip default-gateway** *ip_address*, де – *ip_address* – адреса шлюзу за замовченням. Як правило, в якості шлюзу за замовченням використовується адреса інтерфейсу маршрутизатора, під'єднаного до поточної мережі.

Для налаштування часу використовується команда **clock set** *time date*, де *time* – час, *date* – дата. Час налаштовується в привілейованому режимі! За замовченням використовується показник часу за Грінвічем, тобто за нульовим меридіаном. Для налаштування потрібної часової зони застосовується команда **clock timezone** *timezone offset*, де *timezone* – назва часової зони, може бути будь-який текст, а *offset* – зміщення. Налаштування часової зони здійснюється в режимі глобальної конфігурації.

Для налаштування пароля для консольного доступу необхідно перейти у відповідний режим. Для цього використовується команда **line console 0**. Після переходу в режим налаштування консольного доступу запрошення командного рядку змінить свій вигляд (рис. 4.2.1).

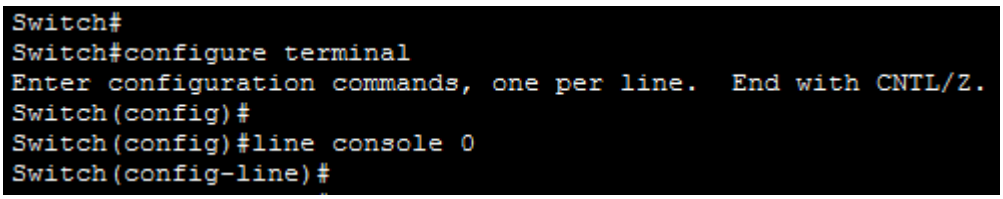

Рисунок 4.2.1 – перехід в режим налаштування консольного доступу.

В режимі налаштування консольного доступу застосовують команду **password** *password_text*, де *password_text* – пароль. Також необхідно ввести команду **login** для обов'язкової автентифікації користувачів.

Для налаштування пароля для віддаленого доступу необхідно перейти у відповідний режим. Для цього використовується команда **line vty** *first_line_number last_line_number*, де *first_line_number* – номер першої лінії зв'язку, дорівнює нулю, *last_line_number* – номер останньої лінії зв'язку, дізнатись його можна за допомогою контекстної довідки. Після переходу в режим налаштування віддаленого доступу запрошення командного рядку змінить свій вигляд (рис. 4.2.2).

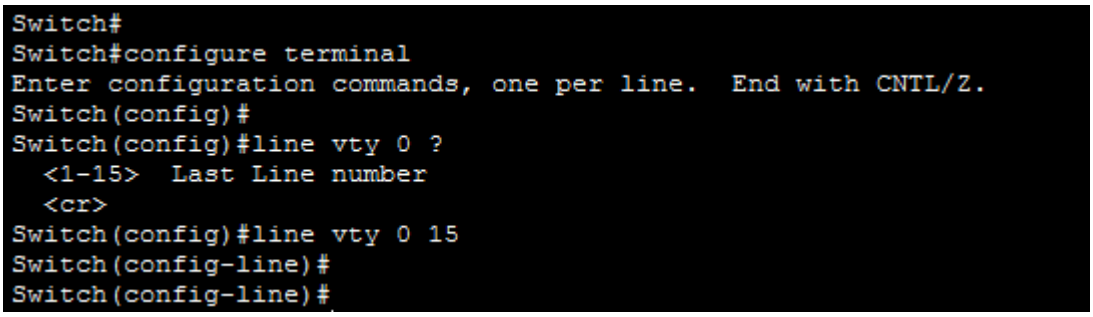

Рисунок 4.2.2 – перехід в режим налаштування віддаленого доступу.

В режимі налаштування віддаленого доступу застосовують команду **password** *password_text*, де *password_text* – пароль. Команду **login** необхідно застосувати для обов'язкової автентифікації користувачів. Також для визначення дозволеного для віддаленого під'єднання протоколу необхідно ввести команду **transport input** *protocol*, де *protocol* – дозволений протокол. В лабораторних умовах це може бути **telnet**, в реальних умовах тільки **ssh**.

Для віддаленого під'єднання на комутаторі має бути налаштована IP-адреса. Оскільки комутатор – це пристрій, що відноситься до другого рівня моделі OSI, він не підтримує IP-адресацію на фізичних інтерфейсах. Для

уможливлення віддаленого під’єднання використовуються віртуальні інтерфейси комутатора (SVI – Switch Virtual Interface). За замовченням використовується інтерфейс VLAN 1. Для його налаштування необхідно перейти у відповідний режим. Для цього використовується команда **interface vlan** *n_int*, де *n_int* – номер vlan, для якої налаштовується інтерфейс. Після переходу в режим налаштування інтерфейсу SVI запрошення командного рядку змінить свій вигляд (рис. 4.2.3).

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#
```

Рисунок 4.2.3 – перехід в режим налаштування інтерфейсі SVI.

Для налаштування IP-адреси на інтерфейсі застосовується команд **ip address** *ip_address subnet_mask*, де *ip_address* – IP-адреса інтерфейсу, *subnet_mask* – маска підмережі. Інтерфейс SVI за замовченням перебуває у вимкненому стані. Активувати його можна командою **no shutdown**.

Для перевірки налаштувань застосовують команди **show ip interface brief, show running-config, show clock**. Для перевірки зв’язку застосовують команду **ping**.

Хід роботи

Завдання 1. Отримайте доступ до командного рядку.

З'єднайте комп'ютер з комутатором за допомогою консольного кабелю. Детально процес під'єднання описаний в лабораторній роботі №1 Також З'єднайте Ethernet порт комп'ютера з будь-яким Ethernet портом комутатора. Хоча налаштування комутатора буде здійснюватися через консольний порт, Ethernet з'єднання використовуватиметься для перевірки. В результаті ви повинні отримати топологію, подібну до рисунку 4.2.4.

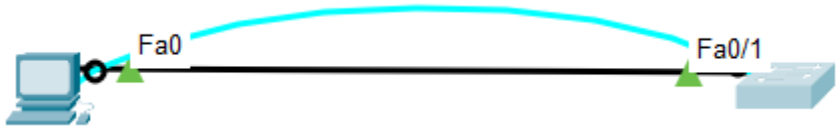

Рисунок 4.2.4 – з'єднання комп'ютера з комутатором за допомогою консольного та Ethernet кабелів.

Завдання 2. Налаштування базових параметрів комутатора.

Після встановлення сеансу зв'язку між комп'ютером та комутатором, ви потрапите в користувацький режим. Для налаштування комутатора необхідно перейти спочатку в привілейований режим, а потім в режим глобальної конфігурації (рис. 4.2.5).

```
Switch>
Switch>
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
```

Рисунок 4.2.5 – перехід в режим глобальної конфігурації.

Змінимо ім'я комутатора. Одразу після налаштування нового імені запрошення командного рядку змінить свій вигляд (рис. 4.2.6).

```
Switch(config)#
Switch(config)#hostname Sw1
Sw1(config)#
```

Рисунок 4.2.6 – Зміна імені комутатора.

Далі вимкнемо функцію DNS-пошуку. За замовчуванням операційна система Cisco IOS намагається знайти введену невідому команду як ім’я хоста, яке потрібно розв’язати через DNS. Тобто, якщо ви випадково введете неправильну команду (наприклад, **shwo** замість **show**), комутатор спробує знайти хост із таким іменем, що призводить до затримки кілька секунд. Після виконання команди **no ip domain-lookup** комутатор не намагатиметься виконувати DNS-запит для невідомих команд і помилки вводитимуться миттєво, без затримки. Вимкнення автоматичний DNS-пошук наведено на рисунку 4.2.7.

```
Sw1(config)#
Sw1(config)#no ip domain-lookup
Sw1(config)#
Sw1(config)#
```

Рисунок 4.2.7 – Зміна імені комутатора.

ВАЖЛИВО! Зверніть увагу, в результаті виконання цієї команди на екран нічого не було виведено. У відповідь на деякі правильно введені команди операційна система виводить інформаційні повідомлення, а не деякі ні. Якщо ж команду було введене не вірно, командний інтерпретатор *обов’язково* виведе на екран повідомлення про помилку.

Налаштуємо часовий пояс, системний час та дату. Для цього застосовуємо команди **clock timezone** та **clock set** (рис. 4.2.8).

```
Sw1#
Sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#clock timezone Kyiv 2
Sw1(config)#exit
Sw1#clock set 20:12:00 2 nov 2025
Sw1#
```

Рисунок 4.2.8 – Налаштування часового поясу, системного часу та дати.

Перейдемо до налаштування паролів. В першу чергу налаштуємо пароль для переходу в привілейований режим. В якості пароля будемо використовувати слово **cisco**. Такий пароль не відповідає вимогам безпеки, може використовуватись виключно з навчальною метою на лабораторному обладнанні і не в жодному разі може бути використаний у виробничих умовах. Налаштування пароля для привілейованого режиму наведено на рисунку 4.2.9.

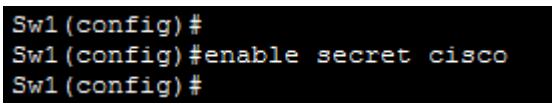

Рисунок 4.2.9 – Налаштування пароля для привілейованого режиму.

Налаштуємо пароль для під'єднання через консольний порт. В якості пароля застосуємо слово **class**. Послідовність команд для налаштування наведена на рисунку 4.2.10.

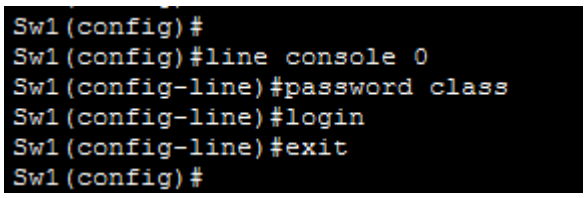

Рисунок 4.2.10 – Налаштування пароля для консольного порту.

Наступним етапом налаштуємо пароль для віддаленого під'єднання через протокол Telnet. Для того, щоб з'ясувати загальну кількість ліній зв'язку VTY, скористуємось контекстною довідкою. В якості пароля також застосуємо слово **class**. Послідовність команд для налаштування наведена на рисунку 4.2.11.

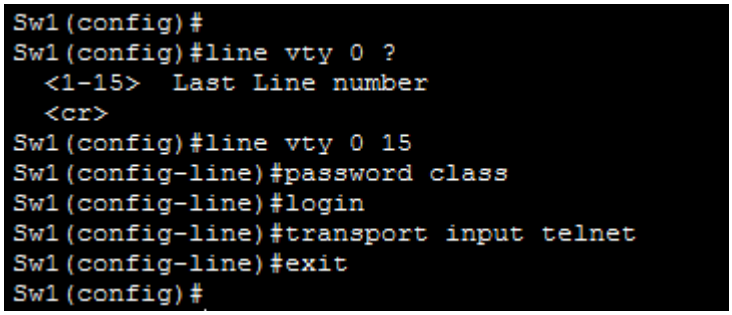

Рисунок 4.2.11 – Налаштування пароля для віддаленого під'єднання через протокол Telnet.

Якщо переглянути файл поточної конфігурації, ми побачимо, що паролі зберігаються у відкритому вигляді (рис. 4.2.12).

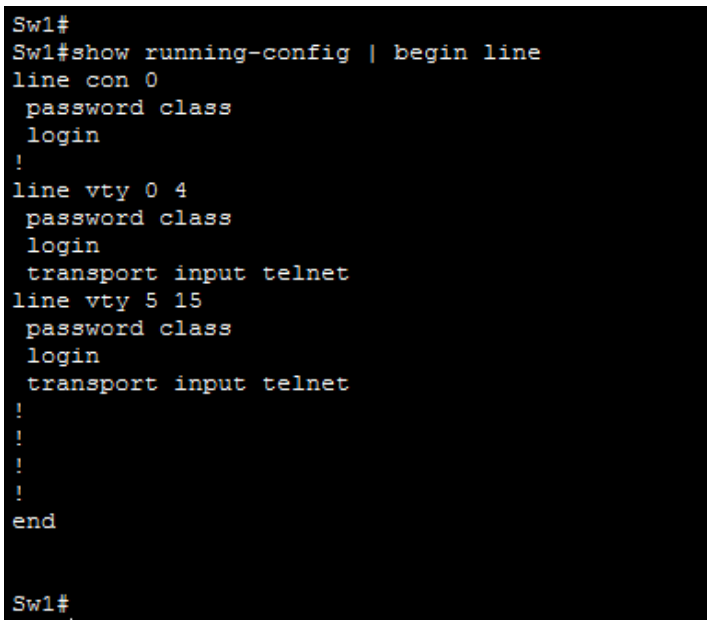

Рисунок 4.2.12 – Файл поточної конфігурації містить паролі у відкритому вигляді.

Для шифрування паролів у файлі конфігурації необхідно активувати відповідну службу. Можна це зробити командою **service password-encryption** (рис. 4.2.13).

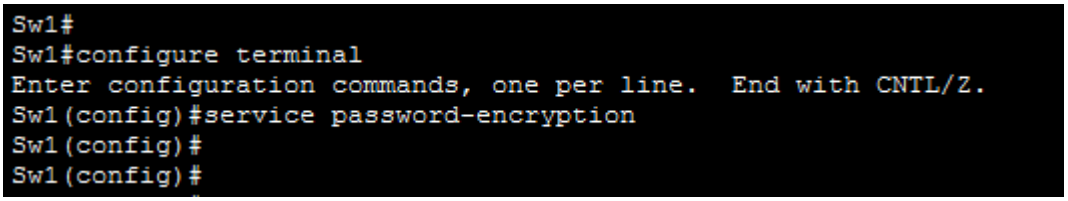

Рисунок 4.2.13 – активація служби шифрування паролів у файлі конфігурації.

Для того, щоб перевірити роботу служби **password-encryption** ще раз переглянемо файл поточної конфігурації (рис. 4.2.14).

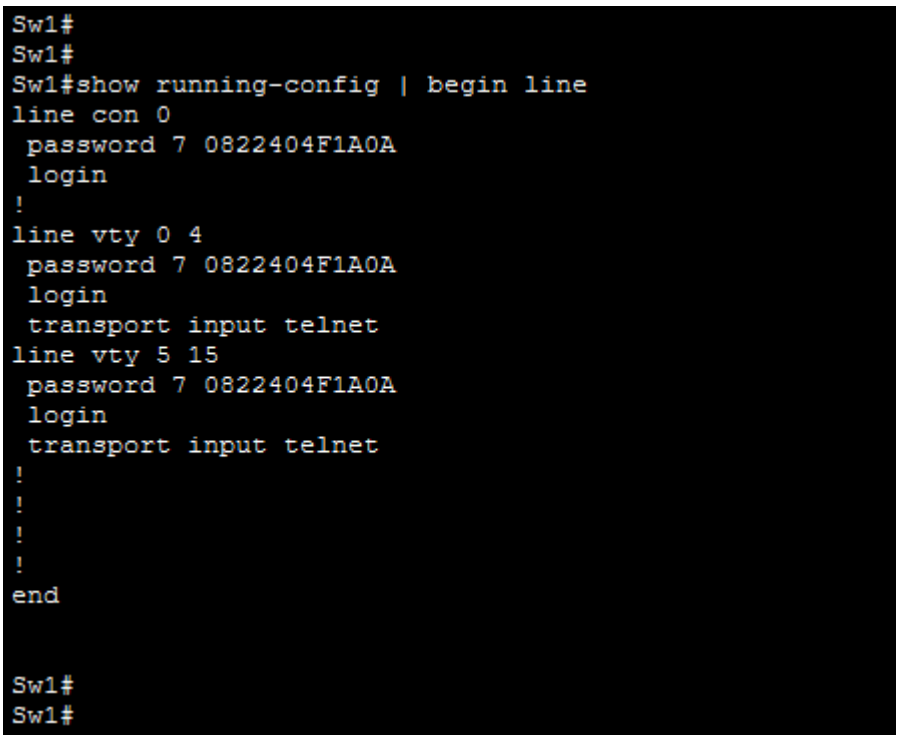

Рисунок 4.2.14 – Файл поточної конфігурації містить паролі у зашифрованому вигляді.

Перейдемо до налаштування банерного повідомлення, яке виводитиметься кожного разу при спробі доєднатись до комутатора. Налаштуємо повідомлення, що складається з декількох рядків. В якості обмежувача використаємо символ «~» (рис. 4.2.15).

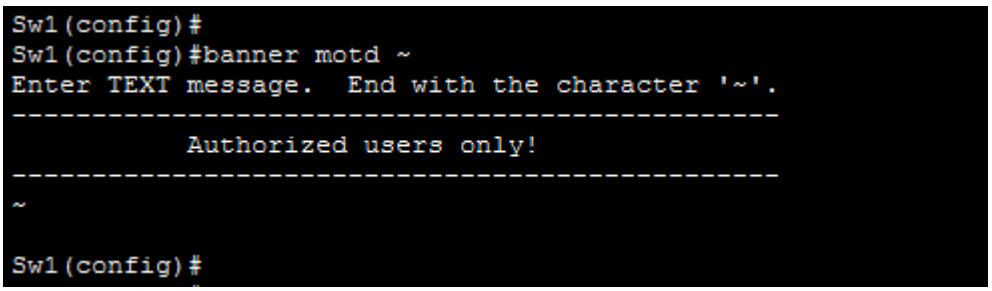

Рисунок 4.2.15 – Налаштування банерного повідомлення.

Перейдемо до налаштування віртуального інтерфейсу комутатора. За замовченням усі порти комутатора відносяться до першої VLAN. Отже налаштуємо IP-адресу 172.16.10.10/24 на інтерфейсі VLAN 1. За замовченням віртуальні інтерфейси комутатора перебувають у вимкненому стані. Активуємо інтерфейс командою **no shutdown** (рис. 4.2.16).

```
Sw1(config)#
Sw1(config)#interface vlan 1
Sw1(config-if)#ip address 172.16.10.10 255.255.255.0
Sw1(config-if)#no shutdown

Sw1(config-if)#
%LINK-3-UPDOWN: Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Sw1(config-if)#exit
Sw1(config)#
Sw1(config)#
```

Рисунок 4.2.16 – Налаштування IP-адреси.

Оскільки в цій лабораторній роботі відсутній маршрутизатор, потреби у налаштуванні шлюзу за замовченням немає.

На цьому початкове налаштування комутатора можна вважати завершеним. Усі налаштовані параметри зберігаються в файлі поточної конфігурації **running-config** в оперативній пам’яті. У випадку перезавантаження операційної системи вони будуть втрачені. Щоб зберегти ці параметри, нам необхідно скопіювати файл поточної конфігурації з оперативної пам’яті в енергонезалежну пам’ять NVRAM в файл під ім’ям **startup-config**. Зробити це можна командою **copy running-config startup-config**. Операційна система запитає ім’я кінцевого файлу, для підтвердження просто натиснемо Enter (рис. 4.2.17).

```
Sw1#
Sw1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Sw1#
Sw1#
```

Рисунок 4.2.17 – Збереження конфігурації.

Далі налаштуємо IP-адресу на комп’ютері. Вона має відноситься до тієї ж мережі, що адреса, налаштована на інтерфейсі VLAN 1 комутатора. Оскільки на комутаторі ми налаштували адресу з довжиною префіксу 24 біти, в адресі комп’ютера повинні відрізнятись тільки останні 8 бітів. Адресу шлюзу за замовченням та DNS-сервера не налаштовуватимемо (рис. 4.2.18).

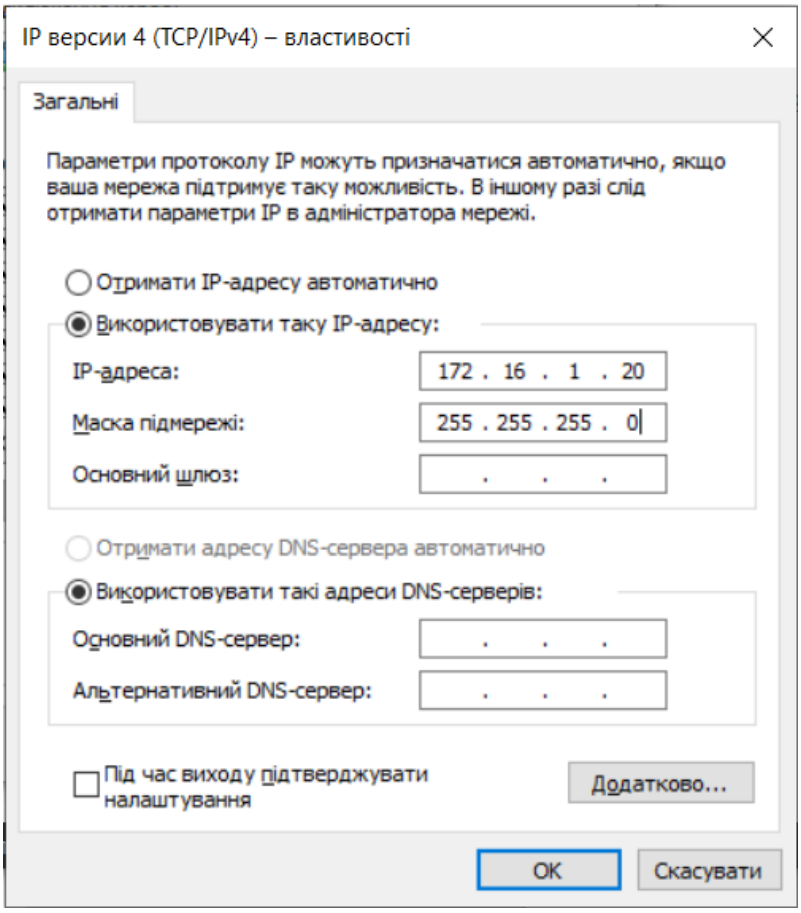

Рисунок 4.2.18 – Налаштування IPv4 на комп’ютері.

Завдання 3. Перевірка параметрів комутатора

Для початку перевіримо зв’язок між комп’ютером та комутатором. Відкриємо командний рядок Windows. Для цього натиснемо комбінацію клавіш <Win> + <R> та виконаємо команду **cmd** (рис. 4.2.19).

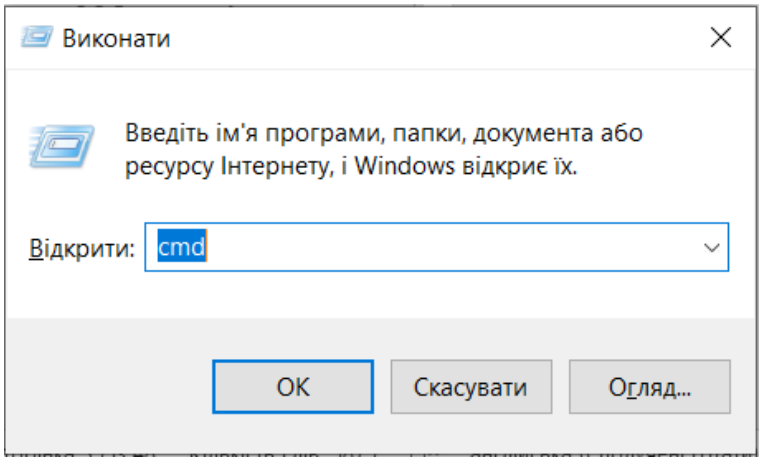

Рисунок 4.2.19 – Запуск командного рядку Windows.

Для перевірки зв’язку з комутатором, у вікні, що відкрилось, введемо команду **ping 172.16.10.10** (рис. 4.2.20).

```
C:\>
C:\>ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.10: bytes=32 time<1ms TTL=255
Reply from 172.16.10.10: bytes=32 time<1ms TTL=255
Reply from 172.16.10.10: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рисунок 4.2.20– Запуск командного рядку Windows.

Після того, як ми переконались у наявності зв’язку, використаємо для віддаленого під’єднання до комутатора команду **telnet** *ip_address* , де *ip_address* – адреса комутатора (рис. 4.2.21).

ВАЖЛИВО! При введенні паролів на екрані не відображається ані введені символи, ані символи – замінювачі, курсор не змінює свого положення.

```
C:\>
C:\>telnet 172.16.10.10
Trying 172.16.10.10 ...Open
------------------------------------------------
          Authorized users only!
------------------------------------------------



User Access Verification

Password:
Sw1>
Sw1>enable
Password:
Sw1#
Sw1#
```

Рисунок 4.2.21 – Встановлення віддаленого сеансу зв’язку з комутатором.

Після під’єднання до комутатора можемо перевірити налаштування IP-адрес та стан інтерфейсів. Для цього застосуємо команду **show ip interface brief** (рис. 4.2.22).

```
Sw1#
Sw1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  172.16.10.10    YES manual up                    up
Sw1#
```

Рисунок 4.2.22 – Перевірка налаштованих IP-адрес та стану інтерфейсів.

Можемо переконатись, що на інтерфейсі VLAN 1 налаштована вірна IP-адреса і він перебуває в активному стані.

Для перевірки системного часу використаємо команду **show clock.** Зазначена команда виводить поточний час, часовий пояс та дату (рис. 4.2.23).

```
Sw1#
Sw1#show clock
20:47:3.185 Kyiv Sun Nov 2 2025
Sw1#
Sw1#
```

Рисунок 4.2.23 – Перевірка поточного часу, часового поясу та дати.

Для перегляду інших налаштувань переглянемо файл поточної конфігурації. Для цього застосуємо команду **show running-config** (рис. 4.2.24).

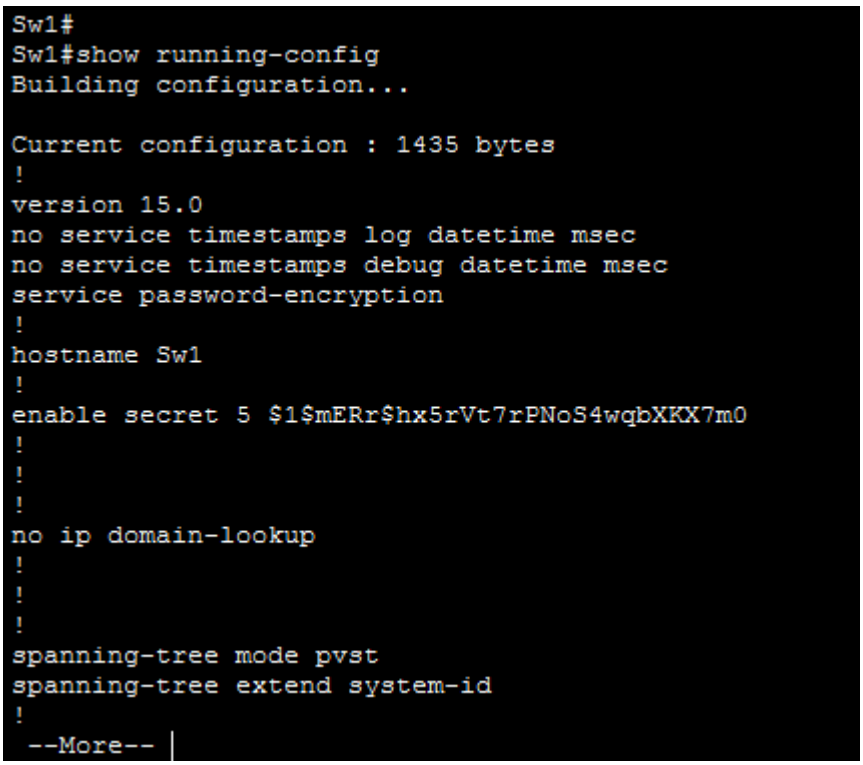

Рисунок 4.2.24 – Перегляд файлу поточної конфігурації.

Слово **--More--** в нижній частині екрану вказує на те, що не весь файл було виведено на екран. Для продовження виведення файлу на екран можна натиснути пробіл або Enter, для переривання – Esc.

Питання для самоперевірки

1. Яка команда використовується для зміни імені комутатора?
2. Якою командою задається пароль для входу в привілейований режим?
3. Як перейти в режим глобальної конфігурації?
4. Як встановити пароль для доступу через консольний порт?
5. Якою командою активується вимога введення пароля при вході через консоль?
6. Як налаштувати пароль для віддаленого доступу через Telnet?
7. Як перевірити, скільки віртуальних термінальних ліній зв’язку (VTY) доступно на комутаторі?
8. Для чого використовується команда banner motd?
9. Яким чином задати IP-адресу комутатору для віддаленого керування ним через мережу?
10. На якому інтерфейсі зазвичай налаштовують IP-адресу керування на комутаторі?
11. Яка команда дозволяє зберегти поточну конфігурацію в NVRAM?
12. Чим відрізняються файли running-config і startup-config?
13. Як переглянути поточну конфігурацію комутатора?
14. Яка команда використовується для перевірки стану інтерфейсів?
15. Як перевірити IP-адресу, налаштовану на VLAN 1?
16. Яка команда дозволяє встановити часову зону на комутаторі?
17. Як налаштувати системний час та дату?
18. Як перевірити, чи активний пароль для доступу через консольний порт?
19. Для чого використовується команда no ip domain-lookup?
20. Яка команда показує стислу інформацію про стан портів комутатора?

Лабораторна робота 3

Дослідження роботи протоколу ARP

Мета: Вивчити принципи роботи протоколу розпізнавання адрес (Address Resolution Protocol, ARP), дослідити структуру ARP-запитів та ARP-відповідей, а також проаналізувати роботу протоколу при взаємодії в межах локальної мережі та з віддаленими мережами.

Завдання: 1. Дослідження ARP-запиту.

2. Дослідження процесу ARP при пінгуванні шлюзу за замовченням.

3. Дослідження процесу ARP при пересиланні пакету у віддалену мережу.

Необхідні ресурси: комп'ютер з доступом до Інтернету, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель, будь-який з комутаторів Cisco Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо та будь-який з маршрутизаторів Cisco 8200, 1941, 4331 тощо.

Теоретичні відомості

Для передачі даних у мережі Ethernet пристрої використовують фізичні адреси (MAC-адреси). Однак на мережевому рівні ми оперуємо логічними IP-адресами. Коли комп'ютер хоче відправити кадр іншому пристрою, він знає IP-адресу отримувача, але для формування Ethernet-кадру йому необхідна MAC-адреса. Саме для вирішення задачі співставлення відомої IP-адреси з невідомою MAC-адресою використовується протокол ARP (Address Resolution Protocol).

Принцип роботи ARP досить простий. Якщо пристрій не знає MAC-адресу отримувача, він надсилає в мережу *широкомовний* запит (ARP Request). Цей запит адресований усім пристроям в локальному сегменті (MAC-адреса призначення FF:FF:FF:FF:FF:FF) і містить питання: «Хто має цю IP-адресу?». Усі

пристрої отримують цей запит, але відповідає лише той, чия IP-адреса співпадає з запитуваною. Цей пристрій надсилає односпрямовану відповідь (ARP Reply), яка містить його MAC-адресу: «Я маю цю IP-адресу, моя MAC-адреса така-то».

Отримані відповідності IP-адрес та MAC-адрес зберігаються в спеціальній ARP-таблиці (ARP-кеші) пристрою, щоб не надсилати запити кожного разу перед відправкою пакету. Переглянути ARP-таблицю на комп'ютері з операційною системою Windows можна за допомогою командного рядка та команди **arp -a** , а на маршрутизаторі Cisco — командою **show arp**

Особлива ситуація виникає, коли необхідно передати дані пристрою, що знаходиться у віддаленій мережі (наприклад, в Інтернеті). У цьому випадку ARP-запит на адресу кінцевого отримувача не надсилається, оскільки широкомовні повідомлення не пересилаються маршрутизаторами у інші мережі. Замість цього комп'ютер визначає MAC-адресу свого шлюзу за замовченням (Default Gateway) і відправляє пакет йому.

Хід роботи

Завдання 1. Дослідження ARP-запиту.

Для виконання цього завдання найкраще використовувати реальне обладнання та аналізатор трафіку (наприклад, Wireshark) або режим симуляції (Simulation Mode) у Cisco Packet Tracer. Для переходу в режим симуляції необхідно натиснути кнопку *Simulation* праворуч в нижній частині екрану (рис. 4.3.1).

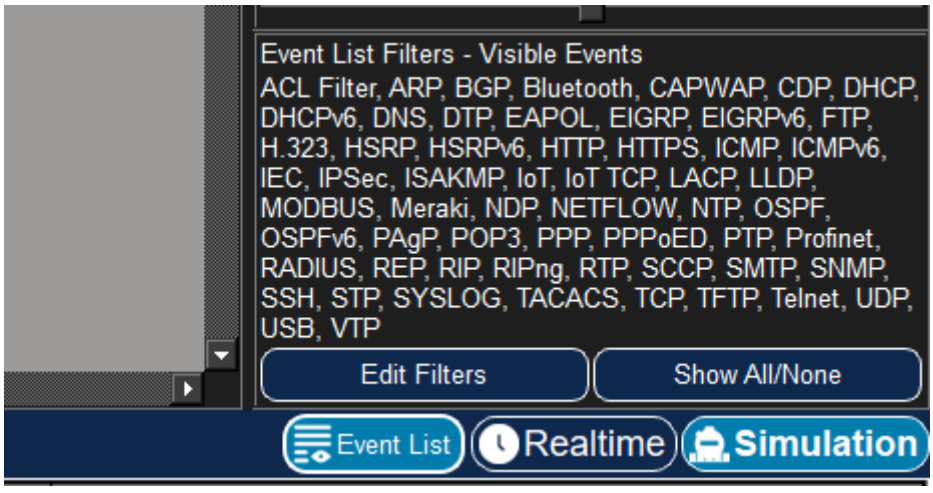

Рисунок 4.3.1 – Режим симуляції в Cisco Packet Tracer.

Спочатку переконайтеся, що ARP-таблиця вашого комп’ютера порожня, щоб ініціювати процес пошуку адреси. У командному рядку Windows це можна зробити командою **arp -d *** (потрібні права адміністратора), а в симуляторі достатньо просто перезавантажити пристрої.

Виконайте команду ping до іншого комп’ютера у вашій локальній мережі. Оскільки комп’ютер ще не знає MAC-адреси отримувача, він сформує ARP-запит. Зверніть увагу на структуру цього запиту. У полі Destination MAC буде вказано широкомовну адресу ff:ff:ff:ff:ff:ff (рис. 4.3.2).

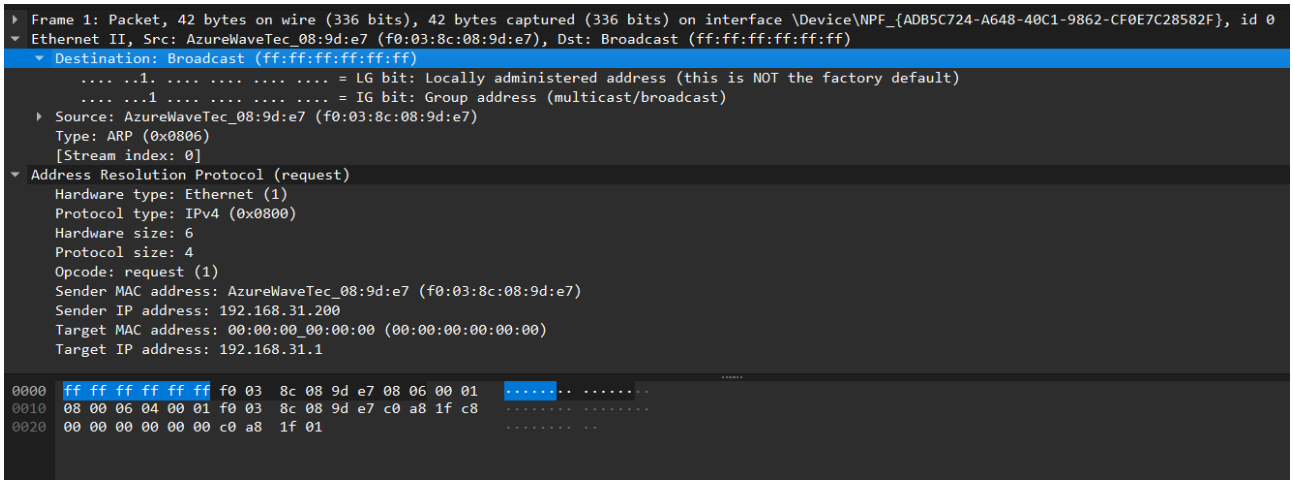

Рисунок 4.3.2 – Широкомовний ARP запит.

Цей запит надійде на комутатор. Оскільки це широкомовний кадр, комутатор перешле його на всі активні порти, окрім того, з якого він надійшов. Це гарантує, що запит досягне всіх пристроїв у мережі. Тільки той комп’ютер, IP-адреса якого зазначена в полі «Target IP address» (192.168.31.1), обробить цей запит і надішле ARP-відповідь. Ця відповідь вже буде односпрямованою (unicast), тобто адресованою безпосередньо ініціатору запиту.

Після завершення обміну перевірте ARP-таблицю командою **arp -a**. Ви побачите новий запис, що зв’язує IP-адресу сусіда з його фізичною адресою (рис. 4.3.3).

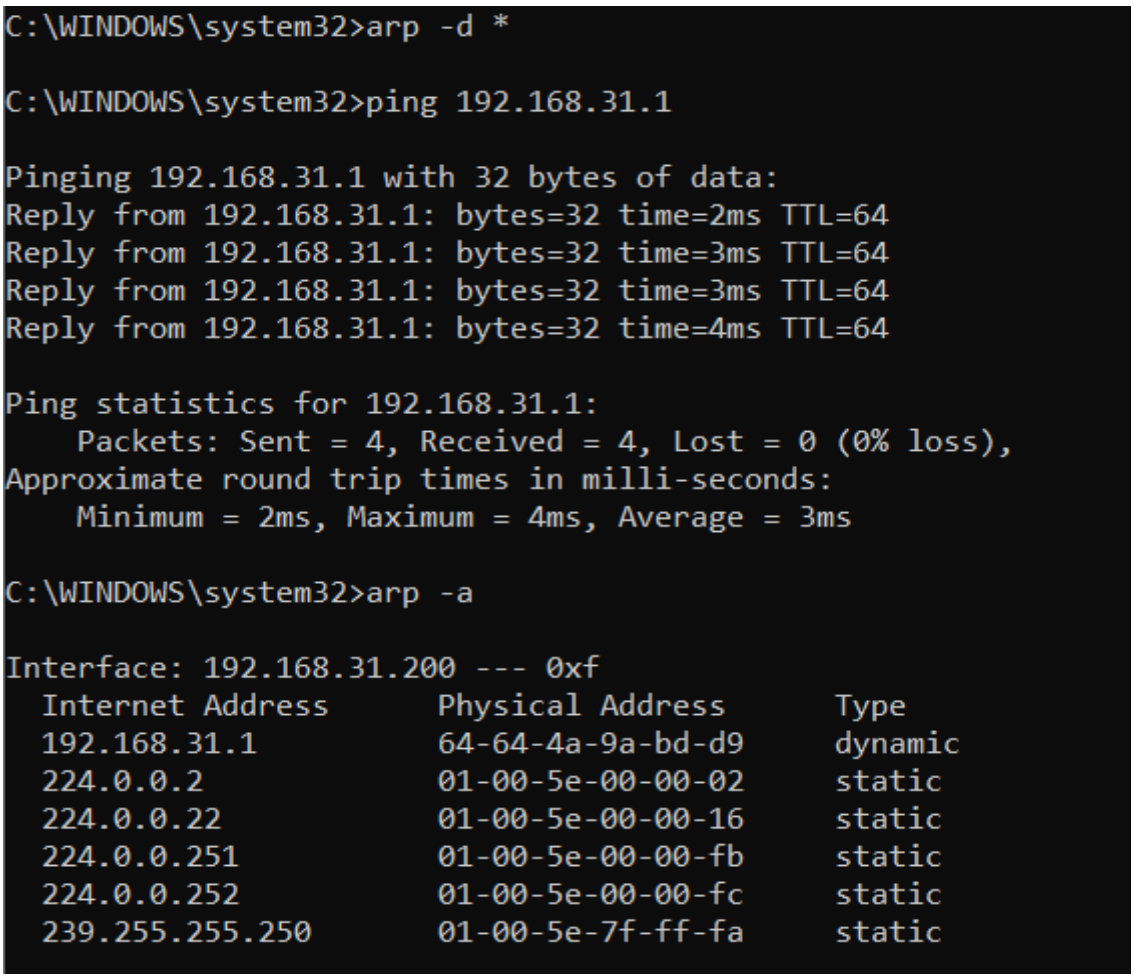

Рисунок 4.3.3 – Очищення таблиці ARP, пінгування вузла 192.168.31.1, перегляд таблиці ARP.

Завдання 2. Дослідження процесу ARP при пінгуванні шлюзу за замовченням.

Шлюз за замовченням — це маршрутизатор, через який комп'ютер «спілкується» із зовнішнім світом. Процес визначення його MAC-адреси нічим не відрізняється від пошуку адреси звичайного комп'ютера.

Дізнайтеся IP-адресу вашого шлюзу за допомогою команди **ipconfig** (рис4.3.4). Зазвичай це перша адреса у вашій підмережі (в нашому прикладі це адреса, 192.168.31.1). Виконайте команду ping на адресу шлюзу. Якщо запису про шлюз ще немає в ARP-таблиці, ваш комп'ютер знову надішле ARP Request. Зверніть увагу, що у відповіді (ARP Reply) маршрутизатор надішле MAC-адресу саме того інтерфейсу, який підключений до вашої локальної мережі (рис. 4.3.5).

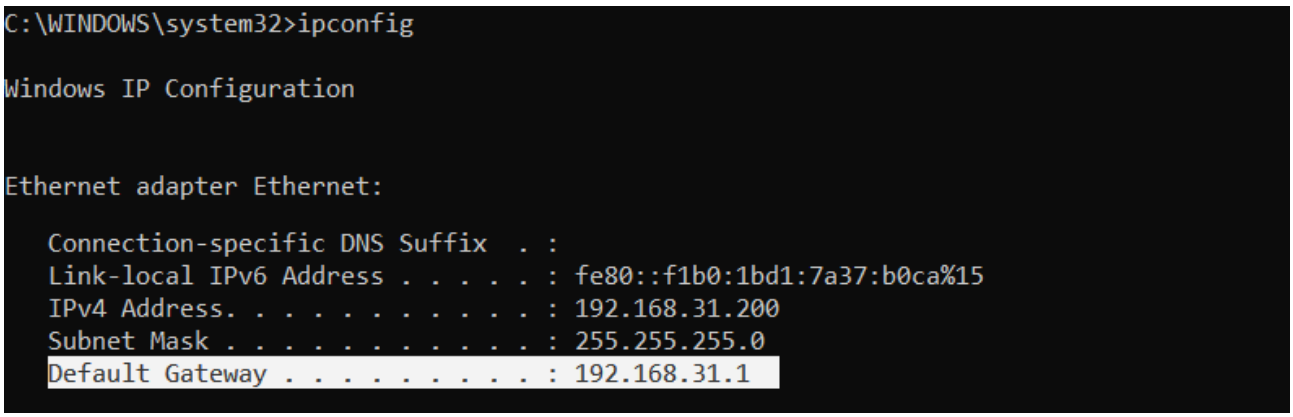

Рисунок 4.3.4 – перегляд інформації про налаштування мережних адаптерів.

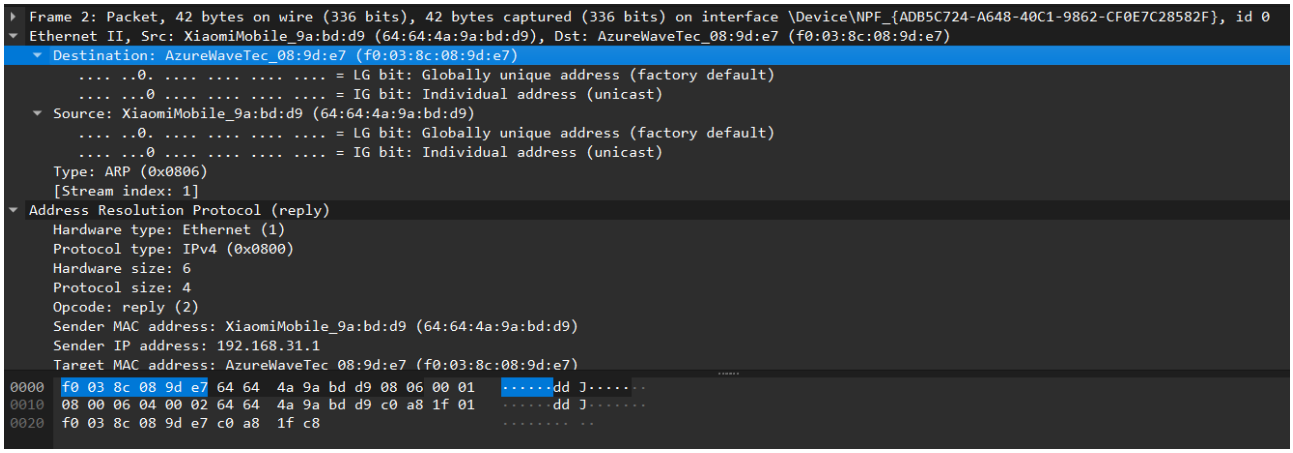

Рисунок 4.3.5 – ARP відповідь, надіслана на unicast адресу пристрою, що здійснював запит.

ВАЖЛИВО! Якщо ви працюєте з реальним обладнанням, пам'ятайте, що маршрутизатори Cisco мають функцію Proxy ARP, яка може бути увімкнена за замовченням. Однак для звичайної роботи в межах однієї підмережі вона не впливає на базовий процес ARP.

Перевірте ARP-таблицю. Тип запису для шлюзу, як і для інших сусідів, буде позначений як «dynamic» (динамічний), що означає, що він був вивчений автоматично і має певний час життя (рис. 4.3.3).

Завдання 3. Дослідження процесу ARP при пересиланні пакету у віддалену мережу.

Це найцікавіший етап. Пропінгуйте адресу, яка знаходиться за межами вашої локальної мережі (наприклад, сервер Google 8.8.8.8 або адресу іншого маршрутизатора в лабораторній топології). Спостерігайте за процесом

формування пакету. Ваш комп’ютер порівняє свою IP-адресу та маску підмережі з IP-адресою призначення. Він виявить, що адреса 8.8.8.8 знаходиться в іншій мережі. В такому випадку комп’ютер НЕ надсилає ARP-запит для адреси 8.8.8.8. Широкомовний запит до глобальної мережі не має сенсу. Замість цього комп’ютер відправляє широкомовний ARP запит з адресою шлюзу за замовченням.

Перегляньте деталі сформованого Ethernet-кадру, що містить ICMP пакет пінгування сервера Google. В якості Destination IP буде вказано адресу кінцевого отримувача (8.8.8.8). Але в якості Destination MAC буде вказано MAC-адресу вашого шлюзу за замовченням (рис. 4.3.6).

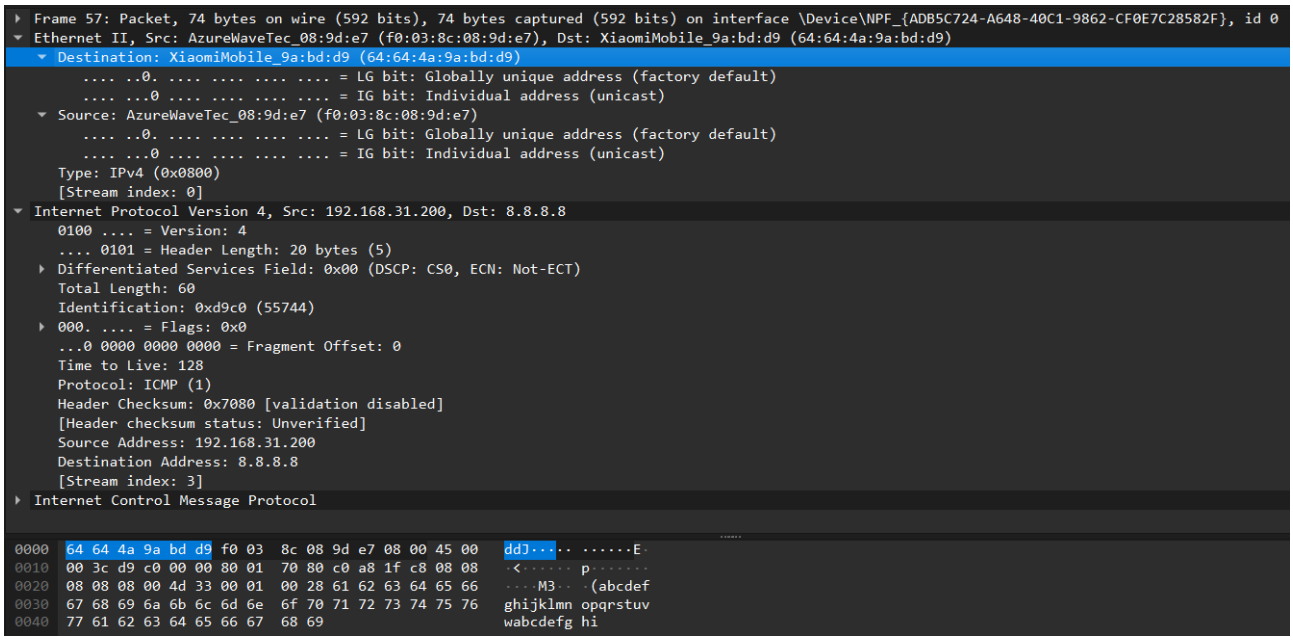

Рисунок 4.3.6 – пінгування вузла у віддаленій мережі (сервер Google, 8.8.8.8).

Таким чином, на рівні Ethernet пакет пересилається від вашого ПК до маршрутизатора. Маршрутизатор, отримавши кадр, здійснює деінкапсуляцію (відкидає заголовок Ethernet), аналізує IP-адресу призначення, звіряється зі своєю таблицею маршрутизації і для подальшої пересилки здійснює інкапсуляцію пакета у новий кадр, зі своєю MAC-адресою як джерела та MAC-адресою призначення маршрутизатора наступного переходу.

Питання для самоперевірки

1. Що таке протокол ARP і для чого він використовується в мережах IPv4?
2. Яка MAC-адреса використовується як адреса призначення в ARP-запиті?
3. Якою командою можна переглянути ARP-таблицю на комп’ютері та на маршрутизаторі Cisco?
4. Чому ARP-запити не проходять через маршрутизатори?
5. Яка MAC-адреса призначення зазначається в кадрі, якщо комп’ютер відправляє пакет у віддалену мережу?
6. Що станеться, якщо видалити запис про шлюз за замовченням з ARP-таблиці під час передачі даних?
7. В чому різниця між статичними та динамічними записами в ARP-таблиці?
8. На якому рівні моделі OSI працює ARP і чому його складно віднести лише до одного рівня?
9. Яку проблему вирішує ARP у процесі передавання пакетів у локальній мережі?
10. Яку інформацію містить ARP-запит (ARP Request)?
11. Чим відрізняється ARP-запит від ARP-відповіді (ARP Reply)?
12. Яка MAC-адреса використовується як адреса призначення в ARP-запиті?
13. Чому ARP-запити надсилаються у вигляді широкомовних кадрів?
14. Як пристрій визначає, чи потрібно надсилати ARP-запит для певної IP-адреси?
15. Що таке ARP-таблиця (ARP cache) і яку інформацію вона зберігає?
16. Яким чином і коли записи з ARP-таблиці видаляються або оновлюються?
17. Яка команда використовується для перегляду ARP-таблиці на комп’ютері або маршрутизаторі Cisco?
18. Чи виконується ARP при передачі пакетів між різними мережами? Поясніть чому.
19. Яку MAC-адресу намагається визначити вузол, якщо пакет потрібно передати до іншої підмережі?

Лабораторна робота 4

Дослідження роботи Neighbor Discovery для IPv6

Мета: Вивчити принципи роботи протоколу виявлення сусідів (Neighbor Discovery Protocol, NDP) в мережах IPv6, дослідити структуру повідомлень Neighbor Solicitation (NS) та Neighbor Advertisement (NA), а також проаналізувати механізми визначення MAC-адреси пристроїв у локальній та віддаленій мережах.

Завдання: 1. Виявлення сусіда IPv6 у локальній мережі.

2. Виявлення сусіда IPv6 у віддаленій мережі.

Необхідні ресурси: комп'ютер з доступом до Інтернету, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель, будь-який з комутаторів Cisco Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо та будь-який з маршрутизаторів Cisco 8200, 1941, 4331 тощо.

Теоретичні відомості

У мережах IPv4 для визначення фізичної (MAC) адреси за відомою IP-адресою використовується протокол ARP, який працює на основі широкомовних розсилань (broadcast). В протоколі IPv6 широкомовні розсилання відсутні, тому ARP більше не використовується. Його функції перебрав на себе протокол Neighbor Discovery Protocol (NDP), який базується на повідомленнях протоколу керуючих повідомлень ICMPv6. Процес визначення MAC-адреси сусіда в IPv6 називається Address Resolution (визначення адреси). Замість широкомовних запитів (broadcast) IPv6 використовує ефективнішу групову адресацію (multicast).

Основні повідомлення NDP для визначення адреси – це NS та NA. NS (Neighbor Solicitation, тип 135) - аналог ARP Request. Відправляється пристроєм, який хоче дізнатися MAC-адресу іншого вузла. Пакет надсилається на

спеціальну групову адресу «solicited-node multicast», яку прослуховує лише цільовий пристрій. NA (Neighbor Advertisement, тип 136): Аналог ARP Reply. Відповідь пристрою, чию адресу шукали. Містить необхідну MAC-адресу і зазвичай надсилається як unicast (односпрямоване повідомлення) ініціатору.

Відповідності між IPv6-адресами та MAC-адресами зберігаються в таблиці сусідів (Neighbor Table). Переглянути її на маршрутизаторі Cisco можна командою **show ipv6 neighbors**, в командному рядку Windows командою **netsh interface ipv6 show neighbors**. Для видалення записів з таблиці сусідів застосовують команду **netsh interface ipv6 delete neighbors**.

Якщо необхідно передати пакет у віддалену мережу, пристрій використовує NDP для визначення MAC-адреси свого шлюзу за замовченням (Default Gateway), а не кінцевого отримувача.

Хід роботи

Завдання 1. Виявлення сусіда IPv6 у локальній мережі.

Для виконання роботи налаштуйте просту топологію з двох ПК та комутатора (або використовуйте режим симуляції в Packet Tracer). Призначте пристроям глобальні unicast адреси (наприклад, 2001:db8:acad:1::1 та 2001:db8:acad:1::2).

Увімкніть захоплення пакетів в аналізаторі трафіка або перейдіть у режим симуляції (Simulation Mode) та відфільтруйте відображення протоколів, залишивши тільки ICMPv6 та NDP. Виконайте команду ping від одного ПК до іншого, використовуючи IPv6-адресу сусіда. Оскільки MAC-адреса отримувача ще невідома, ПК сформує повідомлення Neighbor Solicitation (NS).

Відкрийте деталі пакету NS. Зверніть увагу на IP-адресу призначення. Це не адреса самого комп’ютера і не загальний широкомовний запит. Це спеціальна multicast-адреса вузла, що запитується (solicited-node multicast address), яка починається з FF02::1:FF... (рис. 4.4.1). В полі «ICMPv6 Option» (Target Link-Layer Address) запит може містити MAC-адресу відправника, щоб отримувач міг одразу додати її у свій кеш.

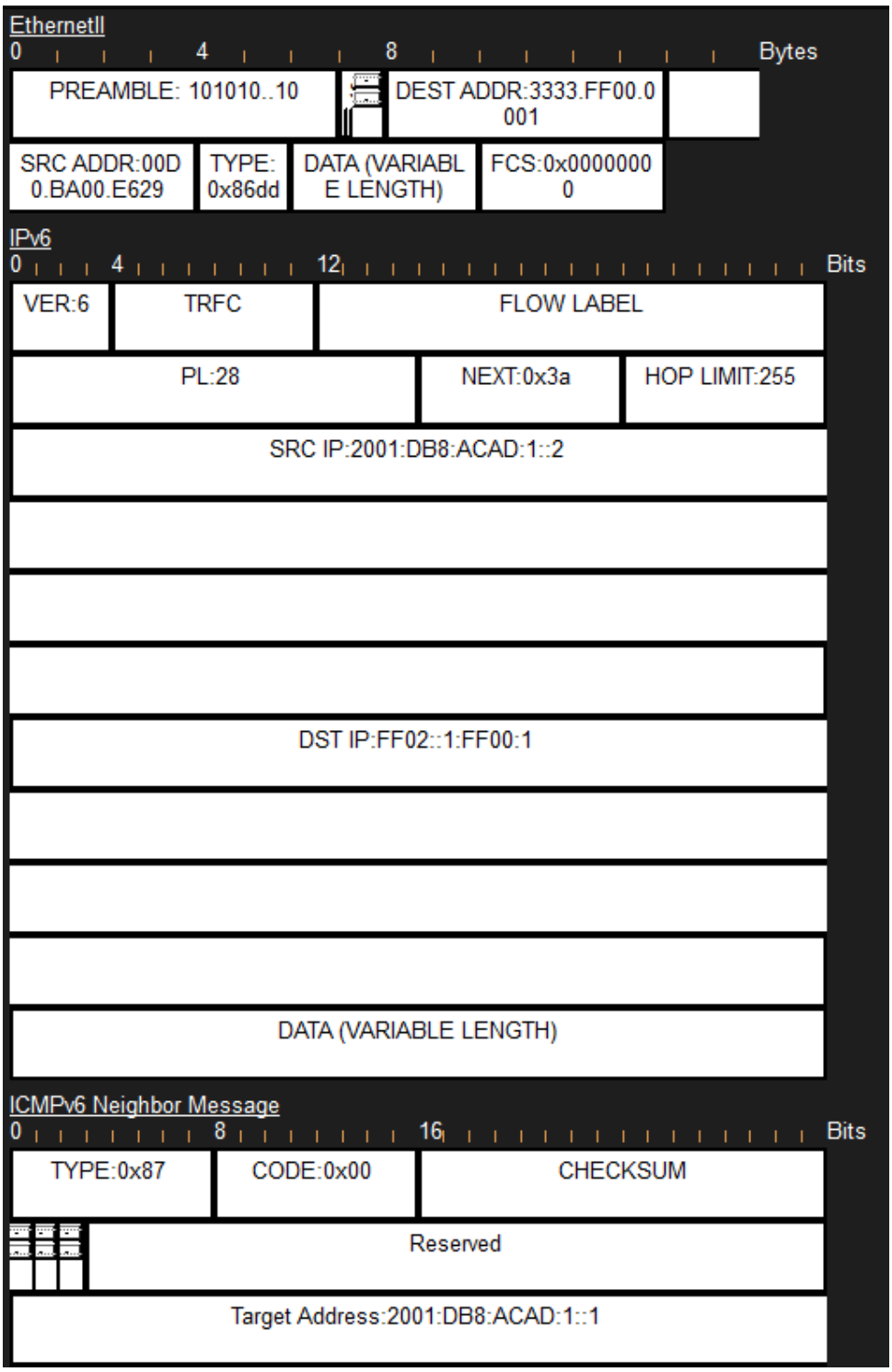

Рисунок 4.4.1 – Структура пакету Neighbor Solicitation.

IPv6 адреса призначення – FF02::1:FF00:1 – спеціальна multicast-адреса вузла, що запитується (solicited-node multicast address).

Комутатор здійснить пересилання цього кадру. Пристрій-отримувач розпізнає свою multicast-адресу, обробить запит і сформує відповідь Neighbor Advertisement (NA). Зверніть увагу, що NA відправляється безпосередньо на

unicast-адресу ініціатора. У тілі повідомлення NA міститься шукана MAC-адреса (Target Link-Layer Address). Після проходження пінгу перевірте таблицю сусідів на комп'ютері командою **netsh interface ipv6 show neighbors**. Ви побачите запис стану «Reachable» (досяжний), що підтверджує успішне визначення адреси.

Завдання 2. Виявлення сусіда IPv6 у віддаленій мережі.

Додайте до топології маршрутизатор, налаштуйте IPv6-адресацію (2001:DB8:ACAD:1::F/64, FE80::F link-local) та вкажіть адресу інтерфейсу маршрутизатора як шлюз за замовченням для ПК (рис. 4.4.2).

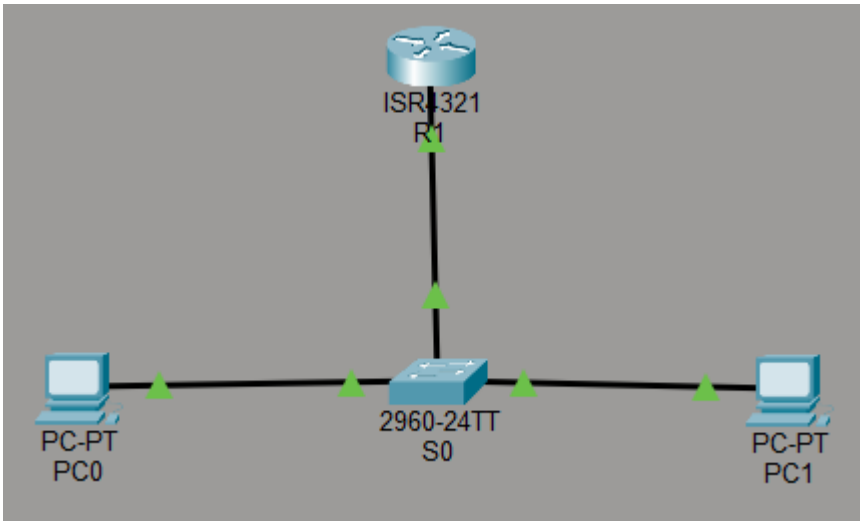

Рисунок 4.4.2 – Топологія мережі з маршрутизатором.

Спробуйте виконати пінг на адресу, що знаходиться за межами локальної мережі, наприклад, адресу сервера Google (2001:4860:4860::8888). Пристрій порівняє префікс мережі призначення зі своїм власним і виявить, що адресата немає в локальному сегменті. У цьому випадку NDP-процес ініціюється не для адреси сервера, а для Link-Local адреси шлюзу за замовченням.

Спостерігайте за пакетами. Комп'ютер сформує NS-запит, де «Target Address» буде Link-Local адресою маршрутизатора FE80::F (рис. 4.4.3).

Маршрутизатор відповість повідомленням NA, надавши MAC-адресу свого інтерфейсу. Після отримання відповіді комп'ютер сформує пакет з даними (ICMPv6 Echo Request). Перегляньте заголовок сформованого кадру.

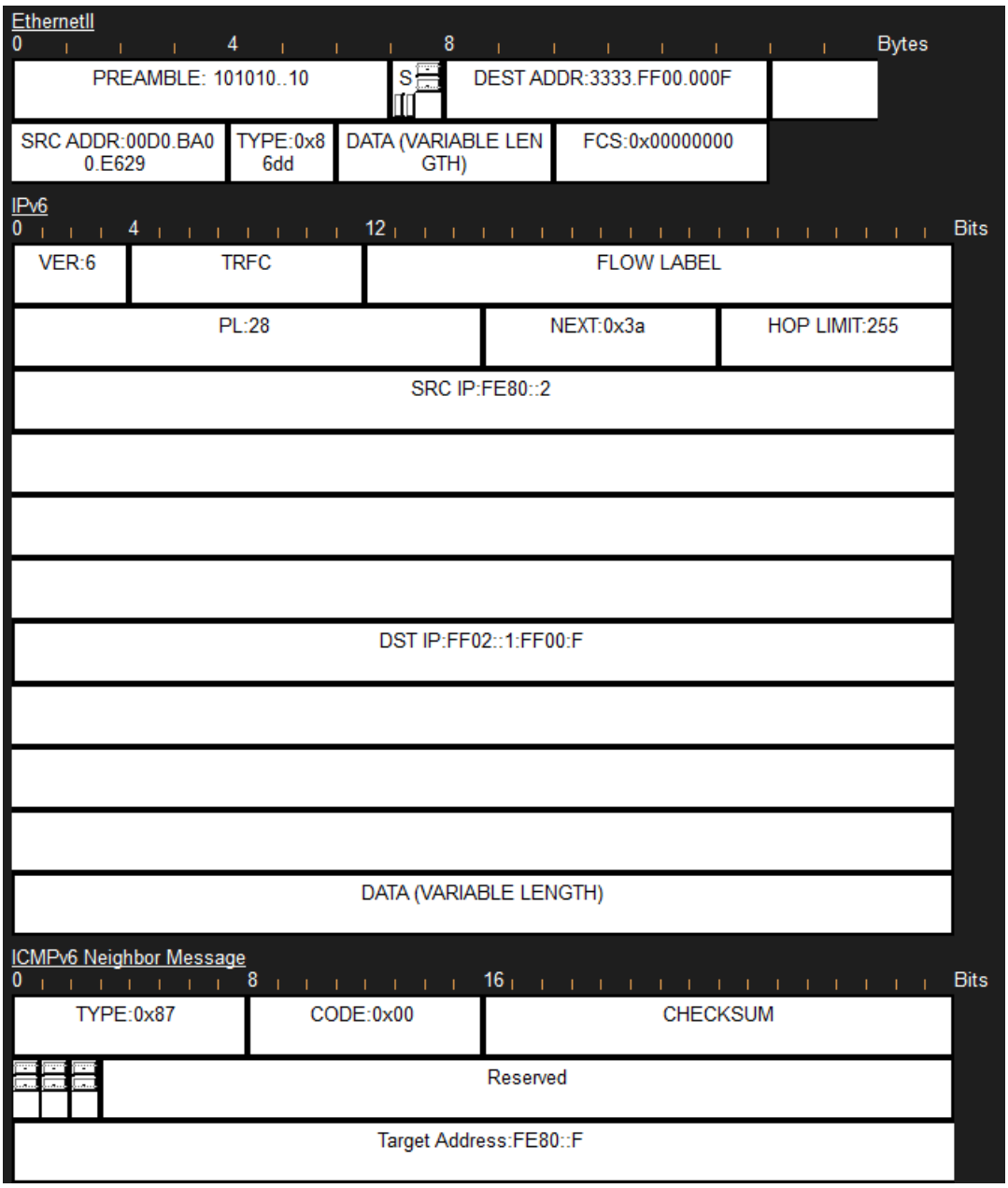

Рисунок 4.4.3 – Незважаючи на те, що пінгувався вузол у віддаленій мережі (2001:4860:4860::8888), в NS повідомленні в полі «Target Address» зазначена Link-Local адреса шлюза за замовченям FE80::F.

Зверніть увагу на поля «IPv6 Destination IP» (адреса вузла призначення у віддаленій мережі) та «Ethernet Destination MAC» (MAC-адреса шлюзу за замовченням). Це демонструє, що на канальному рівні дані передаються до найближчого маршрутизатора, який вже буде приймати рішення про подальшу пересилку.

Питання для самоперевірки

1. Який протокол в IPv6 замінив ARP?
2. Які два типи повідомлень ICMPv6 використовуються для визначення MAC-адреси?
3. Чому IPv6 використовує multicast замість broadcast для пошуку сусідів?
4. Якою командою можна переглянути таблицю сусідів IPv6 на маршрутизаторах Cisco?
5. Якою командою можна переглянути таблицю сусідів IPv6 в командному рядку операційної системи Windows?
6. Що таке «solicited-node multicast address» і як вона формується?
7. Яка MAC-адреса буде вказана в полі Destination MAC кадру, якщо комп’ютер пінгує сервер Google через IPv6?
8. Яку роль відіграють Link-Local адреси (FE80::) у процесі Neighbor Discovery?
9. Для чого призначені повідомлення Neighbor Solicitation (NS) та Neighbor Advertisement (NA)?
10. Які типи IPv6-адрес використовуються як адреси призначення для NS та RS повідомлень?
11. Як відбувається процес визначення MAC-адреси вузла в IPv6?
12. Чим NDP відрізняється від ARP за принципом роботи?
13. Що таке Duplicate Address Detection (DAD) і коли він виконується?

Лабораторна робота 5

Налаштування базових параметрів маршрутизатора

Мета: Навчитись виконувати базове налаштування маршрутизатора Cisco, конфігурувати мережеві інтерфейси, забезпечувати захист доступу до пристрою та зберігати конфігурацію в енергонезалежній пам'яті.

Завдання:
1. Перевірка конфігурації маршрутизатора за замовчуванням.
2. Початкова конфігурація маршрутизатора.
3. Налаштування інтерфейсів маршрутизатора.
4. Перевірка конфігурації.
5. Збереження файлу поточної конфігурації.

Необхідні ресурси: комп'ютер з доступом до Інтернету, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель та будь-який з маршрутизаторів Cisco 8200, 1941, 4331 тощо.

Теоретичні відомості

Маршрутизатори Cisco використовують ту саму операційну систему Cisco IOS, що й комутатори, тому базові команди навігації та налаштування є ідентичними. Проте, на відміну від комутаторів, які працюють на канальному рівні (Layer 2) і мають порти, увімкнені за замовчуванням, інтерфейси маршрутизаторів працюють на мережевому рівні (Layer 3) та за замовченням перебувають у вимкненому стані. Кожен інтерфейс маршрутизатора повинен мати унікальну IP-адресу та маску підмережі. Для налаштування інтерфейсу з режиму глобальної конфігурації перейти у відповідний режим. Це можна зробити командою **interface** *interface_id*, де *interface_id* – назва інтерфейсу. Для налаштування IPv4-адреси застосовуємо команду **ip address** *ip_address subnen_mask*, де *ip_address* – IP_адреса, а *subnen_mask* – маска підмережі. Хорошою практикою вважається описувати інтерфейси.

Зробити це можна командою **description** *any text*. Команда description ніяк не впливає на роботу інтерфейсів, але текст, що іде за нею, дозволяє адміністратору шводко зрозуміти призначення цього інтерфейсу. Інтерфейси маршрутизатора за замовчуванням знаходяться у стані «administratively down» (вимкнені). Для їх активації необхідно використати команду **no shutdown**.

Конфігурація маршрутизатора зберігається у двох файлах. В файлі running-config міститься поточна конфігурація маршрутизатора. Будь-які команди, що змінюють конфігурацію, миттєво вносять зміни в файл running-config. Цей файл міститься в оперативній пам'яті (RAM), а вона, як відомо, втрачає свій вміст при вимкненні маршрутизатора або перезавантаженні операційної системи. Щоб не втрачались налаштування маршрутизатора використовується файл startup-config. Він міститься в енергонезалежній пам'яті (NVRAM). Операційна система одразу після завантаження намагається знайти цей файл. Якщо файл startup-config існує, його вміст копіюється в файл running-config і всі налаштування, що містяться в ньому, вступають в силу. Файлу startup-config за замовченням на маршрутизаторі не існує. Для його створення необхідно застосувати команду **copy running-config startup-config**. Ця команда копіює вміст файлу running-config з RAM в файл startup-config на NVRAM. Для того щоб повернути маршрутизатор до заводських налаштувань необхідно видалити файл startup-config командою **erase startup-config** та перезавантажити операційну систему командою **reload**. Після застосування команди **reload** потрібно підтвердити своє бажання перезавантажити операційну систему натиснувши Enter (рис. 4.5.1). Ці команди вводяться в привілейованому режимі.

```
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R1#
R1#reload
Proceed with reload? [confirm]
```

Рисунок 4.5.1 – Збереження поточної конфігурації
та перезавантаження операційної системи.

Хід роботи

Завдання 1. Перевірка конфігурації маршрутизатора за замовчуванням.

Підключіться до маршрутизатора через консольний порт. Увійдіть у привілейований режим за допомогою команди **enable**. Виведіть на екран поточну конфігурацію командою **show running-config** (рис. 4.5.2). Проаналізуйте отриману інформацію.

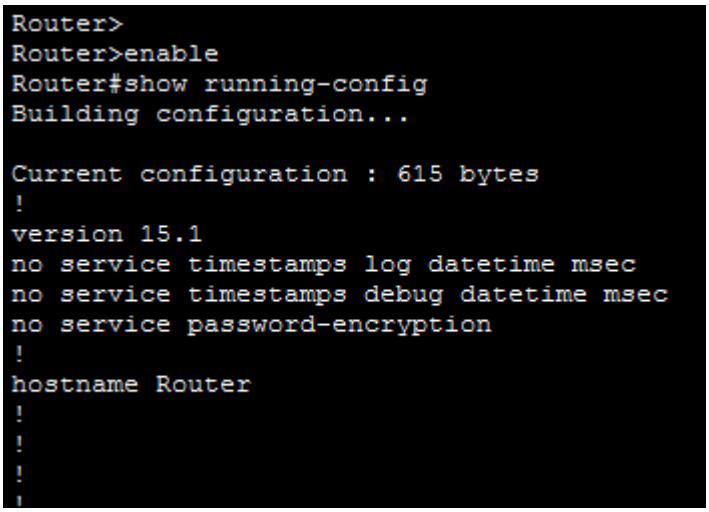

Рисунок 4.5.2 – Перегляд файлу поточної конфігурації (частина файлу).

Зверніть увагу на такі параметри: ім’я хоста за замовчуванням Router, паролі відсутні, інтерфейси не мають IP-адрес (no ip address) і знаходяться у стані shutdown (рисунки 4.5.2, 4.5.3).

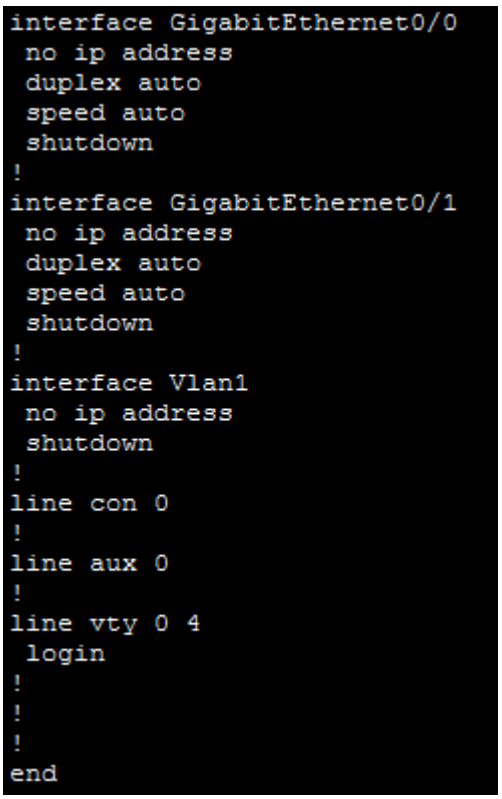

Рисунок 4.5.3 – Фрагмент файлу конфігурації маршрутизатора за замовчуванням.

Завдання 2. Початкова конфігурація маршрутизатора.

Перейдіть у привілейований режим (команда **enable**), а потім у режим глобальної конфігурації (**configure terminal**). Змініть ім’я маршрутизатора на R1 (**hostname R1**). Налаштуйте безпечний доступ до привілейованого режиму, при цьому використовуйте зашифрований пароль class (**enable secret class**). Налаштуйте пароль для доступу через консольний порт (**line console 0, password cisco, login**). Налаштуйте пароль для віртуальних ліній (VTY) для віддаленого доступу через Telnet або SSH (**line vty 0 15, password cisco, login**). Зашифруйте всі паролі, що зберігаються у відкритому вигляді (**service password-encryption**). Встановіть банер дня (Message of the Day), який буде попереджати користувачів про заборону несанкціонованого доступу (**banner motd #Unauthorized access is strictly prohibited!#**). Всі початкові налаштування наведені на рисунку 4.5.4.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Unauthorized access is strictly prohibited!#
R1(config)#
```

Рисунок 4.5.4 – Початкові налаштування маршрутизатора.

Наведені початкові налаштування маршрутизатора не відрізняються від початкових налаштувань комутатора, що детально розглядались в лабораторній роботі 2.

Завдання 3. Налаштування інтерфейсів маршрутизатора.

Це найважливіший етап налаштування маршрутизатора. Припустимо, ми налаштовуємо інтерфейс GigabitEthernet0/0 (залежно від моделі маршрутизатора тип та назва наявних інтерфейсів можуть відрізнятись). Увійдіть у режим конфігурації інтерфейсу (**interface GigabitEthernet0/0**), додайте опис інтерфейсу (**description Link to LAN-1**). Призначте IP-адресу та маску підмережі, наприклад, 192.168.1.1/24 (**ip address 172.16.1.1 255.255.255.0**). Увімкніть інтерфейс (**no shutdown**). Система повинна вивести повідомлення про те, що стан інтерфейсу змінився на up. Без цієї команди порт не запрацює, навіть якщо IP-адреса задана вірно. Вийдіть з режиму конфігурації інтерфейсу (**exit**). Налаштування інтерфейсу наведені на рисунку 4.5.5.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet0/0
R1(config-if)#description Link to LAN-1
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R1(config-if)#exit
R1(config)#
```

Рисунок 4.5.5 – Налаштування та активація інтерфейсу GigabitEthernet0/0.

Завдання 4. Перевірка конфігурації.

Поверніться у привілейований режим (**end**). Перегляд Будь-яких параметрів роботи маршрутизатора здійснюється саме в цьому режимі.

Для швидкої перевірки стану всіх інтерфейсів використовуйте команду **show ip interface brief** (рис4.5.6).

```
R1#
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.16.1.1      YES manual up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
R1#
```

Рисунок 4.5.6 – Швидка перевірка стану всіх інтерфейсів.

Інтерфейс GigabitEthernet0/0 в робочому стані (up/up).

Це одна з найкорисніших команд для швидкої діагностики інтерфейсів. У виводі ви повинні побачити назву інтерфейсу, призначену IP-адресу, статус (up – фізичний рівень працює), протокол (up – канальний рівень працює). Якщо ви бачите статус – administratively down, це означає, що ви забули ввести команду no shutdown.

Також перевірте таблицю маршрутизації, щоб переконатися, що маршрутизатор «бачить» підключену мережу. Для цього застосовується команда **show ip route**. Наявність двох маршрутів з кодами C (Connected) та L (Local) вказує на успішне підключення мережі (рис. 4.5.7).

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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 not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0

R1#
```

Рисунок 4.5.7 – Перегляд таблиці маршрутизації.

Завдання 5. Збереження файлу поточної конфігурації.

Усі зроблені вами налаштування зараз зберігаються в оперативній пам’яті у файлі running-config. Якщо вимкнути живлення маршрутизатора або перезавантажити операційну систему, усі зміни будуть втрачені. Збережіть налаштування в NVRAM (**copy running-config startup-config**). Підтвердіть дію, натиснувши Enter. Переконайтеся, що налаштування збережено, переглянувши командою **show startup-config** вміст стартової конфігурації (рис. 4.5.8).

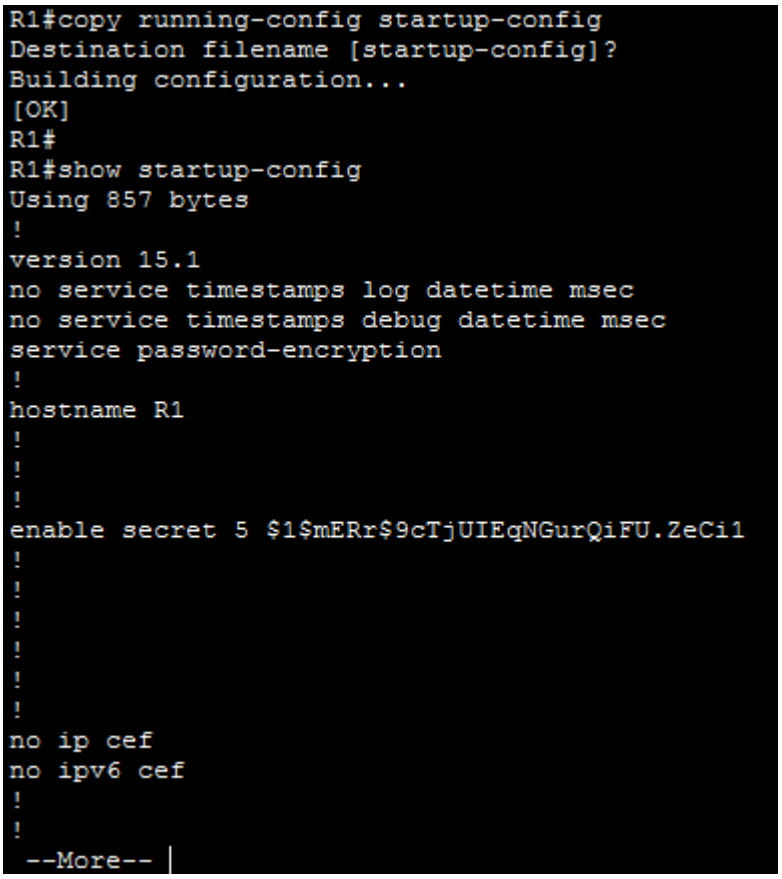

Рисунок 4.5.8 – Перегляд таблиці маршрутизації.

Слово --More-- в нижній частині екрана вказує на те, що на екран виведено не всю наявну інформацію. Можна натиснути клавішу пробіл для виводу наступної порції інформації розміром в один екран, клавішу Enter для виводу одного рядка або бідь-яку іншу клавішу для переривання виводу інформації.

Питання для самоперевірки

1. Яка команда активує інтерфейс маршрутизатора?
2. В чому різниця між файлами running-config та startup-config?
3. Якою командою можна переглянути стислу інформацію про стан та IP-адресу усіх інтерфейсів?
4. Чому важливо використовувати команду service password-encryption?
5. Яку команду потрібно ввести, щоб задати IP-адресу 10.0.0.1 з маскою 255.0.0.0 на інтерфейсі?
6. Що станеться з налаштованими IP-адресами після перезавантаження маршрутизатора, якщо ви не виконали команду copy running-config startup-config?
7. Яке призначення маршрутизатора в комп'ютерній мережі?
8. Які основні режими командного рядка Cisco IOS існують на маршрутизаторі?
9. Для чого використовується режим глобальної конфігурації?
10. Якою командою задається ім'я маршрутизатора?
11. Як налаштувати пароль доступу до привілейованого режиму?
12. Які команди використовуються для захисту віддаленого доступу?
13. Яка команда використовується для активації інтерфейсу?
14. Де зберігаються файли running-config і startup-config?
15. Як зберегти поточну конфігурацію маршрутизатора?
16. Якою командою можна переглянути таблицю маршрутизації маршрутизатора?
17. Як перевірити зв'язок маршрутизатора з іншими пристроями в мережі?

Лабораторна робота 6

Побудова простої мережі з комутатором і маршрутизатором

Мета: Закріпити навички створення фізичної топології мережі, навчитись поєднувати функції комутації та маршрутизації, налаштовувати адресацію кінцевих пристроїв та шлюзу за замовченням, а також діагностувати стан мережі за допомогою команд Cisco IOS.

Завдання: 1. З'єднання топології та ініціалізація пристроїв.

2. Налаштування пристроїв та перевірка з'єднання.

3. Перегляд інформації про пристрої.

Необхідні ресурси: два комп'ютери, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель, прямі та перехресні Ethernet-кабелі, будь-який з комутаторів Cisco Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо та будь-який з маршрутизаторів Cisco 8200, 1941, 4331 тощо.

Теоретичні відомості

У цій лабораторній роботі ми об'єднуємо два рівні мережевої моделі: канальний (L2) та мережевий (L3). Комутатор забезпечує з'єднання пристроїв у межах однієї локальної мережі (LAN). Він оперує MAC-адресами та пересилає кадри безпосередньо між портами. Маршрутизатор використовується для пересилки пакетів між різними мережами, в тому числі для зв'язку із зовнішніми мережами (наприклад, мережею Інтернет). Він оперує IP-адресами і пересилає пакети.

Ключовим поняттям у такій топології є адреса шлюзу за замовченням (Default Gateway). Це IP-адреса інтерфейсу маршрутизатора, до якого підключена локальна мережа. Якщо комп'ютер намагається відправити пакет пристрою, що знаходиться в іншій мережі, він інкапсулює цей пакет в кадр та надсилає його саме на шлюз за замовченням.

Хід роботи

Завдання 1. З’єднання топології та ініціалізація пристроїв.

Увімкніть живлення та з’єднайте пристрої відповідно до топології, наведеної на рисунку 4.6.1.

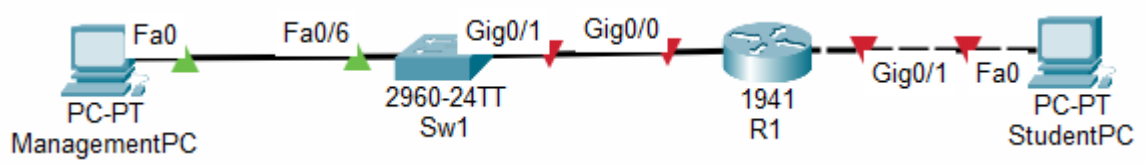

Рисунок 4.6.1 – Топологія мережі.

Для з’єднання комп’ютера з комутатором та комутатора з маршрутизатором використовують прямі кабелі. Для з’єднання комп’ютера з маршрутизатором – перехресні.

ВАЖЛИВО! Перед початком налаштування переконайтеся, що пристрої не містять старих конфігурацій. Для видалення попередньо створених файлів конфігурації на маршрутизаторі та комутаторі використайте команду **erase startup-config** та підтвердіть видалення. На комутаторі додатково треба видалити базу даних VLAN командою **delete vlan.dat**. Перезавантажте пристрої командою **reload**.

Завдання 2. Налаштування пристроїв та перевірка з’єднання.

Налаштуйте статичні IP-адреси, маски підмережі та адреси шлюзу за замовченням на комп’ютерах відповідно до таблиці 4.6.1.

Таблиця 4.6.1 – Адресація мережних пристроїв

Пристрій	Інтерфейс	IP-адреса/Префікс	Шлюз за замовчуванням
R1	G0/0	172.16.10.1/24	–
	G0/1	172.16.20.1/24	
Sw1	VLAN 1	172.16.10.101/24	172.16.10.1
ManagementPC	Fa0	172.16.10.10/24	172.16.10.1
StudentPC	Fa0	172.16.20.10/24	172.16.20.1

Здійсніть початкове налаштування комутатора. До початкового налаштування відноситься: ім’я комутатора, вимкнення пошуку DNS, паролі, банер, точний час. Налаштування віртуального інтерфейсу VLAN 1 та шлюзу за замовчуванням здійснюється відповідно до таблиці 4.6.1. Не забудьте активувати віртуальний інтерфейс VLAN 1 (рис. 4.6.2). Детально початкове налаштування комутатора розглядалось в лабораторній роботі №2.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sw1
Sw1(config)#no ip domain lookup
Sw1(config)#enable secret class
Sw1(config)#line console 0
Sw1(config-line)#password cisco
Sw1(config-line)#login
Sw1(config-line)#exit
Sw1(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
Sw1(config)#line vty 0 15
Sw1(config-line)#password cisco
Sw1(config-line)#login
Sw1(config-line)#exit
Sw1(config)#service password-encryption
Sw1(config)#banner motd # Authorized Users Only! #
Sw1(config)#interface vlan 1
Sw1(config-if)#ip address 172.16.10.101 255.255.255.0
Sw1(config-if)#no shutdown

Sw1(config-if)#
%LINK-3-UPDOWN: Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Sw1(config-if)#exit
Sw1(config)#ip default-gateway 172.16.10.1
Sw1(config)#
Sw1(config)#exit
Sw1#
%SYS-5-CONFIG_I: Configured from console by console

Sw1#clock set 12:10:00 27 Dec 2025
Sw1#
Sw1#
```

Рисунок 4.6.2 – Початкове налаштування комутатора.

Зробіть початкове налаштування маршрутизатора. До початкового налаштування маршрутизатора також відноситься: ім’я, вимкнення пошуку DNS, паролі, банер, точний час. Налаштуйте інтерфейси GigabitEthernet0/0 та GigabitEthernet0/1 відповідно до таблиці 4.6.1 (рис. 4.6.3). Детально початкове налаштування маршрутизатора розглядалось в лабораторній роботі №5.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd @ Authorized Users Only! @
R1(config)#interface g0/0
R1(config-if)#ip address 172.16.10.1 255.255.255.0
R1(config-if)#description Connected to LAN-10
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R1(config-if)#interface g0/1
R1(config-if)#ip address 172.16.20.1 255.255.255.0
R1(config-if)#description Connected to LAN-20
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clock set 12:20:00 27 Dec 2025
R1#
```

Рисунок 4.6.3 – Початкове налаштування маршрутизатора.

Перевірте з’єднання, використовуючи команду **ping** на комп’ютерах.

Пропінгуйте з комп’ютера ManagementPC шлюз за замовченням (**ping 172.16.10.1**). Успішне пінгування означає, що з’єднання з маршрутизатором встановлено (рис. 4.6.4).

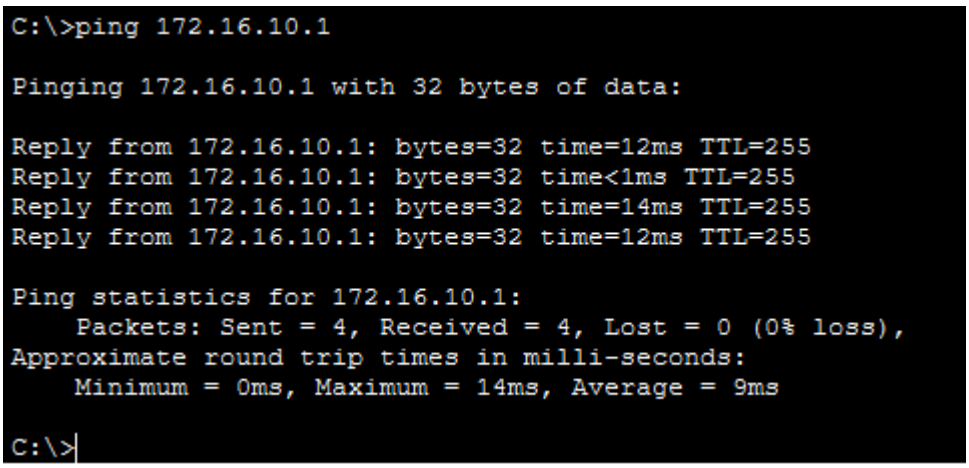

Рисунок 4.6.4 – Перевірка зв'язку комп'ютера ManagementPC з шлюзом за замовченням.

Пропінгуйте з комп'ютера StudentPC шлюз за замовченням (**ping 172.16.20.1**). Пропінгуйте з комп'ютера StudentPC комутатор Sw1 (**ping 172.16.10.101**). Пропінгуйте з комп'ютера StudentPC комп'ютер ManagementPC (**ping 172.16.10.10**). Успішне пінгування означає, що всі пристрої в мережі можуть нормально взаємодіяти між собою (рис. 4.6.5).

Завдання 3. Перегляд інформації про пристрої.

Для діагностики та паспортизації мережі необхідно вміти отримувати інформацію про мережні пристрої. Виконайте наступні команди на маршрутизаторі R1 та проаналізуйте вивід.

Команда **show ip route** виводить на екран таблицю маршрутизації. Ця команда показує, інформація про які мережі відома маршрутизатору. Ви повинні побачити маршрути з кодом «C» (Connected) для мереж 172.16.10.0/24 та 172.16.20.0/24. Це означає, що ці мережі підключені напряму до інтерфейсів маршрутизатор. Також в таблиці маршрутизаціє мають бути маршрути з кодом «L» (Local) для мереж 172.16.10.1/32 та 172.16.20.1/32. Ці маршрути призначені для локальних інтерфейсів маршрутизатора і застосовуються в тих випадках коли пакет призначений самому маршрутизатору і не має бути кудись пересланий.

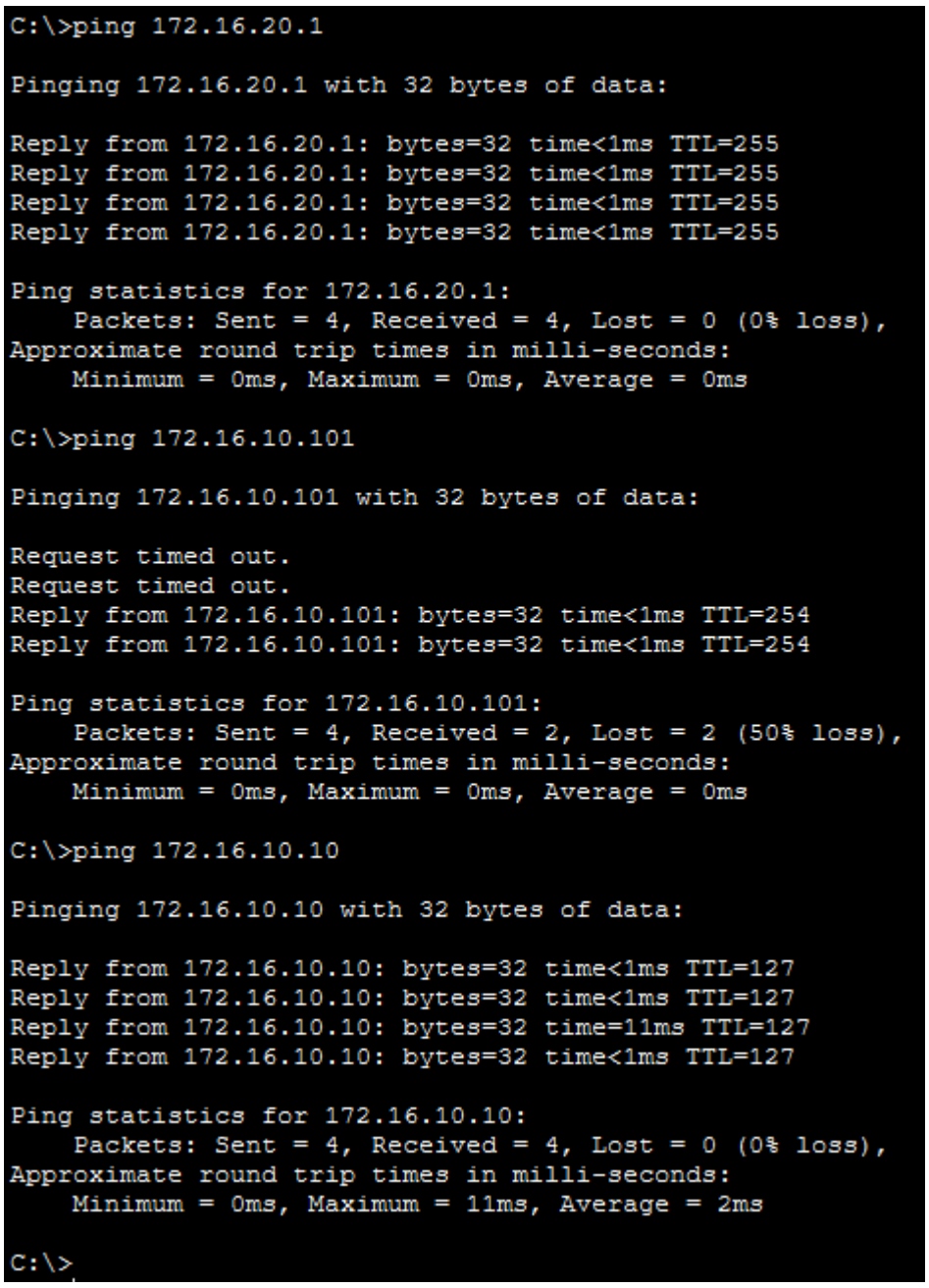

Рисунок 4.6.5 – Перевірка зв’язку комп’ютера StudentPC з шлюзом за замовченням, комутатором Sw1 та комп’ютером ManagementPC.

Команда **show ip interface brief** використовується для перевірки стану інтерфейсів. Це найшвидший спосіб перевірити налаштування та стан усіх інтерфейсів. Переконайтеся, що для інтерфейсу GigabitEthernet0/0 встановлено IP-адресу 172.16.10.1, Status «up», Protocol: «up», а для інтерфейсу GigabitEthernet0/1 IP-адреса 172.16.20.1, Status «up», Protocol: «up».

Команда **show interfaces g0/0** виводить на екран детальну інформацію про інтерфейс. Тут можна побачити MAC-адресу інтерфейсу (Hardware is...), швидкість, дуплекс та статистику помилок (errors, collisions).

Команда **show version** (рис. 4.6.6) застосовується для отримання інформації про в операційну систему та встановлене обладнання. Ця команда виводить версію операційної системи, час безперервної роботи (Uptime), ім'я файлу образу системи, платформу, тип процесора та об'єм пам'яті (DRAM та Flash), значення конфігураційного регістру (Configuration register) тощо.

```
R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 hours, 43 minutes, 52 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

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

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                 SN
-------------------------------------------------
*0        CISCO1941/K9        FTX15248OIU-


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

Рисунок 4.6.6 – Фрагмент виводу команди show version.

Збережіть конфігурацію на обох проміжних мережних пристроях командою **copy running-config startup-config**.

Питання для самоперевірки

1. Що означають статуси «Status: up» та «Protocol: up» у виводі команди show ip interface brief?
2. Яка команда дозволяє побачити MAC-адресу інтерфейсу маршрутизатора?
3. Яка інформація міститься у значенні «Configuration register» у виводі show version?
4. Що станеться з мережею, якщо на маршрутизаторі забути ввести команду no shutdown на інтерфейсі?
5. Яку роль виконує комутатор у локальній мережі, а яку маршрутизатор?
6. На яких рівнях моделі OSI працюють комутатор і маршрутизатор?
7. Чому в мережі з кількома підмережами не можна обійтися без маршрутизатора?
8. Які типи пристроїв зазвичай підключаються до портів доступу комутатора?
9. Який тип кабелю використовується для з’єднання ПК з комутатором?
10. Який тип кабелю використовується для з’єднання комутатора з маршрутизатором?
11. Чому важливо перевіряти стан інтерфейсів після підключення кабелів?
12. Які параметри необхідно налаштувати на ПК для коректної роботи в мережі?
13. Для чого на ПК налаштовується адреса шлюзу за замовчуванням?
14. Яка команда використовується для призначення IP-адреси інтерфейсу маршрутизатора?
15. Для чого використовується команда no shutdown?
16. Яку функцію виконує інтерфейс VLAN 1 на комутаторі?
17. Якою командою можна перевірити зв’язок між ПК і маршрутизатором?
18. Яку інформацію надає команда show ip interface brief?
19. Чому після зміни конфігурації важливо зберігати її в пам’ять пристрою?

Лабораторна робота 7

Проєктування та впровадження схеми адресації підмереж змінної довжини (VLSM)

Мета: Навчитися аналізувати потреби мережі в IP-адресах, розраховувати маски підмереж змінної довжини (VLSM) для ефективного використання адресного простору, а також реалізовувати розроблену схему адресації на реальному обладнанні.

Завдання: 1. Дослідження вимог, що висуваються до мережі.

2. Створення схеми адресації VLSM.

3. Під'єднання кабелів і налаштування мережі IPv4.

Необхідні ресурси: три комп'ютери, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель, прямі та перехресні Ethernet-кабелі, 3 будь-яких комутатора Cisco - Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо та 2 будь-яких маршрутизатора Cisco - 8200, 1941, 4331 тощо.

Теоретичні відомості

Якщо всі пристрої знаходяться в одній великій мережі, це створює цілий ряд проблем: зростає кількість широкомовних (broadcast) повідомлень, складніше керувати безпекою і як наслідок, мережа стає менш ефективною. Тому великі мережі розділяють на декілька мереж меншого розміру – так звані підмережі.

IPv4-адреса складається з 32 біт і зазвичай записується в крапково-десятковому форматі – у вигляді чотирьох чисел в десятковій системі, розділених крапками, наприклад, 192.168.1.10. Будь-яка IPv4-адреса складається з двох частин – мережної та вузлової. В різних мережах довжина мережної частини, яку ще називають префіксом, може відрізнятись. Зазвичай вона становить від 8 до 30 бітів. Щоб зрозуміти, де закінчується мережна частина і починається вузлова,

використовується маска підмережі. Вона показує, які біти в IP-адресі відносяться до мережної частини, а які до вузлової. Чим більше одиниць у масці, тим менше вузлів може бути в такій мережі. Маска підмережі задається також в крапково-десятковому форматі, наприклад, 255.255.255.0. Також довжина мережної частини може зазначатись у вигляді довжини префіксу – числа, що пишеться через скісну риску одразу після IP-адреси, наприклад, 192.168.1.10/24.

Загальний принцип розділення мережі на підмережі полягає у запозиченні (або перенесенні) бітів з вузлової частини в мережну. При цьому довжина префіксу збільшується, а кількість бітів у вузловій частині, а отже і доступних адрес в підмережі, навпаки – зменшується.

При розділенні мережі на підмережі застосовують дві формули. Для розрахунку кількості отриманих підмереж i:

$$i = 2^n \tag{4.7.1}$$

де n – кількість запозичених бітів, та для розрахунку максимальної кількості вузлів j в кожній з отриманих підмереж:

$$j = 2^m - 2 \tag{4.7.2}$$

де m – кількість бітів, що залишилась після запозичення у вузловій частині. Двійка віднімається від загальної кількості адрес, оскільки дві адреси не можуть використовуватись для адресації вузлів. Це адреса самої мережі – перша адреса в підмережі, вузлова частина якої складається з усіх нулів, та широкомовна (broadcast) адреса – остання адреса підмережі, вузлова частина якої складається з усіх одиниць. Наприклад, для мережі 192.168.1.0/25 адреса мережі – 192.168.1.0, широкомовна адреса – 192.168.1.127, а для вузлів доступний діапазон адрес 192.168.1.1 – 192.168.1.126.

Таким чином, при розділені мережі на підмережі нам необхідно дати відповідь на два запитання – скільки підмереж потрібно та скільки пристроїв (вузлів) має бути в кожній підмережі. В залежності від відповідей використовуються формули (4.7.1) та (4.7.2) і приймається рішення щодо кількості бітів для запозичення.

Наприклад, маємо мережу 192.168.10.0/24. Припустимо, нам потрібно 4 підмережі. За формулою (4.7.1) для 4 підмереж нам достатньо запозичити 2 біти, оскільки $i = 2^2 = 4$. Збільшивши довжину префіксу на два біти ми отримаємо нову довжину префіксу /24 + 2 = /26, отже, нова маска 255.255.255.192. Запозичені біти можуть приймати такі значення: 00, 01, 10, 11. Отже, отримані підмережі будуть мати такі адреси:

Таблиця 4.7.1 – Адреси отриманих підмереж

Останній октет в двійковому форматі, запозичені біти виділені жирним шрифтом	Адреса підмереж в десятковому форматі
192.168.10.**00**000000/26	192.168.10.0/26
192.168.10.**01**000000/26	192.168.10.64/26
192.168.10.**10**000000/26	192.168.10.128/26
192.168.10.**11**000000/26	192.168.10.192/26

У кожній з отриманих підмереж загалом $2^6 = 64$ адреси, з яких відповідно до формули (4.7.2) для адресації вузлів доступні $j = 2^6 - 2 = 62$ адреси. Для підмережі 192.168.10.0/26 це діапазон адрес 192.168.10.1 – 192.168.10.62, для підмережі 192.168.10.64/26 діапазон адрес 192.168.10.65 – 192.168.10.126, для підмережі 192.168.10.128/26 діапазон адрес 192.168.129.65 – 192.168.10.190, для підмережі 192.168.10.192/26 діапазон адрес 192.168.10.193 – 192.168.10.254.

Традиційне розбиття на підмережі, яке ще називають FLSM (Fixed Length Subnet Mask) передбачає використання однакової маски для всіх підмереж. Це призводить до неефективного використання адрес. Наприклад, використання для з'єднання двох маршрутизаторів (де потрібно лише 2 адреси) підмережі з довжиною префіксу 24 біти, розрахованої на $2^8 - 2 = 254$ вузли, є неефективним використанням адресного простору. VLSM (Variable Length Subnet Mask) – це технологія, що дозволяє використовувати маски підмереж різної довжини. Основний принцип VLSM полягає в тому, що мережа розбивається на підмережі, а потім кожна з отриманих підмереж розглядається як окрема мережа, яка в свою чергу може бути знову розбита на підмережі.

Для успішного розрахунку VLSM критично важливо дотримуватися правила: завжди починайте розподіл адрес із найбільшої підмережі (тієї, що потребує найбільшої кількості вузлів) і рухайтеся до найменшої.

Хід роботи

Завдання 1. Дослідження вимог, що висуваються до мережі.

Уявіть, що ви отримали технічне завдання на проєктування мережі для невеликого офісу. Вам виділено мережу з адресою 192.168.10.0/24. Вимоги до підмереж:

Для підмережі відділу продажів (LAN Sales) необхідно 25 вузлів.

Для підмережі адміністрації (LAN Administrations) необхідно 60 вузлів.

Для підмережі IT-відділу (LAN IT) необхідно 10 вузлів.

Для з'єднання маршрутизаторів між собою (WAN) необхідно 2 IP-адреси.

Ваше завдання – не просто розбити мережу, а зробити це так, щоб не залишилося «дірок» між адресами, і зберегти максимум вільного адресного простору для майбутнього розширення.

Завдання 2. Створення схеми адресації VLSM.

Для початку відсортуємо вимоги від найбільшого до найменшого.

1. LAN Administrations – 60 вузлів.
2. LAN Sales – 25 вузлів.
3. LAN IT – 10 вузлів.
4. WAN – 2 вузлів.

Далі здійснимо розрахунок для кожної підмережі.

1. LAN Administrations (60 вузлів). Щоб покрити 60 вузлів, нам потрібно 6 бітів ($j = 2^6 - 2 = 62 \geq 60$). Отже, довжина префіксу буде /26 ($32 - 6 = 26$). Маска 255.255.255.192. Адреса підмережі 192.168.10.0/26. Діапазон адрес для вузлів 192.168.10.1 – 192.168.10.62. Broadcast 192.168.10.63.

2. LAN Sales (25 вузлів). Наступна вільна адреса 192.168.10.64. Щоб покрити 25 вузлів, потрібно 5 бітів ($j = 2^5 - 2 = 30 \geq 25$). Довжина префіксу /27 ($32 - 5 = 27$), маска 255.255.255.224, адреса підмережі 192.168.10.64/27. Діапазон адрес для вузлів 192.168.10.65 – 192.168.10.94. Broadcast 192.168.10.95.

3. LAN IT (10 вузлів). Наступна вільна адреса 192.168.10.96. Щоб покрити 10 вузлів, потрібно 4 біти ($j = 2^4 - 2 = 14 \geq 10$). Довжина префіксу /28 ($32 - 4 = 28$). Маска 255.255.255.240. Адреса підмережі:

192.168.10.96/28. Діапазон адрес для вузлів 192.168.10.97 – 192.168.10.110. Broadcast 192.168.10.111.

4. WAN – з'єднання (2 вузли). Наступна вільна адреса 192.168.10.112. Щоб покрити 2 вузли потрібно 2 біти ($j = 2^2 - 2 = 2 \geq 2$). Довжина префіксу /30 ($32 - 2 = 30$). Маска 255.255.255.252. Адреса підмережі 192.168.10.112/30. Діапазон адрес для вузлів 192.168.10.113 – 192.168.10.114. Broadcast 192.168.10.115.

На підставі отриманих даних побудуємо таблицю мереж та таблицю адресації пристроїв.

Таблиця 4.7.2 – Адреси отриманих підмереж

Назва мережі	Необхідно вузлів	Адреса підмережі	Маска (десяткова)	Перша адреса	Остання адреса
LAN-Administrations	60	192.168.10.0/26	255.255.255.192	192.168.10.1	192.168.10.62
LAN Sales	25	192.168.10.64/27	255.255.255.224	192.168.10.65	192.168.10.94
LAN IT	10	192.168.10.96/28	255.255.255.240	192.168.10.97	192.168.10.110
WAN	2	192.168.10.112/30	255.255.255.252	192.168.10.113	192.168.10.114

Таблиця 4.7.3 – Адресація мережних пристроїв

Пристрій	Інтерфейс	IP-адреса/Префікс	Шлюз за замовчуванням
R1	G0/0	192.168.10.113/30	–
	G0/1	192.168.10.1/26	
	G0/2	192.168.10.65/27	
R2	G0/0	192.168.10.114/30	–
	G0/1	192.168.10.97/28	
Sw-Admin	VLAN 1	192.168.10.20	192.168.10.1
Sw-Sales	VLAN 1	192.168.10.85	192.168.10.65
Sw-IT	VLAN 1	192.168.10.105	192.168.10.97
PC-Administration	Fa0	192.168.10.10	192.168.10.1
PC-Sales	Fa0	192.168.10.75	192.168.10.65
PC-IT	Fa0	192.168.10.100	192.168.10.97

Завдання 3. Під’єднання кабелів і налаштування мережі IPv4.

Увімкніть живлення та з’єднайте пристрої відповідно до топології, наведеної на рисунку 4.7.1.

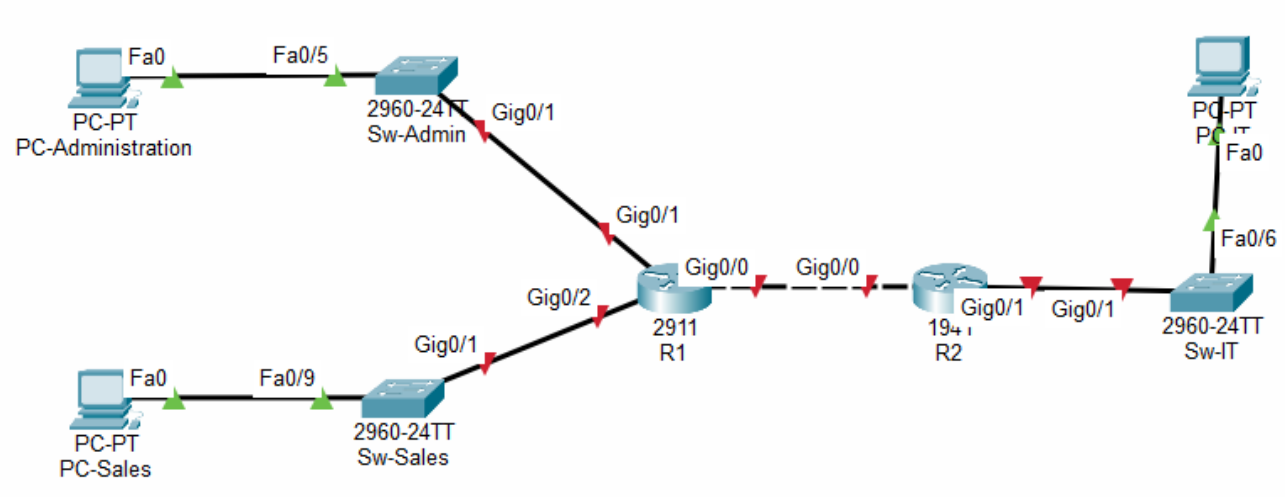

Рисунок 4.7.1 – Топологія мережі.

Для з’єднання комп’ютера з комутатором та комутатора з маршрутизатором використовують прямі кабелі. Для з’єднання комп’ютера з маршрутизатором – перехресні.

Зробимо базові налаштування усіх комутаторів та маршрутизаторів. Налаштуємо IP-адреси на комп’ютерах відповідно до таблиці 4.7.3. Детально ці налаштування розглядались в лабораторних роботах №2 та №5.

Налаштуємо інтерфейси на маршрутизаторі R1 відповідно до таблиці 4.7.3 (рис. 4.7.2).

Також налаштуємо інтерфейси на маршрутизаторі R2 відповідно до таблиці 4.7.3 (рис. 4.7.3).

Перейдемо до налаштувань комутаторів. Налаштуємо віртуальний інтерфейс VLAN 1 та шлюз за замовченням на комутаторі Sw-Admin відповідно до таблиці 4.7.3 (рис. 4.7.4). Цей інтерфейс, а також шлюз за замовченням, потрібні для можливості віддаленого керування комутатором за протоколом SSH/Telnet. Комутатори Sw-Sales та Sw-IT налаштуємо за аналогією.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#description Link to R2
R1(config-if)#ip address 192.168.10.113 255.255.255.252
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#interface gigabitEthernet 0/1
R1(config-if)#description Link to LAN-Administrations
R1(config-if)#ip address 192.168.10.1 255.255.255.192
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)#interface gigabitEthernet 0/2
R1(config-if)#description Link to LAN-Sales
R1(config-if)#ip address 192.168.10.65 255.255.255.224
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

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

R1(config-if)#
R1(config-if)#exit
R1(config)#
```

Рисунок 4.7.2 – Налаштування маршрутизатора R1.

```
R2(config)#interface gigabitEthernet0/0
R2(config-if)#ip address 192.168.10.114 255.255.255.252
R2(config-if)#description Link to R1
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R2(config-if)#interface gigabitEthernet0/1
R2(config-if)#ip address 192.168.10.97 255.255.255.240
R2(config-if)#description Link to LAN-IT
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R2(config-if)#
R2(config-if)#exit
R2(config)#
```

Рисунок 4.7.3 – Налаштування маршрутизатора R2.

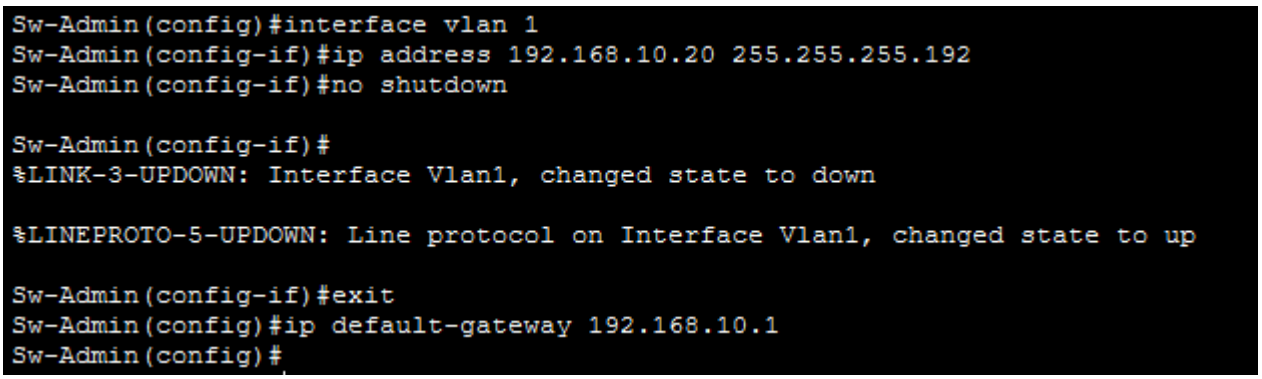

Рисунок 4.7.4 – Налаштування комутатора Sw-Admin.

На цьому етапі всі комп'ютери можуть пінгувати свої шлюзи за замовченням та комутатори, до яких вони під'єднані. Але вони не можуть пінгувати один одного. Це пов'язано з тим, що на маршрутизаторах немає маршрутів до віддалених мереж (детально маршрутизація буде розглядатись пізніше). Налаштуємо на маршрутизаторах R1 та R2 статичні маршрути за замовченням (рисунки 4.7.5 та 4.7.6).

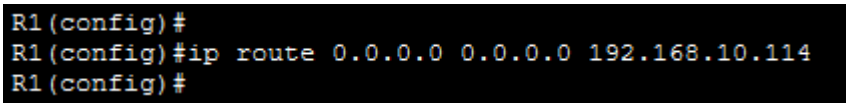

Рисунок 4.7.5 – Налаштування маршруту за замовченням
на маршрутизаторі R1.

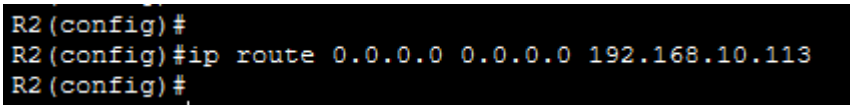

Рисунок 4.7.6 – Налаштування маршруту за замовченням
на маршрутизаторі R2.

Перевіримо таблиці маршрутизації на маршрутизаторі R1 та R2. Вони повинні мати вигляд як на рисунках 4.7.7 та 4.7.8

На цьому налаштування мережі можна вважати закінченим. Будь-який пристрій в мережі має зв'язок з будь-яким іншим пристроєм. Для тестування пропінгуємо з комп'ютера PC-Administration інші комп'ютери (рис. 4.7.9).

```
R1#
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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 192.168.10.114 to network 0.0.0.0

     192.168.10.0/24 is variably subnetted, 6 subnets, 4 masks
C       192.168.10.0/26 is directly connected, GigabitEthernet0/1
L       192.168.10.1/32 is directly connected, GigabitEthernet0/1
C       192.168.10.64/27 is directly connected, GigabitEthernet0/2
L       192.168.10.65/32 is directly connected, GigabitEthernet0/2
C       192.168.10.112/30 is directly connected, GigabitEthernet0/0
L       192.168.10.113/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.10.114

R1#
```

Рисунок 4.7.7 – Таблиця маршрутизації маршрутизатора R1.

```
R2#
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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 192.168.10.113 to network 0.0.0.0

     192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
C       192.168.10.96/28 is directly connected, GigabitEthernet0/1
L       192.168.10.97/32 is directly connected, GigabitEthernet0/1
C       192.168.10.112/30 is directly connected, GigabitEthernet0/0
L       192.168.10.114/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.10.113

R2#
```

Рисунок 4.7.8 – Таблиця маршрутизації маршрутизатора R2.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:64FF:FE86:A299
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.10.10
   Subnet Mask.....: 255.255.255.192
   Default Gateway.....: ::
                                 192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.10.75

Pinging 192.168.10.75 with 32 bytes of data:

Reply from 192.168.10.75: bytes=32 time=1ms TTL=127
Reply from 192.168.10.75: bytes=32 time=13ms TTL=127
Reply from 192.168.10.75: bytes=32 time=8ms TTL=127
Reply from 192.168.10.75: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.10.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 9ms

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=5ms TTL=126
Reply from 192.168.10.100: bytes=32 time=16ms TTL=126
Reply from 192.168.10.100: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 9ms

C:\>
```

Рисунок 4.7.9 – Тестування зв’язку між комп’ютерами мережі.

Питання для самоперевірки

1. Що таке розділення IPv4 мережі на підмережі?
2. З якою метою в мережах використовується розділення мережі на підмережі?
3. Яку роль відіграє маска підмережі в IPv4?
4. Чим відрізняється мережева частина IP-адреси від вузлової?
5. Що означає запис /24, /26, /30 у CIDR-нотації?
6. Скільки бітів містить IPv4-адреса?
7. Які адреси в підмережі не можуть бути призначені вузлам і чому?
8. Скільки доступних вузлів у підмережі з маскою /26?
9. Як обчислити кількість підмереж при зміні маски?
10. Як визначити кількість вузлів у підмережі за відомою маскою?
11. Що таке адреса мережі?
12. Скільки підмереж можна отримати з мережі /24, якщо використати маску /27?
13. Яка мінімальна маска підмережі дозволяє мати 2 вузли?
14. Для яких типів з’єднань найчастіше використовується маска /30?
15. Чи можуть два пристрої з різними масками підмережі знаходитися в одній мережі?
16. Як визначити, чи належать два IPv4-адреси до однієї підмережі?
17. Чому при розрахунку VLSM важливо починати з найбільшої підмережі?
18. Скільки хостів дозволяє адресувати маска /27?
19. Яка маска підмережі (у десятковому вигляді) відповідає префіксу /30?
20. Чи перетинаються адресні простори підмереж 192.168.10.0/26 та 192.168.10.64/26?
21. Чому використання маски /24 для з'єднання двох маршрутизаторів вважається неефективним?
22. Яка адреса буде broadcast-адресою для підмережі 192.168.10.96/28?
23. Чи можна призначити адресу 192.168.10.63 хосту в мережі LAN-Administrations? Чому?

Лабораторна робота 8

Захист мережних пристроїв

Мета: Навчитися застосовувати базові методи захисту мережних пристроїв, налаштовувати адміністративний доступ через захищений протокол SSH, реалізовувати політику безпеки паролів та захист від атак перебором.

Завдання: 1. Налаштування базових параметрів безпеки на маршрутизаторі та комутаторі.

2. Налаштування маршрутизатора для SSH-доступу.

3. Встановлення віддаленого зв'язку за допомогою SSH з маршрутизатором.

Необхідні ресурси: два комп'ютери, програма емуляції терміналу (наприклад, PuTTY, Tera Term або HyperTerminal), консольний кабель, прямі та перехресні Ethernet-кабелі, комутатор Cisco Catalyst 9200, Catalyst 1300, Catalyst 2960, Catalyst 3560, Catalyst 3760 тощо та маршрутизатор Cisco 8200, 1941, 4331 тощо.

Теоретичні відомості

За замовчуванням мережеві пристрої не мають налаштованих параметрів безпеки, що робить їх вразливими до несанкціонованого доступу. Адміністратор повинен застосувати низку заходів для їх захисту мережних пристроїв, серед яких: розробка політики паролів та шифрування паролів, захист від перебору паролів, обмеження тайм-ауту сесій, налаштування протоколу SSH для безпечного віддаленого доступу.

Зберігання паролів у відкритому вигляді в файлах конфігурації (наприклад, пароля консольного порту) є небезпечним. Команда **service password-encryption** дозволяє зашифрувати всі наявні та майбутні паролі слабким алгоритмом типу 7, що захищає їх від випадкового підглядання «через плече». Для посилення паролів використовується команда **security passwords min-length** *length*, яка

забороняє створення паролів, довжиною менших за значення параметру *length*. Для захисту від спроб підбору пароля в IOS існує механізм блокування входу у випадку заданої кількості невдалих спроб. Команда **login block-for** *time* **attempts** *num* **within** *time* тимчасово блокує можливість входу, якщо за визначений час було здійснено певну кількість невдалих спроб. Наприклад, введення команди **login block-for 60 attempts 2 within 10** призведе до блокування на 60 секунд користувача, який намагатиметься отримати доступ до маршрутизатора через Telnet або SSH і протягом 10 секунд двічі введе неправильний пароль.

Залишені без нагляду активні сесії адміністратора є величезним ризиком. Команда **exec-timeout** *minutes seconds*, застосована на лініях зв'язку (console, vty), автоматично розриває з'єднання після заданого періоду бездіяльності.

Протокол віддаленого доступу Telnet передає всі дані, включаючи паролі, у відкритому вигляді, тому він вважається небезпечним і його використання в сучасних мережах заборонено. На відміну від нього SSH забезпечує шифрування сесії, автентифікацію та цілісність даних. Тому для віддаленого керування слід використовувати саме SSH замість застарілого протоколу Telnet. Для налаштування SSH необхідно змінити ім'я вузла за замовченням (команда **hostname**) задати командою **ip domain-name** доменне ім'я, локально створити обліковий запис користувача (команда **username**) та командою **crypto key generate rsa** згенерувати криптографічні ключі RSA. Також необхідно налаштувати віртуальні лінії VTY на прийом лише SSH-з'єднань (команда **transport input ssh**).

Хід роботи

Завдання 1. Налаштування базових параметрів безпеки на маршрутизаторі та комутаторі.

Увімкніть живлення та з'єднайте пристрої відповідно до топології, наведеної на рисунку 4.8.1.

Рисунок 4.8.1 – Топологія мережі.

Здійсніть базові налаштування комутатора та маршрутизатора. Налаштуйте статичні IP-адреси, маски підмережі та адреси шлюзу за замовченням на комп'ютерах, а також адресацію на комутаторі та маршрутизаторі відповідно до таблиці 4.8.1. Ці налаштування детально розглядались в лабораторних роботах №2 та №5.

Таблиця 4.8.1 – Адресація мережних пристроїв

Пристрій	Інтерфейс	IP-адреса/Префікс	Шлюз за замовчуванням
R1	G0/0	172.16.10.1/24	–
	G0/1	172.16.20.1/24	
Sw1	VLAN 1	172.16.10.101/24	172.16.10.1
ManagementPC	Fa0	172.16.10.10/24	172.16.10.1
StudentPC	Fa0	172.16.20.10/24	172.16.20.1

Після цього перейдемо до базових налаштувань безпеки на маршрутизаторі. Налаштуємо паролі для привілейованого режиму та консольного порту, зашифруємо паролі. Захищати лінії зв'язку поки що не будемо, зробимо це згодом при налаштуванні протоколу SSH. Налаштування базових параметрів безпеки маршрутизатора наведено на рисунку 4.8.2.

```
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#
```

Рисунок 4.8.2 – Налаштування базових параметрів безпеки маршрутизатора.

Встановіть мінімальну довжину пароля (наприклад, 10 символів), щоб запобігти використанню слабких паролів. Для цього застосуємо команду **security passwords min-length** 10 (рис. 4.8.3).

```
R1(config)#
R1(config)#security passwords min-length ?
  <0-16>  Minimum length of all user/enable passwords
R1(config)#security passwords min-length 10
R1(config)#
```

Рисунок 4.8.3 – Налаштування мінімальної довжини пароля.

Далі необхідно захистити маршрутизатор від атак перебору, які ще називають атаки грубої сили. Налаштуйте блокування спроб входу. Якщо хтось помилиться при введенні пароля 3 рази протягом 60 секунд, вхід буде заблоковано на 120 секунд, команда **login block-for 120 attempts 3 within 60** (рис. 4.8.4).

```
R1(config)#
R1(config)#login block-for ?
  <1-65535>  Time period in seconds
R1(config)#login block-for 120 attempts ?
  <1-65535>  Fail attempts max value
R1(config)#login block-for 120 attempts 3 within ?
  <1-65535>  Time period in seconds
R1(config)#login block-for 120 attempts 3 within 60
R1(config)#
```

Рисунок 4.8.4 – Захист маршрутизатора від атак перебору.

Тепер командою **exec-timeout 5 0** налаштуємо тайм-аут бездіяльності (5 хвилин 0 секунд) для консольної лінії зв’язку, щоб сесія автоматично закривалася, якщо ви відійшли від комп’ютера і протягом заданого часу не торкнулися клавіатури. Також командою **logging synchronous** налаштуйте синхронізацію виводу логів, щоб системні повідомлення syslog не переривали введення команд (рис. 4.8.5).

```
R1(config)#line console 0
R1(config-line)#exec-timeout ?
  <0-35791>  Timeout in minutes
R1(config-line)#exec-timeout 5 ?
  <0-2147483>  Timeout in seconds
  <cr>
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

Рисунок 4.8.5 – Налаштування тайм-аут бездіяльності.

Налаштування параметрів безпеки на комутаторі здійснюється аналогічно.

Завдання 2. Налаштування маршрутизатора для SSH-доступу.

Для роботи SSH маршрутизатор повинен мати унікальні назву та доменне ім'я. Ці умови є обов'язковими для генерації ключів. Доменне ім'я налаштовується командою **ip domain-name** *domain-name*. Створіть обліковий запис локального адміністратора. Використовуйте команду **secret** для хешування пароля (пароль має бути не коротшим за 10 символів, оскільки раніше ми налаштували мінімальну довжину пароля, наприклад, CiscoAdmin123). Для створення облікового запису введемо команду **username admin secret CiscoAdmin123**.

Тепер можемо перейти до безпосереднього налаштування протоколу SSH. Командою **ip ssh version 2** активуємо другу версію. Командою **crypto key generate rsa** згенеруйте ключі RSA. Система запитає довжину ключа. Введіть 2048 та натисніть Enter (рис. 4.8.6).

```
R1(config)#ip domain-name fit.knu.ua
R1(config)#username admin secret CiscoAdmin123
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R1(config)#crypto key generate rsa
The name for the keys will be: R1.fit.knu.ua
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
```

Рисунок 4.8.6 – Налаштування SSH.

ВАЖЛИВО! Якщо ви зміните назву вузла або доменне ім'я, ключі доведеться генерувати заново.

Налаштуємо віртуальні лінії VTY для віддаленого доступу. Вкажемо, що для входу потрібно використовувати локальну базу користувачів (команда **login local**). Командою **transport input ssh** дозволимо лише протокол SSH, заборонивши Telnet. Командою **exec-timeout 5 0** встановимо тайм-аут бездіяльності 5 хвилин. Налаштування віртуальних ліній VTY наведено на рисунку 4.8.7.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exec-timeout 5 0
R1(config-line)#exit
R1(config)#
```

Рисунок 4.8.7 – Налаштування віртуальних ліній VTY.

Завдання 3. Встановлення віддаленого зв'язку за допомогою SSH з маршрутизатором.

Перейдемо на комп'ютер. Спочатку перевіримо налаштування мережного адаптера та наявність зв'язку з маршрутизатором (рис. 4.8.8).

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:96FF:FEA7:329D
   IPv6 Address.....: ::
   IPv4 Address.....: 172.16.10.10
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 172.16.10.1

C:\>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:

Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рисунок 4.8.8 – Перевірка налаштувань мережного адаптера та зв'язку з маршрутизатором.

Оскільки зв'язок є, спробуємо встановити віддалене з'єднання за допомогою SSH. Використаємо команду Windows **ssh -l** *username target*, де *username* – ім'я користувача, а *target* – IP-адреса відділеного вузла (рис. 4.8.9).

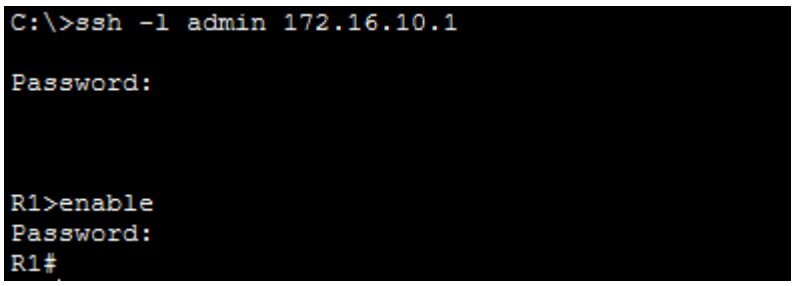

Рисунок 4.8.9 – Успішне встановлення віддаленого з’єднання з маршрутизатором за допомогою протоколу SSH.

При спробі доєднатись до маршрутизатора через Telnet бачимо повідомлення, що з’єднання відхилене віддаленим вузлом (рис. 4.8.10).

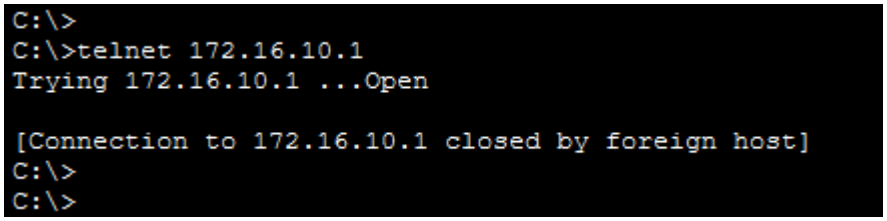

Рисунок 4.8.10 – Невдале встановлення віддаленого з’єднання з маршрутизатором за допомогою протоколу Telnet.

Для перевірки активних сесій на маршрутизаторі виконайте команду **show ssh**. Ви побачите інформацію про поточну активну сесію, версію протоколу та ім’я користувача (рис. 4.8.11).

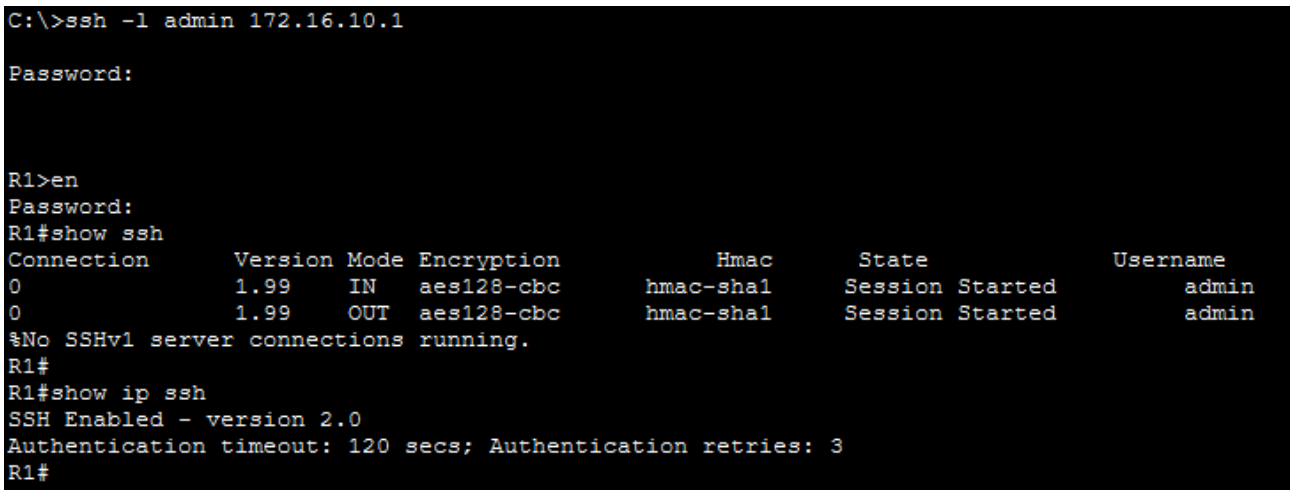

Рисунок 4.8.11 – Активні SSH сесії на маршрутизаторі.

Питання для самоперевірки

1. Чим протокол SSH кращий за Telnet?
2. Яка команда змушує маршрутизатор перевіряти локальну базу користувачів при з’єднанні через VTY лінії?
3. Навіщо потрібно вводити команду **ip domain-name** перед генерацією ключів?
4. Що робить команда **service password-encryption?** Чи надійне це шифрування?
5. Як працює команда **login block-for 180 attempts 4 within 120**?
6. Чому важливо налаштовувати exec-timeout?
7. Якою командою можна видалити існуючі RSA-ключі, якщо необхідно змінити доменне ім’я або розмір ключа?
8. Яка мінімальна довжина ключа (в бітах) необхідна для підтримки протоколу SSH версії 2?
9. Що станеться при спробі підключення через SSH, якщо на лініях VTY не введено команду login local?
10. Скільки одночасних сесій підтримує маршрутизатор, якщо налаштовано діапазон ліній line vty 0 15?
11. Яка команда дозволяє переглянути список користувачів, підключених до маршрутизатора?
12. Яку функцію виконує команда logging synchronous при налаштуванні консольного доступу?

ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. **Cisco Networking Academy**. URL: https://www.netacad.com/ (дата звернення: 20.12.2025).
2. **Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка** (друга редакція): затверджено Вченою радою Київського національного університету імені Тараса Шевченка 11 квітня 2022 року, протокол №15, 2022. – 138 с.
3. **ДСТУ 3008:2015.** Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. / Нац. стандарт України. – Вид. офіц. – [чинний від 2017-01-07]. – Київ: ДП «УкрНДНЦ», 2016. – 31с.
4. **ДСТУ 8302:2015**. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Вид. офіц. – [Уведено вперше ; чинний від 2016-07-01]. – Київ: ДП «УкрНДНЦ», 2016. – 17 с.
5. **Wendell Odom, David Hucaby, Jason Gooley**. CCNA 200-301 Official Cert Guide Library Premium Edition and Practice Test, 2nd Edition. Published 2024 by Cisco Press. Part of the Official Cert Guide series. ISBN-10: 0-13-822139-1, ISBN-13: 978-0-13-822139-3.
6. **Sean Wilkins, Wendell Odom**. CCNA 200-301 Official Cert Guide and Network Simulator Library, Second Edition. Published Aug 29, 2024 by Pearson IT Certification. 2024. ISBN-10: 0-13-537138-4. ISBN-13: 978-0-13-537138-1
7. **S. R. Jena**. Cisco Packet Tracer Implementation: Building and Configuring Networks. Published June 7, 2023, Kindle Edition. Pages: 199. ASIN: B0C7GM18RX.
8. **Renee Gunderson**. CCNA Certification: Essential Labs for Networking Success. Published June 15, 2023, Kindle Edition. Pages: 500. ASIN: B0C895RNY5.
9. **Allan Johnson**. Introduction to Networks Labs and Study Guide (CCNAv7). Published Jun 17, 2020 by Cisco Press. Pages: 464. ISBN-10: 0-13-663445-1. ISBN-13: 978-0-13-663445-4.

10. Editor-in-Chief **Mark Taub**. Networking Essentials Companion Guide (Cisco Networking Academy Program). Published April 4, 2022 by Cisco Press. Pages: 544. ISBN-10:0137660480, ISBN-13:978-0137660483.
11. **Allan Johnson**. 31 Days Before your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam. Published Apr 3, 2020 by Cisco Press. Pages: 464. ISBN-10: 0-13-596408-3. ISBN-13: 978-0-13-596408-8.

ДОДАТКИ

ДОДАТОК А

ЗРАЗОК ОФОРМЛЕННЯ ТИТУЛЬНОЇ СТОРІНКИ ЗВІТУ З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем та технологій

ЗВІТ
з виконання лабораторної роботи №8
з дисципліни «Вступ до мереж»
на тему: «Захист мережних пристроїв»

Виконала:	Перевірив:
студентка групи ІР-21 Світлана ВЕДРІНЦЕВА	к.т.н., доц., доцент кафедри ІСТ Сергій ПАЛІЙ
_____ (дата здачі, підпис)	_____ (оцінка, підпис)

Київ 2026