Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

# БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комп'ютерна мережа для закладу середньої освіти»

08-54.БКР.001.00.000 ПЗ

Виконав: студент 2 курсу, групи КІ-23мсз

спеціальності 123 — Комп'ютерна інженерія

_____Дудник О. В.

Керівник: к.т.н., доцент каф. ОТ

_____Войцеховська О. В.

Рецензент: к.т.н., доцент каф. ПЗ

_____Чехместрук Р. Ю.

Допущено до захисту

Завідувач кафедри ОТ

д.т.н., проф. Азаров О. Д.

«___» _____ 2025 р.

Вінниця ВНТУ — 2025 рік

**ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Освітньо-кваліфікаційний рівень бакалавр

Галузь знань — 12 «Інформаційні технології»

Спеціальність — 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Комп'ютерна інженерія»

**ЗАТВЕРДЖУЮ**

**Завідувач кафедри ОТ**

д.т.н., проф. Азаров О. Д.

«21» березня 2025 р.

**З А В Д А Н Н Я**

**НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Дуднику Олександру Віталійовичу

1 Тема роботи: «Комп'ютерна мережа для закладу середньої освіти», керівник роботи к.т.н., доцент каф. ОТ Войцеховська О. В., затверджена наказом вищого навчального закладу від 20 березня 2025 р. №97.

2 Термін подання студентом роботи 02 червня 2025 р.

3 Вихідні дані до роботи: призначення — проєктування та моделювання комп'ютерної мережі; основні функції — забезпечення доступу до Інтернету, впровадження технологій VLAN, налаштування маршрутизації та захисту даних; пропускна спроможність — не менше 1 Гбіт/с для магістральних каналів.

4 Зміст розрахунково-пояснювальної записки: вступ, теоретичні основи досліджуваної проблеми, обґрунтування обраних засобів реалізації, впровадження локальної мережі у віртуальному середовищі Cisco Packet Tracer, тестування запропонованого рішення.

5 Перелік ілюстративної частини: структурна схема сегментації мережі закладу освіти, логічна схема мережі закладу освіти, схема розподілу підмереж у

мережі закладу середньої освіти.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1 — Консультанти роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийн |
| 1-3 | к.т.н., доц. каф. ОТ Войцеховська О. В. | 21.03.25 | 13.05 |
| Нормоконтроль | асистент каф. ОТ Швець С. І. | 13.05.25 | 30.05 |

7 Дата видачі завдання 21 березня 2025 р.

8 Календарний план виконання БКР приведений в таблиці 2.

Таблиця 2 — Календарний план виконання БКР

| № | Назва етапу | Термін виконання | Підпис |
|---|---|---|---|
| 1 | Аналіз предметної області | 21.03.25 | |
| 2 | Дослідження видів топологій та підходів до моделювання комп'ютерних мереж | 21.03.25— 25.03.25 | |
| 3 | Аналіз та вибір засобів реалізації | 26.03.25— 30.03.25 | |
| 4 | Аналіз та вибір обладнання для проєктування мережі | 31.03.25— 04.04.25 | |
| 5 | Розробка архітектури та структури комп'ютерної мережі | 05.04.25— 12.04.25 | |
| 6 | Розподіл адресного простору | 13.04.25— 14.04.25 | |
| 7 | Організація безпеки комп'ютерної мережі | 15.04.25— 17.05.25 | |
| 8 | Налаштування та тестування роботи мережі | 18.04.25— 30.04.25 | |
| 9 | Оформлення пояснювальної записки та демонстраційної презентації | 01.05.25— 12.05.25 | |
| 10 | Підготовка супровідної документації та перевірка на плагіат | 13.05.25 | |

**Студент** Олександр ДУДНИК

**Керівник роботи** к.т.н., доц. Олена ВОЙЦЕХОВСЬКА

# АНОТАЦІЯ

УДК 004.7

Дудник О. В. Комп'ютерна мережа для закладу середньої освіти. Бакалаврська дипломна робота зі спеціальності 123 «Комп'ютерна інженерія», освітня програма «Комп'ютерна інженерія». Вінниця: ВНТУ, 2025. 88 с.

На укр. мові. Бібліогр.: 21 назв, рис.: 12, табл. 11.

У даній роботі проведено аналіз сучасних технологій проєктування комп'ютерних мереж для освітніх закладів. Розглянуто мережеві топології та обґрунтовано вибір оптимальної структури для закладу середньої освіти. Розроблено логічну схему комп'ютерної мережі з використанням сегментації мережі за допомогою технології VLAN для розділення навчальних та адміністративних секторів. Проведено розподіл адресного простору, налаштування маршрутизаторів та комутаторів, а також конфігурування засобів безпеки. Організовано забезпечення стабільного доступу до Інтернету, захист від несанкціонованого доступу та передбачено можливість масштабування мережі при розширенні навчального закладу.

Ключові слова: комп'ютерна мережа, заклад середньої освіти, Cisco Packet Tracer, VLAN, маршрутизація, мережева безпека, віртуальне моделювання, IP-адресація, топологія мережі.

# ANNOTATION

UDC 004.7

Dudnyk O. V. Computer Network for Secondary Education Institution. Bachelor's thesis in specialty 123 "Computer Engineering", educational program "Computer Engineering". Vinnytsia: VNTU, 2025. 88 p.

In Ukrainian. Bibliography: 21 titles, figures: 12, tables: 11.

This work analyzes modern technologies for designing computer networks for educational institutions. Network topologies are considered and the choice of the optimal structure for a secondary education institution is substantiated. A logical diagram of a computer network is developed using network segmentation using VLAN technology to separate the educational and administrative sectors. The address space was allocated, routers and switches were configured, and security tools were configured. Stable access to the Internet, protection against unauthorized access, and the ability to scale the network when expanding the educational institution were organized.

Keywords: computer network, secondary education institution, Cisco Packet Tracer, VLAN, routing, network security, virtual modeling, IP addressing, network topology.

# ЗМІСТ

# ВСТУП

Сучасний розвиток інформаційних технологій характеризується стрімким впровадженням комп'ютерних мереж у всі сфери людської діяльності, зокрема в освітні процеси. Заклади середньої освіти потребують надійної мережевої інфраструктури, яка забезпечує ефективну взаємодію між учасниками навчального процесу, доступ до освітніх ресурсів та захист інформації. Ця тема є надзвичайно актуальною для освітніх закладів, оскільки правильно спроєктована комп'ютерна мережа дозволяє оптимізувати освітній процес, забезпечити інформаційну безпеку та створити сучасне цифрове навчальне середовище.

**Актуальність** розробки полягає у необхідності впровадження ефективних мережевих рішень для закладів середньої освіти через зростання вимог до якості та доступності цифрової освіти, розширення використання онлайн-ресурсів у навчальному процесі та посилення вимог до захисту персональних даних учнів і вчителів. Проєктування спеціалізованої комп'ютерної мережі дасть можливість автоматизувати адміністративні процеси, забезпечити стабільний доступ до Інтернету для навчальних цілей і, як наслідок, підвищити ефективність освітнього процесу, спростити комунікацію між учасниками навчального процесу та мінімізувати ризики інформаційної безпеки.

**Мета бакалаврської кваліфікаційної роботи** полягає у створенні комп'ютерної мережі для закладу середньої освіти, що забезпечує високий рівень надійності, безпеки та зручності використання, шляхом реалізації сегментації за допомогою технології VLAN, а також налаштування засобів безпеки для захисту мережевої інфраструктури.

Необхідні **завдання** для вирішення поставленої мети БКР:

— провести аналіз існуючих мережевих топологій та підходів до проєктування комп'ютерних мереж для освітніх закладів;

— визначити оптимальну структуру мережі з урахуванням вимог до надійності та масштабованості;

— обґрунтувати вибір технологій для моделювання мережі та симуляції мережевих процесів;

— спроєктувати та реалізувати логічну та фізичну топологію мережі для закладу середньої освіти з використанням Cisco Packet Tracer;

— розробити схему IP-адресації та налаштувати маршрутизацію;

— перевірити працездатність розробленого рішення шляхом моделювання типових сценаріїв використання мережі в освітньому закладі.

**Об'єкт дослідження** — це процес проєктування та впровадження комп'ютерної мережі для закладу середньої освіти.

**Предметом дослідження** є технології віртуального моделювання мереж, методи сегментації мережевої інфраструктури з використанням VLAN та засоби забезпечення безпеки комп'ютерних мереж.

.

# 1 АНАЛІЗ ТЕХНОЛОГІЙ СТВОРЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

## 1.1 Аналіз предметної області

### 1.1.1 Специфіка мережевої інфраструктури закладів середньої освіти

Мережева інфраструктура закладів середньої освіти має ряд специфічних особливостей, які відрізняють її від мереж інших організацій та установ. Розуміння цих особливостей є критично важливим для проєктування ефективного мережевого рішення, що відповідатиме потребам освітнього процесу [1].

Щодо технічного забезпечення, заклади середньої освіти часто характеризуються обмеженим бюджетом на IT-інфраструктуру, що призводить до використання різнорідного та часто застарілого обладнання. Мережеве рішення повинно враховувати ці обмеження та забезпечувати сумісність з наявним обладнанням, а також можливість поетапної модернізації без суттєвих змін в архітектурі.

Важливою проблемою є також необхідність забезпечення безпечного доступу до Інтернету для учнів, що передбачає впровадження систем фільтрації контенту та моніторингу активності для запобігання доступу до небажаних ресурсів. Ця вимога особливо актуальна з огляду на законодавчі обмеження щодо захисту дітей від шкідливої інформації [2].

Крім того, сучасні освітні заклади все частіше впроваджують електронні журнали, системи дистанційного навчання та інші освітні платформи, що вимагають стабільного та захищеного підключення до Інтернету. Це створює додаткові вимоги до надійності та продуктивності мережевої інфраструктури.

Одним з ключових викликів для шкільних мереж є також забезпечення бездротового доступу (Wi-Fi), який стає все більш затребуваним з огляду на поширення мобільних пристроїв та освітніх додатків. Проєктування мережі повинно передбачати оптимальне розміщення точок доступу для забезпечення

повного покриття всіх навчальних приміщень та управління радіочастотним спектром для уникнення інтерференції.

Таким чином, специфіка мережевої інфраструктури закладів середньої освіти полягає у необхідності створення гнучкого, безпечного та економічно ефективного рішення, яке враховує особливості освітнього процесу, різноманітність користувачів та технічні обмеження. Проєктування такої мережі вимагає комплексного підходу з урахуванням як поточних потреб, так і перспектив розвитку цифрових технологій в освіті.

### 1.1.2 Основні вимоги до шкільних комп'ютерних мереж

При проєктуванні та впровадженні комп'ютерних мереж для закладів середньої освіти необхідно враховувати ряд специфічних вимог, що забезпечують ефективне функціонування освітнього процесу та відповідають особливостям шкільного середовища [3].

Шкільна мережа повинна бути спроєктована з можливістю подальшого розширення та модифікації. Це зумовлено постійним розвитком інформаційних технологій в освіті, збільшенням кількості комп'ютерної техніки та впровадженням нових освітніх сервісів. Архітектура мережі має передбачати можливість додавання нових комп'ютерних класів, навчальних кабінетів та адміністративних приміщень без необхідності кардинальної перебудови існуючої інфраструктури.

Сучасний освітній процес передбачає активне використання мультимедійного контенту, відеоконференцій, онлайн-тестування та інших ресурсомістких застосунків. Мережева інфраструктура повинна забезпечувати достатню пропускну здатність для одночасної роботи великої кількості користувачів без помітного зниження швидкості доступу до ресурсів. Важливим аспектом є також правильне планування пропускної здатності з урахуванням пікових навантажень, наприклад, під час проведення уроків інформатики в декількох класах одночасно [4].

Критичною вимогою для шкільних мереж є забезпечення безперебійної роботи, особливо під час проведення занять, іспитів або адміністративних процедур. Мережа повинна бути спроєктована з урахуванням можливих відмов обладнання та передбачати резервування критичних компонентів. Архітектура мережі має мінімізувати "єдині точки відмови", де збій одного компонента може призвести до недоступності всієї мережі або значної її частини.

Для ефективного функціонування мережі необхідно забезпечити розподіл навантаження та ізоляцію різних типів трафіку. Навчальні класи, адміністративні відділи та загальношкільні сервіси повинні бути розділені на окремі логічні сегменти, що забезпечить кращу продуктивність та підвищить рівень безпеки. Технологія віртуальних локальних мереж (VLAN) є одним із основних інструментів для реалізації такої сегментації.

Безпека є критично важливим аспектом шкільної мережі, особливо з огляду на роботу з персональними даними учнів та вчителів. Мережа повинна забезпечувати захист від несанкціонованого доступу, шкідливого програмного забезпечення та мережевих атак. Основні вимоги до безпеки включають впровадження систем фільтрації контенту, використання міжмережевих екранів, налаштування механізмів автентифікації та авторизації користувачів, захист персональних даних відповідно до вимог законодавства, а також моніторинг мережевої активності для виявлення потенційних проблем безпеки [5].

Ефективне адміністрування шкільної мережі вимагає централізованих засобів управління, які дозволяють системним адміністраторам контролювати мережеве обладнання, налаштовувати політики безпеки, відстежувати продуктивність та виявляти проблеми. Централізоване управління особливо важливе для шкіл, де часто відсутній штатний IT-персонал з високим рівнем кваліфікації.

Сучасна освітня мережа повинна забезпечувати надійне Wi-Fi покриття для підтримки мобільних пристроїв, які все частіше використовуються в освітньому процесі. Бездротова мережа має бути спроєктована з урахуванням особливостей шкільних приміщень, забезпечувати достатню ємність для обслуговування великої кількості одночасних підключень та підтримувати сучасні стандарти безпеки.

Заклади освіти часто працюють в умовах обмеженого бюджету, тому мережеве рішення повинно бути економічно обґрунтованим, з оптимальним співвідношенням ціни та функціональності. Важливо враховувати не лише початкові витрати на обладнання та впровадження, але й експлуатаційні витрати, включаючи електроенергію, технічне обслуговування та можливі оновлення [6].

Узагальнюючи ключові вимоги до шкільних комп'ютерних мереж, можна представити їх у вигляді таблиці 1.1, яка демонструє основні аспекти та їх важливість для освітнього процесу.

Таблиця 1.1 — Вимоги до комп'ютерних мереж закладів середньої освіти

| Вимога | Опис | Важливість |
|---|---|---|
| Масштабованість | Можливість розширення мережі без істотної перебудови | Висока |
| Пропускна здатність | Забезпечення достатньої швидкості для одночасної роботи багатьох користувачів | Висока |
| Надійність | Мінімізація простоїв та забезпечення безперебійної роботи | Критична |
| Сегментація | Розділення мережі на логічні сегменти (VLAN) | Середня |
| Безпека | Захист від зовнішніх та внутрішніх загроз | Критична |
| Централізоване управління | Єдина система адміністрування мережевою інфраструктурою | Середня |
| Бездротовий доступ | Забезпечення Wi-Fi покриття для мобільних пристроїв | Висока |
| Економічна ефективність | Оптимальне співвідношення ціни та функціональності | Висока |
| Підтримка освітніх технологій | Сумісність зі спеціалізованими освітніми платформами | Середня |
| Документація | Наявність детальної технічної документації | Середня |

Окрім зазначених вимог, мережа повинна забезпечувати підтримку специфічних освітніх технологій, включаючи системи управління навчанням (LMS), електронні журнали, інтерактивні дошки, системи відеоконференцій для дистанційного навчання та інші спеціалізовані освітні платформи [7].

Важливим аспектом є також наявність детальної документації мережевої інфраструктури та проведення навчання технічного персоналу школи щодо базового обслуговування та усунення простих несправностей. Це особливо актуально для шкіл, де зазвичай немає спеціалізованих IT-відділів.

Врахування всіх цих вимог при проєктуванні комп'ютерної мережі для закладу середньої освіти дозволяє створити надійну, безпечну та ефективну інфраструктуру, яка відповідає сучасним освітнім потребам та має потенціал для подальшого розвитку відповідно до еволюції освітніх технологій [8].

## 1.2 Огляд видів топологій комп’ютерних мереж

### 1.2.1 Фізичні топології мереж

Фізична топологія мережі визначає спосіб фізичного з'єднання мережевих пристроїв за допомогою кабелів або бездротових технологій. Вибір відповідної фізичної топології є основоположним етапом при проєктуванні комп'ютерної мережі для закладу середньої освіти, оскільки безпосередньо впливає на продуктивність, надійність, масштабованість та вартість мережевої інфраструктури.

Розглянемо основні типи фізичних топологій, їх переваги, недоліки та можливості застосування у контексті освітніх закладів.

Топологія типу «шина» є однією з найпростіших, це лінійне з'єднання пристроїв вздовж спільного кабельного сегмента. Усі пристрої підключаються до єдиного комунікаційного кабелю (шини). Дані, що передаються одним пристроєм, поширюються по шині в обох напрямках і доступні всім іншим пристроям.

Незважаючи на простоту і економічність шинної топології, вона має суттєві недоліки, особливо для середовища освітнього закладу. Обрив кабелю в будь-якій точці призводить до виходу з ладу всієї мережі, а при збільшенні кількості пристроїв суттєво знижується продуктивність через колізії даних. Крім того, діагностика несправностей у такій мережі є складною. Саме тому топологія «шина» рідко використовується в сучасних комп'ютерних мережах закладів освіти і більше відноситься до історичних рішень.

Топологія «зірка» передбачає з'єднання всіх пристроїв мережі з центральним комутаційним вузлом (комутатором або концентратором). Кожен пристрій має пряме підключення до центрального вузла, що забезпечує незалежну комунікацію з іншими пристроями [9].

У контексті закладів середньої освіти топологія «зірка» є однією з найбільш поширених і рекомендованих для використання, особливо в комбінації з іншими топологіями, про що буде сказано далі.

Топологія «кільце» передбачає з'єднання кожного пристрою з двома сусідніми, утворюючи замкнуте кільце. Дані передаються послідовно від одного пристрою до іншого в одному напрямку.

Перевагами кільцевої топології є детермінованість доступу до середовища передачі (кожен пристрій має гарантований час доступу), рівномірний розподіл навантаження та відсутність колізій. Проте, вона має суттєві недоліки: складність додавання нових пристроїв, низька відмовостійкість (розрив кільця призводить до виходу з ладу всієї мережі), складність діагностики.

У чистому вигляді кільцева топологія рідко використовується в сучасних шкільних мережах, проте елементи цієї топології можуть застосовуватися для створення резервних з'єднань між комутаторами в рамках більш складних топологій.

Повнозв'язна топологія передбачає пряме з'єднання кожного пристрою з усіма іншими пристроями мережі. Це забезпечує максимальну надійність та продуктивність, але вимагає великої кількості кабельних з'єднань.

Через високу вартість впровадження та складність адміністрування, повнозв'язна топологія в чистому вигляді практично не використовується в шкільних мережах. Проте, елементи цієї топології можуть застосовуватися для ключових вузлів мережі, де потрібна підвищена надійність.

Топологія "дерево" або "розширена зірка" є розвитком топології "зірка", де кілька зіркоподібних сегментів з'єднуються через центральні вузли, утворюючи ієрархічну структуру. Це дозволяє розширювати мережу без зниження продуктивності та забезпечує зручне адміністрування [10].

У таблиці 1.2 наведено порівняльний аналіз основних фізичних топологій з точки зору їх застосовності в мережах закладів середньої освіти.

Таблиця 1.2 — Порівняння фізичних топологій мереж для освітніх закладів

| Топологія | Переваги | Недоліки | Застосовність у школах |
|---|---|---|---|
| Шина | Економність кабелів, проста установка | Низька надійність, складна діагностика, обмежена масштабованість | Низька (застаріла топологія) |
| Зірка | Висока надійність, проста діагностика, легке масштабування | Залежність від центрального вузла, більші витрати на кабельну інфраструктуру | Висока |
| Кільце | Детермінований доступ, рівномірне навантаження | Низька відмовостійкість, складність масштабування | Середня (переважно для резервних з'єднань) |
| Повнозв'язна | Максимальна надійність і продуктивність | Висока вартість, складність адміністрування | Низька (крім критичних сегментів) |
| Дерево | Ієрархічна структура, гнучкість, масштабованість | Залежність від центральних вузлів | Дуже висока |

Для наочного представлення різних фізичних топологій мереж на рисунку 1.2 показано їх схематичне зображення.

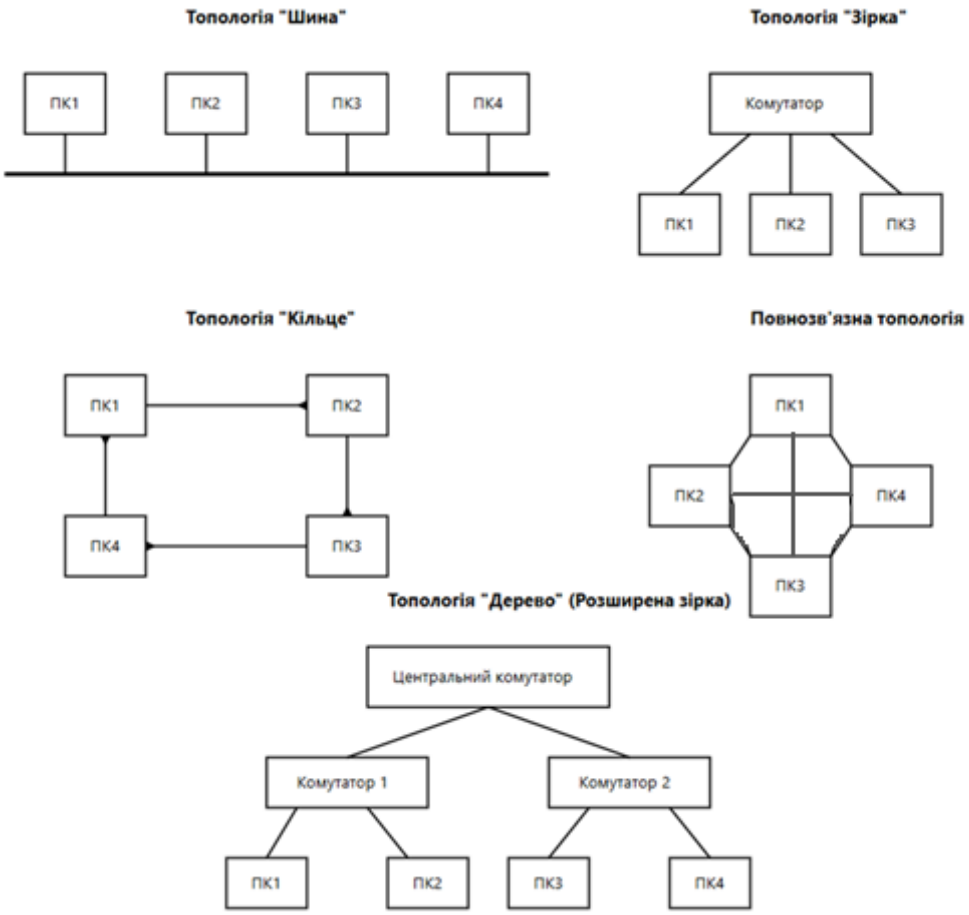



Рисунок 1.1 — Схематичне зображення топологій комп'ютерних мереж

Також важливим аспектом є проєктування з урахуванням фізичної структури будівлі школи, розташування кабінетів та наявної кабельної інфраструктури. Оптимальним підходом є розміщення комутаторів рівня доступу в кожному блоці або на кожному поверсі будівлі, з'єднаних з комутаторами рівня розподілу, які, в свою чергу, підключені до центрального комутатора або маршрутизатора [11].

Вибір фізичної топології для мережі закладу середньої освіти повинен базуватися на комплексному аналізі вимог до надійності, масштабованості,

продуктивності та врахуванні бюджетних обмежень, а також архітектурних особливостей будівлі школи.

### 1.2.2 Логічні топології мереж

На відміну від фізичної топології, яка визначає фізичне розташування кабелів та пристроїв, логічна топологія описує принципи передачі даних та шляхи, якими інформація поширюється в мережі. Логічна топологія може відрізнятися від фізичної і визначає, яким чином пристрої "бачать" мережу і взаємодіють з нею. Розуміння логічних топологій є важливою складовою проєктування ефективної мережевої інфраструктури для закладу середньої освіти [12].

Логічна топологія типу «шина» передбачає, що всі пристрої мережі спільно використовують одне комунікаційне середовище, і дані, передані одним пристроєм, отримуються всіма іншими. Такий підхід характерний для технологій Ethernet з використанням концентраторів (hub), де всі підключені пристрої знаходяться в одному домені колізій. При цьому в мережі застосовується протокол множинного доступу з контролем несучої та виявленням колізій (CSMA/CD).

Основним недоліком такої логічної топології є низька ефективність при збільшенні кількості пристроїв через зростання ймовірності колізій. У сучасних мережах закладів освіти ця топологія майже не використовується через її обмеження у продуктивності та масштабованості [13].

Логічна топологія "зірка" характеризується тим, що комунікація між будь-якими двома пристроями відбувається через центральний пристрій (комутатор). Комутатори працюють на основі MAC-адресів та створюють віртуальні з'єднання між пристроями, що обмінюються даними. Це дозволяє ізолювати трафік і зменшити кількість колізій.

У закладах середньої освіти ця логічна топологія є найбільш поширеною через її ефективність та гнучкість. Вона забезпечує оптимальне використання пропускної здатності мережі та спрощує адміністрування.

Логічна топологія «точка-точка» (point-to-point) являє собою пряме з'єднання між двома мережевими пристроями без проміжних вузлів. Такі з'єднання є основою для побудови більш складних мережевих структур і часто використовуються для зв'язку між комутаторами або маршрутизаторами в ієрархічних мережах [14].

У контексті шкільної мережі з'єднання типу "точка-точка" можуть застосовуватися для з'єднання комутаторів різних поверхів або будівель, а також для підключення до зовнішніх мереж (WAN).

Логічна топологія «кільце» передбачає, що дані передаються послідовно від одного пристрою до іншого в одному напрямку по замкнутому шляху. Ця топологія використовується в технологіях Token Ring та FDDI, де доступ до середовища передачі регулюється спеціальним маркером (token).

Хоча фізично мережа може не мати кільцевої структури, логічно вона функціонує як кільце. У сучасних освітніх мережах ця топологія рідко використовується, але може застосовуватися в специфічних сценаріях, наприклад, при налаштуванні протоколів резервування каналів, таких як STP (Spanning Tree Protocol).

Важливо відзначити, що в сучасних мережах закладів середньої освіти часто використовуються гібридні логічні топології, які поєднують елементи різних базових топологій для оптимізації продуктивності та надійності [15].

В таблиці 1.3 наведено порівняння основних характеристик логічних топологій з точки зору їх застосовності в мережах закладів середньої освіти.

Таблиця 1.3 — Порівняння логічних топологій для освітніх мереж

| Логічна топологія | Ключові особливості | Переваги | Недоліки | Застосовність у школах |
|---|---|---|---|---|
| Шина | Спільне середовище передачі, CSMA/CD | Простота, низька вартість | Колізії, низька масштабованість | Низька |
| Зірка | Комутація по MAC-адресах, віртуальні з'єднання | Висока продуктивність, ізоляція трафіку | Залежність від центрального пристрою | Висока |
| Точка-точка | Пряме з'єднання між двома пристроями | Висока швидкість, надійність | Обмежена кількість з'єднань | Середня (для критичних ліній) |
| Кільце | Послідовна передача, маркерний доступ | Детермінований доступ | Складність реалізації, затримки в разі збоїв | Низька |
| VLAN | Логічна сегментація незалежно від фізичної структури | Гнучкість, безпека, оптимізація трафіку | Потребує підтримки відповідного мережевого обладнання | Дуже висока |

### 1.2.3 Гібридні рішення для освітніх закладів

Сучасні мережі закладів середньої освіти рідко використовують одну стандартну топологію. Натомість застосовуються гібридні рішення, які поєднують переваги різних топологій для створення ефективної, надійної та економічно доцільної мережевої інфраструктури [16].

Для підвищення надійності в критичних сегментах мережі застосовуються елементи кільцевої топології. Наприклад, комутатори рівня розподілу можуть бути з'єднані в кільце з використанням протоколу STP (Spanning Tree Protocol) для запобігання петель та автоматичного перемикання на резервні канали у випадку відмови основного з'єднання.

Ще одним важливим аспектом гібридних рішень є інтеграція дротової та бездротової інфраструктури. Сучасні освітні заклади все частіше впроваджують Wi-Fi мережі для забезпечення мобільності та підтримки різноманітних пристроїв. Бездротові точки доступу інтегруються в загальну мережеву інфраструктуру та підключаються до комутаторів рівня доступу,

часто з використанням технології PoE (Power over Ethernet), що спрощує їх розгортання.

Типове гібридне рішення для закладу середньої освіти включає:

— центральний маршрутизатор з міжмережевим екраном на рівні ядра;

— комутатори рівня розподілу з підтримкою маршрутизації між VLAN;

— комутатори рівня доступу з підтримкою PoE для підключення кінцевих пристроїв та бездротових точок доступу;

— сегментацію мережі на VLAN відповідно до функціональних зон (адміністрація, комп'ютерні класи, навчальні кабінети, серверна);

— систему централізованого управління бездротовою мережею;

— сервери для розміщення освітніх ресурсів та систем управління навчанням.

Переваги гібридних рішень для освітніх закладів:

— оптимальний баланс між вартістю та функціональністю;

— гнучкість та масштабованість;

— висока надійність критичних сегментів;

— ефективне використання пропускної здатності;

— спрощене адміністрування.

Таке гібридне поєднання різних топологій дозволяє створити мережеву інфраструктуру, яка відповідає специфічним потребам закладу середньої освіти та забезпечує ефективне функціонування сучасного освітнього середовища.

## 1.3 Аналіз підходів до моделювання комп'ютерних мереж

Моделювання комп'ютерних мереж є важливим етапом у процесі проєктування мережевої інфраструктури для закладу середньої освіти. Воно дозволяє перевірити працездатність розроблених рішень та виявити потенційні проблеми ще до фізичного впровадження мережі, що значно скорочує витрати часу та ресурсів.

Існує кілька основних підходів до моделювання комп'ютерних мереж, кожен з яких має свої переваги та обмеження. Розглянемо основні з них:

Математичне моделювання базується на використанні математичних формул та алгоритмів для опису поведінки мережі. Цей підхід дозволяє отримати аналітичні оцінки продуктивності, пропускної здатності та інших параметрів мережі. Проте він має обмежену точність при моделюванні складних мережевих сценаріїв та динамічних процесів.

Імітаційне моделювання передбачає створення комп'ютерної моделі мережі, яка відтворює поведінку реальної системи з урахуванням часових залежностей. Цей підхід дозволяє досліджувати динамічні характеристики мережі та проводити експерименти з різними параметрами та сценаріями.

Симуляція є підвидом імітаційного моделювання, де створюється віртуальне середовище, яке імітує роботу мережевих пристроїв та протоколів. Симулятори дозволяють візуалізувати топологію мережі, налаштовувати параметри пристроїв та спостерігати за передачею даних. Перевагами є наочність та можливість моделювання складних мережевих сценаріїв.

Емуляція відрізняється від симуляції тим, що використовує реальні мережеві протоколи та операційні системи в віртуальному середовищі. Це дозволяє досягти високої точності моделювання, але вимагає більше обчислювальних ресурсів.

Прототипування передбачає створення фізичної моделі мережі в зменшеному масштабі для тестування рішень перед повним розгортанням. Цей підхід забезпечує найбільшу точність, але є найбільш затратним та найменш гнучким.

Для проєктування комп'ютерної мережі закладу середньої освіти найбільш доцільним є використання симуляторів, таких як Cisco Packet Tracer. Цей інструмент забезпечує оптимальний баланс між точністю моделювання, зручністю використання та вимогами до ресурсів. Cisco Packet Tracer дозволяє:

— створювати віртуальні мережеві топології;

— налаштовувати маршрутизатори, комутатори та кінцеві пристрої;

— імітувати роботу протоколів маршрутизації та комутації;

— організовувати VLAN та налаштовувати маршрутизацію між ними;

— впроваджувати механізми безпеки (ACL, міжмережеві екрани);

— візуалізувати передачу даних та аналізувати трафік;

— тестувати різні сценарії роботи мережі.

У таблиці 1.4 наведено порівняльний аналіз різних підходів до моделювання комп'ютерних мереж для освітніх закладів.

Таблиця 1.4 — Порівняння підходів до моделювання комп'ютерних мереж

| Підхід | Переваги | Недоліки | Інструменти | Рівень складності | Доцільність для шкільних мереж |
|---|---|---|---|---|---|
| Математичне моделювання | Швидке отримання результатів, аналітичні оцінки | Обмежена точність для складних систем | MATLAB, MathCAD | Високий | Низька |
| Імітаційне моделювання | Аналіз динаміки, сценаріїв, параметрична гнучкість | Потреба в обчислювальних ресурсах | OPNET, NS-3 | Середній | Середня |
| Симуляція | Наочність, простота, навчальна візуалізація | Спрощення моделей, умовна точність | Cisco Packet Tracer, GNS3 | Низький | Висока |
| Емуляція | Реалістичність, використання справжніх стеків протоколів | Ресурсоємність, складність конфігурації | EVE-NG, Mininet | Середній | Середня |
| Прототипування | Реальні тести, найвища точність | Висока вартість, складне оновлення | Реальне обладнання | Високий | Низька |

Для більш складних мережевих інфраструктур можна використовувати комбінацію підходів, наприклад, симуляцію для загальної структури мережі та емуляцію для тестування специфічних сервісів та застосунків.

Важливо відзначити, що вибір підходу до моделювання залежить від конкретних вимог до мережі, доступних ресурсів та рівня кваліфікації персоналу. В контексті закладу середньої освіти, де IT-ресурси зазвичай обмежені, перевагу варто віддавати простим у використанні та економічно ефективним рішенням, таким як симуляція з використанням Cisco Packet Tracer.

## 1.4 Постановка задачі дослідження

На основі проведеного аналізу предметної області, вивчення специфіки мережевої інфраструктури закладів середньої освіти та дослідження існуючих підходів до моделювання комп'ютерних мереж, можна сформулювати основні задачі, які необхідно вирішити в рамках даної бакалаврської роботи.

Головною метою роботи є проєктування та моделювання комп'ютерної мережі для закладу середньої освіти з використанням віртуального середовища Cisco Packet Tracer, яка буде відповідати сучасним вимогам до безпеки, продуктивності та надійності.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

— розробити оптимальну фізичну топологію мережі з урахуванням специфіки закладу середньої освіти, що забезпечить ефективне підключення комп'ютерних класів, навчальних кабінетів, адміністративних приміщень та серверної інфраструктури;

— спроєктувати логічну структуру мережі з використанням технології віртуальних локальних мереж (VLAN) для сегментації та ізоляції різних типів трафіку;

— розробити схему IP-адресації з раціональним використанням адресного простору та можливістю подальшого масштабування мережі;

— налаштувати маршрутизацію між різними сегментами мережі з використанням статичних маршрутів або динамічних протоколів маршрутизації;

— забезпечити доступ до Інтернету для всіх авторизованих користувачів з використанням технології трансляції мережевих адрес (NAT);

— змоделювати розроблену мережу у віртуальному середовищі Cisco Packet Tracer та провести тестування її працездатності в різних сценаріях використання.

# 2 ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ДЛЯ ПРОЄКТУВАННЯ МЕРЕЖІ ДЛЯ ЗАКЛАДУ СЕРЕДНЬОЇ ОСВІТИ

## 2.1 Аналіз та вибір засобів для проєктування мережі

### 2.1.1 Функціональні можливості Cisco Packet Tracer

Cisco Packet Tracer є потужним інструментом для моделювання мережевих інфраструктур, розробленим компанією Cisco Systems спеціально для освітніх цілей. Даний продукт пропонує широкий спектр функціональних можливостей, які роблять його оптимальним рішенням для проєктування комп'ютерної мережі закладу середньої освіти.

Одна з ключових переваг Cisco Packet Tracer полягає у можливості створення віртуальних мережевих топологій будь-якої складності. Користувач може розміщувати на робочому полі різноманітні мережеві пристрої (маршрутизатори, комутатори, хаби, кінцеві пристрої) та з'єднувати їх за допомогою різних типів кабелів. Це дозволяє змоделювати практично будь-яку фізичну топологію, включаючи зіркоподібну, кільцеву, деревоподібну або гібридну, що особливо важливо для проєктування комплексних мереж освітніх закладів [17].

Програма підтримує велику бібліотеку мережевих пристроїв Cisco різних серій та моделей, включаючи маршрутизатори (серії ISR, ASR), комутатори (серії Catalyst, Nexus), бездротові точки доступу, IP-телефони, сервери та робочі станції. Для кожного пристрою доступні детальні настройки, що відповідають реальному обладнанню, що забезпечує високу точність моделювання.

Cisco Packet Tracer надає два режими роботи: режим реального часу (Real-Time Mode) та режим симуляції (Simulation Mode). У режимі реального часу пристрої функціонують як у справжній мережі, реагуючи на команди та події негайно. Цей режим зручний для налаштування пристроїв та тестування загальної працездатності мережі. У режимі симуляції користувач може

спостерігати за процесом передачі даних між пристроями на рівні пакетів, що дозволяє детально аналізувати роботу мережевих протоколів та виявляти потенційні проблеми.

У таблиці 2.1 представлено основні функціональні можливості Cisco Packet Tracer, які можуть бути використані при проєктуванні мережі закладу середньої освіти.

Таблиця 2.1 — Функціональні можливості Cisco Packet Tracer

| Функціональна можливість | Опис | Застосування в проєкті |
|---|---|---|
| Моделювання фізичної топології | Створення віртуальних мережевих схем з різними типами з'єднань | Проєктування загальної структури мережі закладу |
| Емуляція мережевих пристроїв Cisco | Робота з віртуальними моделями реального обладнання | Налаштування маршрутизаторів та комутаторів |
| Підтримка протоколів маршрутизації | Налаштування RIP, EIGRP, OSPF, BGP | Організація ефективної маршрутизації між сегментами |
| Налаштування VLAN | Сегментація мережі, транкові порти, маркування 802.1Q | Логічний розподіл мережі на функціональні зони |
| Засоби безпеки | ACL, NAT, VPN, аутентифікація AAA | Захист мережі від несанкціонованого доступу |
| Режим симуляції | Візуалізація передачі пакетів між пристроями | Аналіз роботи протоколів та виявлення помилок |
| Інтеграція з IoT пристроями | Підтримка моделювання IoT сценаріїв | Можливість інтеграції «розумних» пристроїв у мережу |
| Підтримка IPv4 та IPv6 | Можливість налаштування обох версій IP | Забезпечення сумісності з сучасними вимогами |
| Командний інтерфейс (CLI) | Емуляція реального командного інтерфейсу Cisco IOS | Конфігурація пристроїв аналогічно реальним |

Програма також надає можливість налаштування засобів забезпечення безпеки мережі, таких як списки контролю доступу (ACL), технології трансляції мережевих адрес (NAT), віртуальні приватні мережі (VPN), шифрування трафіку та аутентифікація користувачів. Це дозволяє створити безпечну мережеву інфраструктуру, що особливо важливо для закладу освіти,

де необхідно забезпечити захист персональних даних та контроль доступу до мережевих ресурсів.

Важливою функціональною особливістю Cisco Packet Tracer є підтримка протоколів маршрутизації та комутації. Програма дозволяє налаштовувати та тестувати роботу таких протоколів як RIP, EIGRP, OSPF, BGP для динамічної маршрутизації, а також STP, RSTP, VTP, DTP для комутації. Це надає можливість змоделювати складні мережеві сценарії та перевірити ефективність різних конфігурацій.

Для організації логічної структури мережі Cisco Packet Tracer забезпечує повну підтримку технології віртуальних локальних мереж (VLAN), включаючи маркування кадрів за стандартом 802.1Q, налаштування транкових портів та міжвланової маршрутизації. Це дозволяє ефективно сегментувати мережу закладу середньої освіти відповідно до функціональних зон: комп'ютерні класи, навчальні кабінети, адміністративні приміщення, серверна інфраструктура.

Cisco Packet Tracer включає інструменти для аналізу продуктивності мережі та діагностики проблем. Користувач може використовувати команди ping, traceroute, перевіряти статистику інтерфейсів, аналізувати таблиці маршрутизації та перехоплювати мережевий трафік. Це дозволяє оцінити ефективність розробленої топології та виявити потенційні вузькі місця.

Варто відзначити, що програма підтримує як графічний інтерфейс для швидкої конфігурації пристроїв, так і повноцінний командний інтерфейс (CLI), який емулює реальний інтерфейс операційної системи Cisco IOS. Це дає можливість не лише проєктувати мережу, але й отримувати практичні навички налаштування обладнання Cisco, що може бути корисним для персоналу, який буде в подальшому обслуговувати мережу закладу освіти.

Таким чином, Cisco Packet Tracer надає всі необхідні функціональні можливості для повноцінного проєктування, моделювання та тестування

комп'ютерної мережі закладу середньої освіти, що робить його оптимальним інструментом для реалізації поставлених задач.

### 2.1.2 Засоби візуалізації мережевих процесів

Одним з найбільш значущих переваг Cisco Packet Tracer для проєктування мереж закладів середньої освіти є потужні засоби візуалізації мережевих процесів. Ці інструменти дозволяють не лише створювати мережеві топології, але й наочно спостерігати за роботою мережі та аналізувати передачу даних між пристроями [18].

Cisco Packet Tracer пропонує унікальний режим симуляції (Simulation Mode), який дозволяє відстежувати процеси передачі даних на рівні окремих пакетів. Після переходу в цей режим користувач може генерувати різні типи трафіку (ping, HTTP, FTP, DHCP та інші) та спостерігати за проходженням пакетів через мережеві пристрої в реальному часі або покроково.

В режимі симуляції пакети даних відображаються у вигляді кольорових конвертів, які рухаються між пристроями. Колір конверта вказує на тип протоколу або стан пакета: зелений для успішної передачі, червоний для помилок, жовтий для службових протоколів тощо. Це забезпечує інтуїтивне розуміння процесів, що відбуваються в мережі, та полегшує виявлення проблем.

При виборі конкретного пакета користувач може відкрити вікно інспектора пакетів (Packet Inspector), яке відображає детальну інформацію про структуру пакета на різних рівнях моделі OSI. Це дозволяє аналізувати заголовки IP, TCP/UDP, перевіряти дані протоколів прикладного рівня та вивчати процеси інкапсуляції/декапсуляції даних [19].

Важливим інструментом візуалізації є також вікно подій симуляції (Simulation Panel), яке хронологічно відображає всі події, пов'язані з обробкою пакетів: створення, передача, отримання, відкидання тощо. Для кожної події

вказується час, тип події, задіяні пристрої та протоколи. Ця інформація корисна для детального аналізу мережевих процесів та діагностики проблем.

Cisco Packet Tracer також надає зручний інтерфейс для візуального налаштування мережевих пристроїв. Для кожного пристрою доступне графічне меню конфігурації, організоване у вигляді вкладок, що відповідають різним аспектам налаштування: фізичні інтерфейси, маршрутизація, безпека, VLAN тощо. Це особливо корисно на початкових етапах проєктування, коли необхідно швидко налаштувати базові параметри численних пристроїв.

Для візуалізації логічної структури мережі програма пропонує спеціальні інструменти, що дозволяють наочно відображати VLAN-сегменти, домени колізій та домени широкомовного розповсюдження. Користувач може переключатися між відображенням фізичної та логічної топології, що допомагає краще зрозуміти взаємозв'язок між фізичною інфраструктурою та логічною організацією мережі закладу освіти [20].

Окремо варто відзначити можливість створення користувацьких сценаріїв симуляції. Це дозволяє автоматизувати тестування різних аспектів роботи мережі та демонструвати функціонування мережевої інфраструктури в різних умовах. Наприклад, можна створити сценарій, що імітує пікове навантаження під час проведення уроків інформатики в декількох класах одночасно, або сценарій, що демонструє роботу механізмів безпеки при спробі несанкціонованого доступу.

Важливо відзначити, що Cisco Packet Tracer здебільшого фокусується на продуктах Cisco і має обмежену підтримку обладнання інших виробників. Це може стати проблемою при проєктуванні гетерогенної мережі, де використовується обладнання різних вендорів, що часто зустрічається в освітніх закладах через обмеження бюджету. В реальному середовищі часто доводиться забезпечувати сумісність між пристроями різних виробників, що складно змоделювати в Packet Tracer [21].

У таблиці 2.2 представлено основні засоби візуалізації Cisco Packet Tracer та їх застосування при проєктуванні мережі закладу середньої освіти.

Таблиця 2.2 — Засоби візуалізації мережевих процесів в Cisco Packet Tracer

| Засіб візуалізації | Опис | Застосування в проєкті |
|---|---|---|
| Режим симуляції | Відображення руху пакетів між пристроями у вигляді анімації | Перевірка з'єднань між сегментами мережі, аналіз шляхів проходження трафіку |
| Інспектор пакетів | Аналіз структури пакетів на різних рівнях моделі OSI | Детальний аналіз протоколів, перевірка коректності налаштувань маршрутизації та комутації |
| Панель подій симуляції | Хронологічне відображення всіх подій, пов’язаних з обробкою пакетів | Діагностика помилок, аналіз часових затримок та відмов у доставці пакетів |
| Кольорове кодування | Різні кольори для відображення типів протоколів та стану пакетів | Швидка візуальна ідентифікація проблемних ділянок мережі |
| Таблиці стану пристроїв | Візуалізація таблиць маршрутизації, ARP-таблиць, таблиць MAC-адрес | Перевірка коректності конфігурації та функціонування пристроїв |
| Графіки активності | Відображення завантаженості каналів та пристроїв у вигляді графіків | Аналіз продуктивності мережі, виявлення перевантажених ділянок |

Незважаючи на численні переваги, Cisco Packet Tracer як інструмент для проєктування та моделювання комп'ютерних мереж має певні обмеження та недоліки, які слід враховувати при реалізації проєкту мережі для закладу середньої освіти. Розуміння цих обмежень дозволить більш реалістично оцінити результати моделювання та передбачити потенційні розбіжності між змодельованою та реальною мережею.

Одним із найсуттєвіших недоліків Cisco Packet Tracer є обмежена підтримка можливостей реального обладнання Cisco. Хоча програма імітує роботу багатьох моделей маршрутизаторів та комутаторів, вона підтримує

лише обмежений набір команд IOS та функцій, доступних на реальних пристроях. Деякі просунуті функції, такі як MPLS, детальне налаштування QoS, розширені можливості маршрутизації BGP або складні конфігурації безпеки, можуть бути недоступні або реалізовані спрощено. Це обмежує можливості моделювання складних мережевих рішень та може створювати розбіжності між симуляцією та реальним впровадженням.

Ще одним суттєвим недоліком є обмежена продуктивність при моделюванні великих мереж. При створенні складних топологій з багатьма пристроями та інтенсивним мережевим трафіком програма може працювати повільно або нестабільно, особливо на комп'ютерах з обмеженими ресурсами. Це може ускладнювати моделювання мережі великого закладу освіти з численними комп'ютерними класами та складною інфраструктурою.

Симуляція мережевих процесів у Packet Tracer є спрощеною і не завжди точно відображає реальну поведінку мережі. Зокрема, програма не повністю моделює фізичний рівень передачі даних, не враховує реальні затримки в каналах зв'язку, джиттер, вплив електромагнітних завад та інші фактори, які можуть суттєво впливати на роботу реальної мережі. Це може призвести до того, що мережа, яка працює ідеально в симуляторі, зіткнеться з проблемами продуктивності або стабільності в реальних умовах.

Незважаючи на перелічені недоліки, Cisco Packet Tracer залишається потужним та доступним інструментом для проєктування та моделювання комп'ютерних мереж, особливо в освітньому контексті. Усвідомлення його обмежень дозволяє критично оцінювати результати моделювання та за необхідності компенсувати недоліки шляхом додаткового аналізу, використання альтернативних інструментів для окремих аспектів проєктування або консультацій з фахівцями, що мають досвід роботи з реальним мережевим обладнанням.

У таблиці 2.3 узагальнено основні недоліки Cisco Packet Tracer та їх потенційний вплив на проєктування мережі закладу середньої освіти.

Таблиця 2.3 — Недоліки Cisco Packet Tracer як засобу реалізації

| Недолік | Опис | Потенційний вплив на проєкт |
|---|---|---|
| Обмежена підтримка функціоналу IOS | Реалізовано не всі команди та функції, доступні на реальному обладнанні | Неможливість моделювання деяких складних мережевих рішень |
| Фокус на обладнанні Cisco | Обмежена підтримка пристроїв інших виробників | Складність моделювання гетерогенних мереж з обладнанням різних вендорів |
| Обмеження продуктивності | Повільна робота при моделюванні великих мереж | Складність моделювання масштабних мережевих інфраструктур |
| Спрощена симуляція | Неповне моделювання фізичного рівня та реальних умов передачі даних | Розбіжності між симуляцією та реальною поведінкою мережі |
| Обмежена підтримка сучасних протоколів | Недостатня реалізація новітніх стандартів та протоколів | Ускладнене моделювання мереж з використанням передових технологій |
| Проблеми сумісності версій | Несумісність проєктів між різними версіями програми | Проблеми при колективній роботі або оновленні програмного забезпечення |
| Обмеження в моделюванні серверних систем | Спрощена реалізація серверів та сервісів | Неповне моделювання взаємодії інфраструктури з серверними компонентами |

### 2.1.3 Аналіз альтернативних засобів для моделювання комп’ютерної мережі

При проєктуванні комп'ютерної мережі для закладу середньої освіти важливо розглянути альтернативні програмні засоби для моделювання мереж. Кожен із цих інструментів має свої особливості, переваги та недоліки, які можуть бути суттєвими залежно від конкретних вимог проєкту [22].

GNS3 (Graphical Network Simulator-3) є одним із найпотужніших відкритих інструментів для моделювання мереж, який підтримує емуляцію реального обладнання, а не просто симуляцію, як у випадку з Packet Tracer. Основна перевага GNS3 полягає в тому, що програма використовує справжні образи операційних систем мережевих пристроїв (IOS, IOS-XR, NX-OS та інші), що забезпечує більш точне відтворення їх поведінки.

GNS3 також підтримує інтеграцію з віртуальними машинами, що дозволяє створювати комплексні лабораторії з різноманітними операційними

системами та сервісами. Завдяки активній спільноті користувачів, GNS3 постійно оновлюється та має велику кількість навчальних матеріалів та готових проєктів, що спрощує його впровадження в освітнє середовище.

На відміну від Packet Tracer, GNS3 підтримує обладнання не лише Cisco, але й інших виробників, таких як Juniper, MikroTik, Fortinet, Palo Alto Networks, що може бути важливим при проєктуванні гетерогенних мереж. Однак GNS3 вимагає більше системних ресурсів, має складнішу конфігурацію та потребує окремого отримання образів операційних систем, які часто захищені авторськими правами. Незважаючи на ці обмеження, GNS3 залишається одним із найкращих варіантів для навчальних закладів, які прагнуть надати учням досвід роботи з реалістичними мережевими середовищами.

EVE-NG (Emulated Virtual Environment - Next Generation) є ще одним потужним рішенням для емуляції мереж, яке позиціонується як платформа для мультивендорної мережевої віртуалізації. EVE-NG дозволяє створювати складні віртуальні лабораторії з підтримкою телекомунікаційного обладнання різних виробників.

Платформа працює через веб-інтерфейс, що спрощує колективну роботу та доступ з різних пристроїв. EVE-NG особливо корисна для моделювання великих мережевих інфраструктур з різноманітним обладнанням.

Як і GNS3, EVE-NG потребує потужних апаратних ресурсів та доступу до ліцензійних образів операційних систем. Крім того, повнофункціональна версія EVE-NG Professional є платною, що може бути обмеженням для освітніх проєктів з обмеженим бюджетом.

NetSim від компанії Tetcos - це комерційний симулятор мереж, орієнтований на академічне використання та дослідження. Він підтримує широкий спектр технологій, включаючи IoT, WSN, MANET, LTE та 5G.

NetSim дозволяє проводити детальний аналіз продуктивності мережі, збирати та візуалізувати статистичні дані, а також інтегрується з MATLAB для

розширеного аналізу. Цей інструмент особливо корисний для дослідження нових мережевих технологій та протоколів [24].

Mininet є легким симулятором мереж, який спеціалізується на програмно-конфігурованих мережах (SDN) та протоколі OpenFlow. Він дозволяє створювати реалістичні віртуальні мережі на одному комп'ютері, використовуючи процеси з простору користувача та віртуальні мережеві інтерфейси.

Mininet особливо корисний для експериментів з SDN та контролерами, такими як OpenDaylight або ONOS, але має обмежені можливості для моделювання традиційних мереж з маршрутизаторами та комутаторами.

При виборі програмного забезпечення для моделювання мережі закладу середньої освіти слід враховувати не лише технічні можливості інструментів, але й практичні аспекти їх застосування. Для освітнього закладу важливими факторами є доступність програмного забезпечення, вимоги до апаратних ресурсів, простота використання та можливість отримання підтримки.

Cisco Packet Tracer, незважаючи на свої обмеження, залишається оптимальним вибором для проєктування типових мереж освітніх закладів через свою доступність, низькі вимоги до ресурсів та інтуїтивно зрозумілий інтерфейс. Однак для складних мережевих інфраструктур з гетерогенним обладнанням або специфічними вимогами може бути доцільним використання GNS3 або EVE-NG як доповнення до Packet Tracer для моделювання окремих аспектів мережі.

У таблиці 2.4 представлено порівняльний аналіз альтернативних програм для моделювання мереж з точки зору їх застосовності для проєктування мережі закладу середньої освіти.

Таблиця 2.4 — Порівняння засобів для моделювання мереж

| Програма | Тип | Підтримка обладнання | Точність моделювання | Вимоги до ресурсів | Ліцензування | Зручність використання |
|---|---|---|---|---|---|---|
| GNS3 | Емулятор | Мультивендорна (Cisco, Juniper, MikroTik тощо) | Висока (реальні образи ОС) | Високі | Безкоштовна, потребує ліцензійних образів ОС | Середня (потрібна попередня підготовка) |
| EVE-NG | Емулятор | Широка мультивендорна підтримка | Висока (реальні образи ОС) | Високі | Community — безкоштовна, Professional — платна | Середня (зручний веб-інтерфейс) |
| NetSim | Симулятор | Обмежена, фокус на Cisco | Середня до високої | Середні | Платна | Середня |
| Mininet | Емулятор SDN | Обмежена (SDN, OpenFlow) | Висока для SDN, низька для традиційних мереж | Низькі | Безкоштовна (open source) | Низька (потрібні знання Linux, Python) |
| IMUNES | Емулятор | Обмежена (базові мережеві функції) | Середня | Середні | Безкоштовна (open source) | Середня |
| Cisco Packet Tracer | Симулятор | Переважно Cisco | Середня (спрощена модель) | Низькі | Безкоштовна (для навчальних цілей) | Висока (інтуїтивний інтерфейс, простота) |

## 2.2 Вибір обладнання для проєктування комп’ютерної мережі для закладу середньої освіти

Проєктування мережі для закладу середньої освіти вимагає ретельного підходу до вибору мережевого обладнання, яке забезпечить надійну, безпечну та продуктивну інфраструктуру з урахуванням специфічних потреб освітнього середовища. Основними критеріями вибору обладнання є надійність, масштабованість, безпека, співвідношення ціна/якість та відповідність технічним вимогам мережі. Також важливим фактором є підтримка технологій віртуальних локальних мереж (VLAN), якість обслуговування (QoS) та

можливість централізованого управління. На основі аналізу топології мережі та її структури, необхідно обрати відповідне обладнання для кожного рівня мережевої ієрархії.

Для маршрутизації на рівні ядра мережі було обрано маршрутизатор Cisco ISR4221. Цей маршрутизатор забезпечує потужні можливості для обробки міжмережевого трафіку, підтримує широкий спектр протоколів маршрутизації та має високу продуктивність обробки пакетів. ISR4221 володіє вбудованими засобами безпеки, включаючи брандмауер на основі зон та системи запобігання вторгненням (IPS). Важливою перевагою даного маршрутизатора є можливість підтримки віртуальних приватних мереж (VPN), що потенційно дозволить організувати безпечний віддалений доступ до ресурсів школи для вчителів та адміністраторів. Модель ISR4221 обладнана двома гігабітними портами (Gig0/0/0 та Gig0/0/1), що достатньо для підключення до комутаторів третього рівня та забезпечення взаємодії між різними сегментами мережі. Даний маршрутизатор також має можливість розширення функціональності за допомогою додаткових модулів, що забезпечує гнучкість при подальшому розвитку мережі.

На рівні розподілу використано комутатори третього рівня Cisco Catalyst 3560-24PS, які виконують функції агрегації трафіку та маршрутизації між VLAN. Ці комутатори мають 24 порти Fast Ethernet та 2 порти Gigabit Ethernet, що дозволяє організувати високошвидкісні з'єднання з маршрутизатором та між комутаторами. Модель 3560-24PS підтримує технологію Power over Ethernet (PoE), що в перспективі дозволить живити через мережеві кабелі такі пристрої, як IP-телефони, бездротові точки доступу та IP-камери без необхідності додаткових джерел живлення. Важливою характеристикою цих комутаторів є підтримка протоколів динамічної маршрутизації (OSPF, EIGRP) та можливість налаштування списків контролю доступу (ACL) для фільтрації трафіку між VLAN. Комутатори 3560-24PS також підтримують функції QoS,

що дозволяє пріоритезувати критично важливий трафік, наприклад, відеоконференції або інтернет-тестування.

На рівні доступу для підключення кінцевих пристроїв (комп'ютерів, принтерів) було обрано комутатори другого рівня Cisco Catalyst 2950-24. Ці комутатори забезпечують базову комутацію трафіку та підтримку VLAN, що дозволяє логічно сегментувати мережу та ізолювати трафік різних підрозділів школи.

Модель 2950-24 має 24 порти Fast Ethernet, що є достатнім для підключення всіх необхідних пристроїв у навчальних класах, комп'ютерному класі, кабінеті директора та бухгалтерії.

Комутатори підтримують стандарт 802.1Q для маркування VLAN-трафіку та протокол STP (Spanning Tree Protocol) для запобігання петель комутації. Хоча ці комутатори не є найновішими моделями, вони залишаються надійним та економічно обґрунтованим вибором для шкільних мереж з обмеженим бюджетом, забезпечуючи при цьому всі необхідні базові функції для організації надійної локальної мережі.

Для центрального вузла мережі використовується Multilayer Switch, який поєднує функції комутатора та маршрутизатора. Цей пристрій виконує як функції агрегації трафіку, так і маршрутизації між різними VLAN, що дозволяє оптимізувати шляхи проходження трафіку та зменшити навантаження на основний маршрутизатор.

Multilayer Switch підтримує розширені функції безпеки, включаючи Dynamic ARP Inspection та DHCP Snooping, що захищає від атак типу ARP spoofing та несанкціонованих DHCP-серверів.

Цей комутатор також надає високу щільність портів, що забезпечує можливість підключення великої кількості пристроїв та спрощує управління мережею. У таблиці 2.5 наведені характеристики обраного мережевого обладнання для мережі закладу середньої освіти

Таблиця 2.5 — Характеристики обраного мережевого обладнання

| Характеристика | Cisco ISR4221 | Cisco Catalyst 3560-24PS | Cisco Catalyst 2950-24 |
|---|---|---|---|
| Рівень застосування | Ядро мережі | Рівень розподілу | Рівень доступу |
| Кількість портів | 2 порти GE | 24 порти FE, 2 порти GE | 24 порти FE |
| Підтримка VLAN | До 4096 VLAN | До 1005 VLAN | До 64 VLAN |
| Швидкість комутації | До 2 Gbps | До 32 Gbps | До 8.8 Gbps |
| Підтримка PoE | Відсутня | Є (15.4W на порт) | Відсутня |
| Підтримка QoS | Повна | Повна | Базова |
| Функції безпеки | Firewall, IPS, VPN | ACL, 802.1X, BPDU Guard | Базова безпека портів |
| Споживання енергії | 60—80W | 100—560W (з PoE) | 30—45W |
| Приблизна вартість | $1500—2000 | $1200—1500 | $200—400 |

Вибір даного обладнання для проєктування комп'ютерної мережі закладу середньої освіти обумовлений необхідністю створення надійної, безпечної та масштабованої інфраструктури, яка відповідає вимогам сучасного освітнього процесу. Маршрутизатор ISR4221 забезпечує стабільне підключення до Інтернету та організацію маршрутизації між VLAN, комутатори третього рівня 3560-24PS надають функціональність для агрегації та маршрутизації трафіку, а комутатори другого рівня 2950-24 забезпечують економічно ефективне рішення для підключення кінцевих пристроїв. Така структура обладнання дозволяє створити ієрархічну модель мережі, яка легко масштабується та адмініструється, що особливо важливо для освітніх закладів з обмеженими IT-ресурсами. Крім того, вибране обладнання забезпечує необхідний рівень безпеки та якості обслуговування, що є критичним фактором для захисту даних учнів та забезпечення стабільної роботи освітніх програм та сервісів.

# 3 ПРОЄКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ДЛЯ ЗАКЛАДУ СЕРЕДНЬОЇ ОСВІТИ

## 3.1 Проєктування структурної схеми мережі

При проєктуванні структурної схеми мережі для закладу середньої освіти необхідно враховувати специфічні особливості освітнього середовища. Шкільні мережі характеризуються неоднорідною структурою приміщень, що включають навчальні класи, комп'ютерні лабораторії, адміністративні кабінети та інші функціональні зони. Особливістю також є циклічність навантаження, пов'язана з розкладом занять, коли у певні години спостерігається пікове навантаження на мережу. Крім того, необхідно враховувати наявність різних категорій користувачів (учні, вчителі, адміністрація, технічний персонал), що потребують різних рівнів доступу до мережевих ресурсів.

Як топологію для реалізації мережі обрано фізичну топологію «розширена зірка» (або «дерево»), яка забезпечує гнучкість, надійність та простоту адміністрування. Ця топологія є оптимальним рішенням для навчальних закладів, оскільки забезпечує збалансоване співвідношення між вартістю впровадження, продуктивністю та масштабованістю мережевої інфраструктури.

Топологія «розширена зірка» реалізує ієрархічну трирівневу модель мережі, що складається з:

— рівня ядра, який представлений маршрутизатором Cisco ISR4221, який забезпечує з'єднання з Інтернетом та виконує функції основного шлюзу;

— рівня розподілу, що реалізований за допомогою комутаторів третього рівня Cisco Catalyst 3560-24PS, що забезпечують маршрутизацію між різними VLAN та агрегацію трафіку від комутаторів доступу;

— рівня доступу, він представлений комутаторами другого рівня Cisco Catalyst 2950-24, які забезпечують підключення кінцевих пристроїв користувачів.

Проєктована мережа логічно розділена на віртуальні локальні мережі (VLAN) відповідно до функціональних зон закладу освіти, як показано на рисунку Б.1:

— VLAN 10: комп'ютерні класи;

— VLAN 20: навчальні кабінети;

— VLAN 30: адміністрація;

— VLAN 40: бухгалтерія (серверна інфраструктура);

— VLAN 99: управління мережевими пристроями.

Таке логічне розділення забезпечує ізоляцію трафіку різних підрозділів, що підвищує рівень безпеки та оптимізує використання пропускної здатності мережі. Впровадження VLAN також забезпечує:

— зменшення доменів широкомовної розсилки, що покращує продуктивність мережі;

— гнучке управління політиками безпеки на рівні мережевих сегментів;

— можливість впровадження диференційованої якості обслуговування (QoS) для різних типів трафіку;

— спрощення впровадження змін та оновлень мережі без фізичної комутації.

Для забезпечення високої надійності в схемі мережі передбачено використання технології Multilayer Switch для центрального вузла, що дозволяє зменшити кількість "єдиних точок відмови". З'єднання між комутаторами рівня розподілу організовані за допомогою високошвидкісних гігабітних портів, що забезпечує достатню пропускну здатність для передачі агрегованого трафіку.

Для корпусів на першому та другому поверхах передбачено окремі комутатори доступу, що підключені до комутаторів рівня розподілу через

порти Fast Ethernet. Це забезпечує оптимальне розміщення обладнання відповідно до фізичної структури будівлі школи.

Важливим елементом структурної схеми є серверний сегмент, відокремлений у VLAN 40 з окремим комутатором та DHCP-сервером. Це підвищує рівень безпеки та стабільності мережі. Для централізованого управління мережевим обладнанням створено окрему VLAN 99, що дозволяє системним адміністраторам контролювати мережеве обладнання, налаштовувати політики безпеки та відстежувати продуктивність.

Для забезпечення взаємодії між різними VLAN необхідно налаштувати маршрутизацію між ними, яка реалізована на комутаторі 3-го рівня. Це дозволяє контролювати доступ між сегментами за допомогою списків контролю доступу (ACL), які забезпечують додатковий рівень безпеки. Наприклад, можна дозволити доступ із комп'ютерних класів до серверів з навчальними матеріалами, але обмежити доступ до адміністративних ресурсів.

Всі мережеві з'єднання між комутаторами рівня розподілу та маршрутизатором налаштовані як транкові з'єднання (Trunk), що забезпечує передачу трафіку різних VLAN по одному фізичному каналу. Це оптимізує використання наявних фізичних з'єднань та спрощує масштабування мережі в майбутньому.

При проєктуванні VLAN важливо враховувати потенційне зростання мережі та залишати резерв для майбутніх розширень. Рекомендується також документувати схему IP-адресації кожного VLAN та правила маршрутизації між ними, що спростить подальше адміністрування мережі та усунення несправностей.

## 3.2 Сегментація мережі закладу середньої освіти

Сегментація мережі є одним із ключових аспектів проєктування ефективної та безпечної мережевої інфраструктури для закладу середньої освіти. Раціональний поділ мережі на логічні сегменти дозволяє оптимізувати

використання мережевих ресурсів, підвищити рівень безпеки та спростити адміністрування.

Розроблена мережева інфраструктура закладу середньої освіти базується на ієрархічній модулі з логічною сегментацією, яка забезпечує ефективний розподіл та ізоляцію мережевого трафіку відповідно до функціональних потреб різних категорій користувачів.

На основі проведеного аналізу специфіки освітнього закладу та його функціональних потреб було розроблено структуру мережі, яка представлена на рисунку 3.1, де зображено топологію мережі, реалізовану в середовищі Cisco Packet Tracer.

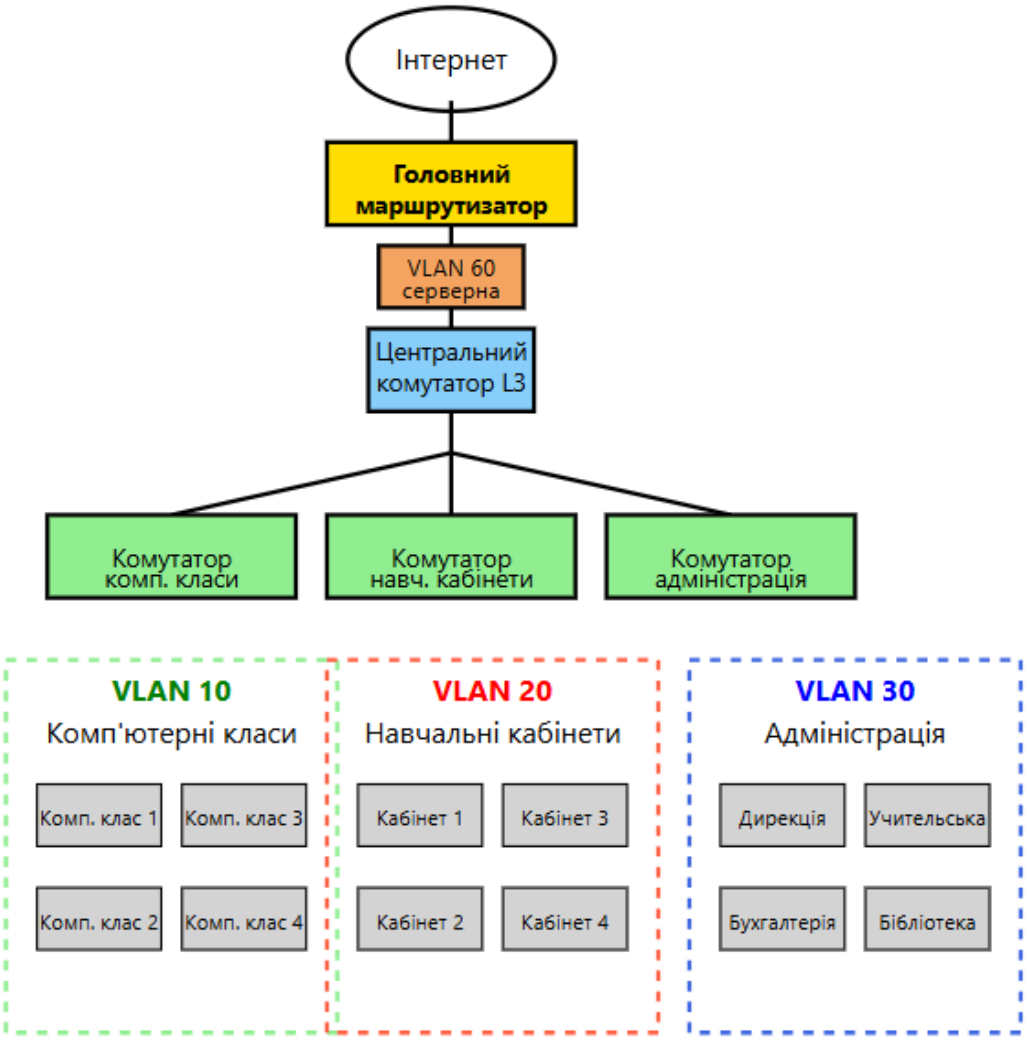



Рисунок 3.1 — Структурна схема сегментації мережі закладу

Як видно на рисунку 3.1, мережа має трирівневу ієрархічну структуру:

— рівень ядра, представлений головним маршрутизатором, який забезпечує підключення до Інтернету та міжмережеву маршрутизацію;

— рівень розподілу, представлений центральним комутатором 3-го рівня, який забезпечує маршрутизацію між різними сегментами мережі;

— рівень доступу, представлений комутаторами 2-го рівня, які забезпечують безпосереднє підключення кінцевих пристроїв.

Основна сегментація мережі реалізована за допомогою технології віртуальних локальних мереж (VLAN), що дозволяє логічно розділити єдину фізичну мережу на ізольовані сегменти. У проєкті впроваджено наступні VLAN:

VLAN 10: комп'ютерні класи — сегмент, призначений для комп'ютерних класів, де проводяться уроки інформатики та інші заняття з використанням комп'ютерної техніки. Цей сегмент характеризується високим рівнем мережевої активності під час уроків та потребує спеціальних політик безпеки для обмеження доступу учнів до певних ресурсів.

VLAN 20: навчальні кабінети — сегмент, що об'єднує робочі місця вчителів у навчальних кабінетах, інтерактивні дошки, проєктори та інше обладнання, яке використовується для проведення уроків. Цей сегмент потребує стабільного доступу до освітніх ресурсів та навчальних матеріалів.

VLAN 30: адміністрація — сегмент, що включає робочі місця адміністративного персоналу школи: дирекції, бухгалтерії, учительської та бібліотеки. Цей сегмент має підвищені вимоги до безпеки, оскільки тут обробляються персональні дані учнів та вчителів, фінансова інформація та інші конфіденційні документи.

VLAN 40: серверна — сегмент для розміщення серверів та іншої критичної інфраструктури закладу. Включає сервери для електронного журналу, системи управління навчанням (LMS), веб-сервер школи, файловий сервер та сервер резервного копіювання.

VLAN 99: управління — службовий сегмент для адміністрування мережевого обладнання, моніторингу та управління мережевою інфраструктурою.

Така сегментація забезпечує ряд переваг:

— підвищення безпеки — ізоляція критичних сегментів мережі (адміністрація, серверна) від загальнодоступних (комп'ютерні класи), що зменшує ризик несанкціонованого доступу та поширення шкідливого програмного забезпечення;

— оптимізація використання смуги пропускання — локалізація широкомовного трафіку в межах окремих VLAN, що зменшує навантаження на мережу та покращує її загальну продуктивність;

— спрощення адміністрування — можливість застосування різних політик безпеки, фільтрації та якості обслуговування (QoS) для різних сегментів мережі без необхідності фізичної реконфігурації;

— гнучкість та масштабованість — можливість легкого розширення мережі шляхом додавання нових VLAN або пристроїв без суттєвих змін в існуючій інфраструктурі.

Маршрутизація між різними VLAN здійснюється на рівні центрального комутатора 3-го рівня (L3), який підтримує функції міжвланової маршрутизації. Це дозволяє забезпечити контрольований доступ між різними сегментами мережі з використанням списків контролю доступу (ACL).

Для підключення кінцевих пристроїв до мережі використовуються комутатори 2-го рівня, які розташовані в різних частинах будівлі школи:

— комутатор навчального блоку — для підключення комп'ютерних класів та навчальних кабінетів у головному корпусі;

— комутатор адміністрації — для підключення адміністративних приміщень;

— комутатор додаткових приміщень — для підключення бібліотеки, актової зали, спортзалу та інших допоміжних приміщень.

## 3.3 Розробка логічної схеми комп'ютерної мережі для закладу середньої освіти

На рисунку Б.2 показана реалізація даної структури в середовищі моделювання з конкретними мережевими пристроями та з'єднаннями.

Підключення до Інтернету забезпечується через головний маршрутизатор, який також виконує функції міжмережевого екрану та реалізує механізм трансляції мережевих адрес (NAT) для спільного використання одної зовнішньої IP-адреси всіма пристроями внутрішньої мережі.

Така структура мережі дозволяє ефективно вирішувати основні завдання, що постають перед мережевою інфраструктурою закладу середньої освіти: забезпечення безпечного доступу до Інтернету, захист конфіденційної інформації, розділення мережевих ресурсів між різними групами користувачів та підтримка навчального процесу з використанням сучасних інформаційних технологій.

Технологія віртуальних локальних мереж (VLAN) є ключовим елементом у проєктуванні сучасних мережевих інфраструктур, особливо для закладів середньої освіти. VLAN дозволяє логічно розділяти фізичну мережу на окремі сегменти, що функціонують як незалежні локальні мережі, незалежно від фізичного розташування пристроїв. Це особливо актуально для шкільних мереж, де різні категорії користувачів (учні, вчителі, адміністрація) потребують різних рівнів доступу до мережевих ресурсів.

У проєкті комп'ютерної мережі для закладу середньої освіти технологія VLAN реалізована відповідно до стандарту IEEE 802.1Q, який визначає метод маркування кадрів Ethernet для вказання їх приналежності до певної віртуальної мережі. Цей стандарт передбачає додавання 4-байтового тегу до заголовка Ethernet-кадру, що містить ідентифікатор VLAN (VLAN ID) [30].

У контексті нашого проєкту VLAN використовуються для вирішення наступних завдань:

— логічне групування пристроїв за функціональним призначенням;

— ізоляція трафіку між різними групами користувачів;

— оптимізація використання пропускної здатності мережі;

— підвищення загального рівня безпеки мережевої інфраструктури;

— спрощення адміністрування та управління мережею.

Для реалізації сегментації мережі закладу середньої освіти були визначені наступні VLAN з використанням діапазону адрес 172.16.0.0/16, який добре підходить для середніх за розміром організацій, включаючи освітні заклади (таблиця 3.1):

Таблиця 3.1 — Структура VLAN мережі закладу середньої освіти

| VLAN ID | Назва | Призначення | IP-мережа | Маска підмережі |
|---|---|---|---|---|
| 10 | Комп'ютерні класи | Робочі станції та обладнання комп'ютерних класів | 172.16.10.0 | 255.255.255.0 |
| 20 | Навчальні кабінети | Комп'ютери вчителів та мультимедійне обладнання | 172.16.20.0 | 255.255.255.0 |
| 30 | Адміністрація | Робочі станції адміністративного персоналу | 172.16.30.0 | 255.255.255.0 |
| 40 | Серверна | Сервери та критична інфраструктура | 172.16.40.0 | 255.255.255.0 |
| 99 | Управління | Інтерфейси управління мережевим обладнанням | 172.16.99.0 | 255.255.255.0 |

Вибір адресного простору 172.16.0.0/16 обумовлений наступними факторами:

— це приватний діапазон адрес згідно RFC 1918, який не маршрутизується в Інтернеті;

— діапазон дозволяє виділити до 65 534 IP-адрес, що більш ніж достатньо для закладу середньої освіти;

— використання другого октету (16) для ідентифікації мережі та третього октету для ідентифікації VLAN спрощує адміністрування та забезпечує логічну структуру адресації.

Реалізація технології VLAN у проєкті передбачає налаштування як портів доступу (access ports), так і транкових портів (trunk ports). Порти доступу налаштовані на комутаторах рівня доступу і призначені для підключення кінцевих пристроїв (робочих станцій, принтерів, IP-телефонів). Кожен порт доступу асоційований з конкретною VLAN і приймає/передає тільки немарковані кадри. Наприклад, порти, до яких підключені комп'ютери в навчальних класах, налаштовані як порти доступу для VLAN 10. Транкові порти налаштовані для з'єднань між мережевими пристроями (комутатор-комутатор, комутатор-маршрутизатор) і передають трафік різних VLAN через одне фізичне з'єднання. Транкові порти передають і приймають марковані кадри з тегами 802.1Q, які вказують на приналежність кадру до певної VLAN.

На рисунку 3.2 схематично зображено принцип роботи транкових з'єднань в мережі закладу освіти.

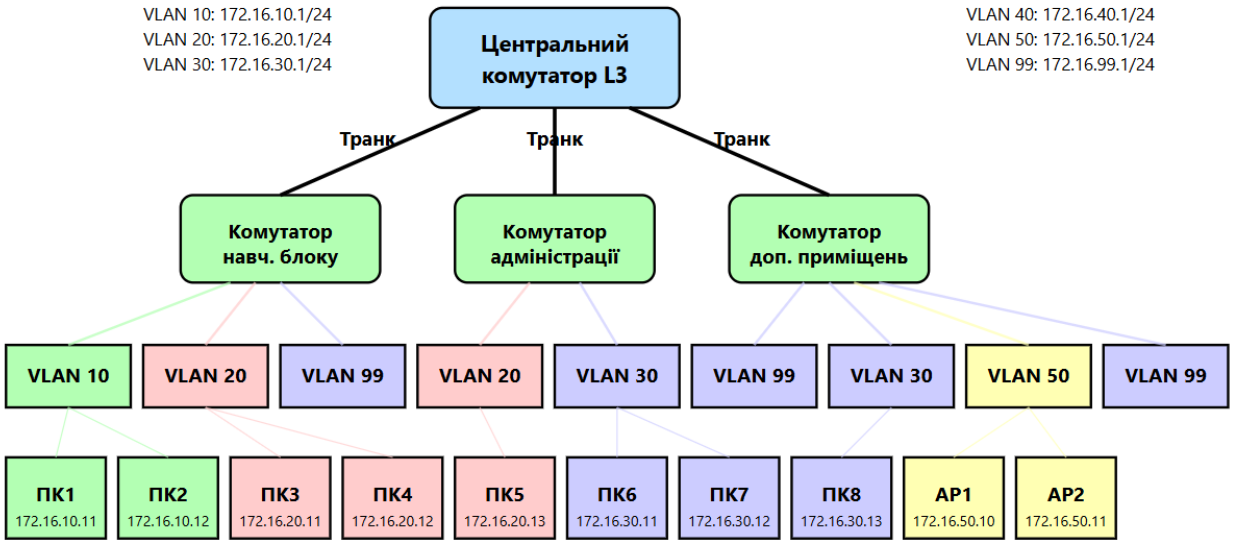



Рисунок 3.2 — Схема організації транкових з'єднань в мережі закладу освіти

Нижче представлений приклад базової конфігурації VLAN для комутатора навчального блоку (лістинг 3.1).

Лістинг 3.1 — Налаштування коматутора навчального блоку

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name ComputerClasses
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ClassRooms
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
// Налаштування портів доступу для VLAN 10
Switch(config)#interface range fastEthernet 0/1-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
// Налаштування портів доступу для VLAN 20
Switch(config)#interface range fastEthernet 0/13-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
// Налаштування транкового порту
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,99
Switch(config-if)#exit
```

Для комутатора 3-го рівня, який забезпечує маршрутизацію між різними VLAN, додатково налаштовуються віртуальні інтерфейси SVI (Switch Virtual Interface, лістинг 3.2).

Лістинг 3.2 — Налаштування SVI на L3-комутаторі

```
L3Switch>enable
L3Switch#configure terminal
L3Switch(config)#interface vlan 10
L3Switch(config-if)#ip address 172.16.10.1 255.255.255.0
L3Switch(config-if)#no shutdown
L3Switch(config-if)#exit
L3Switch(config)#interface vlan 20
L3Switch(config-if)#ip address 172.16.20.1 255.255.255.0
L3Switch(config-if)#no shutdown
```

```
L3Switch(config-if)#exit
L3Switch(config)#interface vlan 30
L3Switch(config-if)#ip address 172.16.30.1 255.255.255.0
L3Switch(config-if)#no shutdown
L3Switch(config-if)#exit
L3Switch(config)#interface vlan 40
L3Switch(config-if)#ip address 172.16.40.1 255.255.255.0
L3Switch(config-if)#no shutdown
L3Switch(config-if)#exit
L3Switch(config)#ip routing
```

Для забезпечення ізоляції окремих VLAN застосовуються списки контролю доступу (ACL), які дозволяють детально регулювати трафік між різними сегментами мережі. Наприклад, для обмеження доступу з комп'ютерних класів (VLAN 10) до адміністративного сегменту (VLAN 30) використовується наступна конфігурація (лістинг 3.3).

Лістинг 3.3 — Налаштування ACL на L3-комутаторі

```
L3Switch(config)#access-list 101 deny ip 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255
L3Switch(config)#access-list 101 permit ip any any
L3Switch(config)#interface vlan 10
L3Switch(config-if)#ip access-group 101 in
L3Switch(config-if)#exit
```

У проєкті також реалізована технологія VTP (VLAN Trunking Protocol) для централізованого управління конфігурацією VLAN. Центральний комутатор 3-го рівня налаштований як VTP-сервер, а комутатори рівня доступу — як VTP-клієнти. Це дозволяє централізовано створювати, видаляти та модифікувати VLAN, що суттєво спрощує адміністрування мережі.

Налаштування VTP на центральному комутаторі (сервер) показані на лістингу 3.4.

Лістинг 3.4 — Налаштування списків доступу на L3-комутаторі

```
L3Switch(config)#vtp mode server
L3Switch(config)#vtp domain SchoolNet
L3Switch(config)#vtp password Sch00lN3t
#Налаштування VTP на комутаторах доступу (клієнти):
Switch(config)#vtp mode client
```

```
Switch(config)#vtp domain SchoolNet
Switch(config)#vtp password Sch00lN3t
```

Для забезпечення додаткового рівня безпеки, на портах доступу активовано технології Port Security та DHCP Snooping, які запобігають несанкціонованому підключенню пристроїв до мережі та захищають від атак на інфраструктуру. Налаштування Port Security наведене на лістингу 3.5.

Лістинг 3.5 — Налаштування Port Security

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
```

Технологія VLAN є фундаментом для побудови ефективної та безпечної мережевої інфраструктури закладу середньої освіти. Вона забезпечує логічну сегментацію, ізоляцію трафіку, оптимізацію використання ресурсів мережі та спрощує адміністрування.

Ефективна схема IP-адресації є ключовим компонентом успішного проєктування мережевої інфраструктури закладу середньої освіти. Правильно спланована система адресації забезпечує логічну організацію мережі, спрощує адміністрування, підвищує безпеку та створює основу для масштабування в майбутньому.

Загальний адресний простір 172.16.0.0/16 було розділено на окремі підмережі відповідно до визначеної структури VLAN. При цьому використовувався принцип зручності адміністрування: номер третього октету відповідає ідентифікатору VLAN. Таке рішення забезпечує інтуїтивно зрозумілу схему адресації, яка спрощує діагностику та управління мережею (таблиця 3.2).

Таблиця 3.2 — Схема розподілу IP-адрес за підмережами

| VLAN ID | Призначення | Адресний простір | Маска підмережі | Кількість доступних хостів | Діапазон адрес |
|---|---|---|---|---|---|
| 10 | Комп'ютерні класи | 172.16.10.0 | 255.255.255.0 (/24) | 254 | 172.16.10.1 — 172.16.10.254 |
| 20 | Навчальні кабінети | 172.16.20.0 | 255.255.255.0 (/24) | 254 | 172.16.20.1 — 172.16.20.254 |
| 30 | Адміністрація | 172.16.30.0 | 255.255.255.0 (/24) | 254 | 172.16.30.1 — 172.16.30.254 |
| 40 | Серверна | 172.16.40.0 | 255.255.255.0 (/24) | 254 | 172.16.40.1 — 172.16.40.254 |
| 99 | Управління | 172.16.99.0 | 255.255.255.0 (/24) | 254 | 172.16.99.1 — 172.16.99.254 |

Для проєкту комп'ютерної мережі закладу середньої освіти було обрано приватний адресний простір 172.16.0.0/16, який належить до класу B згідно з RFC 1918. Цей діапазон дозволяє організувати до 65 534 хостів, що значно перевищує поточні потреби типового освітнього закладу, але забезпечує достатній запас для майбутнього розширення.

Для кожної підмережі використовується маска 255.255.255.0 (префікс /24), яка забезпечує до 254 хостів у кожному сегменті. Такий розмір підмережі є оптимальним для типового закладу середньої освіти, де кількість пристроїв у кожному функціональному сегменті зазвичай не перевищує кількох десятків.

На рисунку Б.3 показано схему розподілу підмереж та основні шлюзи для кожного сегмента мережі.

Таке планування IP-адресації має ряд переваг для мережі закладу середньої освіти:

— логічна організація — чіткий зв'язок між ідентифікатором VLAN та номером підмережі спрощує адміністрування та діагностику;

— стандартизація — використання однакової маски підмережі (/24) для всіх сегментів забезпечує простоту конфігурації та запобігає помилкам;

— масштабованість — обраний адресний простір класу B дозволяє легко додавати нові підмережі та збільшувати кількість пристроїв у майбутньому;

— адміністративна зручність — виділення окремих діапазонів для статичних та динамічних адрес полегшує управління та обслуговування.

Для забезпечення автоматичного призначення IP-адрес робочим станціям та іншим кінцевим пристроям у проєкті реалізовано службу DHCP (Dynamic Host Configuration Protocol). DHCP-сервер налаштований на центральному комутаторі 3-го рівня і забезпечує видачу адрес для різних VLAN з відповідних пулів.

Для серверів та критичної мережевої інфраструктури використовуються статичні IP-адреси, що забезпечує стабільний доступ до цих ресурсів. Наприклад, сервери в VLAN 40 мають наступні статичні адреси:

— веб-сервер школи: 172.16.40.10;

— файловий сервер: 172.16.40.11;

— сервер електронного журналу: 172.16.40.12;

— сервер системи управління навчанням: 172.16.40.13;

— сервер резервного копіювання: 172.16.40.15.

Мережеве обладнання в VLAN 99 також налаштоване зі статичними адресами:

— комутатор навчального блоку: 172.16.99.10;

— комутатор адміністрації: 172.16.99.11;

— комутатор додаткових приміщень: 172.16.99.12.

Для забезпечення доступу до зовнішніх мереж (Інтернет) використовується механізм трансляції мережевих адрес (NAT), налаштований на головному маршрутизаторі. Цей механізм дозволяє всім пристроям внутрішньої мережі використовувати одну або кілька публічних IP-адрес для доступу до зовнішніх ресурсів. Конфігурація NAT на головному роутері показана на лістингу 3.6.

Лістинг 3.6 — Конфігурація NAT на головному маршрутизаторі

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 203.0.113.2 255.255.255.0
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip nat inside source list 1
interface GigabitEthernet0/0 overload
Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

У цій конфігурації зовнішній інтерфейс маршрутизатора (GigabitEthernet0/0) має публічну IP-адресу 203.0.113.2, а внутрішній інтерфейс (GigabitEthernet0/1) підключений до внутрішньої мережі з адресою 172.16.1.1.

Для забезпечення коректної маршрутизації між різними VLAN та зовнішніми мережами на комутаторі 3-го рівня та маршрутизаторі налаштовані відповідні маршрути (лістинг 3.7).

Лістинг 3.7 — Налаштування маршрутів на обладнанні

```
// На комутаторі 3-го рівня:
L3Switch(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
// На маршрутизаторі:
Router(config)#ip route 172.16.10.0 255.255.255.0 172.16.1.2
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.1.2
Router(config)#ip route 172.16.30.0 255.255.255.0 172.16.1.2
Router(config)#ip route 172.16.40.0 255.255.255.0 172.16.1.2
Router(config)#ip route 172.16.50.0 255.255.255.0 172.16.1.2
Router(config)#ip route 172.16.99.0 255.255.255.0 172.16.1.2
```

На комутаторі 3-го рівня налаштований маршрут за замовчуванням, який вказує, що весь трафік, призначений для зовнішніх мереж, повинен направлятися на головний маршрутизатор (172.16.1.1). На маршрутизаторі, в свою чергу, налаштовані статичні маршрути для кожної VLAN, що дозволяє правильно маршрутизувати трафік, призначений для внутрішніх підмереж.

Така схема IP-адресації та розподілу підмереж забезпечує ефективне функціонування мережі закладу середньої освіти, дозволяючи раціонально організувати мережеві ресурси, розмежувати доступ між різними функціональними зонами та створити основу для подальшого розвитку мережевої інфраструктури.

## 3.4 Організація безпеки комп'ютерної мережі

Забезпечення надійного контролю доступу та ефективної автентифікації користувачів є критично важливим аспектом безпеки мережевої інфраструктури закладу середньої освіти. Ці механізми дозволяють обмежити доступ до мережевих ресурсів лише авторизованим користувачам, запобігають несанкціонованому використанню мережі та забезпечують захист конфіденційної інформації, такої як персональні дані учнів та вчителів.

У проєкті комп'ютерної мережі закладу середньої освіти впроваджено комплексний підхід до контролю доступу та автентифікації, який поєднує кілька методів та технологій для досягнення оптимального рівня безпеки. Розглянемо основні компоненти цієї системи.

Централізована автентифікація користувачів реалізована за допомогою протоколу RADIUS (Remote Authentication Dial-In User Service), який забезпечує єдину точку автентифікації для всіх користувачів мережі. RADIUS-сервер розміщено в серверному сегменті (VLAN 40) і налаштовано для роботи з різними мережевими пристроями та сервісами.

Налаштування RADIUS-сервера на комутаторі 3-го рівня показане на лістингу 3.8.

Лістинг 3.8 — Налаштування сервера автентифікації користувачів

```
L3Switch(config)#aaa new-model
L3Switch(config)#radius-server host 172.16.40.20 auth-port 1812 acct-port 1813 key SecureKey123
L3Switch(config)#aaa authentication login default group radius local
```

```
     L3Switch(config)#aaa authorization network default group radius
local
     L3Switch(config)#aaa accounting network default start-stop group
radius
```

У цій конфігурації radius-server host вказує IP-адресу RADIUS-сервера та порти для автентифікації та обліку. Команда aaa authentication login default group radius local налаштовує використання RADIUS для автентифікації з локальною базою даних як резервним варіантом.

Автентифікація 802.1X впроваджена для проводової мережі та забезпечує контроль доступу на рівні портів комутаторів. Цей стандарт вимагає від користувачів автентифікації перед отриманням доступу до мережі. Налаштування 802.1X на комутаторі доступу (лістинг 3.9).

Лістинг 3.9 — Налаштування автентифікації 802.1X

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#interface range fastEthernet 0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#dot1x port-control auto
Switch(config-if-range)#dot1x pae authenticator
Switch(config-if-range)#exit
```

На рисунку 3.2 представлено схему організації системи контролю доступу та автентифікації користувачів.

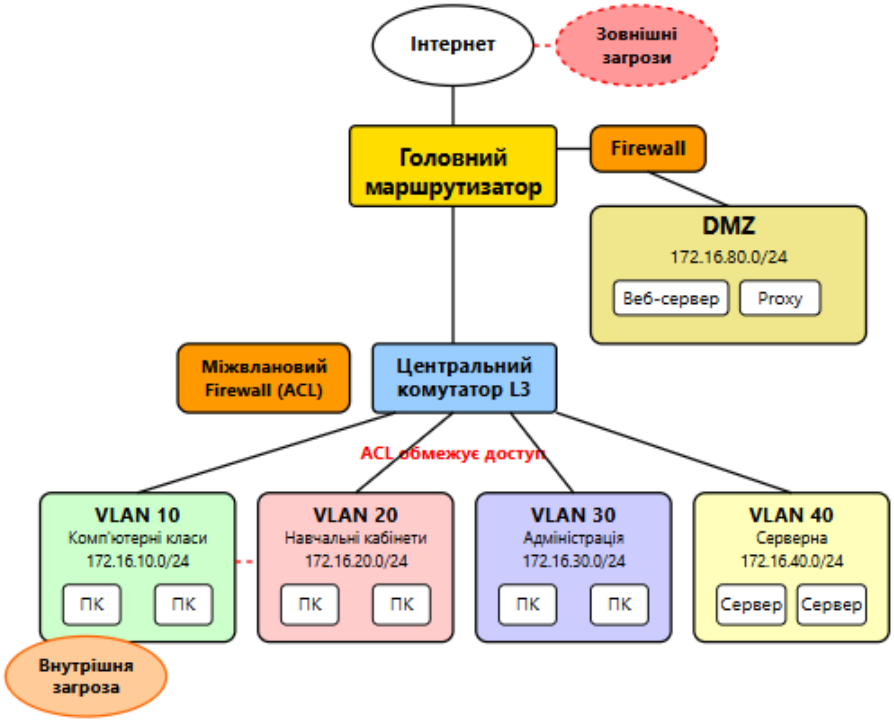



Рисунок 3.2 — Схема контролю доступу та автентифікації користувачів

# 4 НАЛАШТУВАННЯ ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ МЕРЕЖІ

## 4.1 Налаштування комутаторів рівня доступу

Комутатори рівня доступу є важливою складовою мережевої інфраструктури закладу середньої освіти, оскільки вони забезпечують безпосереднє підключення кінцевих пристроїв до мережі. У проєкті мережі використовуються комутатори Cisco Catalyst 2960, які поєднують оптимальне співвідношення ціни та функціональності, необхідної для освітнього середовища.

Налаштування комутаторів рівня доступу в середовищі Cisco Packet Tracer включає декілька етапів, починаючи з базового конфігурування та закінчуючи налаштуванням специфічних функцій безпеки.

Базова конфігурація включає встановлення імені пристрою, налаштування паролів доступу та налаштування IP-адреси для управління, що показано на лістингу 4.1.

Лістинг 4.1 — Базова конфігурація комутатора

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SwitchEducation
SwitchEducation(config)#enable secret Sch00l@dm1n
SwitchEducation(config)#line console 0
SwitchEducation(config-line)#password ConsoleP@ss
SwitchEducation(config-line)#login
SwitchEducation(config-line)#exit
SwitchEducation(config)#line vty 0 15
SwitchEducation(config-line)#password TelnetP@ss
SwitchEducation(config-line)#login
SwitchEducation(config-line)#transport input ssh telnet
SwitchEducation(config-line)#exit
SwitchEducation(config)#service password-encryption
```

Після базової конфігурації необхідно створити віртуальні локальні мережі (VLAN) згідно з проєктом мережі та налаштувати порти доступу. У

наведеному прикладі показана конфігурація для комутатора навчального блоку (лістинг 4.2).

Лістинг 4.2 — Налаштування VLAN, перегляд інформації

```
SwitchEducation(config)#vtp mode client
SwitchEducation(config)#vtp domain SchoolNet
SwitchEducation(config)#vtp password Sch00lN3t
SwitchEducation(config)#exit
SwitchEducation#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- ------
1    default   active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
               Fa0/13, Fa0/14, Fa0/15, Fa0/16
               Fa0/17, Fa0/18, Fa0/19, Fa0/20
     Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/2
10   ComputerClasses                     active
20   ClassRooms                          active
30   Administration                      active
40   ServerRoom                          active
50   WiFi                                active
99   Management                          active
```

Налаштування портів для підключення комп'ютерних класів (VLAN 10, лістинг 4.3).

Лістинг 4.3 — Налаштування портів для підключення VLAN10

```
SwitchEducation(config)#interface range fastEthernet 0/1-8
SwitchEducation(config-if-range)#switchport mode access
SwitchEducation(config-if-range)#switchport access vlan 10
SwitchEducation(config-if-range)#spanning-tree portfast
SwitchEducation(config-if-range)#spanning-tree bpduguard enable
SwitchEducation(config-if-range)#exit
```

Налаштування портів для підключення навчальних кабінетів (VLAN 20, лістинг 4.4).

Лістинг 4.4 — Налаштування портів для підключення VLAN20

```
SwitchEducation(config)#interface range fastEthernet 0/9-16
SwitchEducation(config-if-range)#switchport mode access
SwitchEducation(config-if-range)#switchport access vlan 20
SwitchEducation(config-if-range)#spanning-tree portfast
```

```
SwitchEducation(config-if-range)#spanning-tree bpduguard enable
SwitchEducation(config-if-range)#exit
```

Налаштування транкового порту для зв'язку з комутатором рівня розподілу (лістинг 4.5).

Лістинг 4.5 — Налаштування транкового з’єднання

```
SwitchEducation(config)#interface gigabitEthernet 0/1
SwitchEducation(config-if)#switchport mode trunk
SwitchEducation(config-if)#switchport trunk allowed vlan 10,20,99
SwitchEducation(config-if)#switchport trunk native vlan 99
SwitchEducation(config-if)#spanning-tree guard root
SwitchEducation(config-if)#exit
```

Для запобігання атакам типу MAC Flooding і підміни DHCP-серверів налаштовуються додаткові функції безпеки (лістинг 4.6).

Лістинг 4.6 — Налаштування додаткових функцій безпеки

```
SwitchEducation(config)#ip dhcp snooping
SwitchEducation(config)#ip dhcp snooping vlan 10,20
SwitchEducation(config)#no ip dhcp snooping information option
SwitchEducation(config)#interface gigabitEthernet 0/1
SwitchEducation(config-if)#ip dhcp snooping trust
SwitchEducation(config-if)#exit
SwitchEducation(config)#interface range fastEthernet 0/1-16
SwitchEducation(config-if-range)#ip dhcp snooping limit rate 5
SwitchEducation(config-if-range)#exit
```

Аналогічні налаштування виконуються для всіх комутаторів рівня доступу відповідно до їх ролі в мережі та підключених до них пристроїв.

## 4.2 Конфігурація маршрутизаторів та шлюзів

У даному проєкті центральним елементом мережі виступають три багатошарові комутатори 3600-24PS Multilayer Switch, розміщені в серверному приміщенні. Ці пристрої забезпечують основну маршрутизацію трафіку між різними сегментами мережі (адміністрацією, комп'ютерними класами та навчальними кабінетами).

Конфігурація центрального комутатора 3600-24PS починається зі стандартних базових налаштувань (лістинг 4.7):

Лістинг 4.7 — Конфігурація центрального комутатора 3600-24PS

```
Switch#configure terminal
Switch(config)#hostname CentralSwitch
CentralSwitch(config)#enable secret Sch00l@dm1n
CentralSwitch(config)#line console 0
CentralSwitch(config-line)#password ConsoleP@ss
CentralSwitch(config-line)#login
CentralSwitch(config-line)#exit
CentralSwitch(config)#service password-encryption
```

Налаштування віртуальних локальних мереж (VLAN) відповідно до функціональних зон школи показано у лістингу 4.8.

Лістинг 4.8 — Налаштування VLAN-мереж

```
CentralSwitch(config)#vtp mode server
CentralSwitch(config)#vtp domain SchoolNet
CentralSwitch(config)#vtp password Sch00lN3t
CentralSwitch(config)#vlan 10
CentralSwitch(config-vlan)#name ComputerClass
CentralSwitch(config-vlan)#exit
CentralSwitch(config)#vlan 20
CentralSwitch(config-vlan)#name Administration
CentralSwitch(config-vlan)#exit
CentralSwitch(config)#vlan 30
CentralSwitch(config-vlan)#name ClassRooms
CentralSwitch(config-vlan)#exit
CentralSwitch(config)#vlan 40
CentralSwitch(config-vlan)#name Servers
CentralSwitch(config-vlan)#exit
CentralSwitch(config)#vlan 99
CentralSwitch(config-vlan)#name Management
CentralSwitch(config-vlan)#exit
```

Для основних мережевих пристроїв необхідно налаштувати транкові з'єднання, які дозволяють передавати трафік різних VLAN через одне фізичне з'єднання (лістинг 4.9).

Лістинг 4.9 — Налаштування порту trunk

```
CentralSwitch(config)#interface range gigabitEthernet 0/1 - 2
```

```
CentralSwitch(config-if-range)#switchport trunk encapsulation dot1q
CentralSwitch(config-if-range)#switchport mode trunk
CentralSwitch(config-if-range)#sw trunk allowed vlan 10,20,30,40,99
CentralSwitch(config-if-range)#spanning-tree portfast trunk
CentralSwitch(config-if-range)#exit
```

Для забезпечення маршрутизації між різними VLAN необхідно налаштувати віртуальні інтерфейси SVI (Switch Virtual Interface) для кожної VLAN та включити функцію маршрутизації (лістинг 4.10).

Лістинг 4.10 — Налаштування VLAN-адресації

```
CentralSwitch(config)#ip routing
CentralSwitch(config)#interface vlan 10
CentralSwitch(config-if)#ip address 172.16.10.1 255.255.255.0
CentralSwitch(config-if)#no shutdown
CentralSwitch(config-if)#exit
CentralSwitch(config)#interface vlan 20
CentralSwitch(config-if)#ip address 172.16.20.1 255.255.255.0
CentralSwitch(config-if)#no shutdown
CentralSwitch(config-if)#exit
CentralSwitch(config)#interface vlan 30
CentralSwitch(config-if)#ip address 172.16.30.1 255.255.255.0
CentralSwitch(config-if)#no shutdown
CentralSwitch(config-if)#exit
CentralSwitch(config)#interface vlan 40
CentralSwitch(config-if)#ip address 172.16.40.1 255.255.255.0
CentralSwitch(config-if)#no shutdown
CentralSwitch(config-if)#exit
```

Для підключення до маршрутизатора ISR2921, через який здійснюється доступ до Інтернету, налаштовується фізичний інтерфейс(лістинг 4.11).

Лістинг 4.11 — Налаштування фізичного інтерфейсу роутера

```
CentralSwitch(config)#interface gigabitEthernet 0/0
CentralSwitch(config-if)#no switchport
CentralSwitch(config-if)#ip address 172.16.1.2 255.255.255.0
CentralSwitch(config-if)#no shutdown
CentralSwitch(config-if)#exit
```

Важливою складовою мережевої інфраструктури є налаштування DHCP-сервера для автоматичного призначення IP-адрес кінцевим пристроям (лістинг 4.12).

Лістинг 4.12 — Налаштування DHCP-сервера

```
CentralSwitch(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.10
CentralSwitch(config)#ip dhcp excluded-address 172.16.20.1 172.16.20.10
CentralSwitch(config)#ip dhcp excluded-address 172.16.30.1 172.16.30.10
CentralSwitch(config)#ip dhcp pool ComputerClass
CentralSwitch(dhcp-config)#network 172.16.10.0 255.255.255.0
CentralSwitch(dhcp-config)#default-router 172.16.10.1
CentralSwitch(dhcp-config)#dns-server 172.16.40.10 8.8.8.8
CentralSwitch(dhcp-config)#domain-name school.local
CentralSwitch(dhcp-config)#lease 7
CentralSwitch(dhcp-config)#exit
CentralSwitch(config)#ip dhcp pool Administration
CentralSwitch(dhcp-config)#network 172.16.20.0 255.255.255.0
CentralSwitch(dhcp-config)#default-router 172.16.20.1
CentralSwitch(dhcp-config)#dns-server 172.16.40.10 8.8.8.8
CentralSwitch(dhcp-config)#domain-name school.local
CentralSwitch(dhcp-config)#lease 7
CentralSwitch(dhcp-config)#exit
CentralSwitch(config)#ip dhcp pool ClassRooms
CentralSwitch(dhcp-config)#network 172.16.30.0 255.255.255.0
CentralSwitch(dhcp-config)#default-router 172.16.30.1
CentralSwitch(dhcp-config)#dns-server 172.16.40.10 8.8.8.8
CentralSwitch(dhcp-config)#domain-name school.local
CentralSwitch(dhcp-config)#lease 7
CentralSwitch(dhcp-config)#exit
```

Для забезпечення безпеки трафіку між різними VLAN налаштовуються списки контролю доступу (ACL), які обмежують передачу даних між різними сегментами мережі (лістинг 4.13).

Лістинг 4.13 — Налаштування списків доступу ACL

```
CentralSwitch(config)#access-list 110 deny ip 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255
CentralSwitch(config)#access-list 110 permit ip any any
CentralSwitch(config)#interface vlan 10
CentralSwitch(config-if)#ip access-group 110 in
CentralSwitch(config-if)#exit
```

```
CentralSwitch(config)#access-list 120 deny ip 172.16.30.0 0.0.0.255 172.16.20.0 0.0.0.255
CentralSwitch(config)#access-list 120 permit ip any any
CentralSwitch(config)#interface vlan 30
CentralSwitch(config-if)#ip access-group 120 in
CentralSwitch(config-if)#exit
```

Для забезпечення доступу до мережі Інтернет для всіх пристроїв внутрішньої мережі закладу середньої освіти використовується маршрутизатор ISR2921, який виконує функції трансляції мережевих адрес (NAT) та забезпечує безпечне з'єднання із зовнішніми мережами.

Першим кроком є налаштування зовнішнього інтерфейсу для підключення до провайдера послуг Інтернет (лістинг 4.14).

Лістинг 4.14 — Налаштування зовнішнього інтерфейсу роутера

```
ISR2921(config)#interface gigabitEthernet 0/1
ISR2921(config-if)#ip address 203.0.113.2 255.255.255.248
ISR2921(config-if)#no shutdown
ISR2921(config-if)#description WAN Connection to ISP
ISR2921(config-if)#exit
```

Для трансляції мережевих адрес (NAT) необхідно визначити, які внутрішні адреси будуть транслюватися та налаштувати процес трансляції (лістинг 4.15).

Лістинг 4.15 — Налаштування NAT

```
// Визначення внутрішніх мереж для трансляції
ISR2921(config)#access-list 1 permit 172.16.0.0 0.0.255.255
// Налаштування трансляції адрес з перевантаженням (PAT)
ISR2921(config)#ip nat inside source list 1
interface gigabitEthernet 0/1 overload
// Визначення внутрішнього та зовнішнього інтерфейсів для NAT
ISR2921(config)#interface gigabitEthernet 0/0
ISR2921(config-if)#ip nat inside
ISR2921(config-if)#exit
ISR2921(config)#interface gigabitEthernet 0/1
ISR2921(config-if)#ip nat outside
ISR2921(config-if)#exit
```

Важливою складовою безпеки мережі є налаштування фільтрації вхідного та вихідного трафіку. Для цього використовуються розширені списки

контролю доступу (ACL) (лістинг 4.16).

Лістинг 4.16 — Налаштування розширених ACL

```
// Дозвіл HTTP та HTTPS трафіку для веб-сервера
R(config)#access-list 110 permit tcp any host 203.0.113.3 eq 80
R(config)#access-list 110 permit tcp any host 203.0.113.3 eq 443
// Блокування небезпечних портів та протоколів
ISR2921(config)#access-list 110 deny tcp any any eq 23
ISR2921(config)#access-list 110 deny tcp any any eq 21
ISR2921(config)#access-list 110 deny tcp any any range 135 139
ISR2921(config)#access-list 110 deny udp any any range 135 139
// Дозвіл встановлених та споріднених з'єднань
ISR2921(config)#access-list 110 permit tcp any any established
ISR2921(config)#access-list 110 permit icmp any any echo-reply
ISR2921(config)#access-list 110 permit icmp any any time-exceeded
ISR2921(config)#access-list 110 permit icmp any any unreachable
// Заборона всього іншого вхідного трафіку
ISR2921(config)#access-list 110 deny ip any any
// Застосування списку доступу до зовнішнього інтерфейсу
ISR2921(config)#interface gigabitEthernet 0/1
ISR2921(config-if)#ip access-group 110 in
ISR2921(config-if)#exit
```

Така комплексна конфігурація маршрутизаторів, шлюзів та підключення до Інтернету забезпечує надійне та безпечне функціонування мережевої інфраструктури закладу середньої освіти, дозволяючи ефективно використовувати мережеві ресурси для навчального процесу та адміністративних потреб.

## 4.3 Тестування працездатності мережі

Після завершення налаштування мережевої інфраструктури закладу середньої освіти необхідно перевірити її працездатність з використанням різних методів тестування. Cisco Packet Tracer надає зручні інструменти для комплексної перевірки функціональності мережі.

Команда Ping є базовим інструментом для тестування з'єднання між пристроями в мережі. Вона використовує протокол ICMP для перевірки доступності пристроїв та визначення часу проходження пакетів.

Приклад використання команди Ping для перевірки з'єднання між робочою станцією комп'ютерного класу та сервером (рисунок 4.1).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.99.17 -n 6

Pinging 172.16.99.17 with 32 bytes of data:

Reply from 172.16.99.17: bytes=32 time<1ms TTL=125
Reply from 172.16.99.17: bytes=32 time=1ms TTL=125
Reply from 172.16.99.17: bytes=32 time<1ms TTL=125
Reply from 172.16.99.17: bytes=32 time<1ms TTL=125
Reply from 172.16.99.17: bytes=32 time<1ms TTL=125
Reply from 172.16.99.17: bytes=32 time<1ms TTL=125

Ping statistics for 172.16.99.17:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Рисунок 4.1 — Перевірка зв'язку між пристроями з використанням команди ping

Успішне виконання команди Ping підтверджує правильність налаштування маршрутизації між різними VLAN та працездатність основних компонентів мережі.

Утиліта Traceroute (tracert) дозволяє відстежити маршрут проходження пакетів від джерела до пункту призначення, показуючи всі проміжні маршрутизатори.

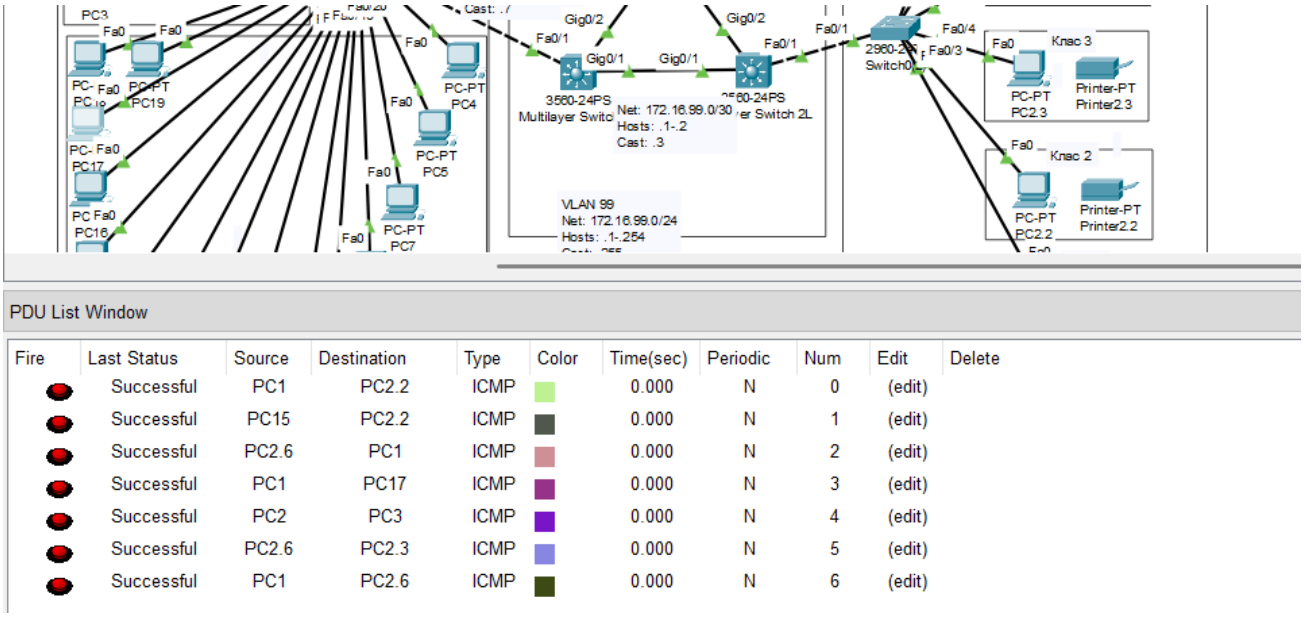
Покажемо використання даної команди при передачі пакету з першого поверху до другого, прослідкувавши його маршрут (рисунок 4.2).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 172.16.20.5

Tracing route to 172.16.20.5 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.16.40.254
  2    0 ms      0 ms      0 ms      172.16.99.2
  3    *         0 ms      0 ms      172.16.20.5

Trace complete.
```

Рисунок 4.2 — Відстеження маршруту проходження пакетів з використанням команди traceroute

Результати виконання команди показують точний шлях проходження пакетів через всі проміжні пристрої, що дозволяє виявити можливі проблеми з маршрутизацією.

Режим реального часу в Cisco Packet Tracer дозволяє взаємодіяти з пристроями та спостерігати за їх реакцією на команди та події безпосередньо під час роботи. Цей режим корисний для перевірки функціональності мережевих служб (HTTP, DHCP, DNS) та оцінки загальної працездатності мережі (рисунок 4.3).




PDU List Window

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|---|---|---|---|---|---|---|---|---|---|---|
| | Successful | PC1 | PC2.2 | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | PC15 | PC2.2 | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | PC2.6 | PC1 | ICMP | | 0.000 | N | 2 | (edit) | |
| | Successful | PC1 | PC17 | ICMP | | 0.000 | N | 3 | (edit) | |
| | Successful | PC2 | PC3 | ICMP | | 0.000 | N | 4 | (edit) | |
| | Successful | PC2.6 | PC2.3 | ICMP | | 0.000 | N | 5 | (edit) | |
| | Successful | PC1 | PC2.6 | ICMP | | 0.000 | N | 6 | (edit) | |

Рисунок 4.3 — Тестування працездатності мережі в режимі RealTime

Режим симуляції в Cisco Packet Tracer надає унікальну можливість спостерігати за процесом передачі пакетів на рівні окремих PDU (Protocol Data Unit), що дозволяє детально аналізувати роботу мережевих протоколів (рисунок 4.4).

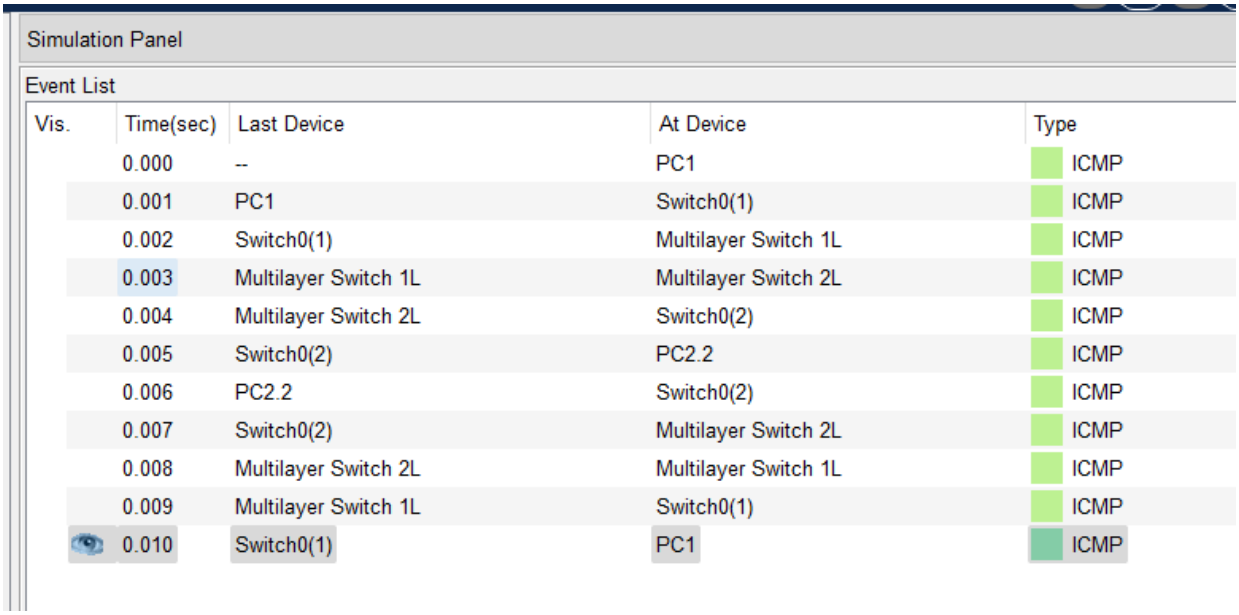
Основні кроки для проведення тестування в режимі симуляції:

— переключитися в режим Simulation Mode;

— згенерувати мережевий трафік (ping, відкриття веб-сторінки);

— спостерігати за проходженням пакетів через мережу;

— аналізувати вміст пакетів за допомогою інспектора пакетів.



Simulation Panel

Event List

| Vis. | Time(sec) | Last Device | At Device | Type |
|---|---|---|---|---|
| | 0.000 | -- | PC1 | ICMP |
| | 0.001 | PC1 | Switch0(1) | ICMP |
| | 0.002 | Switch0(1) | Multilayer Switch 1L | ICMP |
| | 0.003 | Multilayer Switch 1L | Multilayer Switch 2L | ICMP |
| | 0.004 | Multilayer Switch 2L | Switch0(2) | ICMP |
| | 0.005 | Switch0(2) | PC2.2 | ICMP |
| | 0.006 | PC2.2 | Switch0(2) | ICMP |
| | 0.007 | Switch0(2) | Multilayer Switch 2L | ICMP |
| | 0.008 | Multilayer Switch 2L | Multilayer Switch 1L | ICMP |
| | 0.009 | Multilayer Switch 1L | Switch0(1) | ICMP |
| | 0.010 | Switch0(1) | PC1 | ICMP |

Рисунок 4.4 — Відстеження проходження пакетів через мережу в режимі симуляції

Комплексне використання описаних методів тестування дозволяє переконатися в правильності налаштування всіх компонентів мережевої інфраструктури закладу середньої освіти та забезпечити її надійне функціонування.

# ВИСНОВКИ

У ході виконання бакалаврської кваліфікаційної роботи спроектовано та змодельовано комп'ютерну мережу для закладу середньої освіти, що забезпечує ефективну, безпечну та надійну інфраструктуру для підтримки освітнього процесу та адміністративних функцій.

Проведено аналіз специфіки мережевої інфраструктури освітніх закладів з виявленням їх особливих вимог та обмежень. Обґрунтовано необхідність створення сегментованої мережі з чітким розділенням адміністративних, навчальних та серверних ресурсів. Як топологію для реалізації мережі обрано фізичну топологію "розширена зірка" з логічним розділенням на VLAN, що забезпечує гнучкість, надійність та простоту адміністрування.

Спроектовано ієрархічну структуру мережі з трьома рівнями, що забезпечує масштабованість та ефективне управління трафіком. Розроблено схему IP-адресації з використанням приватного адресного простору 172.16.0.0/16, що дозволяє логічно організувати мережу та забезпечити простір для подальшого розширення. Реалізовано технологію VLAN для сегментації мережі на функціональні зони: комп'ютерні класи, навчальні кабінети, адміністрація, серверна інфраструктура та управління.

Створено комплексну систему безпеки, що включає налаштування міжмережевих екранів, списків керування доступом, трансляції мережевих адрес та механізмів захисту від різних типів атак. Впроваджено динамічне призначення IP-адрес з використанням DHCP-сервера, що спрощує адміністрування та підключення нових пристроїв до мережі.

Розроблена комп'ютерна мережа має значні переваги перед традиційними рішеннями. Серед них — висока надійність завдяки мінімізації "єдиних точок відмови", підвищений рівень безпеки через логічне розділення мережі та впровадження контролю доступу, оптимізація використання

пропускної здатності каналів, а також гнучкість та масштабованість для задоволення майбутніх потреб закладу освіти.

Проведене у віртуальному середовищі Cisco Packet Tracer тестування підтвердило працездатність розробленої мережі, правильність налаштування маршрутизації, функціонування механізмів безпеки та ефективність сегментації мережі. Використання різних методів тестування, включаючи перевірку зв'язності, трасування маршрутів та аналіз проходження пакетів у режимі симуляції, дозволило комплексно оцінити роботу всіх компонентів мережі.

Розроблена мережева інфраструктура надає закладу середньої освіти ефективну платформу для впровадження сучасних освітніх технологій, забезпечує безпечний доступ до внутрішніх та зовнішніх інформаційних ресурсів, спрощує адміністрування мережі та захищає конфіденційні дані учнів і вчителів.

Подальший розвиток проєкту може включати впровадження системи моніторингу мережевої інфраструктури для швидкого виявлення проблем, інтеграцію з системами контролю доступу до приміщень, розширення бездротового покриття з використанням технологій Mesh Wi-Fi, а також впровадження додаткових сервісів для підтримки дистанційного навчання.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров О. Д., Захарченко С. М., Кадук О. В. Комп'ютерні мережі: підручник. Вінниця: ВНТУ, 2020. 378 с.

2. Захарченко С. М., Кадук О. В. Комп'ютерні мережі: навчальний посібник. Вінниця: ВНТУ, 2013. 500 с.

3. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі: навч. посібник. Львів: Видавництво Львівської політехніки, 2022. 228 с.

4. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO: навч. посібник. Львів: Видавництво Львівської політехніки, 2021. 180 с.

5. Азаров О. Д., Черняк О. І., Савицька Л. А. Прикладне програмування у комп'ютерних мережах: навчальний посібник. Вінниця: ВНТУ, 2016. 130 с.

6. Городецька О. С., Гикавий В. А., Онищук О. В. Комп'ютерні мережі: навчальний посібник. Вінниця: ВНТУ, 2017. 129 с.

7. Захарченко С. М., Азаров О. Д., Яремчук Є. В., Дубінін В. М. Основи роботи та адміністрування мережних операційних систем: навчальний посібник. Вінниця: ВДТУ, 2001. 144 с.

8. Мокін В. Б. Інформаційні технології моніторингу та аналізу даних: навчальний посібник. Вінниця: ВНТУ, 2023. 256 с.

9. Папінов В. М., Кулик Я. А. Багатофункціональна комп'ютеризована лабораторія для наскрізної практичної підготовки студентів спеціальності 151. Оптико-електронні інформаційно-енергетичні технології. 2018. №2(36). С. 89-104.

10. Lammle T. CCNA Cisco Certified Network Associate Study Guide: Exam 200-301. 9th Edition. Sybex, 2020. 1056 p.

11. Lammle T. CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125. 2nd Edition. Sybex, 2016. 1008 p.

12. Odom W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press, 2019. 832 p.

13. Odom W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press, 2019. 848 p.

14. Tanenbaum A. S., Wetherall D. J. Computer Networks. 6th Edition. Pearson, 2021. 992 p.

15. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th Edition. Pearson, 2020. 864 p.

16. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. 6th Edition. Morgan Kaufmann, 2021. 960 p.

17. Stevens W. R. TCP/IP Illustrated, Volume 1: The Protocols. 2nd Edition. Addison-Wesley Professional, 2011. 1017 p.

18. IEEE 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. IEEE, 2022. 2163 p.

19. RFC 1918. Address Allocation for Private Internets. IETF, 1996. URL: https://tools.ietf.org/html/rfc1918 (дата звернення: 25.05.2025).

20. RFC 791. Internet Protocol - DARPA Internet Program Protocol Specification. IETF, 1981. URL: https://tools.ietf.org/html/rfc791 (дата звернення: 25.05.2025).

21. Cisco Networking Academy. Introduction to Networks (ITN). URL: https://www.netacad.com/courses/networking (дата звернення: 25.05.2025).

22. Cisco Systems. Packet Tracer Network Simulation Software. URL: https://www.netacad.com/courses/packet-tracer (дата звернення: 25.05.2025).

23. Wallace K. CCNP Enterprise Certification Study Guide: Implementing and Operating Cisco Enterprise Network Core Technologies. Sybex, 2020. 1248 p.

# ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
проф., д.т.н.. Азаров О.Д.
_____ 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання бакалаврської кваліфікаційної роботи
«Комп’ютерна мережа для закладу середньої освіти»

08-54.БКР.001.00.000 ТЗ

Науковий керівник: к.т.н., доцент каф. ОТ
_____Войцеховська О. В.

Студент групи КІ-23мсз
_____Дудник О. В.

м. Вінниця — 2025

1 Підстава для використання бакалаврської кваліфікайціної роботи (БКР)

1.1 Актуальність розробки полягає у необхідності впровадження надійних мережевих рішень для закладів середньої освіти через зростання обсягів переданої інформації, збільшення кількості підключених пристроїв та підвищені вимоги до безпеки навчального середовища. Проєктування комп'ютерної мережі для закладу середньої освіти з використанням сучасних технологій дасть можливість оптимізувати освітній процес, забезпечити якісний доступ до електронних освітніх ресурсів та гарантувати належний рівень захисту персональних даних учнів і вчителів.

1.2 Головним завданням розробки є створення сучасної, надійної та ефективної комп'ютерної мережі для закладу середньої освіти з використанням ієрархічної архітектури, технологій VLAN, механізмів безпеки та оптимізації IP-адресації, а також моделювання мережі у віртуальному середовищі Cisco Packet Tracer.

1.3 Наказ про затвердження теми бакалаврської дипломної роботи від 21 березня 2025 р. №97.

2 Мета і призначення БКР

2.1 Мета проєкту полягає у створенні комп'ютерної мережі для закладу середньої освіти, що забезпечує високий рівень надійності, безпеки та зручності використання, шляхом реалізації сегментації за допомогою технології VLAN, а також налаштування засобів безпеки для захисту мережевої інфраструктури.

2.2 Призначення розробки полягає у виконанні бакалаврської дипломної роботи, за результатами якої буде створено проєкт комп'ютерної мережі закладу середньої освіти, що може бути використаний як типове рішення при модернізації існуючих або розгортанні нових мережевих інфраструктур освітніх закладів.

3 Вихідні дані для виконання БКР

3.1 Опис типової структури закладу середньої освіти, включно з адміністративними приміщеннями, навчальними класами, комп'ютерними класами та додатковими приміщеннями, а також специфічних вимог до організації мережевої інфраструктури.

3.2 Огляд і аналіз сучасних мережевих технологій: топологій мереж, IP-адресації (IPv4), технологій віртуальних локальних мереж (VLAN), трансляції мережевих адрес (NAT) та методів забезпечення безпеки.

3.3 Визначення вимог до програмного забезпечення для моделювання мережі, аналіз наявних рішень та обґрунтування вибору Cisco Packet Tracer як інструменту для створення віртуальної моделі проєктованої мережі.

3.4 Планування структури та топології мережі, включаючи фізичне та логічне розміщення мережевих вузлів, сегментацію через VLAN та налаштування маршрутизації між підмережами.

3.5 Аналіз наявних мережевих рішень та вибір оптимальних варіантів з погляду ефективності, надійності та безпеки для забезпечення потреб закладу середньої освіти.

3.6 Розробка методики тестування спроєктованої мережі з урахуванням необхідності перевірки внутрішньої комунікації, доступу до зовнішніх ресурсів та функціонування механізмів безпеки.

4 Вимоги до виконання БКР

Головна вимога полягає в проєктуванні ефективної та надійної комп'ютерної мережі для закладу середньої освіти, яка забезпечить:

— логічне розділення мережі через VLAN для ізоляції різних функціональних зон (комп'ютерні класи, навчальні кабінети, адміністрація, серверна);

— надійну маршрутизацію між підмережами з використанням статичних маршрутів або протоколів динамічної маршрутизації;

— ефективне використання адресного простору через оптимальну схему IP-адресації та NAT;

— високий рівень безпеки з використанням ACL, фільтрації трафіку та міжмережевого екрану;

— можливість моделювання та тестування спроєктованої мережі у середовищі Cisco Packet Tracer;

— наочне представлення результатів проєктування у вигляді схем, таблиць та рекомендацій.

5 Етапи БКР та очікувані результати

Етапи розробки БКР та очікувані результати наведено у Таблиці А.1

Таблиця А.1 — Етапи БКР

| № етапу | Назва етапу | Термін виконання | | Очікувані результати |
|---|---|---|---|---|
| | | Початок | Кінець | |
| 1 | Аналіз предметної області і виявлення наявних проблем | 03.09.24 | 06.03.25 | Розділ 1 |
| 2 | Дослідження видів топологій та підходів до моделювання комп'ютерних мереж | 07.03.25 | 18.03.25 | Розділ 1 |
| 3 | Аналіз та обґрунтування вибору засобів реалізації | 19.03.25 | 27.03.25 | Розділ 2 |
| 4 | Розробка архітектури та структуризація комп'ютерної мережі | 28.04.25 | 04.05.25 | Розділ 3 |
| 5 | Налаштування засобів безпеки та тестування роботи мережі | 05.05.25 | 08.05.25 | Розділ 4 |
| 6 | Підготовка тезових матеріалів для публікації | 09.05.25 | 12.05.25 | Тези |
| 7 | Оформлення пояснювальної записки та демонстраційної презентації | 13.05.25 | 16.05.25 | ПЗ, презентація |
| 8 | Підготовка супровідної документації та перевірка на плагіат | 18.05.25 | 26.05.25 | ПЗ, презентація |

6 Матеріали, що подаються до захисту БКР

До захисту подаються: пояснювальна записка БКР, ілюстративні матеріали (схеми логічної та фізичної топології мережі, діаграми розподілу IP-адрес, схеми налаштування VLAN, схеми маршрутизації), протокол

попереднього захисту БКР на кафедрі, відгук наукового керівника, анотації до БКР українською та іноземною мовами, довідка про відповідність оформлення БКР чинним вимогам, файл проєкту мережі.

## 7 Порядок контролю виконання та захисту БКР

Виконання етапів графічної та розрахункової документації БКР контролюється науковим керівником к.т.н., доц. каф. ОТ Войцеховською О. В. згідно зі встановленими термінами. Захист БКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

## 8 Вимоги до оформлювання та порядок виконання БКР

При оформлюванні БКР використовуються:

– ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

– ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

– методичні вказівки до виконання бакалаврських кваліфікаційних робіт для студентів спеціальності 123 «Комп'ютерна інженерія» (освітня програма «Комп'ютерна інженерія») — кафедра обчислювальної техніки, ВНТУ 2023.

Порядок виконання БКР викладено в «Положення про кваліфікаційні роботи на першому (бакалаврському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21»

# ДОДАТОК Б

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи:
Комп'ютерна мережа для закладу середньої освіти

Тип роботи: Бакалаврська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

**Показники звіту подібності StrikePlagiarism**

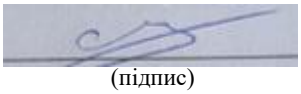
Оригінальність 94% Схожість 6%

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.

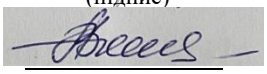
□ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку  Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Дудник О. В.
(підпис) (прізвище, ініціали)

Керівник роботи  Войцеховська О. В.
(підпис) (прізвище, ініціали)

# ДОДАТОК В

## ІЛЮСТРАТИВНА ЧАСТИНА

КОМП’ЮТЕРНА МЕРЕЖА ДЛЯ ЗАКЛАДУ СЕРЕДНЬОЇ ОСВІТИ

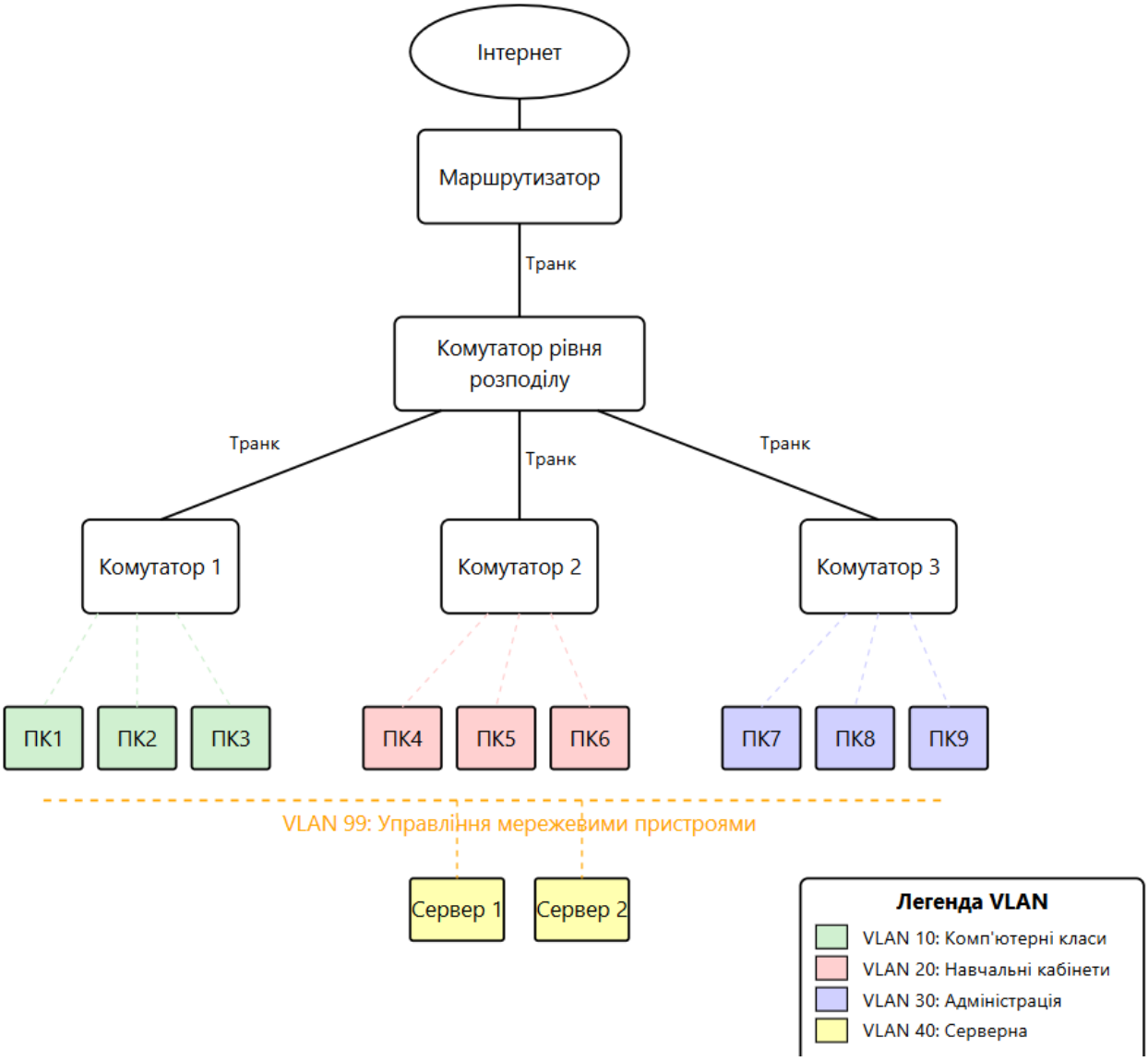



Рисунок В.1 — Структура мережі з використанням VLAN

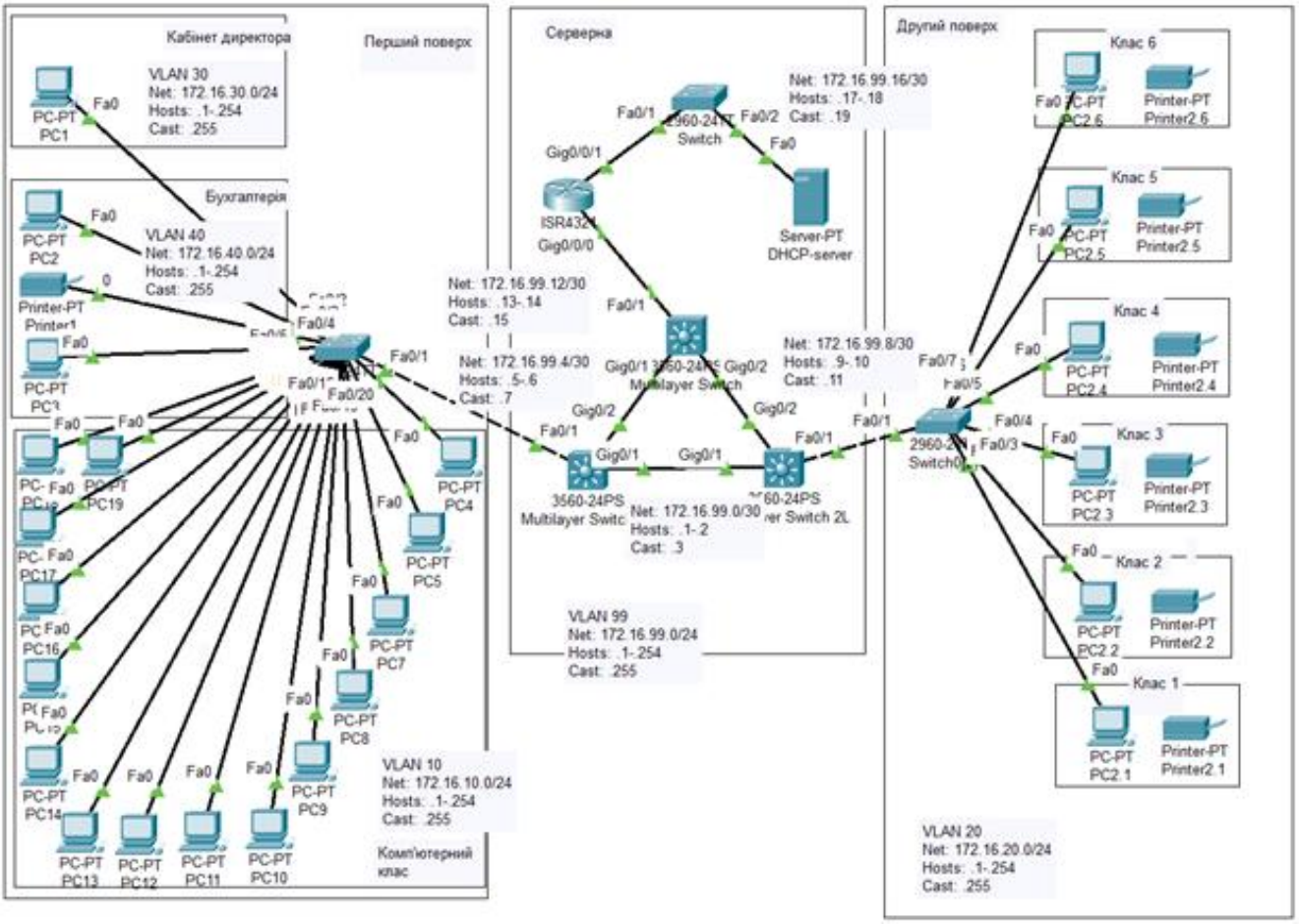



Рисунок В.2 — Логічна схема комп'ютерної мережі закладу освіти

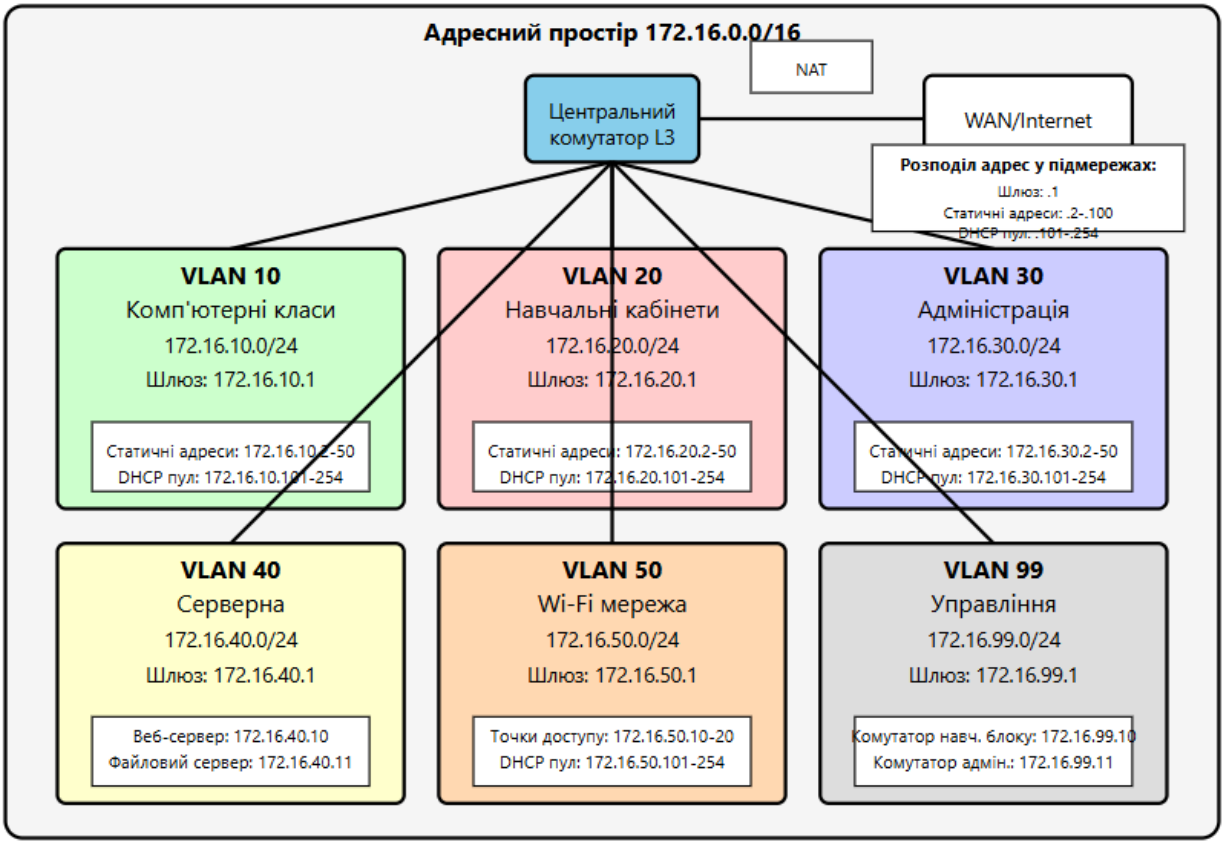



Рисунок В.3 — Схема розподілу підмереж у мережі закладу середньої освіти

# ДОДАТОК Г

Лістинги конфігураційних файлів

Лістинг Г.1 — Вміст конфігураційного файлу комутатора Multilayer Switch L1

```
MSL1#show run
Building configuration...
Current configuration : 1911 bytes
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname MSL1
ip routing
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
 no switchport
 ip address 172.16.99.1 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 no switchport
```

```
 ip address 172.16.99.5 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
interface Vlan10
 mac-address 0007.ec71.2a01
 ip address 172.16.10.254 255.255.255.0
 ip helper-address 172.16.99.17
interface Vlan30
 mac-address 0007.ec71.2a03
 ip address 172.16.30.254 255.255.255.0
 ip helper-address 172.16.99.17
interface Vlan40
 mac-address 0007.ec71.2a04
 ip address 172.16.40.254 255.255.255.0
 ip helper-address 172.16.99.17
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1
 network 172.16.99.0 0.0.0.3 area 0
 network 172.16.99.4 0.0.0.3 area 0
ip classless
ip route 172.16.99.16 255.255.255.252 172.16.99.6
ip route 172.16.20.0 255.255.255.0 172.16.99.2
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

Лістинг Г.2 — Вміст конфігураційного файлу комутатора Multilayer Switch L2

```
MSL2#show run
Building configuration...
Current configuration : 1770 bytes
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname MSL2
ip routing
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
```

```
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface GigabitEthernet0/1
 no switchport
 ip address 172.16.99.2 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 no switchport
 ip address 172.16.99.10 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
interface Vlan20
 mac-address 0001.632c.d601
 ip address 172.16.20.254 255.255.255.0
 ip helper-address 172.16.99.17
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1
 network 172.16.99.0 0.0.0.3 area 0
 network 172.16.99.8 0.0.0.3 area 0
ip classless
ip route 172.16.99.16 255.255.255.252 172.16.99.9
ip route 172.16.10.0 255.255.255.0 172.16.99.1
ip route 172.16.30.0 255.255.255.0 172.16.99.1
ip route 172.16.40.0 255.255.255.0 172.16.99.1
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
```

```
end
```

Лістинг Г.3 — Вміст конфігураційного файлу комутатора Multilayer Switch

```
MSL#show run
Building configuration...
Current configuration : 1817 bytes
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname MSL
ip routing
spanning-tree mode pvst
interface FastEthernet0/1
 no switchport
 ip address 172.16.99.14 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
 no switchport
 ip address 172.16.99.6 255.255.255.252
 duplex auto
 speed auto
```

```
interface GigabitEthernet0/2
 no switchport
 ip address 172.16.99.9 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1
 network 172.16.99.0 0.0.0.3 area 0
 network 172.16.99.4 0.0.0.3 area 0
 network 172.16.99.8 0.0.0.3 area 0
ip classless
ip route 172.16.99.16 255.255.255.252 172.16.99.13
ip route 172.16.10.0 255.255.255.0 172.16.99.5
ip route 172.16.30.0 255.255.255.0 172.16.99.5
ip route 172.16.40.0 255.255.255.0 172.16.99.5
ip route 172.16.20.0 255.255.255.0 172.16.99.10
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```