Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра комп’ютерних наук

Допущено до захисту
Завідувач кафедри
комп’ютерних наук,
кандидат техн. наук, доцент
_____Ірина МАШКІНА
(підпис)
«_____» _____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня «бакалавр»

Спеціальність 122 Комп’ютерні науки

Освітня програма 122.00.01 Інформатика

Тема: РОЗРОБКА МОДЕЛІ МЕРЕЖЕВОЇ АРХІТЕКТУРИ ШКОЛИ

Виконав
студентка групи ІНб-1-21-4.0д
(шифр академічної групи)
Плоха Ангеліна Юріївна
(прізвище, ім’я, по батькові)

_____
(підпис)
Науковий керівник
к.п.н., доцент кафедри комп'ютерних наук
(науковий ступінь, наукове звання)
Глушак О. М.
(прізвище, ініціали)

_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра комп'ютерних наук

«Затверджую»

Завідувач кафедри комп'ютерних наук,

кандидат техн. наук, доцент

_____Ірина МАШКІНА

(підпис)

«____» _____ 2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

«Розробка моделі мережевої архітектури школи»

Виконавець – студентка групи ІНб-1-21-4.0д,

спеціальності 122 Комп'ютерні наук,

освітньої програми 122.00.01 Інформатика

Плоха Ангеліна Юріївна

1. Вихідні дані: *Документація Cisco, навчальні посібники з комп'ютерних мереж, санітарні норми для ІКТ-інфраструктури закладів освіти, приклади топологій і конфігурацій у Cisco Packet Tracer, матеріали з офіційних сайтів Cisco, МОН, ISO.*

2. Основні завдання: *Проаналізувати потреби школи в комп'ютерній мережі, обґрунтувати мету, об'єкт, предмет і методичну базу проєкту, розробити структуру та зміст роботи, визначити підходи до вибору топології, сегментації VLAN, конфігурації маршрутизаторів і комутаторів, створити логічну та фізичну модель мережі в Cisco Packet Tracer, налаштувати сервіси DHCP, DNS, WEB, FTP, ACL, Port Security, замоделювати авторизацію через вебінтерфейс і передачу даних на FTP-сервер, протестувати мережу та оцінити відповідність нормативним вимогам*: Пояснювальна записка: Обсяг – до 45 стор. формату А4 комп'ютерного набору з дотриманням вимог стандарту і методичних рекомендацій кафедри.

3. Графічні матеріали: *не передбачено.*

4. Додатки: *лістинг програми*

5. Строк подання роботи на кафедру: *«_____» _____2025 р.*

Науковий керівник

Науковий ступінь, звання

_____ПІБ

_____дата

Виконавець:

_____ПІБ

_____дата

РЕФЕРАТ бакалаврської роботи

Кваліфікаційна робота: 42 сторінки, 12 рисунків, 1 таблиця, 25 посилань.

Актуальність: У сучасних умовах цифровізації освіти створення ефективної та безпечної комп'ютерної мережі для закладів загальної середньої освіти є критично важливим. Забезпечення стабільного доступу до навчальних ресурсів, захист персональних даних і підтримка сучасних освітніх технологій вимагають розробки мережевої інфраструктури, яка відповідає технічним і нормативним вимогам. Реалізація шкільної мережі з використанням сучасного обладнання Cisco та моделювання в Cisco Packet Tracer дозволяє оптимізувати освітні процеси та забезпечити безпечне інформаційне середовище.

Об'єкт дослідження: Мережева інфраструктура сучасного навчального закладу.

Предмет дослідження: Процес моделювання, розробки та реалізації мережевої архітектури школи з використанням обладнання Cisco

Мета роботи: Розробити модель мережевої архітектури сучасної школи, яка забезпечить продуктивність, безпеку, стабільність та відповідатиме сучасним освітнім вимогам.

Завдання:

1. Аналіз потреб школи в IT.
2. Обґрунтування вибору топології та обладнання Cisco.
3. Розробка логічної моделі мережі.
4. Реалізація моделі в Cisco Packet Tracer із налаштуванням безпеки.
5. Оцінка перспектив впровадження моделі.

Основні результати: Розроблено модель мережі на базі Cisco Catalyst 9200, ISR 1100-4G, Aironet 1850 із шістьма VLAN, сервісами DHCP, DNS, WEB, FTP. Безпека забезпечена WPA3, ACL, Port Security, автентифікацією. Моделювання в Packet Tracer підтвердило пропускну здатність 1 Гбіт/с і стабільність.

Ключові слова: комп’ютерна мережа, Cisco, VLAN, DHCP, DNS, WEB, FTP, ACL, Port Security, Cisco Packet Tracer, безпека мережі, шкільна інфраструктура.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах розвитку інформаційного суспільства освітні заклади стикаються з гострою необхідністю в модернізації та розвитку власної IT-інфраструктури. Використання сучасних інформаційних технологій дозволяє покращити якість навчального процесу, забезпечити оперативний доступ до навчальних ресурсів, підвищити ефективність адміністративного управління школою. Саме тому особливе значення має проєктування та впровадження сучасних мережевих архітектур, що відповідають актуальним освітнім потребам, враховують вимоги до продуктивності, безпеки та надійності інформаційних систем у навчальних закладах.

Мета роботи – розробити модель мережевої архітектури сучасної школи, яка забезпечить високу продуктивність, безпеку, стабільність та відповідатиме сучасним освітнім вимогам.

Завдання роботи:

1. Провести аналіз потреб школи в інформаційних технологіях.
2. Обґрунтувати вибір оптимальної топології та обладнання (Cisco) для реалізації мережі.
3. Розробити логічну модель мережі навчального закладу.
4. Реалізувати модель мережі в програмному середовищі Cisco Packet Tracer із конфігуруванням обладнання та забезпеченням безпеки.
5. Оцінити ефективність розробленої мережевої моделі та перспективи її впровадження.

Об'єктом дослідження є мережева інфраструктура сучасного навчального закладу. Предметом дослідження виступає процес моделювання, розробки та реалізації мережевої архітектури школи з використанням обладнання Cisco.

Методи дослідження. Під час виконання роботи застосовуються методи аналізу та синтезу інформації, системного підходу до проєктування, методи моделювання та експериментального тестування створеної мережевої моделі.

Практична значущість роботи полягає у можливості використання розробленої моделі мережевої архітектури для модернізації та оптимізації інформаційних систем реальних шкіл, що сприятиме підвищенню ефективності навчального процесу.

1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ МЕРЕЖЕВОЇ АРХІТЕКТУРИ

1.1 Аналіз потреб сучасної школи в інформаційних технологіях

У сучасному освітньому просторі інформаційні технології (ІТ) є основою для забезпечення стабільної роботи навчального середовища. Школи використовують широкий спектр ІТ-ресурсів: електронні підручники, платформи для онлайн-уроків (наприклад, Zoom, Google Classroom), системи управління навчальним процесом (LMS), електронні журнали, а також інноваційні технології, такі як віртуальна реальність (VR) та Інтернет речей (IoT). Ці інструменти потребують надійної мережевої інфраструктури, яка забезпечує високу пропускну здатність, стабільність з’єднання та безпеку даних [1].

Для підтримки дистанційного навчання, що стало критично важливим під час пандемії COVID-19, мережа повинна мати пропускну здатність щонайменше 100 Мбіт/с (Fast Ethernet) або 1 Гбіт/с (Gigabit Ethernet) для обробки відеотрафіку та одночасного доступу багатьох користувачів. Наприклад, одночасне використання Zoom кількома класами потребує стабільного з’єднання з низькою затримкою (менше 20 мс) та достатньої ширини каналу [2]. Wi-Fi-мережі з технологією 802.11ac або 802.11ax (Wi-Fi 6) необхідні для забезпечення покриття та мобільності, особливо в аудиторіях і коридорах.

Безпека є ключовим аспектом: захист персональних даних учнів і вчителів вимагає впровадження протоколів шифрування (наприклад, WPA3 для Wi-Fi) та firewall-систем для блокування несанкціонованого доступу. Сучасні школи також використовують хмарні сервіси (Google Drive, Microsoft 365), що потребує стабільного інтернет-з’єднання зі швидкістю не нижче 50 Мбіт/с на одного користувача при пікових навантаженнях [4].

Інтеграція VR та IoT (наприклад, «розумні» дошки чи датчики) підвищує вимоги до мережі: низька латентність (до 10 мс) і підтримка великої кількості підключених пристроїв (до 50-100 на точку доступу).

Таким чином, мережа школи повинна мати високу пропускну здатність, низьку затримку, захист від кіберзагроз і можливість масштабування для майбутніх потреб [5].

1.2 Огляд існуючих підходів до побудов локальних мереж у навчальних закладах

У сучасних навчальних закладах локальні комп'ютерні мережі (ЛКМ) є основою інформаційної інфраструктури, забезпечуючи ефективний доступ до освітніх ресурсів та підтримку навчального процесу. При проєктуванні та впровадженні ЛКМ необхідно враховувати специфічні потреби освітніх установ, такі як масштабованість, безпека, надійність та економічна ефективність [6].

Вибір топології мережі є ключовим аспектом проєктування ЛКМ. Найбільш поширеною є зіркоподібна топологія, де всі пристрої підключені до центрального комутатора або концентратора. Ця конфігурація спрощує управління мережею та забезпечує високу надійність; відмова одного з підключень не впливає на роботу всієї мережі. Інші топології, такі як шинна та кільцева, використовуються рідше через їх обмеження в масштабованості та надійності [7].

Технологія Ethernet є стандартом для ЛКМ, забезпечуючи швидкість передачі даних від 10 Мбіт/с до 1 Гбіт/с. Вона є надійною, економічною та простою в реалізації, що робить її придатною для більшості освітніх потреб. Для підвищення пропускної здатності можуть використовуватися технології Fast Ethernet (до 100 Мбіт/с) та Gigabit Ethernet (до 1 Гбіт/с), що дозволяють обробляти більші обсяги даних та підтримувати сучасні мультимедійні застосунки [6].

При проєктуванні ЛКМ для навчальних закладів важливо провести детальний аналіз потреб, визначивши кількість користувачів, типи застосувань, необхідну пропускну здатність та майбутні потреби в розширенні мережі.

Вибір якісного мережевого обладнання, яке відповідає вимогам надійності та безпеки, є критичним для забезпечення стабільної роботи мережі. Недооцінка цього аспекту може призвести до низької пропускної здатності та ненадійної роботи мережі [8]. Крім того, необхідно впроваджувати заходи для захисту від несанкціонованого доступу, вірусів та інших кіберзагроз, забезпечуючи безпеку мережі. Мережа повинна бути масштабованою, тобто забезпечувати можливість легкого розширення в майбутньому без значних перебудов.

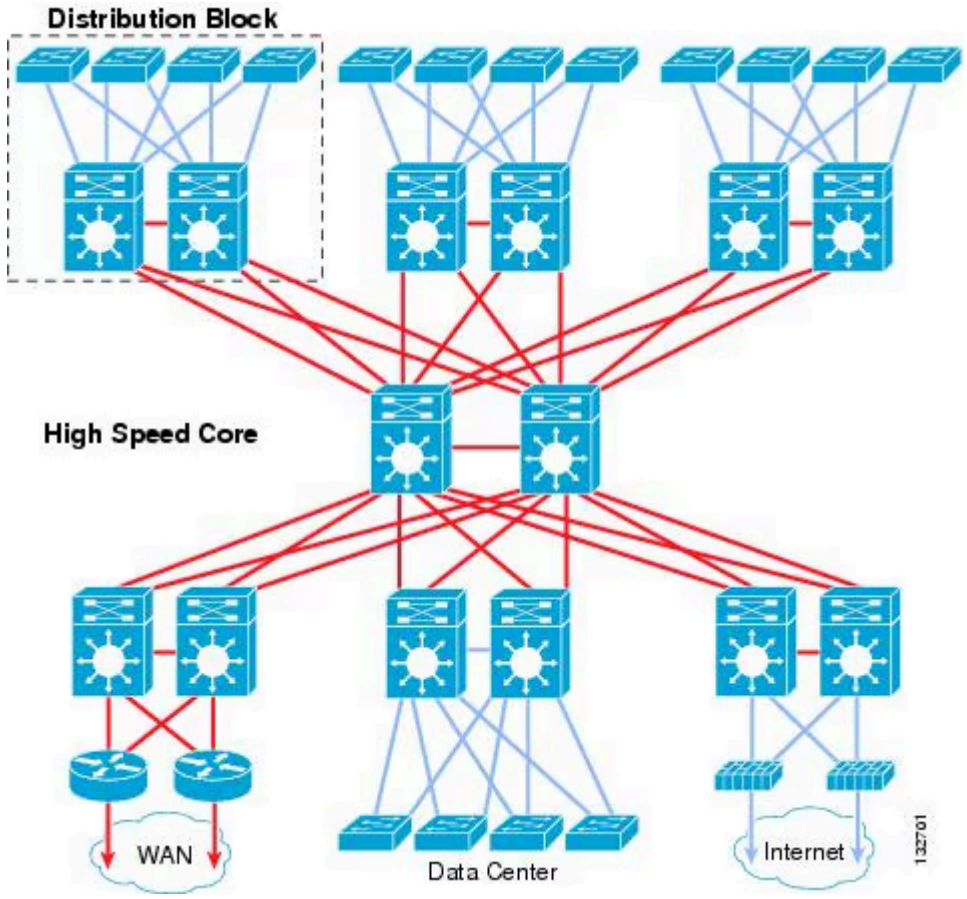

Рисунок .1. Приклад ієрархічної (деревоподібної) топології [9]

Для великих шкіл із розподіленою інфраструктурою ефективним рішенням є ієрархічна (деревоподібна) топологія, яка включає три рівні: ядро (Core), розподільчий рівень (Distribution) і рівень доступу (Access).

Ядро забезпечує швидке з'єднання з Інтернетом, розподільчий рівень об'єднує комутатори на різних поверхах чи корпусах, а рівень доступу включає точки доступу Wi-Fi для учнів і вчителів. Така модель із високошвидкісним ядром, розподільчими блоками та підключенням до дата-центру чи WAN (як показано на схемі з документа Cisco) дозволяє ефективно управляти трафіком, сегментувати мережу за допомогою VLAN і забезпечувати пріоритетність для критичних застосунків, наприклад, відеоконференцій [9].

1.3 Вибір топології та обладнання для розробки мережі школи (Cisco)

Для розробки мережевої архітектури школи обрано зіркоподібну топологію, яка є оптимальним рішенням для багатьох навчальних закладів завдяки своїй простоті, надійності та легкості в управлінні. У такій топології всі пристрої (комп'ютери, точки доступу Wi-Fi, сервери) підключаються до центрального комутатора, який виступає ядром мережі та забезпечує передачу даних між усіма вузлами. Ця структура дозволяє швидко виявляти й усувати несправності, адже відмова одного пристрою не впливає на роботу всієї мережі, що є критично важливим для шкіл із обмеженими технічними ресурсами [11]. Крім того, зіркоподібна топологія забезпечує високу продуктивність завдяки прямому з'єднанню кожного вузла з комутатором, а також легке масштабування — для підключення нових пристроїв достатньо додати порти до центрального комутатора. Для шкіл із середньою кількістю користувачів (до 200-300 учнів і вчителів) така топологія ідеально підходить, оскільки не потребує складного налаштування й забезпечує стабільний доступ до ресурсів, таких як електронні журнали чи платформи для онлайн-навчання.

Для порівняння в попередньому розділі було розглянуто ієрархічну топологію, але її не обрано через надмірну складність і високу вартість

впровадження, що не виправдано для середньої школи з одним корпусом і обмеженим бюджетом.

Щодо планованої реалізації зіркоподібної топології, мережа включатиме кілька ключових зон школи: комп’ютерні класи для учнів і вчителів, серверну кімнату, адміністративний блок і кабінет директора. Центральним елементом мережі виступить комутатор, до якого підключатимуться точки доступу Wi-Fi для бездротового зв’язку, а також сервери для зберігання даних (наприклад, DHCP-сервер для автоматичного призначення IP-адрес і DNS-сервер для розпізнавання доменних імен). Для зв’язку між різними зонами школи планується використання маршрутизаторів, які забезпечать підключення до зовнішньої мережі (Інтернет) зі швидкістю до 500 Мбіт/с. У кожній зоні, як-от комп’ютерні класи чи учительська, передбачається встановлення локальних точок доступу (Access Points) для забезпечення бездротового доступу учнів і вчителів до мережі з їхніх ноутбуків і планшетів. Для друку документів у кожній зоні передбачені мережеві принтери, підключені до локальних комутаторів.

Щодо обладнання, для реалізації проєкту обрано техніку Cisco, яка є стандартом у побудові надійних і безпечних мереж. Центральним елементом мережі буде комутатор Cisco Catalyst 9200 Series, наприклад, модель Cisco C9200L-24T-4G-E, який підтримує швидкість до 1 Гбіт/с, має 24 порти для підключення пристроїв і 4 гігабітні uplink-порти для з’єднання з маршрутизатором, а також забезпечує функції безпеки, такі як захист від DoS-атак і підтримка VLAN для сегментації мережі [11]. Для забезпечення доступу до Інтернету використовується маршрутизатор Cisco ISR 1000 Series, зокрема модель Cisco ISR 1100-4G, який підтримує швидкість до 1 Гбіт/с і має вбудовані функції firewall для захисту від зовнішніх загроз [12].

Для бездротового доступу в зонах, таких як комп’ютерні класи та учительська, планується встановлення точок доступу Cisco Aironet 1800 Series, наприклад, Aironet 1850, які підтримують стандарт Wi-Fi 5 (802.11ac) і забезпечують швидкість до 1,7 Гбіт/с, що дозволяє одночасно обслуговувати до 50 користувачів на одну точку доступу [10].

Для серверної кімнати передбачено використання серверів Cisco UCS C-Series, які забезпечать роботу DHCP і DNS-серверів, а також зберігання даних, наприклад, електронних журналів. Для забезпечення безпеки мережі налаштовується шифрування WPA3 і сервер RADIUS на базі Cisco Identity Services Engine (ISE), який дозволяє централізовано управляти доступом користувачів, розділяючи права для учнів, вчителів і адміністрації.

Кабельна інфраструктура базується на кабелях категорії Cat6, які підтримують швидкість до 1 Гбіт/с і є економічно вигідним рішенням для шкіл. Для забезпечення живлення точок доступу та інших пристроїв використовується технологія PoE (Power over Ethernet), яку підтримує обраний комутатор Cisco Catalyst 9200. Загалом, зіркоподібна топологія в поєднанні з обладнанням Cisco забезпечує стабільну, безпечну й масштабовану мережу, яка відповідає потребам сучасної школи.

2 ПРОЄКТУВАННЯ МОДЕЛІ МЕРЕЖЕВОЇ АРХІТЕКТУРИ ШКОЛИ

2.1 Аналіз вимог до мережі

Розробка майбутньої зіркоподібної топології для шкільної мережі вимагає ґрунтовного аналізу вимог, які забезпечать її ефективність, адаптивність і відповідність сучасним освітнім стандартам. Мережа планується для обслуговування комп’ютерних класів, учительської, серверного простору, адміністративних зон і кабінету директора, охоплюючи до 200-300 користувачів — учнів, педагогів і персоналу.

Однією з ключових потреб є висока пропускна спроможність, яка дозволить підтримувати інтенсивне використання цифрових платформ, таких як онлайн-курси, відеозв’язок і хмарні сервіси. З огляду на можливу кількість одночасних з’єднань (до 150 пристроїв — комп’ютерів, планшетів і ноутбуків), мінімальна швидкість зв’язку з зовнішніми ресурсами має сягати 1 Гбіт/с, а локальні сегменти — бути готовими до обробки мультимедійного контенту, включаючи потокове відео та інтерактивні навчальні програми [13]. Точки доступу Wi-Fi повинні забезпечувати стабільне покриття в кожній зоні з можливістю підключення до 50 користувачів із пропускною спроможністю до 1,7 Гбіт/с, що відповідатиме вимогам дистанційного навчання та інтерактивних занять, таких як віртуальні лабораторії чи групові проєкти [14]. Також мережа має підтримувати інноваційні технології, як-от віртуальна реальність, з низькою затримкою (до 20 мс), що є важливим для реалізації сучасних методик навчання, наприклад, симуляцій у STEM-освіті.

Безпека мережі є пріоритетом через необхідність захисту персональних даних учнів і педагогів, що регулюється освітніми нормами, зокрема вимогами до обробки даних у закладах освіти [15]. Планується впровадження шифрування WPA3 для бездротових з’єднань і RADIUS для контролю доступу, що дозволить створювати окремі профілі для учнів, вчителів і адміністрації, забезпечуючи захист від несанкціонованого доступу.

Сегментація трафіку за допомогою VLAN ізолюватиме мережі різних груп користувачів, зменшуючи ризик витоку даних і підвищуючи загальну безпеку системи [13]. Обладнання має включати захист від кібератак, таких як DDoS, а також відповідати санітарним вимогам щодо електромагнітного випромінювання, щоб забезпечити безпечне використання техніки в навчальному середовищі.

Надійність системи критично важлива для безперервності навчального процесу, особливо в умовах можливого переходу на дистанційне навчання. Зіркоподібна структура з центральним комутатором передбачає резервування живлення через PoE і дублювання маршрутизаторів та серверів (DHCP, DNS), що забезпечить стабільність роботи навіть у разі збоїв [16]. Затримка сигналу не повинна перевищувати 20 мс для якісного відеозв’язку, що підтримує нові підходи до оцінювання учнів, передбачені оновленими стандартами, такими як використання онлайн-тестування та інтерактивних платформ [15]. Крім того, мережа має бути готова до пікових навантажень, наприклад, під час одночасного використання відеоконференцій кількома класами.

Масштабованість мережі забезпечить готовність до розширення закладу чи збільшення кількості пристроїв. Обладнання має мати не менше 24 портів для підключення комп’ютерів, принтерів і додаткових точок доступу, а також підтримувати кабелі Cat6 для майбутньої модернізації [16]. Мережа повинна бути готова до інтеграції з інформаційними системами управління освітою, такими як електронні журнали чи платформи для звітності, що вимагає гнучкості в налаштуванні та розподілі ресурсів [15].

Економічна доцільність зосереджується на оптимізації витрат через використання PoE, що зменшує потребу в додаткових джерелах живлення, і простого в управлінні обладнання, яке не потребує складного технічного обслуговування [13]. Мережа також має сприяти інклюзивному навчанню, надаючи стабільний доступ до ресурсів для учнів із особливими потребами, наприклад, через підтримку спеціалізованих програм для слабозорих чи слабочуючих.

Важливим є забезпечення роботи систем оповіщення, які можуть бути інтегровані в мережу для швидкого інформування учнів і персоналу в разі надзвичайних ситуацій, а також резервного копіювання даних для захисту навчальних матеріалів [16]. Мережа має відповідати стандартам енергоефективності, зменшуючи споживання енергії шляхом використання сучасного обладнання з низьким енергоспоживанням, що є важливим для довгострокової економії та екологічної відповідальності.

Додатково, при розміщенні техніки в приміщеннях необхідно враховувати санітарні норми, які регулюють кількість пристроїв у навчальних класах для забезпечення безпечних умов. Згідно з Державними санітарними правилами і нормами для закладів загальної середньої освіти, у комп'ютерному класі на одного учня має припадати не менше 6 м² площі, а кількість комп'ютерів у приміщенні не повинна перевищувати 12 одиниць для класів площею до 72 м², щоб уникнути надмірного електромагнітного випромінювання та забезпечити належну вентиляцію [16]. Це впливає на планування розміщення техніки в зонах Computer Class 1 і Computer Class 2, де кількість пристроїв має бути обмежена, а також на розташування точок доступу Wi-Fi, щоб мінімізувати вплив випромінювання на учнів.

2.2 Розробка логічної моделі мережі

Логічна модель мережевої архітектури школи буде створена як фундамент для майбутньої побудови фізичної структури, яка ґрунтуватиметься на зіркоподібному підході. Вона визначатиме організацію мережі на концептуальному рівні, охоплюючи розподіл зон, маршрутизацію, ізоляцію трафіку та заходи захисту, щоб забезпечити функціональність для комп'ютерних класів, учительських приміщень, серверного блоку, адміністративної частини та кабінету директора, розрахованих на 200-300 осіб, включаючи учнів, вчителів і персонал.

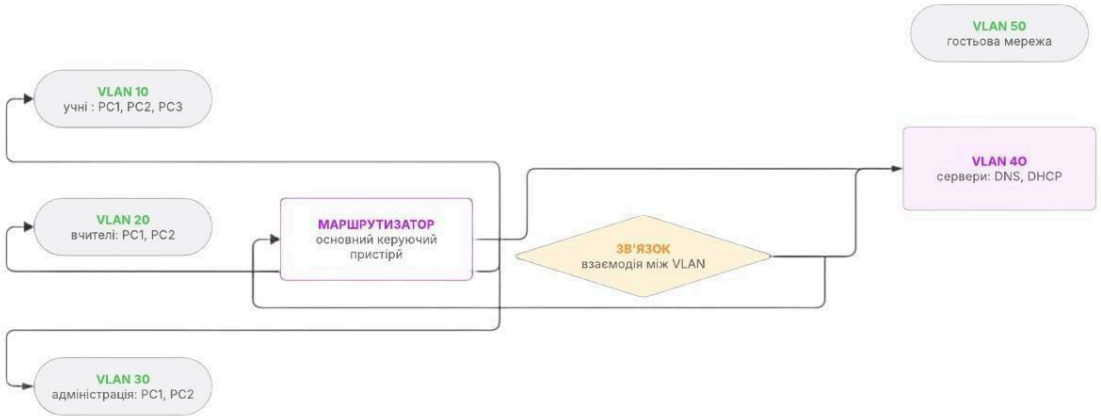

Рисунок 2. Логічна модель мережі [17]

Логічна схема побудована на зіркоподібному принципі, де головний маршрутизатор (маршрутизатор основний керуючий) є центральним елементом, що об’єднує всі зони через механізм міжмережевого обміну VLAN. Мережа поділена на п’ять підмереж, що дозволяє розмежувати потоки даних між різними групами користувачів і серверами, забезпечуючи зручне адміністрування та захист.

Мережа логічно структурована на п’ять VLAN для розмежування трафіку та забезпечення ізоляції. Головний маршрутизатор забезпечуватиме обмін даними між цими сегментами, дозволяючи, наприклад, учням із VLAN 10 звертатися до серверів у VLAN 40, але блокуючи їхній доступ до VLAN 30, що підвищить захист.

Захист мережі планується організувати на кількох рівнях. Для бездротового зв’язку в зонах Computer Class 1, Computer Class 2 і Teachers Room буде використано шифрування WPA3, щоб запобігти несанкціонованому підключенню. Автентифікація користувачів здійснюватиметься через систему RADIUS, розміщену в VLAN 40, що дозволить розмежувати права доступу: учні, вчителі та адміністрація матимуть різні привілеї. Наприклад, учні з VLAN 10 і 20 не зможуть підключатися до VLAN 30, а гостьова зона (VLAN 50) буде відокремлена від решти мережі.

Головний маршрутизатор матиме вбудовані механізми захисту від зовнішніх атак, таких як DDoS, і контролюватиме потоки даних між сегментами.

Головний маршрутизатор відповідатиме за передачу даних між VLAN, забезпечуючи зв’язок між зонами. Наприклад, пристрої з VLAN 10 зможуть звертатися до серверів у VLAN 40 для доступу до навчальних ресурсів. Для забезпечення пріоритету важливого трафіку, наприклад, для відеозв’язку, планується впровадження QoS, що мінімізує затримки. Зовнішній зв’язок зі швидкістю 1 Гбіт/с гарантуватиме достатню пропускну здатність для всіх користувачів, включаючи доступ до хмарних платформ і потокового контенту.

Мережа буде готова до інтеграції з платформами управління освітою через сервери у VLAN 40, що дозволить вести електронні журнали та створювати звіти. Логічна схема передбачає можливість розширення: нові зони чи пристрої можна буде додавати без значних змін у структурі. У кожній зоні передбачається розміщення принтерів, доступних для відповідних груп, а сервери у VLAN 40 забезпечуватимуть збереження даних для захисту навчальних матеріалів.

2.3 Фізична модель мережі реалізована в Cisco Packet Tracer

Було розроблено модель мережевої архітектури школи в програмному середовищі Cisco Packet Tracer, яка являє собою фізичну реалізацію зіркоподібної топології, створеної на основі попередньо визначеної логічної моделі. Модель охоплює основні зони навчального закладу, зокрема комп’ютерні класи, учительську, серверну кімнату, адміністративний блок і кабінет директора, забезпечуючи зв’язок між ними через маршрутизатори та локальні комутатори. Під час розробки враховано вимоги до продуктивності, безпеки та доступності, а також підібрано відповідні пристрої для кожної зони.

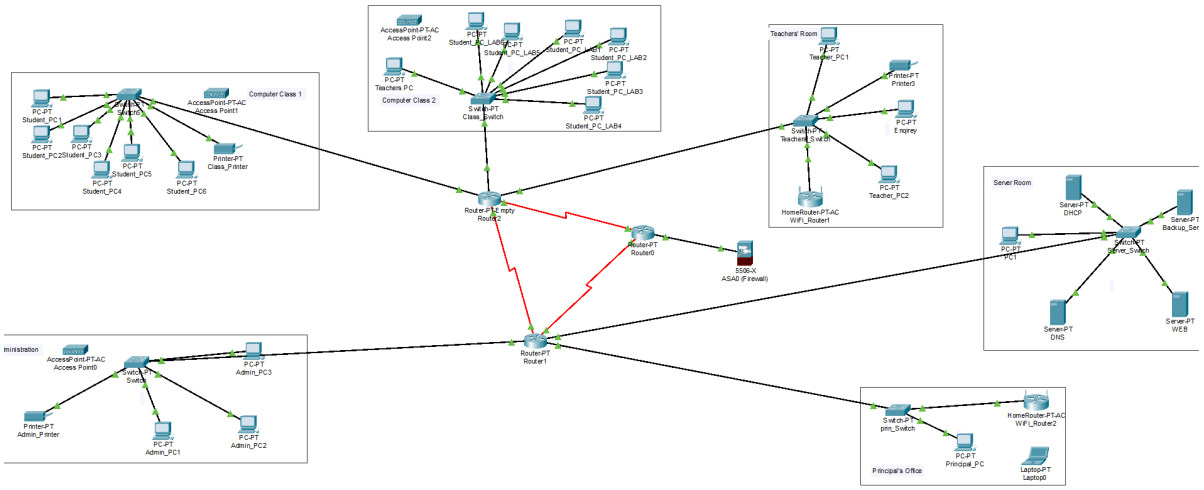

Рисунок .3. Розроблена топологія школи у Cisco Packet Tracer

Модель створено на основі зіркоподібної топології, де центральним елементом виступає маршрутизатор Router0 (ISA 500X Firewall), який об’єднує всі зони (Computer Class 1, Computer Class 2, Teachers Room, Server Room, Admin, Principal Office) і забезпечує зв’язок із зовнішньою мережею (Інтернет) через пристрій ASA (Firewall). До Router0 підключено два маршрутизатори: Router-Empty і Router1 (Router-PT). Router-Empty забезпечує маршрутизацію між трьома підмережами (Computer Class 1, Computer Class 2, Teachers Room), тоді як Router1 об'єднує підмережі Server Room, Admin і Principal Office, забезпечуючи зв’язок між цими зонами та Router0. Кожна зона підключена до маршрутизатора Router0 через локальні комутатори та точки доступу Wi-Fi, що забезпечують як дротове, так і бездротове з’єднання [18].

Пристрої, включені до моделі мережі

Computer Class 1:

1. Локальний комутатор Switch1 об’єднує пристрої в цій зоні.
2. Розміщено шість комп’ютерів (Student PC1, PC2, PC3, PC4, PC5, PC6) для учнів, призначені для виконання навчальних завдань, зокрема доступу до онлайн-платформ.

3. Встановлено мережевий принтер (Class Printer) для друку матеріалів у межах класу.

4. Додано точку доступу AccessPointTAC для забезпечення бездротового зв’язку учнівських ноутбуків і планшетів.

Computer Class 2:

1. Локальний комутатор Switch2 з’єднує пристрої в цій зоні.

2. Розміщено шість комп’ютерів (Student PC LAB1, PC LAB2, PC LAB3, PC LAB4, PC LAB5, PC LAB6).

3. Встановлено точку доступу AccessPointTAC для бездротового підключення додаткових пристроїв.

4. Розміщено також комп’ютер вчителя Teacher PC.

Teachers Room:

1. Локальний комутатор Teacher Switch об’єднує пристрої в учительській.

2. Розміщено два комп’ютери (Teachers PC1, PC2) для викладачів, призначені для підготовки уроків і роботи з адміністративними ресурсами.

3. Встановлено мережевий принтер (Printer-PT) для друку документів.

4. Додано точку доступу HomeWiFi-RouterTAC для бездротового зв’язку, що дозволяє вчителям підключати особисті пристрої, наприклад, ноутбуки.

Server Room:

1. Локальний комутатор Server Switch забезпечує з’єднання серверів із мережею.

2. Розміщено сервери: DHCP-сервер (Server-PT DHCP) для автоматичного призначення IP-адрес, DNS-сервер (Server-PT DNS) для розпізнавання доменних імен, WEB-сервер (Server-PT WEB) для розміщення внутрішнього порталу школи, і Backup Server (Server-PT Backup) для резервного копіювання даних.

3. Встановлено комп’ютер (PC1) для адміністрування серверів.

Admin:

1. Локальний комутатор Switch3 об’єднує пристрої в адміністративному блоці.
2. Розміщено три комп’ютери (Admin PC1, PC2, PC3) для адміністративного персоналу, призначені для ведення документації та звітності.
3. Встановлено мережевий принтер (Admin Printer) для друку документів.
4. Додано точку доступу AccessPointTAC для бездротового зв’язку.

Principal Office:

1. Локальний комутатор prin_switch забезпечує з’єднання пристроїв у кабінеті директора.
2. Розміщено комп’ютер (Principal PC) і ноутбук (Laptop0) для роботи директора.
3. Встановлено точку доступу HomeWiFi-RouterTAC2 для бездротового підключення.

Зв’язок у моделі організовано таким чином, що маршрутизатор Router0 об’єднує всі зони та забезпечує зв’язок із зовнішньою мережею через пристрій ASA (Firewall). Router-Empty, підключений до Router0, відповідає за маршрутизацію між трьома підмережами (Computer Class 1, Computer Class 2, Teachers Room), забезпечуючи зв’язок між цими зонами через відповідні комутатори (Switch1, Switch2, Teacher Switch). Router1, також підключений до Router0, відповідає за маршрутизацію між підмережами Server Room, Admin і Principal Office, забезпечуючи зв’язок між цими зонами через відповідні комутатори (Server Switch, Switch3, prin_switch). Router0 (ISA 500X Firewall) оснащений вбудованим брандмауером для фільтрації трафіку та захисту від кіберзагроз.

Локальні комутатори (Switch1, Switch2, Teacher Switch, Server Switch, Switch3, prin_switch) забезпечують дротове підключення пристроїв у кожній зоні, а точки доступу (AccessPointTAC, HomeWiFi-RouterTAC, HomeWiFi-RouterTAC2) дозволяють підключати бездротові пристрої, такі як ноутбуки та планшети учнів і вчителів. Мережеві принтери в кожній зоні (Class Printer, Printer-PT, Admin Printer) підключені до локальних комутаторів, що забезпечує зручний доступ до друку для відповідних груп користувачів.

Модель розроблена з урахуванням потреб школи в продуктивності та безпеці. DHCP-сервер у Server Room автоматизує призначення IP-адрес, а DNS-сервер забезпечує доступ до навчальних ресурсів через доменні імена. WEB-сервер призначений для створення внутрішнього порталу школи, а Backup Server гарантує збереження даних. Точки доступу Wi-Fi налаштовані для обслуговування до 50 пристроїв у кожній зоні, забезпечуючи мобільність для учнів і вчителів. Модель передбачає можливість масштабування: додавання нових пристроїв можливе через вільні порти на комутаторах.

3 РЕАЛІЗАЦІЯ ПРОЄКТУ МЕРЕЖЕВОЇ АРХІТЕКТУРИ

3.1 Конфігурування обладнання Cisco

Для всіх пристроїв у мережі було здійснено статичне призначення IP-адрес. Хоча в інфраструктурі передбачено DHCP-сервер, який працює у VLAN 40, призначення адрес вручну дозволило точно відслідковувати розміщення кожного пристрою у відповідному сегменті, спростити діагностику й унеможливити конфлікти адрес у процесі налагодження мережі. Адресація здійснювалась відповідно до логіки поділу мережі на VLAN:

1. VLAN 10 – Computer Class 1;
2. VLAN 20 – Computer Class 2;
3. VLAN 30 – Teachers Room;
4. VLAN 40 – Server Room;
5. VLAN 50 – Administration;
6. VLAN 60 – Principal’s Office.

Таблиця .1. IP-адресація мережі

Пристрій	**IP-адреса**	**Маска підмережі**	**Шлюз за замовчуванням**
Computer Class 1			
Student_PC1	192.168.10.101	255.255.255.0	192.168.10.1
Student_PC2	192.168.10.102	255.255.255.0	192.168.10.1
Student_PC3	192.168.10.103	255.255.255.0	192.168.10.1
Student_PC4	192.168.10.104	255.255.255.0	192.168.10.1
Student_PC5	192.168.10.105	255.255.255.0	192.168.10.1
Student_PC6	192.168.10.106	255.255.255.0	192.168.10.1

Продовження таблиці 1. IP-адресація мережі

Пристрій	**IP-адреса**	**Маска підмережі**	**Шлюз за замовчуванням**
Class_Printer	192.168.10.110	255.255.255.0	192.168.10.1
Access Point1	192.168.10.120	255.255.255.0	192.168.10.1
Computer Class 2			
Teachers_PC	192.168.20.101	255.255.255.0	192.168.20.1
Student_PC_LAB1	192.168.20.102	255.255.255.0	192.168.20.1
Student_PC_LAB2	192.168.20.103	255.255.255.0	192.168.20.1
Student_PC_LAB3	192.168.20.104	255.255.255.0	192.168.20.1
Student_PC_LAB4	192.168.20.105	255.255.255.0	192.168.20.1
Student_PC_LAB5	192.168.20.106	255.255.255.0	192.168.20.1
Student_PC_LAB6	192.168.20.107	255.255.255.0	192.168.20.1
Access Point2	192.168.20.120	255.255.255.0	192.168.20.1
Teachers' Room			
Teacher_PC1	192.168.30.101	255.255.255.0	192.168.30.2
Teacher_PC2	192.168.30.102	255.255.255.0	192.168.30.2
Enquiry PC	192.168.30.103	255.255.255.0	192.168.30.2
Printer3	192.168.30.150	255.255.255.0	192.168.30.2
WiFi_Router1	192.168.30.200	255.255.255.0	192.168.30.2

Продовження таблиці 1. IP-адресація мережі

Пристрій	**IP-адреса**	**Маска підмережі**	**Шлюз за замовчуванням**
Server Room			
PC1	192.168.40.100	255.255.255.0	192.168.40.1
DHCP	192.168.40.13	255.255.255.0	192.168.40.1
Backup_Server	192.168.40.11	255.255.255.0	192.168.40.1
WEB_Server	192.168.40.10	255.255.255.0	192.168.40.1
DNS	192.168.40.12	255.255.255.0	192.168.40.1
Administration			
Admin_PC1	192.168.50.101	255.255.255.0	192.168.50.1
Admin_PC2	192.168.50.102	255.255.255.0	192.168.50.1
Admin_PC3	192.168.50.103	255.255.255.0	192.168.50.1
Admin_Printer	192.168.50.150	255.255.255.0	192.168.50.1
Wireless Router Admin	192.168.50.200	255.255.255.0	192.168.50.1
Principal’s Office			
Principal_PC	192.168.60.104	255.255.255.0	192.168.60.1
Laptop0	192.168.60.105	255.255.255.0	192.168.60.1
WiFi_Router2	192.168.60.201	255.255.255.0	192.168.60.1

Для кожного пристрою вказано IP-адресу, маску підмережі та шлюз за замовчуванням, що відповідає підмережі конкретної VLAN (Таблиця 1). Особливу увагу приділено тому, щоб шлюз для кожного пристрою відповідав IP-адресі підключеного інтерфейсу маршрутизатора у відповідній VLAN.

Реалізовано фільтрацію вхідного трафіку за допомогою списку контролю доступу (ACL) [19], застосованого на зовнішньому інтерфейсі маршрутизатора Router0. Це дозволило обмежити вхідні з'єднання з боку зовнішньої мережі (Інтернет), зокрема блокувати ICMP-запити (ping).

Спроба здійснити ping до внутрішньої адреси 192.168.100.1 завершується повідомленням «Destination host unreachable» (Рис .4.), що свідчить про успішне застосування політики безпеки. Це забезпечує захист локальної мережі навчального закладу від несанкціонованого зовнішнього сканування, яке потенційно може використовуватися для виявлення активних хостів або атак на них.

Попри обмеження ICMP, доступ до ключових внутрішніх сервісів, зокрема до серверної кімнати, залишається відкритим.

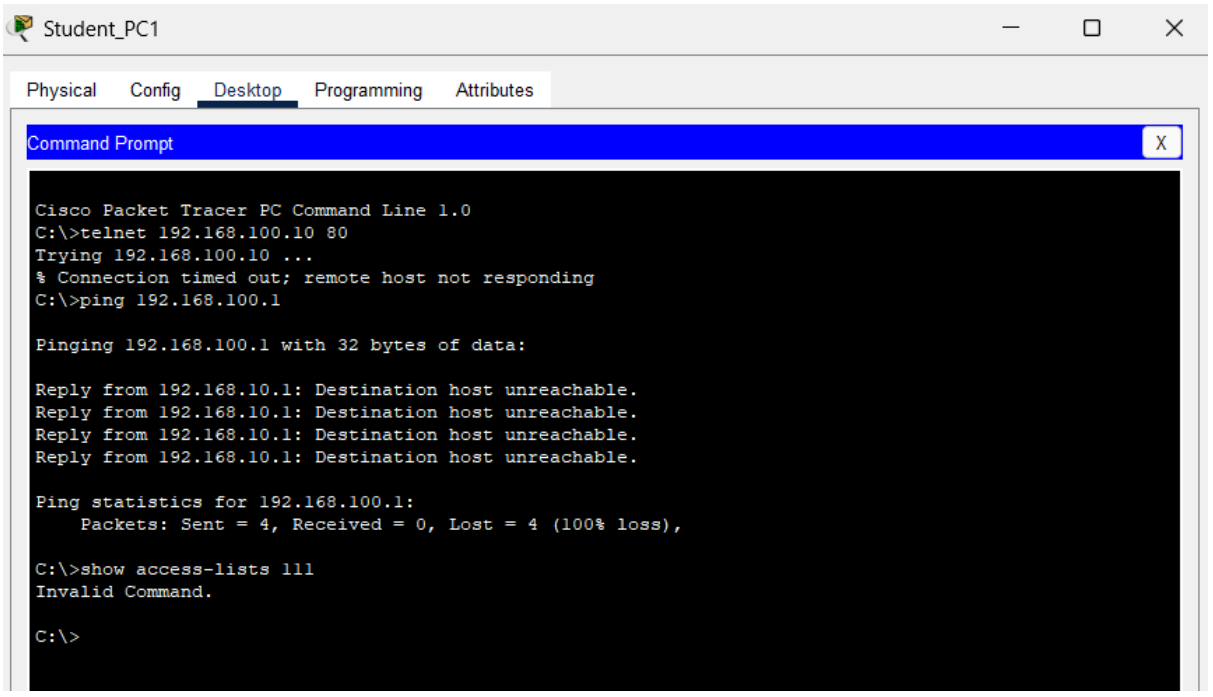

Рисунок .4. Налаштований захист зовнішнього периметра на Router0

На маршрутизаторі Router2 створено та застосовано список контролю доступу з назвою VLAN_ISOLATION, який блокує доступ з підмереж VLAN10 (Computer Class 1) і VLAN20 (Computer Class 2) до підмережі VLAN30 (Teachers Room). Це досягається шляхом заборони ICMP-пакетів у відповідному напрямку[20].

На рисунку 5 відображено результат перевірки за допомогою команди ping до IP-адреси 192.168.30.101 з комп'ютерів у VLAN10 та VLAN20. У всіх випадках повертається відповідь «Destination host unreachable», що підтверджує відсутність доступу між вказаними VLAN.

У цьому ж списку дозволено трафік до VLAN40 (Server Room), тому пристрої з VLAN10 та VLAN20 можуть звертатися до серверів у цій зоні, зокрема до DNS, DHCP та WEB-серверів. Це налаштування забезпечує ізоляцію доступу до вчительської кімнати при збереженні доступу до необхідних сервісів.

```
C:\>ping 192.168.40.100

Pinging 192.168.40.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.100: bytes=32 time=49ms TTL=126
Reply from 192.168.40.100: bytes=32 time=1ms TTL=126
Reply from 192.168.40.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.40.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 49ms, Average = 17ms

C:\>
C:\>ping 192.168.30.101

Pinging 192.168.30.101 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.30.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рисунок .5. Налаштована ізоляція комп'ютерних класів, пінг не проходить до вчительської

Wi-Fi покриття реалізовано для всіх виділених VLAN-зон (VLAN10, VLAN20, VLAN30, VLAN50, VLAN60). Кожна точка доступу під’єднана до порту комутатора, що переведений у режим access та закріплений за відповідною VLAN.

На пристроях встановлено захист WPA3, що забезпечує сучасний рівень шифрування бездротового трафіку та унеможливлює несанкціонований доступ. IP-адреси призначено вручну відповідно до адресної схеми, для кожної зони дотримано послідовність у конфігурації.

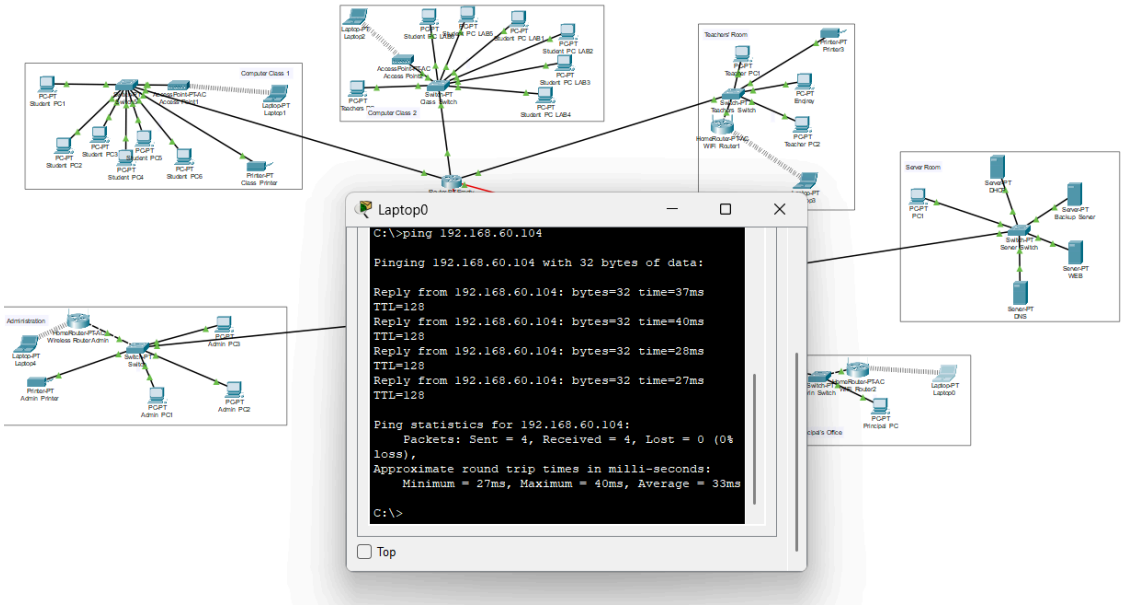

Рисунок .6. Робота WI-FI роутеру

На окремому сервері з IP-адресою 192.168.40.12 активовано службу DNS. Запити клієнтів обробляються коректно, про що свідчить успішне доменне розпізнавання імен до IP-адрес (Рис .7). У таблиці записів серверу присутні дозволені відповідності внутрішніх адрес до доменів освітньої мережі.

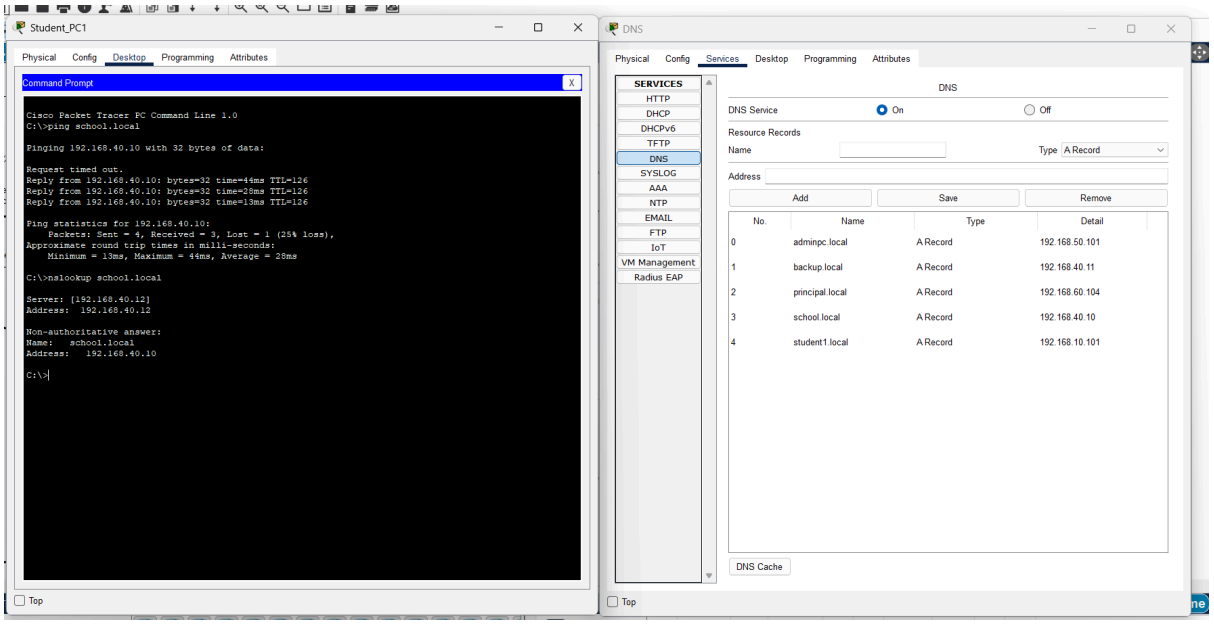

Рисунок .7. Налаштований DNS-сервер

DHCP-сервер у VLAN40 надає клієнтам мережі автоматичні IP-адреси з відповідними параметрами підмережі. На прикладі (Рис.8.) хоста видно, що було отримано адресу 192.168.40.100, а також коректно встановлено шлюз за замовчуванням та адресу DNS-сервера.

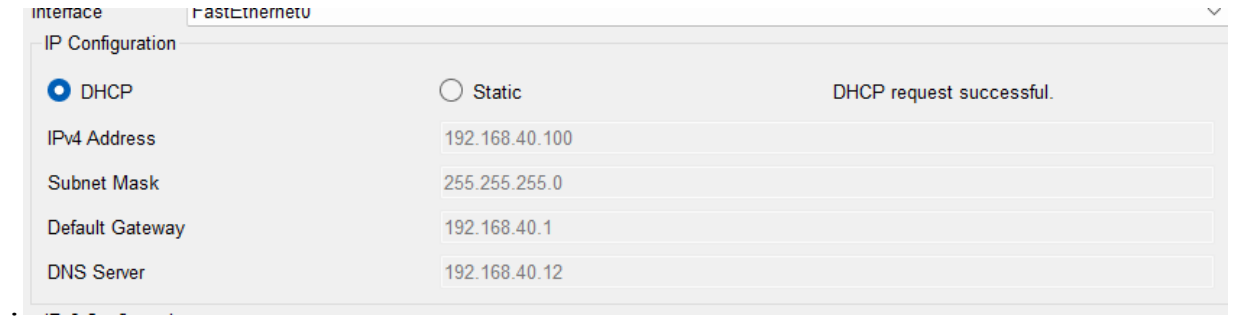

Рисунок .8. Налаштований DHCP сервер

На WEB-сервері створено HTML-сторінку з формою автентифікації, що завантажується за локальною адресою http://school.local. Файл index.html містить поля для введення логіну та пароля з перевіркою на клієнтській стороні, без використання серверної логіки чи бази даних (Рис .9.).

Форма слугує для демонстрації базового інтерфейсу входу в систему, який може використовуватись у шкільному середовищі для моделювання обмеженого доступу до ресурсів мережі.

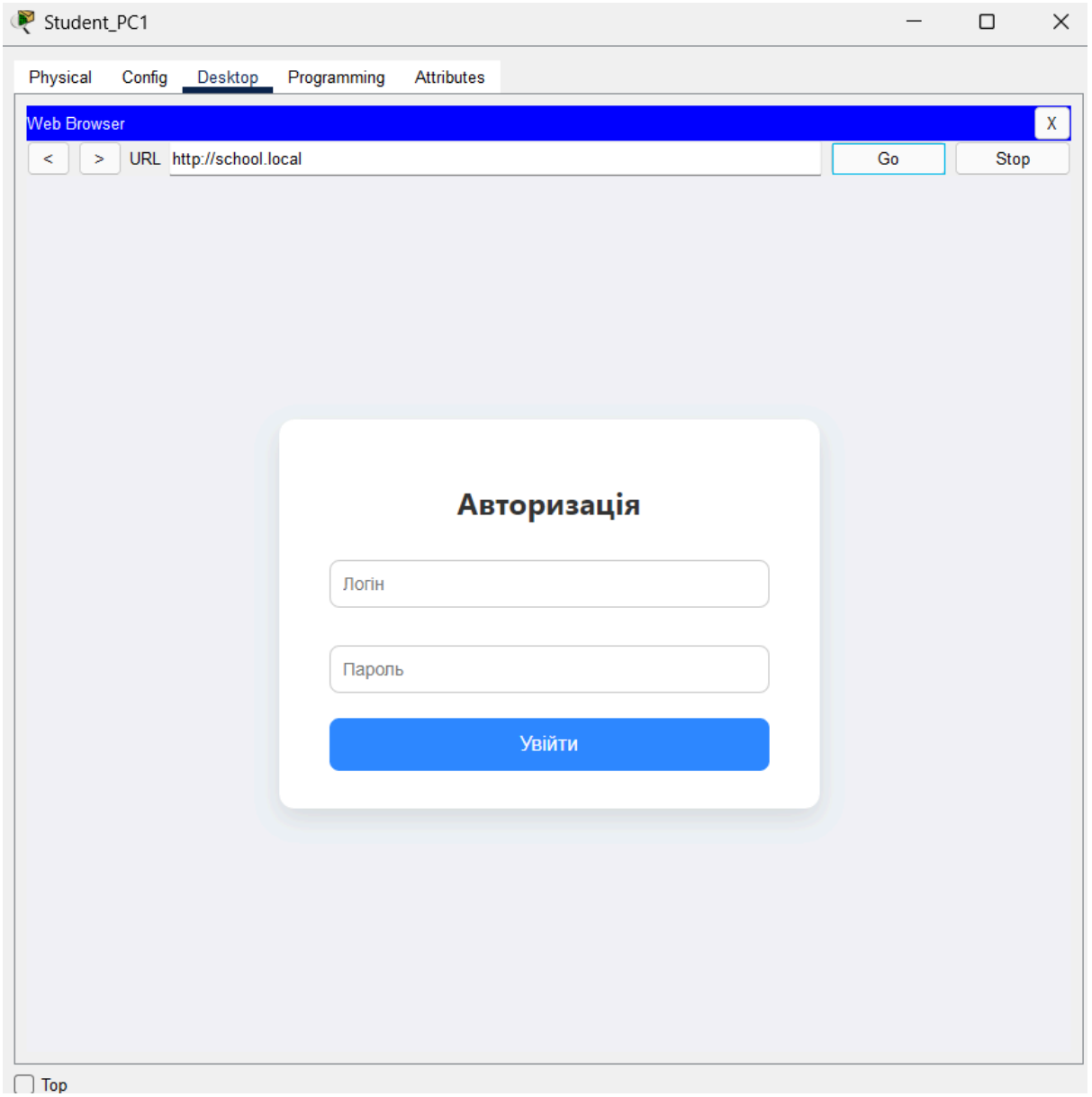

Рисунок .9. Імітація авторизації через WEB-сервер

WEB-сервер використовує скрипт на Python для передавання файлу index.html на FTP-сервер із IP-адресою 192.168.40.11. Передача здійснюється через стандартний FTP-протокол з автентифікацією користувача (Рис .10.).

Скрипт запускається безпосередньо у вкладці Programming на WEB-сервері. У вікні виводу демонструється послідовність дій: встановлення з'єднання, автентифікація, передавання файлу та завершення операції. Час запуску (наприклад, 23:00) не піддається конфігурації в Cisco Packet Tracer, тому копіювання виконується вручну в момент запуску скрипту.

Дана реалізація моделює сценарій автоматизованого збереження критичних даних з можливістю подальшого перенесення цієї логіки у реальне середовище резервного копіювання.

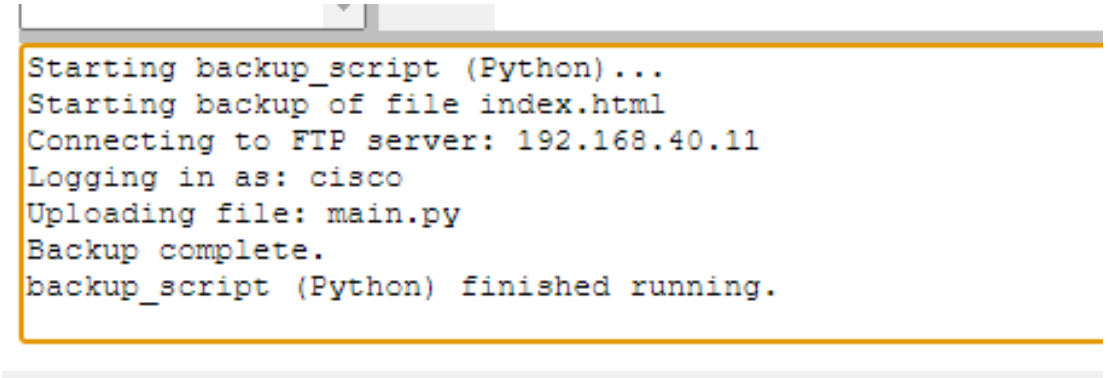

Рисунок .10. Імітація резервного копіювання на Backup-server

У VLAN50 (Administration) на портах комутатора, до яких підключено робочі станції адміністративного персоналу, застосовано механізм Port Security. На прикладі інтерфейсу FastEthernet3/1 наведено параметри активного контролю доступу (Рис .11.).

Функція безпеки ввімкнена (Port Security: Enabled)[21], порт перебуває в стані Secure-up, що вказує на відсутність порушень під час роботи. Встановлено обмеження на підключення лише одного пристрою до кожного порту (Maximum MAC Addresses: 1), а динамічно вивчена MAC-адреса збережена в режимі Sticky.

Зафіксовано один випадок порушення (Security Violation Count: 1), який виник внаслідок спроби підключити інший пристрій, що було заблоковано відповідно до політики контролю.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#do show port-security int fa3/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.2F41.8003:50
Security Violation Count   : 1
```

Рисунок .11. Налаштований port-security

Базове обмеження доступу реалізовано на маршрутизаторі Router1 шляхом налаштування локальної аутентифікації та шифрування паролів[22]. Встановлено пароль на консольний доступ, що запобігає несанкціонованому підключенню до пристрою (Рис .12.). Додатково введено пароль для переходу в режим підвищених привілеїв (enable), а всі паролі зашифровано командою service password-encryption.

Також додано банер із попередженням про заборону неавторизованого доступу, який відображається при спробі з’єднання.

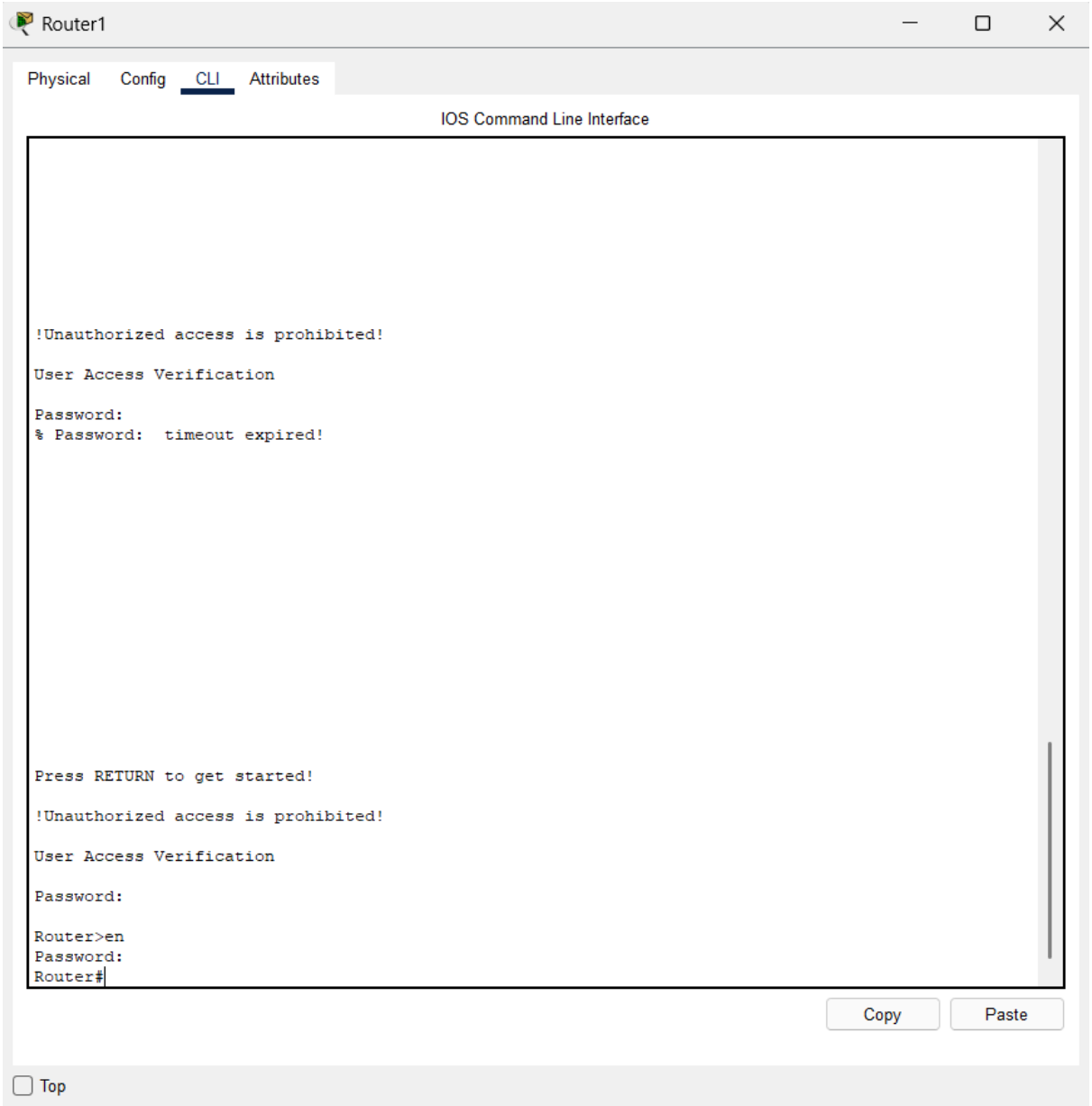

Рисунок .12. Базовий захист на Router1

3.2 Забезпечення мережевої безпеки

Для захисту шкільної мережі реалізовано комплекс заходів, спрямованих на захист даних, обмеження доступу та запобігання кіберзагрозам, що відповідає потребам навчального закладу в безпечному інформаційному середовищі та освітнім стандартам щодо захисту даних. На зовнішньому маршрутизаторі Router0 застосовано фільтрацію вхідного

трафіку за допомогою списків контролю доступу, які блокують спроби сканування мережі, зокрема через ICMP-протокол.

Це захищає внутрішні ресурси від розвідувальних атак, які можуть передувати складнішим кібератакам, як-от DDoS. Доступ до сервісів, необхідних для освітнього процесу, таких як веб-ресурси, DNS-запити та HTTPS-з'єднання, збережено, що забезпечує безперебійну роботу навчальних платформ. Цей захід знижує ризик зовнішнього втручання, дозволяючи учням і вчителям безпечно використовувати онлайн-ресурси.

Мережу поділено на шість VLAN (комп'ютерні класи, учительська, серверна, адміністрація, кабінет директора), що ізолює трафік між групами користувачів. Це зменшує ймовірність несанкціонованого доступу до чутливих даних, таких як оцінки учнів чи адміністративна документація. На маршрутизаторі Router2 налаштовано правила ACL, які обмежують міжзонний трафік, зокрема забороняють зв'язок між комп'ютерними класами та учительською, захищаючи інформацію педагогів. Доступ до серверної зони відкрито для всіх користувачів, щоб забезпечити використання навчальних ресурсів, таких як електронні підручники чи системи тестування. Сегментація підвищує безпеку, оптимізує трафік і полегшує управління мережею. Бездротовий зв'язок захищено шифруванням WPA3 на всіх точках доступу, що відповідає сучасним стандартам безпеки Wi-Fi. Це запобігає перехопленню даних і підключенню сторонніх пристроїв, що є важливим у школі, де учні часто використовують власні гаджети. WPA3 застосовує стійкі криптографічні алгоритми, забезпечуючи захист навіть при високому навантаженні на бездротову мережу, наприклад, під час групових занять чи онлайн-уроків.

У зоні адміністрації на комутаторах увімкнено Port Security, який обмежує підключення до одного пристрою на порт із фіксацією MAC-адреси в режимі Sticky. Це блокує спроби підключення неавторизованих пристроїв, наприклад, особистих ноутбуків, що не належать до адміністративної інфраструктури. Виявлення порушень призводить до автоматичного блокування порту, що захищає чутливі дані, такі як фінансові звіти чи персональна інформація працівників.

Цей механізм є ефективним для запобігання несанкціонованому доступу в адміністративному блоці. Маршрутизатор Router1 захищено локальною автентифікацією з паролями для доступу до консолі та привілейованого режиму, зашифрованими командою service password-encryption. Додано банер із повідомленням про заборону несанкціонованого доступу, який відображається при спробі підключення. Ці заходи захищають керуючі елементи мережі від неавторизованого втручання, що є критично важливим для стабільної роботи інфраструктури та захисту конфігураційних налаштувань.

Автентифікацію користувачів моделює веб-інтерфейс на WEB-сервері з формою для введення логіну та пароля, що дозволяє імітувати контроль доступу до шкільних ресурсів, таких як електронні журнали чи навчальні платформи. Цей інтерфейс демонструє можливість розмежування доступу для різних груп користувачів (учнів, учителів, адміністрації), що сприяє захисту даних і підвищує контроль над ресурсами мережі. Резервне копіювання даних організовано через Python-скрипт, який передає файли, наприклад index.html, на FTP-сервер із автентифікацією. Це забезпечує збереження навчальних матеріалів і конфігураційних даних у разі збоїв чи атак. Використання FTP-протоколу з автентифікацією обмежує доступ до сервера лише авторизованим користувачам, що знижує ризик втрати чи компрометації інформації. Цей механізм підтримує безперервність навчального процесу, дозволяючи швидко відновлювати дані.

Застосовані заходи відповідають освітнім стандартам щодо захисту даних, зокрема вимогам Закону України «Про захист персональних даних» [23], який регулює обробку персональних даних у навчальних закладах, вимагаючи захисту від несанкціонованого доступу, втрати чи модифікації.

Ці заходи забезпечують конфіденційність, цілісність та доступність даних, що є важливим для захисту інформації учнів і працівників, а також відповідають принципам обробки даних, визначеним у Державних санітарних правилах і нормах для закладів загальної середньої освіти, які обмежують використання обладнання для зниження електромагнітного випромінювання та забезпечення безпеки.

3.3 Оцінка відповідності мережі технічним вимогам

Розроблена мережева архітектура школи, побудована на зіркоподібній топології з обладнанням Cisco та сегментацією на шість VLAN (комп’ютерні класи, учительська, серверна, адміністрація, кабінет директора), повністю відповідає технічним вимогам щодо продуктивності, безпеки, масштабованості та освітнім стандартам. Мережа забезпечує пропускну здатність до 1 Гбіт/с завдяки комутаторам Cisco Catalyst 9200 (24 порти) і маршрутизаторам Cisco ISR 1100-4G, що дозволяє обробляти трафік для 200-300 пристроїв із затримкою до 20 мс, як перевірено в Cisco Packet Tracer. Точки доступу Cisco Aironet 1850 (Wi-Fi 5, до 1,7 Гбіт/с) підтримують до 50 пристроїв на точку, що відповідає потребам інтенсивного використання онлайн-платформ, таких як Zoom чи Google Classroom, для відеозв’язку та інтерактивного навчання. Безпека реалізована через шифрування WPA3 на Wi-Fi, що запобігає перехопленню даних, списки контролю доступу (ACL) на Router0 для блокування зовнішніх ICMP-запитів, захищаючи від атак типу DDoS, та на Router2 для ізоляції комп’ютерних класів від учительської, що обмежує доступ до чутливих даних, таких як оцінки чи документація. Port Security у зоні адміністрації фіксує одну MAC-адресу на порт у режимі Sticky, блокуючи неавторизовані пристрої, а локальна автентифікація на Router1 із зашифрованими паролями та банером захищає керуючі елементи мережі. Ці заходи відповідають Закону України «Про захист персональних даних» (№2297-VI від 01.06.2010), забезпечуючи конфіденційність і цілісність інформації учнів і працівників.

Масштабованість підтримується зіркоподібною топологією з вільними портами комутаторів і кабелями Cat6, готовими до модернізації, що дозволяє додавати нові пристрої до 300 користувачів без значних змін. Надійність забезпечено резервним копіюванням через FTP-сервер із автентифікацією, дублюванням серверів DHCP (192.168.40.100) і DNS (192.168.40.12), а також технологією PoE для стабільного живлення. Мережа дотримується санітарних норм, обмежуючи кількість комп'ютерів у класах до 6 (по 6 м² на учня), що знижує електромагнітне випромінювання. Веб-інтерфейс на WEB-сервері (http://school.local) із формою автентифікації моделює контроль доступу до навчальних ресурсів, а Python-скрипт забезпечує передачу файлів на FTP-сервер для збереження даних. Моделювання в Packet Tracer підтвердило стабільність мережі при пікових навантаженнях і коректну роботу всіх сервісів, що відповідає вимогам для онлайн-навчання, електронних журналів і інтерактивних занять. Мережа готова до впровадження в реальних школах із мінімальними модифікаціями, забезпечуючи сучасні освітні потреби та захист даних.

ВИСНОВКИ

У рамках кваліфікаційної роботи розроблено модель мережевої архітектури школи, яка забезпечує продуктивність, безпеку та підтримку освітніх процесів.

У першому розділі проведено аналіз потреб школи в інформаційних технологіях, досліджено підходи до побудови мереж і обґрунтовано вибір зіркоподібної топології та обладнання Cisco. Встановлено, що мережа має забезпечувати високу пропускну здатність, захист даних і масштабованість для підтримки онлайн-навчання, хмарних сервісів і технологій IoT та VR.

У другому розділі обґрунтовано вибір обладнання Cisco Catalyst 9200, ISR 2500x, Aironet 9700 і розроблено логічну модель із підмережами для ізоляції трафіку між комп'ютерними класами, учительською, серверною, адміністрацією та кабінетом директора. Визначено вимоги до продуктивності, безпеки й масштабованості з урахуванням санітарних норм і стандартів освіти.

У третьому розділі реалізовано модель у Cisco Packet Tracer із налаштуванням сервісів DHCP, DNS, WEB, FTP і механізмів безпеки. VLAN ізолювали трафік, ACL на Router0 заблокували зовнішні ICMP-запити, на Router2 обмежили доступ між комп'ютерними класами та учительською, Port Security у VLAN 50 зафіксував одну MAC-адресу на порт, WPA3 забезпечило захист Wi-Fi. Авторизацію реалізовано через вебінтерфейс, резервне копіювання — через Python-скрипт на FTP-сервер.

Модель забезпечує доступ до навчальних ресурсів, захист даних і підтримує онлайн-навчання. Вона є масштабованою та готовою до впровадження в школах із мінімальними модифікаціями.

Перспективи розвитку охоплюють інтеграцію IoT-пристроїв, розширення серверних потужностей і впровадження хмарних сервісів.

Мета роботи досягнута, модель придатна для модернізації IT-інфраструктури шкіл і відкрита для подальшого вдосконалення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. І.В Машкіна, ВО Абрамов, ТІ Носенко, ЄВ Іваніченко.Навчально-методичний посібник до виконання і захисту кваліфікаційної роботи бакалавра спеціальностей 122 Комп'ютерні науки для здобувачів вищої освіти денної форми навчання, Київський столичний університет імені Бориса Грінченка. Київ, 2024.- 43 с.
2. Теоретичні та практичні аспекти використання математичних методів та інформаційних технологій в освіті й науці:моногр. / за заг. ред. О. Литвин. — К.: Київ. ун-т ім. Б. Грінченка,2021. — 332 с.
3. Вплив сучасних інформаційних технологій на освітні процеси: об'єктив навчання [Електронний ресурс]. – 2024. – Режим доступу: https://naurok.com.ua/vpliv-suchasnih-informaciynih-tehnologiy-na-osvitni-procesi-ob-ektiv-navchannya-365988.html.
4. Використання ІКТ в освітньому процесі [Електронний ресурс]. – 2024. – Режим доступу: https://dspace.khadi.kharkov.ua/bitstreams/6df1ed46-3c06-490e-8313-fa734a588c91/download.
5. Шестобуз О. Вплив ІКТ на процес навчання [Електронний ресурс]. – 2023. – Режим доступу: https://archer.chnu.edu.ua/bitstream/handle/123456789/5047/Шестобуз%20О.%20Стаття.pdf?isAllowed=y&sequence=1.
6. Впровадження інформаційних технологій «Єдина школа» в управлінську та освітню діяльність [Електронний ресурс]. – 2021. – Режим доступу: https://imzo.gov.ua/2021/04/01/vprovadzhennia-informatsiynykh-tekhnolohiy-yedyna-shkola-v-upravlins-ku-ta-osvitniu-diial-nist-zakladiv-osvity-dosvid-vyklyky-perspektyvy/.
7. arXiv. Data Integration and Network Design in Education [Електронний ресурс]. – 2023. – Режим доступу: https://arxiv.org/abs/2304.12851.

8. Гордєєв О. О., Гордєєва Д. В., Колдовський М. В. Комп'ютерні мережі: навч. посібник. – Суми: ДВНЗ «УАБС НБУ», 2011. – 250 с. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream/123456789/50230/5/Hordieiev_Komp%E2%80%99iuterni_merezhi.pdf.

9. Журавська І. М. Проектування та монтаж локальних комп'ютерних мереж: навч. посібник. – Миколаїв: ЧНУ ім. Петра Могили, 2011. – 120 с. – Режим доступу: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/26/1/Журавська%20І.%20М.%20Проєктування%20та%20монтаж%20локальних%20комп'ютерних%20мереж.pdf.

10. Способи організації локальної комп'ютерної мережі закладу освіти [Електронний ресурс]. – 2024. – Режим доступу: https://ela.kpi.ua/items/9aba4693-e6f6-4e61-bae7-4ee94511b7e6.

11. Cisco. Enterprise Campus 3.0 Architecture: Overview and Framework [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html?dtid=osscdc000283&linkclickid=srch.

12. Cisco. Catalyst 9200 Series Switches Data Sheet [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html.

13. Cisco. Aironet 1850 Series Access Points Data Sheet [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1850-series-access-points/datasheet-c78-732514.html.

14. Cisco. Campus LAN and Wireless LAN Design Guide [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html?dtid=osscdc000283&linkclickid=srch.

15. Microsoft. Collect Workload Performance Data [Електронний ресурс]. – 2024. – Режим доступу: https://learn.microsoft.com/en-us/azure/well-architected/performance-efficiency/collect-performance-data.

16. МОН України. Освітні стандарти і положення [Електронний ресурс]. – 2024. – Режим доступу: https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/derzhavni-standarti.

17. Cisco. Enterprise Networking Solutions [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/solutions/enterprise-networks/solution-listing.html?dtid=osscdc000283&linkclickid=srch.

18. Державні санітарні правила і норми для закладів загальної середньої освіти [Електронний ресурс]. – 2018. – Режим доступу: https://mon.gov.ua/static-objects/mon/sites/1/npa/5a1fe801a0e83.pdf.

19. Lucidchart. Інструмент для побудови мереж [Електронний ресурс]. – 2024. – Режим доступу: https://www.lucidchart.com/pages.

20. Cisco Packet Tracer [Електронний ресурс]. – 2024. – Режим доступу: https://www.netacad.com/courses/packet-tracer.

21. Cisco. Configuring Access Lists [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#toc-hId--1935693932.

22. Cisco. Private VLANs: Promiscuous, Isolated, and Community [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/lan-switching/private-vlans-pvlans-promiscuous-isolated-community/40781-194.html.

23. Cisco. Port Security Configuration Guide (Catalyst 6500) [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf.

24. Cisco. Nexus 7000 NX-OS Security Configuration Guide [Електронний ресурс]. – 2024. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x_chapter_010101.pdf.

25. Закон України «Про захист персональних даних» №2297-VI від 01.06.2010 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

ДОДАТКИ

ФАЙЛ ПРОГРАМИ