Міністерство освіти і науки України
Луцький національний технічний університет

Адміністрування комп’ютерних систем та мереж

Методичні вказівки до лабораторних робіт
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Комп’ютерні науки»
галузі знань 12 (F) Інформаційні технології
спеціальності 122 (F3) Комп’ютерні науки
денної та заочної форм навчання

Луцьк 2025

УДК 004.65 (07)
А-81

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № від « ___» 2025 року

Голова вченої ради факультету КІТ І.С. Кондіус

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки Н. П. Поліщук

Розглянуто і схвалено на засіданні кафедри комп'ютерних наук
ЛНТУ, протокол № від « » 2025 року

Завідувач кафедри КН В. О. Ліщина

Укладач: В. А. Кошелюк, кандидат технічних наук,
доцент кафедри комп'ютерних наук ЛНТУ

Рецензент: С. В. Лавренчук, кандидат технічних наук,
доцент кафедри комп'ютерної інженерії та
безпеки ЛНТУ

Відповідальний
за випуск: В. О. Ліщина, кандидат технічних наук,
завідувач кафедри комп'ютерних наук ЛНТУ

А-81 **Адміністрування комп'ютерних систем та мереж**: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерні науки» галузі знань 12 (F) Інформаційні технології спеціальності 122 (F3) Комп'ютерні науки денної та заочної форм навчання / уклад. В.А. Кошелюк – Луцьк: ЛНТУ, 2025. 24 с.

Видання містить рекомендації до виконання лабораторних робіт з дисципліни « Адміністрування комп'ютерних систем та мереж ».

Призначене для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 122 (F3) Комп'ютерні науки.

ЗМІСТ

ВСТУП		4
Лабораторна робота № 1	Характеристика моделей TCP/IP і OSI	7
Лабораторна робота № 2	Визначення MAC-адрес та IP-адрес	8
Лабораторна робота № 3	Дослідження ARP-таблиці	9
Лабораторна робота № 4	Базова конфігурація IPv6	10
Лабораторна робота № 5	Розподіл мережі IPv4 на підмережі	11
Лабораторна робота № 6	Сценарій розподілу на підмережі	12
Лабораторна робота № 7	Проектування та впровадження VLSM	13
Лабораторна робота № 8	Розробка схеми адресації VLSM	14
Лабораторна робота № 9	Поділу адресного простору методом VLSM	15
Лабораторна робота № 10	Налаштування IPv6-адресації	16
Лабораторна робота № 11	Реалізація схеми адресації підмережі IPv6	17
Лабораторна робота № 12	Перевірка адресації IPv4 і IPv6	18
Лабораторна робота № 13	Використання ping і traceroute для перевірки мережевого з’єднання	19
Лабораторна робота № 14	Використання ICMP для перевірки та виправлення мережного з’єднання	20
Лабораторна робота № 15	Захист мережевих пристроїв	21
Список використаних джерел		22

1. ВСТУП

Лабораторна робота – вид навчального заняття, на якому здобувач під керівництвом науково-педагогічного (педагогічного) працівника і навчально-допоміжного персоналу особисто проводить натурні або імітаційні експерименти чи досліди з метою практичного підтвердження окремих теоретичних положень даної навчальної дисципліни (освітнього компонента), набуває практичних навичок роботи з лабораторним устаткуванням, обладнанням, обчислювальною технікою, вимірювальною апаратурою, методикою експериментальних досліджень у конкретній предметній галузі.

Лабораторні роботи проводяться у спеціально обладнаних навчальних лабораторіях з використанням устаткування, пристосованого до умов освітнього процесу (лабораторні макети, установки тощо). В окремих випадках лабораторні заняття можуть проводитися в умовах реального професійного середовища (наприклад, на виробництві, в наукових лабораторіях тощо). Лабораторне заняття проводиться, як правило, зі здобувачами вищої освіти, чисельність яких не перевищує 15. Перелік тем лабораторних занять визначається робочою програмою навчальної дисципліни. Заміна лабораторних занять іншими видами навчальних занять, як правило, не дозволяється. Для організації та проведення лабораторної роботи необхідно дотримуватися наступних умов:

– наявність спеціально обладнаних приміщень, устаткування, обладнання тощо;

– наявність навчально-методичного забезпечення з урахуванням специфіки занять та із застосуванням новітніх технологій;

– відповідність устаткування, обладнання, приладдя тощо вимогам охорони праці та санітарним нормам;

– необхідність проведення інструктажу здобувачів вищої освіти з питань охорони праці та безпеки, який підтверджується записами у журналі обліку;

– забезпечення матеріальними засобами;

– наявність елементів дослідження і творчого підходу при виконанні окремих завдань, створення наукових продуктів;

– наявність нормативно-методичної літератури.

Оцінки, отримані здобувачем вищої освіти за виконання лабораторних робіт, враховуються при виставленні підсумкової оцінки з відповідної навчальної дисципліни (освітньої компоненти).

Курс дисципліни: «Адміністрування комп'ютерних систем та мереж» має важливе значення в теоретичній підготовці майбутніх фахівців і є обов’язковою

компонентою підготовки здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп’ютерні науки» спеціальності 122 «Комп’ютерні науки».

Мета дисципліни: сформувати у здобувачів необхідний обсяг теоретичних і практичних знань про термінологічний апарат та теоретичні концепції адміністрування комп'ютерних систем та мереж, принципи організації і побудови комп'ютерних мереж, систем адміністрування комп'ютерних систем, методи проектування і засоби використання комп'ютерних мереж як складових елементів комп’ютерних систем.

Основними завданнями, що мають бути вирішені у процесі викладання дисципліни, є надання здобувачам вищої освіти:

– навичок проектування комп'ютерних мереж, визначення вимог, створення схем, розробки моделей мереж та забезпечення відповідності цілям і вимогам бізнесу;

– здатності оптимізації роботи мереж, забезпечення цілісності та безпеки даних, а також ведення адміністрування комп'ютерних систем і мереж;

– вмінь інтегрувати різноманітні програмні застосунки в мережі, розробляючи зв'язки між застосунками та комп'ютерними системами,

– створюючи API та інтерфейси для взаємодії з даними;

– знань про сучасні тенденції в галузі адміністрування комп'ютерних систем та мереж, такі як віртуалізація, кібербезпека, хмарні обчислення.

Предмет дисципліни: основи сучасної теорії адміністрування комп'ютерних систем та мереж, введення в архітектуру комп'ютерних мереж, управління мережами, безпека комп'ютерних систем і мереж. Структура навчального курсу дозволяє здобувачам застосовувати теоретичні знання до практичного адміністрування комп'ютерних систем і мереж, проектувати логічні та фізичні моделі мереж, створювати та оптимізувати мережеві структури, забезпечувати їх безпеку та ефективність функціонування.

На лабораторних роботах кожен здобувач опрацьовує теоретичні відомості, виконуючи при цьому наведені в них приклади, а потім виконує завдання, оформляє звіт до латораторної роботи та дає відповіді на питання викладача (усно, з переліку контрольних питань). Виконання наступних робіт може опиратися на результати попередніх, тому не рекомендовано їх виконувати в довільному порядку.

Оцінювання лабораторних робіт здіснюється за критеріями:

1. Теоретична підготовка (розуміння основних понять та вміння пояснити теоретичні концепції).

2. Практичне виконання завдань (повнота та точність).

3. Технічна реалізація (правиьність структури налаштування, коректна організація коду, логічна огранізація скриптів тощо).

4. Документація (наявність коментарів до конфігурації, якість оформлення звіту – чіткий та детальний звіт, в якому студент пояснює, які завдання виконувалися, які труднощі виникали, як були вирішені проблеми. Звіт має бути структурованим і зрозумілим).

5. Дотримання термінів – оцінюється, наскільки здобувач дотримується дедлайнів і вчасно здає лабораторну роботу.

6. Вміння захистити роботу – студент повинен продемонструвати здатність чітко і впевнено відповісти на питання щодо виконаних завдань, пояснити вибір рішень і відповісти на технічні запитання.

7. Вміння виправляти помилки – наскільки студент здатний виявляти і виправляти помилки в конфігурації мережевих налаштувань.

Для отримання максимального балу за лабораторну роботу також оцінюється інноваційність, ініціативність та креативність, наприклад чи застосовуються додаткові інструменти або методи, які не входять до завдання, але можуть покращити результат. Ці критерії дають змогу об’єктивно оцінити навички студента, його здатність до самостійної роботи, розуміння теорії та застосування знань на практиці.

Найважливішим інформаційним джерелом вивчення навчальної дисципліни «Адміністрування комп’ютерних систем та мереж» є ресурси мережі Інтернет. Основна частина матеріалу в Інтернеті розрахована на професіоналів, тому при вивченні навчальної дисципліни спочатку необхідно користуватися літературою навчального характеру.

Для зручності користування записами необхідно залишати поля для заміток і вільні рядки для доповнень. Записи не повинні бути одноманітними. В них необхідно виділяти важливі місця, головні слова, які акцентуються різним шрифтом або різним кольором шрифтів, підкреслюванням, замітками на полях, рамками, стовпчиками тощо. Записи можуть бути у вигляді конспекту, простих або розгорнутих тез, цитат, виписок, систематизованих таблиць, графіків, діаграм, схем.

Знання з дисципліни «Адміністрування комп’ютерних систем та мереж» становлять основу для подальшого поглибленого засвоєння матеріалу з того чи іншого розділу. З позицій випереджаючої освіти навчання тільки за конспектом лекцій і основною літературою, зазначеною у навчальній програмі, є недостатнім. У більшості випадків належна підготовка потребує вмінь швидко знаходити та опрацьовувати необхідний матеріал за першоджерелами, науковою і спеціальною літературою та коректно цитувати знайдене. Перелік такої літератури, як правило, наводиться у навчально-методичному комплексі навчальної дисципліни. Тому завдання студента зводиться до самостійного знаходження цих матеріалів шляхом пошуку у паперових або електронних фондах бібліотек.

Лабораторна робота № 1

Тема. Характеристика моделей TCP/IP і OSI

Мета: вивчення та розуміння стеку протоколів TCP/IP і його взаємозв'язку з моделлю OSI.

Література: [1, 5, 11]

Теоретичні відомості

Моделювання покликане сформувати засади для розуміння стеку протоколів TCP/IP і його взаємозв'язку з моделлю OSI. Режим симуляції дозволяє переглядати вміст даних на кожному рівні в процесі надсилання мережею.

Під час передавання по мережі дані розбиваються на менші частини та ідентифікуються з метою повторного збирання при надходженні до пункту призначення. Кожному блоку, відповідно до певних рівнів моделей TCP/IP та OSI, призначена власна назва. Режим моделювання Packet Tracer дає можливість переглядати кожен рівень і пов'язані з ним PDU. Наступні кроки познайомлять користувача з процесом запиту веб-сторінки з веб-сервера за допомогою браузера на клієнтському ПК.

Моделювання демонструє приклад сеансу зв'язку між веб-клієнтом і веб-сервером у локальній мережі. Клієнт робить запити щодо визначених сервісів, запущених на сервері. Сервер повинен бути налаштований на прослуховування конкретних портів у очікуванні запитів від клієнтів. На підставі інформації, отриманої під час перехоплення за допомогою Packet Tracer, зазначте, який номер порту прослуховує Web Server, очікуючи на веб-запити.

Завдання для виконання:

1. Вивчення та дослідження веб-трафіку HTTP.
2. Відображення елементів стеку протоколів TCP/IP.
3. Перехоплення DNS-запитів веб-серверу.

Контрольні питання

1. Яка інформація наведена за допомогою пронумерованих записів нижче полів In Layers (Вхідні рівні) та Out Layers для рівня 7?
2. Яке значення має Dest IP-для Layer 3(Рівень 3) у колонці Out Layers ?
3. Яка інформація показана на Layer 2 (рівні 2) у колонці Out Layers?
4. Який Вузол вказаний у розділі HTTP деталей PDU? З яким рівнем пов'язана ця інформація у вкладці OSI Model ?
5. Які додаткові типи подій (Event Types) відображаються?
6. На якому пристрої було захоплено PDU?
7. Який порт прослуховує Web Server щодо DNS-запитів?
8. Яке значення для Dst Port (Порт призначення) для Layer 4 (Рівень 4) міститься у колонці Out Layers ?
9. Яка інформація традиційно міститься у розділі TCP PDU Details, порівняно з інформацією на вкладці OSI Model?
10. Яке значення вказане поряд з ADDRESS: у частині DNS ANSWER Inbound PDU Details?

Лабораторна робота № 2

Тема. Визначення MAC-адрес та IP-адрес

Мета: дослідження та вивчення блоку даних протоколу.

Література: [2, 4, 12]

Теоретичні відомості

Для встановлення успішного підключення до мережі потрібні як IP-, так і MAC-адреси. Коли пристрій хоче зв’язатися з іншим пристроєм у тій же мережі, він використовує MAC-адресу для звернення до пакетів даних. Однак, коли дані потрібно надіслати через різні мережі, в гру вступають IP-адреси. IP-адреси використовуються для маршрутизації пакетів даних до відповідного пункту призначення через Інтернет. Маршрутизатори відіграють важливу роль у цьому процесі, перевіряючи IP-адресу вхідних пакетів і пересилаючи їх до наступного переходу на основі таблиць маршрутизації.

IP-адреса (адреса Інтернет-протоколу) і MAC-адреса (адреса керування доступом до середовища) є важливими компонентами в області комп’ютерних мереж. Вони служать різним цілям і працюють на різних рівнях мережевого стеку. У цьому поясненні ми розглянемо детальне та вичерпне розуміння як IP, так і MAC-адрес, підкреслюючи їх значення та функції.

IP-адреса — це унікальна цифрова мітка, присвоєна кожному пристрою, підключеному до мережі, яка використовує Інтернет-протокол для зв’язку. Він служить ідентифікатором для джерела та призначення пакетів даних у мережі. IP-адреси необхідні для маршрутизації даних між мережами, що дозволяє пристроям спілкуватися один з одним через Інтернет. IP-адреси поділяються на дві основні версії: IPv4 і IPv6. Адреси IPv4 складаються з чотирьох наборів чисел, розділених крапками, з кожним набором у діапазоні від 0 до 255. Наприклад, 192.168.0.1. Адреси IPv4 забезпечують приблизно 4.3 мільярда унікальних адрес, яких стає недостатньо через експоненціальне зростання пристроїв, підключених до Інтернету.

Завдання для виконання:

1. Збір інформації PDU у випадку зв’язку в локальній мережі.
2. Збір інформації PDU у випадку зв’язку з віддаленою мережею.

Контрольні питання

1. Скільки слотів розширення доступно для приєднання додаткових модулів до маршрутизатора East?
2. Скільки хостів можна під'єднати до маршрутизатора за допомогою цього модуля?
3. Яка пропускна здатність за замовчуванням цього інтерфейсу?
4. Скільки фізичних інтерфейсів у списку?
5. Які порти керування доступні?

Лабораторна робота № 3

Тема. Дослідження ARP-таблиці

Мета: навчитися використовувати протокол перетворення адрес мережевого рівня в адреси канального рівня.

Література: [3, 8, 13]

Теоретичні відомості

Протокол ARP призначений для динамічного визначення MAC-адреси віддаленого вузла за відомою його IP-адресою версії 4. Протокол RARP виконує зворотну процедуру. Частіше поряд із терміном ,,визначення адрес" застосовують терміни ,,встановлення" або ,,перетворення адрес". Спочатку протоколи ARP/RARP були розроблені як універсальні протоколи для мереж різних технологій та різних протокольних стеків, сьогодні, у першу чергу, вони застосовуються у мережах Ethernet та Wi-Fi у поєднанні з протокольним стеком TCP/IP за умови застосування IP версії 4.

Стосовно моделі OSI протоколи ARP/RARP належать до мережного рівня. Таке позиціонування пов'язане з тим, що протоколи ARP/RARP не застосовують повідомлення мережного рівня для передачі власної службової інформації, а формують власні повідомлення, які надалі інкапсулюються у кадри технології канального рівня. Слід зазначити, що протокол ARP орієнтований на функціонування у межах одного канального сегмента (широкомовного домену). За необхідності передачі ARP-повідомлень між різними канальними сегментами, об'єднаними за допомогою маршрутизаторів/багаторівневих комутаторів, застосовується спеціально розроблений механізм Proxy-ARP.

Обмін інформацією між вузлами мережі для формування адресних відповідностей між IP-адресами і MAC-адресами у протоколі ARP здійснюється із застосуванням механізму ,,запит-відповідь" (Request-Reply). Результати обміну зберігаються у таблиці, що називається ARP-таблицею/ARP-кешем.

Завдання для виконання:

1. Вивчення ARP-запиту.
2. Вивчення таблиці MAC-адрес комутатора.
3. Вивчення процесу ARP у випадку віддаленого зв'язку.

Контрольні питання

1. Скільки копій PDU зробив Switch1?
2. Яка IP-адреса пристрою, що прийняв PDU?
3. Скільки копій PDU зробив комутатор під час ARP-відповіді?
4. Чи збігаються MAC-адреси джерела та призначення з їхніми IP-адресами?
5. Якій IP-адресі відповідає запис MAC-адреси?
6. Скільки відповідей було надіслано та отримано?
7. Чому дві MAC-адреси пов'язані з одним портом?
8. Яка IP-адреса нового запису в ARP-таблиці?
9. Яка цільова IP-адреса призначення ARP-запиту?
10. Що відбувається з першою командою ping у випадку, коли маршрутизатор відповідає на ARP-запит?

Лабораторна робота № 4

Тема. Базова конфігурація IPv6

Мета: розглянути основні команди конфігурації протоколу IPv6 та здійснити тестування наскрізного з'єднання.

Література: [4, 6, 14]

Теоретичні відомості

Розвиток глобальної мережі йде дуже активно і скоро стане неможливим без розширення адресного простору. Цей процес передбачає поступовий перехід з IPv4 на IPv6. Приклад адреси: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210. Незначні нулі в числах або нульові блоки – опускаються. Замість пропущеного числа ставиться двокрапка. Наприклад, 1024:0:0:0:75:332:208B:717A може бути записаний як 1024::75:332:208B:717A. Розділені двокрапкою числа називаються октетами.

Адресу IPv6 можна поділити на три складові частини: глобальний префікс (з 1-го по 3-й блоки); ідентифікатор підмережі (4-й блок); ідентифікатор інтерфейсу (з 5-го по 8-й блоки). IPv6 містить поліпшені механізми безпеки, як-от IPsec, що забезпечує конфіденційність, цілісність і аутентифікацію даних у мережі. Впровадження IPv6 також створює нові загрози та ризики, такі як атаки на нові протоколи та несанкціонований доступ до мережі.

Завдання для виконання:

1. Заповнити мережеву документацію.
2. Виконати базові налаштування на маршрутизаторі і комутаторі.
3. Перевірити зв'язок та усунути недоліки роботи мережі.

Контрольні питання

1. Які основні переваги IPv6 порівняно з IPv4, що робить його впровадження необхідним?
2. Опишіть відмінності між глобальною унікальною адресою (Global Unicast Address - GUA), локальною адресою каналу (Link-Local Address - LLA) та унікальною локальною адресою (Unique Local Address - ULA) в IPv6. Для чого використовується кожна з них?
3. Які існують методи автоматичного призначення IPv6-адрес (крім ручного налаштування)? Опишіть їхню роботу та відмінності.
4. Поясніть роль та значення адреси Link-Local (LLA) в IPv6. Як вона генерується та чи можна її відключити?
5. Як відбувається процес визначення сусідів (Neighbor Discovery Protocol - NDP) в IPv6? Які повідомлення використовуються в NDP і для чого?
6. Що таке "розширення приватності" (Privacy Extensions) в IPv6 і навіщо вони потрібні? Як вони впливають на генерацію IPv6-адрес?
7. Як IPv6-адресу встановити значення 2001:db8:1:1::4 з префіксом /64.
8. Як IPv6-адресу шлюзу за замовчуванням встановити локальну адресу fe80::1.
9. Як IPv6-адресу встановити значення 2001:db8:1:2::3 з префіксом /64.

Лабораторна робота № 5

Тема. Розподіл мережі IPv4 на підмережі

Мета: створення схеми підмереж та вивчення можливостей розподілу IPv4.

Література: [5, 9, 15]

Теоретичні відомості

В даний час все ще існує багато мереж, що використовують адресацію IPv4, навіть організації, що їх використовують, здійснюють перехід на IPv6. Тому для мережних адміністраторів як і раніше, дуже важливо знати все про адресацію IPv4. Він включає в себе, як сегментувати мережу в підмережі та як створити маску підмережі змінної довжини (VLSM) в межах загальної схеми адресації IPv4.

Маска підмережі дозволяє розділити мережу на кілька мереж меншого розміру (на підмережі) з певною кількістю адрес під хости. Підмережа - це логічне поділ мережі IP. В усіх хостів однієї мережі або підмережі одна й та ж маска підмережі. Маска 255.255.255.0 (/ 24) визначає всю підмережу класу C, тобто 254 адреси, а 255.255.255.255 (/ 32) дозволяє вказати одиничний вузол мережі. Якщо в наборі правил міжмережевого екрану Ви одночасно використовуєте дозволяючі та забороняючі правила, то в цьому випадку, правила, що дозволяють, повинні розташовуватися вище тих, що забороняють. Спочатку створюйте дозволяючі правила для певних адрес або підмереж, а потім забороняючі.

Завдання для виконання:

1. Розроблення схеми розподілу мережі на підмережі
2. Налаштування пристроїв
3. Перевірка та усунення неполадок у мережі

Контрольні питання

1. Яким чином розподіл мережі IPv4 на підмережі допомагає оптимізувати використання IP-адрес та підвищити безпеку мережі?
2. Назвіть основні кроки, які необхідно виконати для ефективного розподілу мережі IPv4 на підмережі.
3. Які переваги надає розподіл мережі IPv4 на підмережі для великих корпоративних мереж?
4. Опишіть, як визначити необхідну кількість підмереж та розмір кожної з них при розподілі мережі IPv4.
5. Які інструменти або калькулятори ви використовуєте для розподілу мережі IPv4 на підмережі та розрахунку масок підмереж?
6. Що визначають нулі в масці мережі?
7. Що визначають одиниці в масці мережі?
8. Мережа, яку необхідно розподілити на підмережі, має адресу - 192.168.0.0/24. Якою буде маска підмережі /24 в двійковому форматі?
9. Яка мінімальна необхідна кількість підмереж?
10. Скільки необхідно адрес вузлів у найбільшій підмережі?

Лабораторна робота № 6

Тема. Сценарій розподілу на підмережі

Мета: проаналізувати елементи розподілу мережі IPv4 та скласти схему IP-адресації мережі

Література: [6, 8, 16]

Теоретичні відомості

Процес сегментації мережі шляхом розподілу її на дрібніші мережі називається розбиттям на підмережі. Ці дрібніші мережі називаються підмережами. Мережеві адміністратори можуть групувати пристрої і служби в підмережі за їх географічним місцем (наприклад, 3-й поверх будівлі) розташування, організаційному підрозділу (наприклад, відділ продажів) або за типом пристроїв (принтери, сервери, глобальна мережа) або за іншим значущим для мережі принципом. Розбиття на підмережі може понизити загальне навантаження на мережу і підвищити її продуктивність.

Префікс і маска підмережі – це різні способи представлення одного і того ж – мережевої частини адреси. Для створення IPv4 -підмереж ми задіюємо один або декількох біт з вузлової частини в якості біт мережевої частини. Для цього ми розширюємо маску підмережі. Чим більше запозичено біт з вузлової частини, тим більше підмереж можна створити. Для кожного запозиченого біта кількість доступних підмереж подвоюється. Наприклад, якщо запозичувати один біт, можна створити дві підмережі. Для двох біт – 4 підмережі, для трьох біт – 8 підмереж і т. д. Проте з кожним запозиченим бітом зменшується кількість адрес вузлів в кожній підмережі.

Завдання для виконання:

1. Розроблення схеми IP-адресації
2. Призначення IP-адрес мережним пристроям і перевірка з’єднань

Контрольні питання

1. Яка основна мета розподілу на підмережі в даному сценарії?
2. Які конкретні вимоги до мережі повинні бути враховані при розподілі на підмережі?
3. Який тип мережі розглядається в цьому сценарії?
4. Чи існують якісь обмеження або особливості інфраструктури, які впливають на розподіл на підмережі?
5. Чи передбачається масштабування мережі в майбутньому, і як це вплине на поточний розподіл на підмережі?
6. З якими потенційними проблемами ви можете зіткнутися при реалізації даного сценарію розподілу на підмережі?
7. Як ви плануєте вирішувати проблеми, пов'язані з вичерпанням IP-адрес у майбутньому?
8. Які переваги та недоліки пропонованого сценарію розподілу на підмережі?
9. Чи розглядалися альтернативні сценарії розподілу на підмережі, і чому був обраний саме цей?

Лабораторна робота № 7

Тема. Проектування та впровадження VLSM

Мета: навчитися використовувати розподіл адресного простору методом маски змінної довжини.

Література: [3, 7, 17]

Теоретичні відомості

Розбиття підмережі на декілька підмереж або використання маски підмережі змінної довжини (VLSM) призначені для того, щоб уникнути створення непотрібних адрес. Розбиття IPv6 -мережі на підмережі має на увазі використання іншого підходу, ніж розбиття на підмережі IPv4 -мережі. Простір IPv6 -адрес розбивається не з метою економії адрес, а для забезпечення ієрархічної логічної структури мережі. Якщо IPv4 -мережі розбиваються на підмережі в основному для боротьби з нестачею адрес, то метою розбиття IPv6 -мережі на підмережі являється створенням ієрархії адрес на основі кількості маршрутизаторів і обслуговуваних ними мереж.

Завдання для виконання:

1. Дослідження вимог, що висуваються до мережі
2. Створення схеми адресації VLSM
3. Призначення IP-адрес пристроям та перевірка їх з’єднань

Контрольні питання

1. Що таке VLSM (Variable Length Subnet Mask) і чому він є важливим для ефективного використання IP-адрес у мережах?
2. Які ключові переваги використання VLSM порівняно з традиційноюsubnetting?
3. Як VLSM допомагає у боротьбі з "виснаженням" IP-адрес
4. Опишіть покроковий процес проектування мережі з використанням VLSM, починаючи з заданого адресного простору.
5. Які критерії ви б використовували для визначення розмірів підмереж при проектуванні з VLSM?
6. Як ви враховуєте майбутній ріст мережі при проектуванні з VLSM, щоб уникнути необхідності перерозподілу адрес?
7. Які інструменти або методи ви використовуєте для обчислення підмереж та масок при VLSM-проектуванні?
8. Які типові проблеми можуть виникнути при впровадженні VLSM і як їх можна уникнути або вирішити?
9. Покажіть приклад конфігурації маршрутизатора для підтримки VLSM у заданій мережевій топології.
10. Як VLSM співвідноситься з іншими стратегіями оптимізації IP-адрес, такими як CIDR?

Лабораторна робота № 8

Тема. Розробка схеми адресації VLSM

Мета: вивчення та дослідження принципів поділу адрес маскою змінної довжини

Література: [2, 5, 18]

Теоретичні відомості

У сучасних мережах класова IP -адресація більше не використовується, і маски підмережі неможливо визначити за значенням першого октету. Безкласові протоколи маршрутизації IPv4 (RIPv2, EIGRP, OSPF і IS - IS) включають в оновлення маршрутизації дані про маску. підмережі разом з мережевою адресою. Безкласові протоколи маршрутизації підтримують використання VLSM і CIDR.

Протоколи маршрутизації IPv6 є безкласовими. Розрізняти класові і безкласові протоколи маршрутизації має сенс тільки при використанні протоколів маршрутизації IPv4. Усі протоколи маршрутизації IPv6 вважаються безкласовими, оскільки включають довжину префікса разом з IPv6 -адресою.

Класові або безкласові протоколи (використання VLSM): класові протоколи маршрутизації не включають маску підмережі і не підтримують використання VLSM. Безкласові протоколи маршрутизації включають в оновлення маску підмережі. Безкласові протоколи маршрутизації підтримують використання VLSM і забезпечують якісніше об’єднання маршрутів

Завдання для виконання:

1. Дослідження вимог, що висуваються до мережі
2. Створення схеми адресації VLSM
3. Призначення IP-адрес пристроям та перевірка їх з’єднань

Контрольні питання

1. Які основні переваги та недоліки використання VLSM (Variable Length Subnet Mask) при розробці схеми адресації мережі?
2. У яких сценаріях розробка схеми адресації на основі VLSM є найбільш доцільною, а в яких — ні?
3. Які математичні розрахунки є ключовими при визначенні масок підмереж та адрес для кожної VLAN/підмережі в схемі VLSM?
4. Як VLSM допомагає оптимізувати використання IP-адрес порівняно з традиційним FLSM (Fixed Length Subnet Mask)?
5. З якими типовими проблемами можна зіткнутися при впровадженні схеми адресації VLSM і як їх можна уникнути або вирішити?
6. Яким чином майбутні зміни або розширення мережі повинні враховуватися при початковій розробці схеми адресації VLSM для забезпечення її масштабованості?
7. Як можна інтегрувати принципи VLSM з іншими стратегіями управління IP-адресами, такими як приватні IP-адреси та NAT, для створення комплексної схеми адресації?

Лабораторна робота № 9

Тема. Поділу адресного простору методом VLSM

Мета: одержання навичок з реалізації поділу адресного простору методом VLSM

Література: [5, 7, 19]

Теоретичні відомості

Розбиття підмережі на декілька підмереж з використанням маски підмережі змінної довжини (VLSM, variable length subnet mask) дозволяє розподіляти значно менше «зайвих» адрес. VLSM -розбиття на підмережі схоже на традиційне тим, що в ньому для створення підмереж запозичуються біти. Формули розрахунку кількості можливих підмереж і кількості вузлів в кожній підмережі також застосовні. Відмінність полягає в тому, що розбиття на підмережі виконується у декілька етапів. При використанні VLSM мережа спочатку розбивається на підмережі, а потім підмережі знову діляться на підмережі. Цей процес може повторюватися багато разів для створення підмереж різного розміру.

Кожен вузол в мережевій інфраструктурі повинен мати унікальну адресу. Без належного планування і документування адреса може бути призначена декільком вузлам, що приведе до проблем доступу до мережі цих вузлів. Деякі вузли, такі як сервери, надають ресурси і внутрішнім, і зовнішнім вузлам. Призначену серверу адресу 3-го рівня можна використовувати для управління доступом до цього сервера. Якщо адреса призначена випадковим чином і ніде не задокументована, управляти доступом буде складніше. У рамках моніторингу мережевий трафік аналізується на наявність адрес, які генерують або отримують велике число пакетів. При належному плануванні і документуванні адресації в мережі проблемні пристрої можна легко виявити.

Завдання для виконання:

1. Розробити схему IP-адресації VLSM з урахуванням вимог.
2. Налаштувати адресацію на мережних пристроях і вузлах.
3. Перевірити IP-з’єднання.
4. Виявити та усунути неполадки в мережних з'єднаннях.

Контрольні питання

1. Що таке VLSM і в чому його основна відмінність від FLSM? (Це базове запитання для перевірки розуміння концепції).
2. Які переваги надає використання VLSM при плануванні мережі?
3. В яких сценаріях використання VLSM є найбільш доцільним і чому?
4. Які інструменти або методи ви використовуєте для ефективного планування та документування VLSM-мереж?
5. Як VLSM впливає на маршрутизацію в мережі і які протоколи маршрутизації підтримують VLSM?

Лабораторна робота № 10

Тема. Налаштування IPv6-адресації

Мета: розглянути основні концепції конфігурації IPv6

Література: [3, 8, 20]

Теоретичні відомості

Протокол IPv6 з 128-бітовою адресою надає 340 ундециліонів адрес. Таким чином, адресний простір не є проблемою. Протокол IPv6 був розроблений, щоб усунути необхідність в NAT для IPv4 з його перетворенням між публічними і приватними IPv4 -адресами. Проте, IPv6 дійсно реалізує певну форму NAT. IPv6 включає і власний простір приватних IPv6 -адрес, і перетворення NAT, реалізовані інакше, ніж для IPv4.

Унікальні локальні IPv6 -адреси (unique local addresses, ULA) схожі на приватні адреси RFC 1918 в IPv4, але при цьому істотно відрізняються від них. Мета унікальних локальних адрес – забезпечити простір IPv6 -адрес для взаємодії в межах локального об'єкту. Це не означає ні надання додаткового простору IPv6 -адрес, ні забезпечення рівня безпеки. Унікальна локальна адреса використовує префікс FC00::/7, і тому перший гекстет знаходиться в діапазоні від FC00 до FDFF. Якщо префікс призначається локально, наступний 1 біт встановлений рівним 1. Сенс значення 0 буде визначений пізніше. Наступні 40 бітів – це глобальний ідентифікатор, за яким йде 16-бітовий ідентифікатор підмережі. Ці перші 64 біта об'єднуються для створення префікса унікальної локальної адреси. Це залишає 64 біта для ідентифікатора інтерфейсу або, згідно термінології IPv4 – вузлової частини адреси.

Завдання для виконання:

1. Налаштування адресації IPv6 на маршрутизаторі
2. Налаштування адресації IPv6 на серверах
3. Налаштування адресації IPv6 на клієнтських вузлах
4. Тестування та перевірка зв'язку в мережі

Контрольні питання

1. Які основні кроки необхідно виконати для налаштування IPv6-адресації на мережевому пристрої (наприклад, маршрутизаторі або сервері)?
2. Які існують методи автоматичного налаштування IPv6-адрес (наприклад, SLAAC, DHCPv6) і в яких сценаріях доцільно використовувати кожен з них?
3. З якими поширеними проблемами можна зіткнутися під час налаштування IPv6 і як їх діагностувати та усунути?
4. Як правильно спланувати та впровадити IPv6-адресацію в корпоративній мережі?
5. Які інструменти діагностики та моніторингу ефективні для перевірки налаштувань IPv6?
6. Як забезпечити безпеку мережі при переході на IPv6 або при використанні Dual Stack?
7. Які найкращі практики для ефективного управління IPv6-адресами у великих мережах?

Лабораторна робота № 11

Тема. Реалізація схеми адресації підмережі IPv6

Мета: навчитися використовувати службові команди для налаштування IPv6

Література: [1, 4, 21]

Теоретичні відомості

Адміністратори мережі повинні знати, як реалізувати IPv6 у своїх мережах. Вас попросили створити мережу для використання торговим персоналом для демонстрації клієнтам. Мережа буде використовувати ряд послідовних підмереж IPv6 для чотирьох локальних мереж. Вашим завданням є призначення підмереж локальним мережам і налаштування на маршрутизаторах та комп'ютерах параметрів адресації IPv6. Обов'язково налаштуйте всі необхідні компоненти для маршрутизації IPv6 на маршрутизаторах.

Реалізація і потенційні сфери застосування унікальних локальних IPv6 - адрес все ще вивчається інтернет-співтовариством. Наприклад, IETF аналізує можливість створення префікса унікальних локальних адрес локально, використовуючи FC00::/8, або призначення його автоматично сторонньою організацією, починаючи з FD00:: /8.

NAT для IPv6 використовується в зовсім іншому контексті, ніж NAT для IPv4. Різноманітні варіанти NAT для IPv6 використовуються з метою надання прозорого доступу між мережами, в яких використовується тільки протокол IPv6, і мережами, в яких використовується тільки протокол IPv4. NAT для IPv6 не застосовується для перетворення приватних IPv6 -адрес в глобальні IPv6 - адреси.

Завдання для виконання:

1. Визначити підмережі IPv6 та схему адресації.
2. Налаштувати адресацію IPv6 на маршрутизаторах та ПК.
3. Перевірити IPv6-з'єднання.

Контрольні питання

1. Які ключові відмінності в підході до підмережі між IPv4 та IPv6, і як це впливає на планування мережі?
2. Як виглядає типова стратегія виділення префіксів IPv6 для підмереж у великих корпоративних мережах? Які найкращі практики ви б рекомендували?
3. Які інструменти та методи ви використовуєте для автоматизації призначення IPv6-адрес та управління підмережами (наприклад, DHCPv6, SLAAC, або їх комбінація)?
4. З якими основними викликами ви стикалися при міграції існуючих IPv4-підмереж на IPv6, і як ви їх долали?
5. Як ви забезпечуєте безпеку підмереж IPv6, враховуючи такі аспекти, як автоматична конфігурація адрес та великий адресний простір?
6. Які переваги та недоліки використання різних розмірів префіксів для підмереж IPv6 (наприклад, /64, /48) у різних сценаріях розгортання?

Лабораторна робота № 12

Тема. Перевірка адресації IPv4 і IPv6

Мета: ознайомитись та отримати навички налаштування та конфігурації мережевих пристроїв за протоколами IPv4 і IPv6

Література: [2, 3, 22]

Теоретичні відомості

Структурно IP-адреса версії 6 складається із двох однакових за довжиною частин – одна частина (64 біти ліворуч) містить IP-адресу (номер) мережі, до якої належить вузол, інша (64 біти праворуч) – IP-адресу (номер) вузла в цій мережі. Відокремлення номера мережі від номера вузла здійснюється за допомогою префікса мережі /64. Особливістю IP-адреси версії 6 є те, що номер мережі містить у собі номери багатьох підмереж. Відповідно застосовується кілька префіксів підмереж.

Унікальна адреса IPv6 однозначно ідентифікує інтерфейс на пристрої з підтримкою IPv6. Пакет, який надсилається на таку адресу, буде отримано інтерфейсом, призначеним для цієї адреси. Аналогічно до IPv4, IPv6-адреса джерела повинна бути унікальною адресою. IPv6-адреса призначення може бути як унікальною, так і груповою. Унікальні локальні адреси (діапазон від fc00::/7 до fdff::/7) ще не реалізовано. Однак унікальні локальні адреси можуть з часом використовуватися для адресації пристроїв, які не мають бути доступними зовні, такі як внутрішні сервери та принтери

Завдання для виконання:

1. Доповнення документування таблиці адресації
2. Перевірка з’єднання за допомогою команди ping
3. Виявлення шляху трасуванням маршруту

Контрольні питання

1. Які основні відмінності між адресацією IPv4 та IPv6, і як ці відмінності впливають на методи перевірки?
2. Які типові проблеми можуть виникнути при некоректній адресації IPv4 або IPv6, і як їх виявити за допомогою базових інструментів перевірки?
3. Опишіть кроки, які ви б зробили для перевірки доступності хосту за його IPv4-адресою, а потім порівняйте їх з кроками для IPv6-адреси
4. Уявіть, що користувач не може отримати доступ до певного веб-сайту. Визначте можливі проблеми з адресацією IPv4/IPv6 та кроки для їх діагностики.
5. Ви налаштовуєте новий сервер у мережі. Які перевірки адресації IPv4 та IPv6 ви б виконали, щоб переконатися в його коректній роботі та доступності?
6. Мережа переходить з IPv4 на IPv6. Які ключові моменти потрібно перевірити для забезпечення безперебійного переходу з точки зору адресації?

Лабораторна робота № 13

Тема. Використання ping і traceroute для перевірки мережевого з’єднання

Мета: вивчення та дослідження вбудованих засобів ОС моніторингу передачі даних

Література: [3, 6, 23]

Теоретичні відомості

Traceroute відрізняє себе від простіших інструментів, таких як ping, складним відображенням шляху пакетів даних через різні маршрутизатори. Важливо розуміти, що маршрут, обраний під час зворотного трасування, може відрізнятися від прямого маршруту, підкреслюючи складність мережевих маршрутів та інфраструктури. Під час запуску traceroute ваш пристрій надсилає дані на сервер, записуючи всі проміжні маршрутизатори. Якщо на певному вузлі виникають проблеми, програма визначає проблемну ділянку мережі. Онлайн-інструменти, такі як traceroute від Host Tracker, ще більше покращують розуміння маршруту даних і мережевих проблем. Інструмент Traceroute від HostTracker забезпечує зручний інтерфейс, що дозволяє користувачам відстежувати веб-сайти з різних місць і проводити постійний моніторинг мережевого маршруту. Цей метод пропонує розширені функціональні можливості, що робить його потужним вибором як для новачків, так і для досвідчених користувачів, яким потрібна комплексна діагностика та аналіз.

Завдання для виконання:

1. Перевірка та відновлення IPv4-з’єднання
2. Перевірка та відновлення IPv6-з’єднання

Контрольні питання

1. Які основні відмінності між командами ping та traceroute з точки зору інформації, яку вони надають для діагностики мережевого з'єднання?
2. Наведіть сценарії, коли використання traceroute буде більш інформативним (ping) при виявленні проблем з мережевим з'єднанням.
3. Як можна інтерпретувати різні типи відповідей, отриманих від команд ping (наприклад, "Request timed out", "Destination host unreachable"), для визначення характеру проблеми?
4. Які параметри команд ping та traceroute ви вважаєте найкориснішими для поглибленої діагностики, і чому?
5. Як досвідчений мережевий адміністратор буде поєднувати використання ping та traceroute для системного пошуку та усунення несправностей у складній мережевій інфраструктурі?
6. Чи можуть ping та traceroute бути використані зловмисниками для отримання інформації про мережеву інфраструктуру? Якщо так, то яким чином, і як можна мінімізувати ці ризики?
7. Які існують альтернативні або більш сучасні інструменти для діагностики мережевого з'єднання, які доповнюють або перевершують можливості ping та traceroute?
8. Наскільки надійними є дані, отримані за допомогою ping та traceroute, для прийняття рішень щодо оптимізації мережі? Які фактори можуть спотворювати ці результати?

Лабораторна робота № 14

Тема. Використання ICMP для перевірки та виправлення мережного з’єднання

Мета: навчитися використовувати міжмережевий протокол керуючих повідомлень для перевірки з’єднання.

Література: [1, 4, 24]

Теоретичні відомості

ICMP – це протокол третього рівня (мережевого рівня) в семирівневої моделі OSI. Це допомагає діагностувати проблеми з мережевим підключенням або передачею даних між пристроями шляхом надсилання, отримання та обробки повідомлень ICMP для повідомлення про проблеми з підключенням до мережного пристрою.

ICMP – це протокол, який мережеві пристрої, такі як маршрутизатори, використовують для генерації повідомлень про помилки, коли мережеві проблеми перешкоджають проходженню IP-пакетів. ICMP створює і відправляє повідомлення на вихідний IP-адреси, які вказують на те, що шлюз в Інтернет, служба або хост не можуть бути досягнуті для доставки пакетів.

ICMP – це протокол imap про помилки, який мережеві пристрої, такі як маршрутизатори, використовують для генерації повідомлень про помилки на вихідний IP-адресу, коли мережеві проблеми перешкоджають доставці IP-пакетів.

Завдання для виконання:

1. Використання ICMP для пошуку проблем у мережних з’єднаннях.
2. Налаштування мережних пристроїв для виправлення проблем у мережних з’єднаннях.

Контрольні питання

1. Як протокол ICMP (Internet Control Message Protocol) використовується для діагностики та вирішення проблем мережевого з'єднання?
2. Які типи повідомлень ICMP є найбільш важливими при перевірці доступності вузлів та маршрутів у мережі?
3. Чим відрізняється використання команд ping та traceroute (або tracert у Windows) для діагностики мережі, і як обидві ці утиліти спираються на ICMP?
4. Уявіть ситуацію, коли команда ping успішна, але мережевий додаток не працює. Які можливі причини такого явища, і як ICMP може допомогти у подальшій діагностиці?
5. Як можна використовувати повідомлення ICMP Destination Unreachable для ідентифікації проблем маршрутизації або фільтрації трафіку в мережі? Наведіть приклади.
6. Які обмеження існують при використанні ICMP для повної діагностики мережі, і які додаткові інструменти або протоколи можуть бути потрібні для комплексного виправлення проблем?
7. Опишіть кроки, які ви б зробили для діагностики проблеми з'єднання з віддаленим сервером, починаючи з використання ICMP-утиліт. Які висновки можна зробити на кожному етапі?

Лабораторна робота № 15

Тема. Захист мережевих пристроїв

Мета: одержання навичок з конфігурації на налаштування параметрів безпеки на мережевих пристроях

Література: [6, 9, 25]

Теоретичні відомості

Мережева безпека є критичним компонентом кібербезпеки – і першою лінією захисту мережі від кібератак. Без належних заходів безпеки мережі залишаються вразливими до кіберзагроз (зокрема, несанкціонованого доступу та DDoS-атак). Завдяки впровадженню різних заходів мережевої безпеки організації можуть ефективно запобігати цим загрозам, виявляти їх і боротися з ними. Хоча мережева безпека в основному стосується підприємств із великими та складними комп'ютерними мережами, багато її інструментів і методів також можуть бути використані для захисту вашої домашньої мережі.

Брандмауер - це частина або набір програмного, або апаратного забезпечення, призначеного для блокування несанкціонованого доступу до комп'ютерів і мереж. Простіше кажучи, брандмауер – це набір правил, які керують вхідний і вихідний мережевий трафік. Комп'ютери та мережі, які «дотримуються правил», допускаються до точок доступу, а ті, які цього не роблять, не мають доступу до всієї системи.

Брандмауери стають все більш і більш витонченими (разом з хакерами), і новітніми є інтегровані платформи мережевої безпеки, які складаються з безлічі підходів і методів шифрування, які працюють в тандемі для запобігання зломів.

Завдання для виконання:

1. Налаштування базових параметрів безпеки на маршрутизаторі;
2. Налаштування базових параметрів безпеки на комутаторі;
3. Конфігурація безпечних паролів і SSH.

Контрольні питання

1. Які механізми аутентифікації та авторизації є найбільш ефективними для контролю доступу до мережевих пристроїв?
2. Опишіть роль та принципи роботи мережевих екранів (firewalls) у захисті мережевих пристроїв. Які їхні основні типи та відмінності?
3. Як системи виявлення та запобігання вторгненням (IDS/IPS) допомагають захистити мережеві пристрої від атак?
4. Яке значення має шифрування трафіку для безпеки даних, що передаються через мережеві пристрої? Наведіть приклади протоколів шифрування.
5. Як сегментація мережі може підвищити рівень захисту мережевих пристроїв?
6. Які вразливості часто зустрічаються у мережевих пристроях і як їх можна усунути?
7. Опишіть процес патчингу та оновлення програмного забезпечення мережевих пристроїв. Чому це так важливо для безпеки?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буров Є.В., Митник М.М. Комп'ютерні мережі : навчальний посібник. Львів: Видавництво «Магнолія 2006», 2021. Том 1. 340 с
2. Євсеєв С.П., Дженюк Н.В. Комп'ютерні мережі : навчальний посібник. Львів: Видавництво ПП «Новий Світ – 2000», 2024. Кн. 1 : Технології комп'ютерних мереж. 471 с.
3. Тарнавський Ю.А., Кузьменко І.М.. Організація комп'ютерних мереж : підручник для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2022. 328 с.
4. Хомуляк М.О. Адміністрування комп'ютерних систем і мереж : навчальний посібник. Львів: Видавництво «Магнолія 2006», 2023. 153 с
5. Глухов В.С., Костик А.Т. Дослідження та проектування комп'ютерних систем та мереж : навчальний посібник. Львів: Видавництво «Магнолія 2006», 2024. 253 с
6. Буров Є.В., Митник М.М. Комп'ютерні мережі : навчальний посібник. Львів: Видавництво «Магнолія 2006», 2021. Том 2. 400 с.
7. Євсеєв С.П., Дженюк Н.В. Комп'ютерні мережі : навчальний посібник. Львів: Видавництво ПП «Новий Світ – 2000», 2024. Кн. 2 : Архітектура комп'ютерів. 346 с.
8. Network Essentials Course Resources // Cisco Network Academy. URL: https://www.netacad.com/courses/networking/networking-essentials (дата звернення: 10.05.2025).
9. CCNA 7: Introduction to Networks Course Resources // Cisco Network Academy. URL: https://www.netacad.com/portal/resources/course-resources/ccna-itn (дата звернення: 11.05.2025).
10. Packet Tracer Resources // Симулятор мережі передачі. URL: https://www.netacad.com/portal/resources/packet-tracer (дата звернення: 12.05.2025).
11. Investigate the TCP-IP and OSI Models in Action. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164714 (дата звернення: 12.05.2025).
12. Connect the Physical Layer. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164715 (дата звернення: 13.05.2025).
13. Examine the ARP Table. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164716 (дата звернення: 13.05.2025).
14. IPv6 Neighbor Discovery. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164717 (дата звернення: 14.05.2025).
15. Subnet an IPv4 Network. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164718 (дата звернення: 14.05.2025).
16. Use a Port Scanner to Detect Open Ports. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164719 (дата звернення: 15.05.2025).
17. VLSM Design and Implementation Practice. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164720 (дата звернення: 15.05.2025).
18. Design and Implement a VLSM Addressing Scheme. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164721 (дата звернення: 15.05.2025).
19. Explore File and Data Encryption. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164722 (дата звернення: 16.05.2025).
20. Configure IPv6 Addressing. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164723 (дата звернення: 16.05.2025).
21. Implement a Subnetted IPv6 Addressing Scheme. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164724 (дата звернення: 16.05.2025).
22. Verify IPv4 and IPv6 Addressing. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164725 (дата звернення: 17.05.2025).
23. Use Ping and Traceroute to Test Network Connectivity. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164726 (дата звернення: 17.05.2025).
24. Use ICMP to Test and Correct Network Connectivity. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164727 (дата звернення: 17.05.2025).
25. Secure Network Devices. *Packet Tracer*. URL: https://mdl.lntu.edu.ua/mod/resource/view.php?id=164728 (дата звернення: 18.05.2025).

ДЛЯ НОТАТОК

Адміністрування комп’ютерних систем та мереж: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерні науки» галузі знань 12 (F) Інформаційні технології спеціальності 122 (F3) Комп’ютерні науки денної та заочної форм навчання / уклад. В.А. Кошелюк – Луцьк: ЛНТУ, 2025. 24 с.

Видання містить рекомендації до виконання лабораторних робіт з дисципліни « Адміністрування комп’ютерних систем та мереж ».

Призначене для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 122 (F3) Комп’ютерні науки.

Комп’ютерний набір та верстка: В.А. Кошелюк

Редактор: В.А. Кошелюк

Підп. до друку «_____»_____2025 р.
Формат 60×84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. ____ Тираж ___ прим. Зам. ___

Відділ іміджу та промоції
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75