МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

АРХІТЕКТУРА ВІРТУАЛЬНОЇ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ

Виконав:
студент групи 2К-22
Спеціальності
123 «Комп’ютерна інженерія»
Денис ШИЯН
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____Наталя ФАЛЬЧЕНКО

(підпис)

«_____» _____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Шияну Денису Сергійовичу

1. Тема кваліфікаційної роботи «Архітектура віртуальної мережі навчального закладу»

   Керівник роботи Медолиз Маргарита Миколаївна, викладач вищої категорії, затверджені наказом закладу передвищої освіти від «06» жовтня 2025 року № 84/1у.
2. Строк подання студентом кваліфікаційної роботи 08.06.2026
3. Вихідні дані до кваліфікаційної роботи: стандарти побудови локальних мереж, середовище моделювання, джерела з інформацією про віртуальні мережі; правила адресації локальних мереж
4. Зміст кваліфікаційної роботи: структуру фізичної комп’ютерної мережі навчального закладу; принципи функціонування віртуальних локальних мереж VLAN; розробка логічної структури мережі з виділенням окремих сегментів для студентів, викладачів та адміністрації; перевірка моделі мережі в середовищі Cisco Packet Tracer.
5. Дата видачі завдання 15.10.2025 р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Структура фізичної та віртуальної мереж	09.12.2025	
3	Розділ 2 Практична реалізація віртуальної мережі	10.03.2026	
4	Розділ 3 Аналіз результатів VLAN–мережі	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	05.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачу ЦК (за 7 днів до захисту)	08.06.2026	

Студент _____ Денис ШИЯН
(підпис)

Керівник роботи _____ Маргарита МЕДОЛИЗ
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота присвячена застосуванню локальних мереж у навчальних закладах. в роботі було досліджено особливості фізичної та віртуальної мережевої архітектури, виконано проєктування VLAN-мережі. Реалізовано модкль мережі в середовищі Cisco Packet Tracer та проведено тестування працездатності й безпеки. У роботі розглянуто принципи сегментації мережі за допомогою VLAN, налаштування trunk-портів, міжвланової маршрутизації та списків контролю доступу ACL.

Практичним результатом стало створення моделі мережі навчального закладу з окремими сегментами для студентів, викладачів та адміністрації, що забезпечує підвищення керованості, безпеки та ефективності використання мережевих ресурсів.

Ключові слова: VPN, МЕРЕЖЕВА ІНФРАСТРУКТУРА, ІНФОРМАЦІЙНА БЕЗПЕКА, OPENVPN, ACL, МАРШРУТИЗАЦІЯ, СЕГМЕНТАЦІЯ МЕРЕЖІ, CISCO PACKET TRACER.

ABSTRACT

The qualification work is devoted to the use of local networks in educational institutions. The work investigated the features of the physical and virtual network architecture, designed a VLAN network. The network module was implemented in the Cisco Packet Tracer environment and tested for performance and security. The work considered the principles of network segmentation using VLAN, trunk port configuration, inter-VLAN routing and ACL access control lists.

The practical result was the creation of a model of an educational institution network with separate segments for students, teachers and administration, which provides increased manageability, security and efficiency of network resources.

Keywords: VPN, NETWORK INFRASTRUCTURE, INFORMATION SECURITY, WIREGUARD, OPENVPN, ACL, ROUTING, NETWORK SEGMENTATION, CISCO PACKET TRACER.

ЗМІСТ

ВСТУП

Комп'ютерна мережа є фундаментальним компонентом сучасної установи, інтегруючи комп'ютери, сервери, мережеві принтери, точки бездротового доступу, системи відеоспостереження та інші пристрої у єдину систему для обміну даними. Вона забезпечує користувачам доступ до інформації, спільних ресурсів, передачу файлів та функціонування внутрішніх сервісів. Ефективність функціонування, стабільність підключення та безпека даних значною мірою залежать від належної організації мережевої інфраструктури.

Базова архітектура локальної мережі передбачає підключення всіх пристроїв до одного або кількох комутаторів у спільному мережевому сегменті. Така конфігурація є прийнятною на початкових етапах розвитку мережі, коли кількість користувачів і пристроїв обмежена. Однак зі зростанням масштабу мережі виникає необхідність у більш чіткому логічному поділі. Збереження всіх пристроїв в одному логічному сегменті призводить до ускладнення адміністрування, зниження ефективності контролю доступу та зростання мережевого навантаження [1].

Кожна функціональна група всередині установи має свої специфічні вимоги до доступу до мережевих ресурсів. Наприклад, обґрунтованим є розмежування мережевих сегментів для комп'ютерів адміністрації, студентів та викладачів. У традиційних мережах, що не мають логічного поділу, реалізація такого розмежування є значно ускладненою [2].

Для розв'язання цієї проблеми застосовується технологія VLAN, яка дозволяє розділяти єдину фізичну мережу на кілька незалежних логічних сегментів. Пристрої можуть бути об'єднані у групи не тільки за фізичним розташуванням, а й за функціональним призначенням. Наприклад, можуть бути створені окремі VLAN для студентів, викладачів та адміністративного

персоналу. Це сприяє підвищенню прозорості та упорядкованості мережевої структури.

Впровадження VLAN сприяє мінімізації небажаних взаємодій між різними групами пристроїв, спрощує управління мережею та підвищує її організованість. Адміністратор отримує можливість здійснювати окремий контроль доступу між сегментами та ефективніше моніторити роботу системи.

Об'єктом дослідження є мережева інфраструктура закладу та процеси організації мережевої взаємодії між її користувачами, сервісами й інформаційними ресурсами.

Предмет дослідження – принципи, технології та засоби побудови традиційної та віртуальної мережі закладу.

Мета роботи – провести порівняльний аналіз структури фізичної та віртуальної мережі, розробити модель VLAN-мережі з виділеними сегментами, зіставити її з мережею без логічного поділу та визначити переваги використання технології VLAN.

Для досягнення цієї мети передбачається виконання наступних кроків:

- Розглянути принципи фізичної реалізації комп'ютерної мережі.
- Охарактеризувати особливості віртуальної мережі.
- Провести порівняльний аналіз фізичної та віртуальної структур мережі.
- Розробити модель VLAN-мережі.
- Здійснити аналіз функціонування розробленої моделі.
- Визначити переваги застосування VLAN порівняно з класичною мережею без логічного поділу.

Практичне значення роботи полягає у розробленні архітектури віртуальної мережі навчального закладу, яка забезпечує ефективне використання мережевих ресурсів, підвищує рівень інформаційної безпеки, спрощує адміністрування мережної інфраструктури та створює умови для гнучкого масштабування інформаційних сервісів. Запропоновані рішення можуть бути використані під час модернізації існуючих локальних мереж

закладів освіти, впровадження дистанційного навчання, організації доступу до хмарних ресурсів та оптимізації роботи комп'ютерних лабораторій і серверних систем.

РОЗДІЛ 1 СТРУКТУРА ФІЗИЧНОЇ ТА ВІРТУАЛЬНОЇ МЕРЕЖ

1.1 Структура фізичної реалізації комп'ютерної мережі

Фізична реалізація комп'ютерної мережі визначає її матеріальну основу, включаючи обладнання, кабелі, способи з'єднання та топологію [1]. Вона забезпечує передавання даних між пристроями та зовнішніми мережами. Така інфраструктура має бути масштабованою, керованою та здатною підтримувати різноманітні підключення. Її проєктування охоплює не лише прокладання комунікацій, а й вибір активного обладнання та планування майбутнього розширення.

Основою дротових сегментів більшості локальних мереж є технологія Ethernet. Вона забезпечує стандартизоване підключення кінцевих пристроїв до комутаторів, формуючи базове середовище обміну інформацією. Завдяки Ethernet дозволяє інтегрувати обладнання різних виробників, підтримувати різні швидкості та гнучко розширювати мережу.

Фізична структура мережі визначається її топологією, яка впливає на надійність та масштабованість. Для сучасних мереж найдоцільнішою є топологія «зірка» або її ієрархічне розширення, де пристрої підключаються до комутаторів, що дозволяє локалізувати несправності. У складних інфраструктурах застосовується багаторівнева побудова: рівень доступу для кінцевих пристроїв, рівень розподілу для агрегації трафіку та централізованого керування, а також магістральний рівень для високошвидкісного міжсегментного обміну.

Комутатор є ключовим елементом локальної мережі, забезпечуючи підключення пристроїв та пересилання кадрів. Його придатність для сучасної інфраструктури визначається кількістю портів, швидкістю, підтримкою керованих функцій та віртуальних локальних мереж [2].

Маршрутизатор виконує функцію передавання даних між різними мережами, забезпечуючи вихід до Інтернету та взаємодію із зовнішніми

ресурсами. У VLAN-мережах маршрутизація трафіку між віртуальними сегментами реалізується маршрутизатором або комутатором третього рівня [2].

Точки бездротового доступу інтегрують мобільні пристрої в локальну мережу, фізично з'єднуючись з комутаторами для забезпечення покриття. Їх розгортання залежить від площі, кількості користувачів та вимог до стабільності бездротового зв'язку. Основні елементи фізичної структури комп'ютерної мережі наведено у табл. 1.1.

Таблиця 1.1 – Основні елементи фізичної структури комп'ютерної мережі

Елемент мережі	Призначення	Приклад застосування
Комутатор	Об'єднання пристроїв у локальній мережі	Підключення комп'ютерів, принтерів, камер і точок доступу
Маршрутизатор	Передавання даних між мережами	Організація доступу до Інтернету та зв'язку між підмережами
Сервер	Надання внутрішніх мережевих служб	Зберігання файлів, робота баз даних, автентифікація
Точка доступу Wi–Fi	Підключення бездротових клієнтів	Доступ ноутбуків, планшетів і смартфонів
Кабельна система	Фізичне передавання сигналів	З'єднання робочих місць із комутаційним обладнанням
Патч–панелі	Упорядкування кабельних ліній	Організація підключень у телекомунікаційній шафі

Кабельна система є базовим компонентом мережевої інфраструктури. Її склад охоплює горизонтальні кабельні лінії, магістральні з'єднання, телекомунікаційні розетки, патч-корди та допоміжні монтажні елементи. Для підключення пристроїв, як правило, використовується мідний кабель "вита пара", тоді як оптичні лінії застосовуються для магістральних каналів, забезпечення зв'язку між поверхами або віддаленими комутаційними вузлами. Впровадження структурованого кабелювання сприяє упорядкованій побудові мережі. Кабельні лінії від робочих місць прокладаються до комутаційних шаф, де їх термінують на патч-панелях [1].

Надалі ці з'єднання встановлюються з портами комутаторів за допомогою коротких комутаційних шнурів. Цей підхід оптимізує технічне обслуговування, надає можливість оперативно змінювати конфігурацію підключень та мінімізує ймовірність помилок під час експлуатації. Комутаційні шафи використовуються для розміщення активного та пасивного мережевого обладнання, включаючи комутатори, маршрутизатори, патч-панелі, а також, за необхідності, серверні пристрої та джерела безперебійного живлення.

Централізоване розміщення обладнання спрощує обслуговування мережі та сприяє ефективній організації кабельних ліній. Для об'єктів значного масштабу рекомендується передбачати кілька телекомунікаційних вузлів, розташованих у стратегічно різних частинах будівлі [2]. При проєктуванні фізичної інфраструктури мережі необхідно враховувати перспективи її подальшого розширення. Це передбачає резервування портів на комутаторах, забезпечення можливості для інсталяції додаткових точок доступу, виділення вільного простору для нового обладнання у комутаційних шафах та планування кабельних маршрутів для майбутніх підключень. Недостатній облік цих аспектів може ускладнити модернізацію мережі та спричинити необхідність повторного монтажу. Поширені фізичні топології локальних мереж наведено у табл. 1.2.

Топології «зірка» та «дерево» визнаються оптимальними для мережі, оскільки вони забезпечують централізовану архітектуру підключень. Цей підхід є сумісним із застосуванням керованих комутаторів. Крім того, така конфігурація спрощує подальше розгортання технології VLAN, надаючи можливість логічної сегментації трафіку без внесення змін до фізичної схеми підключення пристроїв.

Фізична структура впливає також на надійність роботи мережі. Наявність чіткої схеми підключень, маркування портів, правильного розташування комутаційних вузлів і резерву обладнання скорочує час пошуку

несправностей. Наприклад, адміністратор може швидко визначити, до якого комутатора та порту під’єднаний конкретний комп’ютер або точка доступу. Відсутність такої організації може суттєво ускладнити відновлення функціональності мережі навіть у випадку незначних збоїв.

Таблиця 1.2 – Характеристика основних фізичних топологій мережі

Тип топології	Характеристика	Переваги	Недоліки
Зірка	Кожен пристрій підключений до центрального комутатора	Простота адміністрування, локалізація несправностей, зручне масштабування	Залежність роботи сегмента від центрального комутатора
Дерево	Кілька зіркоподібних сегментів об’єднуються в ієрархічну структуру	Придатність для великих мереж, поділ за зонами	Низька надійність, складна діагностика, обмежене масштабування
Шина	Усі пристрої працюють через спільну лінію зв’язку	Простота початкової побудови	Відмова окремої ділянки може порушити роботу сегмента
Кільце	Вузли послідовно утворюють замкнений контур	Впорядкований напрям передавання даних	

Хоча фізична реалізація мережі безпосередньо не визначає політику доступу користувачів, вона формує фундаментальну основу для її подальшої імплементації. За умови побудови мережі з використанням керованих комутаторів та упорядкованої схеми підключень, стає можливим впровадження VLAN-сегментації, конфігурація ізольованих підмереж для різних груп користувачів та організація маршрутизації між ними. Таким чином, якість фізичної інфраструктури має прямий вплив на ефективність наступних етапів проєктування системи.

Отже, фізична структура комп'ютерної мережі установи включає в себе активне мережеве обладнання, кабельну систему, комутаційні вузли та обрані

топологічні рішення. Вона детермінує технічні характеристики мережі, її надійність, потенціал до масштабування та готовність до подальшої логічної сегментації. Раціонально спроєктована фізична інфраструктура забезпечує стабільне функціонування мережевих сервісів та створює передумови для реалізації віртуальних мереж на основі технології VLAN.

1.2. Структура віртуальної мережі на основі VLAN

Фізична мережа забезпечує підключення пристроїв, проте не встановлює механізмів їх логічної сегментації. У корпоративних або освітніх мережах такі пристрої, як комп'ютери адміністрації, навчальні, сервери, гостьові бездротові клієнти та технічне обладнання, можуть використовувати спільну комутаційну інфраструктуру, проте вимагають диференційованих умов доступу та індивідуалізованого керування трафіком.

Задля вирішення цієї задачі використовується технологія віртуальних локальних мереж VLAN, яка дозволяє формувати ізольовані логічні сегменти в межах єдиної фізичної мережевої інфраструктури. Стандарт IEEE 802.1Q регламентує функціонування VLAN у мостових Ethernet-мережах. Віртуальна локальна мережа консолідує пристрої в окремий логічний сегмент, забезпечуючи їх функціонування як елементів однієї локальної мережі. Розподіл трафіку в такій конфігурації базується на приналежності пристрою до конкретної VLAN, а не на його фізичному розташуванні. Це дає змогу використовувати єдину кабельну та комутаційну інфраструктуру для обслуговування кількох функціонально відмінних мережевих груп.

У мережах застосування VLAN є доцільним для логічного відокремлення адміністративного сегмента, робочих станцій навчальних кабінетів, серверних ресурсів, гостьового доступу та технічного обладнання. Така сегментація спрощує керування мережею, оптимізує адресний простір і формує основу для подальшої конфігурації правил доступу між визначеними групами пристроїв. Однією з ключових функцій технології VLAN є створення

незалежних широкомовних доменів, див. рис.1.1. У мережах без сегментації VLAN широкомовні повідомлення поширюються по всьому комутованому сегменту.

Впровадження VLAN обмежує поширення таких повідомлень межами відповідної віртуальної мережі [3]. Цей механізм знижує надмірне розповсюдження службового трафіку, тим самим підвищуючи керованість мережевої інфраструктури.

Рисунок 1.1 – Приклад логічного поділу фізичної мережі на окремі VLAN

Кожна VLAN характеризується унікальним числовим ідентифікатором – VLAN_ID. Цей ідентифікатор застосовується для визначення приналежності кадру до конкретного логічного сегмента. Під час передачі даних між мережевими пристроями, що оперують з кількома VLAN, використовується механізм тегування кадрів згідно зі стандартом IEEE 802.1Q. До службового поля Ethernet-кадру додається інформація про VLAN ID, що дозволяє комутатору ідентифікувати віртуальну мережу, до якої належить трафік [4].

У мережах VLAN функціонують два ключові режими роботи портів комутатора: access (доступу) та trunk (магістральний). Порт доступу асоціюється з однією VLAN і призначений для підключення кінцевих пристроїв, таких як персональні комп'ютери, ноутбуки або принтери. Магістральний порт забезпечує передачу трафіку від кількох VLAN через

єдиний фізичний канал. Його застосовують для з'єднання комутаторів між собою або для підключення комутатора до маршрутизуючого пристрою.Основні компоненти VLAN–структури наведено у табл. 1.3.

Технологія VLAN дозволяє формувати мережеві групи на основі функціонального призначення пристроїв. Наприклад, комп'ютери викладачів, розташовані в різних аудиторіях та кабінетах, можуть належати до однієї VLAN. Водночас пристрої, фізично підключені до одного комутатора, можуть обслуговувати різні категорії користувачів і бути віднесені до різних логічних сегментів.

Таблиця 1.3 – Основні елементи віртуальної мережі на основі VLAN

Елемент	Сутність	Призначення
VLAN	Логічно ізольований сегмент мережі	Поділ груп користувачів і пристроїв
VLAN ID	Числовий ідентифікатор VLAN	Розмежування трафіку між сегментами
Access–порт	Порт, що належить до однієї VLAN	Підключення кінцевих пристроїв
Trunk–порт	Порт для передавання кількох VLAN	З’єднання комутаторів і маршрутизувальних пристроїв
802.1Q–тег	Службова позначка в Ethernet–кадрі	Визначення належності кадру до VLAN
Міжвланова маршрутизація	Передавання даних між різними VLAN	Організація контрольованої взаємодії сегментів

Такий підхід забезпечує більшу гнучкість в організації мережі порівняно з поділом, що базується виключно на фізичному розташуванні обладнання. На практиці кожній VLAN зазвичай присвоюється окрема IP-підмережа [5]. Цей підхід спрощує адресацію пристроїв, конфігурацію шлюзів та формування логічної схеми маршрутизації. Наприклад, для студентського сегмента може бути виділена одна підмережа, для викладачів – інша, а для адміністрації – третя. Це дозволяє систематизувати адресний простір і оперативно ідентифікувати приналежність пристрою до конкретного сегмента мережі.

Запропонована сегментація на VLAN дозволяє чітко відокремити основні категорії користувачів в інституційній мережі. Студентський сегмент

може бути виділений для комп'ютерів навчальних аудиторій та лабораторій, сегмент викладачів – для робочих місць педагогічного персоналу, а адміністративний сегмент – для службових комп'ютерів та внутрішніх ресурсів управління. Ця структура слугує логічною основою для подальшого проектування IP-адресації та конфігурації правил взаємодії між сегментами.

Пристрої, що належать до різних VLAN, не обмінюються даними безпосередньо на канальному рівні (рівень 2 моделі OSI) [5]. Для забезпечення взаємодії між ними необхідна міжвланова маршрутизація, яка реалізується за допомогою маршрутизатора або комутатора третього рівня (рівень 3 моделі OSI). Це надає адміністратору можливість визначити дозволені напрямки руху трафіку. Наприклад, адміністративний сегмент може отримати доступ до службових ресурсів, викладацька VLAN – до певних внутрішніх сервісів, а студентська VLAN – лише ті права доступу, які є необхідними для виконання навчальних завдань.

Застосування VLAN формує основу для систематизованого контролю доступу. Сегментація на VLAN сама по собі не є повноцінною заміною механізмів кіберзахисту, проте значно спрощує їх імплементацію. Після формування окремих логічних сегментів стає можливим застосування правил маршрутизації, списків контролю доступу (ACL) та інших засобів обмеження трафіку між групами пристроїв. Це має особливе значення для адміністративного сегмента, оскільки службові комп'ютери не повинні мати неконтрольованого доступу з боку інших користувацьких сегментів [5].

У мережах з множинними комутаторами ключову роль відіграють магістральні з'єднання. Вони забезпечують передачу трафіку від різних VLAN між комутаційними вузлами, що дозволяє підтримувати єдину логічну структуру мережі в межах розподіленої інфраструктури закладу. У випадках, коли пристрої студентського, викладацького або адміністративного сегментів підключені до різних комутаторів, trunk-канали забезпечують передачу

відповідного VLAN-трафіку між ними без необхідності створення окремого фізичного каналу для кожної групи, це показано на рисунку 1.2.

Передача трафіку кількох VLAN між комутаторами через магістральний порт є необхідною у випадках, коли ідентичні віртуальні мережі повинні функціонувати на різних комутаційних пристроях [6]. Приміром, пристрої VLAN_10 (Студенти) підключені як до комутатора S1, так і до S2, аналогічна ситуація спостерігається з VLAN_20 (Викладачі).

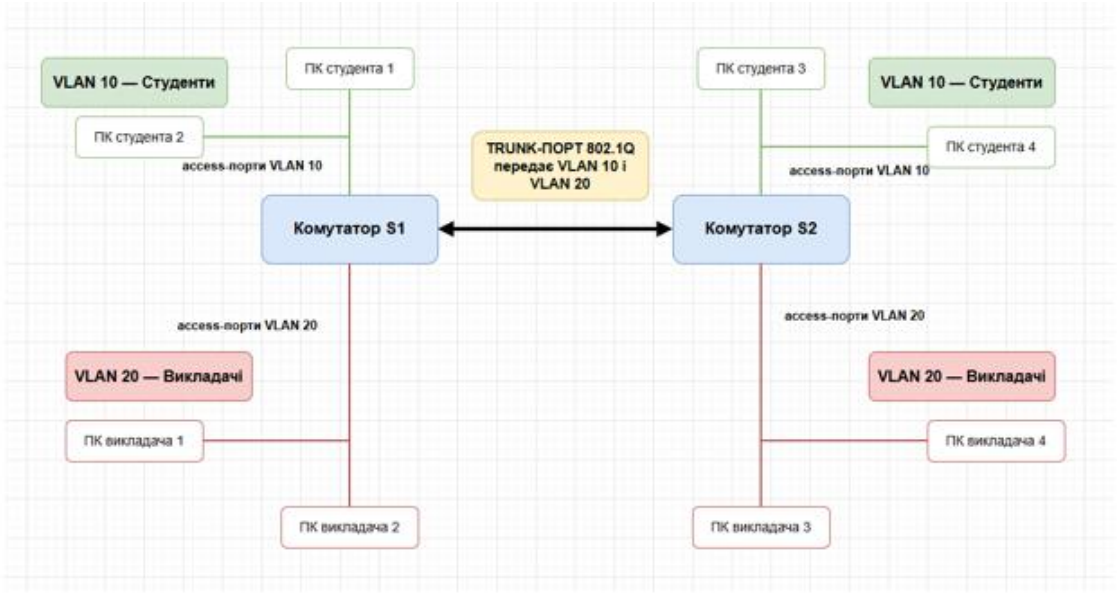

Рисунок 1.2 – Передавання трафіку між комутаторами

Для забезпечення обміну даними між комп'ютерами однієї VLAN, незалежно від їх фізичного підключення до різних комутаторів, між S1 та S2 встановлюється trunk-з'єднання [7]. Цим з'єднанням передається трафік від декількох VLAN одночасно. Комутатор, який отримав кадр від пристрою VLAN_10 або VLAN_20, додає до нього службову позначку стандарту 802.1Q, що містить номер VLAN. Надалі кадр передається через trunk-порт до цільового комутатора. Приймаючий комутатор зчитує VLAN-позначку, визначає приналежність трафіку до певного сегмента та скеровує його виключно на порти відповідної VLAN. Таким чином, єдиний фізичний канал між комутаторами може обслуговувати кілька логічних мереж без змішування трафіку різних сегментів, таких як студентський та викладацький.

1.3 Порівняння фізичної та віртуальної структури мережі

Фізична та віртуальна структури мережі описують різні аспекти її архітектури та функціонування. Фізична структура визначає матеріальне втілення інфраструктури, включаючи обладнання, кабельні лінії, комутаційні вузли, топологію та просторове розміщення пристроїв. Віртуальна структура, реалізована за допомогою VLAN, визначає логічний поділ цієї інфраструктури на дискретні сегменти, методи групування вузлів та правила взаємодії між ними.

Для інституційних мереж ефективним є не вибір між цими підходами, а їх інтегроване поєднання. Фізична мережа відповідає за забезпечення доступності з'єднання як базового технічного ресурсу. У разі відсутності кабелю, вільного порту комутатора або необхідного комутаційного вузла, підключення нового пристрою стає неможливим.

Віртуальна мережа не усуває цих фізичних обмежень, але дозволяє ефективніше організувати існуючу фізичну інфраструктуру. Один комутатор може обслуговувати кілька логічних сегментів одночасно, а функціональна сегментація користувачів не вимагає встановлення окремого апаратного забезпечення для кожної групи. Ключова відмінність полягає у принципі групування мережевих пристроїв. У фізичній структурі об'єднання пристроїв здебільшого визначається місцем їх підключення до конкретного комутатора або кабельної ділянки.

Натомість у VLAN-структурі приналежність пристрою до сегмента детермінується конфігурацією порту або логікою тегованого трафіку. Як наслідок, пристрої, що знаходяться в різних приміщеннях, можуть бути частиною одного логічного сегмента, тоді як пристрої в одному кабінеті – розподілені між різними VLAN. Це забезпечує можливість проектування мережі відповідно до організаційної структури закладу, а не виключно до

фізичної геометрії будівлі. Порівняння основних характеристик фізичної та віртуальної структури наведено у таблиці 1.4 [8].

Відмінність між фізичною та віртуальною моделями мережі стає особливо очевидною в процесі її масштабування. Фізичне розширення передбачає фізичне додавання кабелів, портів, комутаторів або формування нових комутаційних зон. Віртуальне розширення включає створення додаткової VLAN, модифікацію конфігурації портів та налаштування відповідної маршрутизації.

Таблиця 1.4 – Порівняння фізичної та віртуальної структури мережі

Ознака	LAN	VLAN
Предмет організації	Обладнання та кабельні з'єднання	Логічні сегменти й трафік
Основа побудови	Топологія, порти, кабелі, комутаційні шафи	VLAN ID, access–порти, trunk–порти
Критерій групування	Розташування та підключення	Функціональне призначення пристроїв
Зміна структури	Монтаж або перепідключення	Зміна конфігурації
Межі широкомовного трафіку	Фізичний комутований сегмент	Окрема VLAN
Підтримка контролю доступу	Обмежена	Створює основу для логічного розмежування
Масштабування	Через розширення обладнання	Через додавання логічних сегментів на наявній основі

Хоча це не виключає потреби у фізичних ресурсах, такий підхід дозволяє зробити розвиток мережі більш передбачуваним та керованим. Фізична структура мережі має фундаментальне значення для її надійності. Неправильно організована кабельна система, відсутність резервних портів або хаотичне розміщення обладнання суттєво ускладнюють експлуатацію мережі, незалежно від якості конфігурації VLAN. Віртуальна структура не компенсує недоліків фізичної реалізації, натомість використовує її як базову платформу.

Отже, пріоритетним є створення впорядкованої кабельної інфраструктури, після чого може бути здійснена логічна сегментація мережі.

Віртуальна структура надає суттєві переваги в адмініструванні мережі. При зміні функціонального призначення робочого місця адміністратор може перепризначити порт до іншої VLAN без необхідності фізичного перепідключення кабелю. У випадку, якщо певна група пристроїв потребує ізоляції від інших, достатньо віднести її до окремого логічного сегмента та налаштувати відповідні правила міжвланової взаємодії. Ця гнучкість є особливо актуальною де склад користувачів, обсяг обладнання та вимоги до доступу до ресурсів можуть динамічно змінюватися. Порівняння особливостей експлуатації обох підходів наведено у таблиці 1.5.

Таблиця 1.5 – Особливості експлуатації фізичної та VLAN–структури

Критерій	LAN	VLAN–структура
Підключення нового пристрою	Потребує порту та кабельної лінії	Потребує призначення порту до відповідної VLAN
Зміна функціональної належності пристрою	Може вимагати перепідключення	Реалізується налаштуванням порту
Розподіл за групами користувачів	Відображається фізично	Відображається логічно
Робота з широкомовним трафіком	Залежить від фізичного сегмента	Обмежується межами VLAN
Реакція на організаційні зміни	Повільніша	Швидша

Фізична структура та сегментація на основі VLAN також демонструють відмінності у впливі на безпеку мережі. Само по собі фізичне розміщення пристроїв не забезпечує логічного відокремлення трафіку. У ситуації, коли адміністративні комп'ютери, гостьові пристрої та технічне обладнання перебувають в одному широкомовному домені, мережа залишається недостатньо структурованою.

VLAN створює логічні межі між такими групами, а міжвланова маршрутизація надає інструменти для регламентації дозволених напрямків передачі даних. У практичному сенсі це підвищує керованість налаштувань безпеки, хоча повний захист вимагає впровадження додаткових політик доступу. Крім того, використання VLAN сприяє зменшенню обсягів

широкомовного трафіку, що позитивно впливає на продуктивність мережі та ефективність використання її ресурсів. Логічна сегментація також спрощує адміністрування мережевої інфраструктури, оскільки дозволяє групувати користувачів відповідно до їхніх функціональних ролей незалежно від фізичного розташування обладнання. Водночас впровадження VLAN потребує належного налаштування комутаційного обладнання та міжвланової маршрутизації, а також постійного контролю конфігурації мережі для запобігання помилкам і несанкціонованому доступу. Переваги та обмеження обох підходів наведено у таблиці 1.6.

Фізична структура мережі формує технічну основу її функціонування, тоді як віртуальна структура, реалізована за допомогою VLAN, підвищує гнучкість, керованість та упорядкованість передачі даних.

Таблиця 1.6 – Переваги та обмеження фізичної та віртуальної організації мережі

Тип структури	Переваги	Недоліки
LAN	1. Забезпечує реальне підключення всіх пристроїв до мережі. 2. Дає стабільну основу для передавання даних через кабелі, комутатори та маршрутизатори. 3. Дозволяє чітко визначити місце підключення кожного вузла. 4. Спрощує пошук апаратних несправностей за наявності правильної схеми кабелювання. 5. Підтримує підключення різних типів обладнання: ПК, серверів, принтерів, точок доступу, пристроїв.	1. Поділ користувачів залежить від фізичного розташування та кабельних підключень. 2. Зміна структури мережі часто потребує перепідключення кабелів або встановлення додаткового обладнання. 3. Для окремого виділення груп користувачів без VLAN може знадобитися більша кількість комутаторів. 4. Масштабування мережі пов’язане з монтажними роботами та додатковими витратами. 5. Сама по собі не забезпечує логічної ізоляції студентів, викладачів та адміністрації.
VLAN	1. Дозволяє поділити одну фізичну мережу на окремі логічні сегменти. 2. Дає змогу відокремити студентів, викладачів та адміністрацію без створення окремої кабельної мережі для кожної групи.	1. Потребує керованих комутаторів із підтримкою VLAN. 2. Вимагає точного налаштування VLAN ID, access–портів, trunk–портів і маршрутизації.

	3. Зменшує поширення широкомовного трафіку завдяки окремим broadcast–доменам. 4. Полегшує адміністрування: зміну належності пристрою до сегмента можна виконати через налаштування порту комутатора. 5. Створює основу для керованої міжвланової маршрутизації та обмеження доступу між сегментами. 6. Ефективніше використовує наявну комутаційну інфраструктуру.	3. Помилки конфігурації можуть призвести до втрати доступу до окремих ресурсів. 4. Для обміну даними між різними VLAN необхідна міжвланова маршрутизація. 5. VLAN не замінює повноцінні засоби кіберзахисту, а лише створює основу для подальшого контролю доступу.

Для побудови мережі навчального закладу оптимальним є поєднання обох підходів: якісно спроектованої фізичної інфраструктури та логічної сегментації на VLAN для студентського, викладацького та адміністративного персоналу. Такий підхід дозволяє забезпечити надійне функціонування мережевого обладнання та каналів зв'язку, одночасно створюючи гнучку систему керування мережевим трафіком і доступом до ресурсів. Фізична структура формує основу для стабільного передавання даних, тоді як VLAN забезпечує раціональний розподіл користувачів за функціональними групами, зменшує обсяг широкомовного трафіку та спрощує адміністрування мережі.

У результаті досягається підвищення продуктивності, безпеки та масштабованості мережевої інфраструктури, що є особливо важливим для сучасних закладів освіти з великою кількістю користувачів та інформаційних сервісів.

РОЗДІЛ 2 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВІРТУАЛЬНОЇ МЕРЕЖІ

2.1 Проєктування структури VLAN та IP–адресації

Для побудови моделі віртуальної мережі використовується середовище Cisco Packet Tracer, що є доцільним завдяки його можливостям щодо проєктування, налаштування та тестування мережевих рішень без необхідності використання реального мережевого обладнання. Даний програмний засіб дозволяє моделювати роботу маршрутизаторів, комутаторів та кінцевих пристроїв, виконувати налаштування VLAN, trunk-з'єднань, міжвланової маршрутизації та списків контролю доступу ACL із використанням командного інтерфейсу, наближеного до реальних пристроїв Cisco. Крім того, Packet Tracer надає можливість візуального спостереження за передаванням пакетів у режимі моделювання, що спрощує аналіз мережевих процесів і перевірку правильності конфігурації [7].

У межах роботи було створено модель локальної мережі, яка складається з маршрутизатора, п'яти комутаторів і кінцевих пристроїв, розподілених між кількома логічними сегментами, архітектура якої показана на рисунку 2.1. Основною метою побудови такої мережі є демонстрація роботи VLAN–сегментації та міжвланової маршрутизації.

У моделі використано каскадну фізичну структуру комутаторів. Комутатори з'єднані між собою послідовно, утворюючи ланцюг передавання трафіку. Маршрутизатор R1 підключений до нижнього комутатора S5, після чого трафік передається через інші комутатори мережі. Така структура дозволяє показати, що VLAN можуть функціонувати не лише на одному комутаторі, а й поширюватися через кілька комутаційних пристроїв за допомогою trunk–з'єднань.

У мережі створено три основні логічні сегменти:

- VLAN_10 – студентський сегмент;
- VLAN_20 – сегмент викладачів;

- VLAN_30 – адміністративний сегмент.

Особливістю цієї моделі є те, що пристрої однієї VLAN розміщені не на одному окремому комутаторі, а розподілені між кількома комутаторами [8].

Наприклад, студентські ПК підключені до різних комутаторів, але логічно належать до VLAN_10. Аналогічно комп'ютери викладачів належать до VLAN_20, а комп'ютери адміністрації – до VLAN_30. Це демонструє основну перевагу: логічна структура мережі не залежить від фізичного місця підключення пристрою.

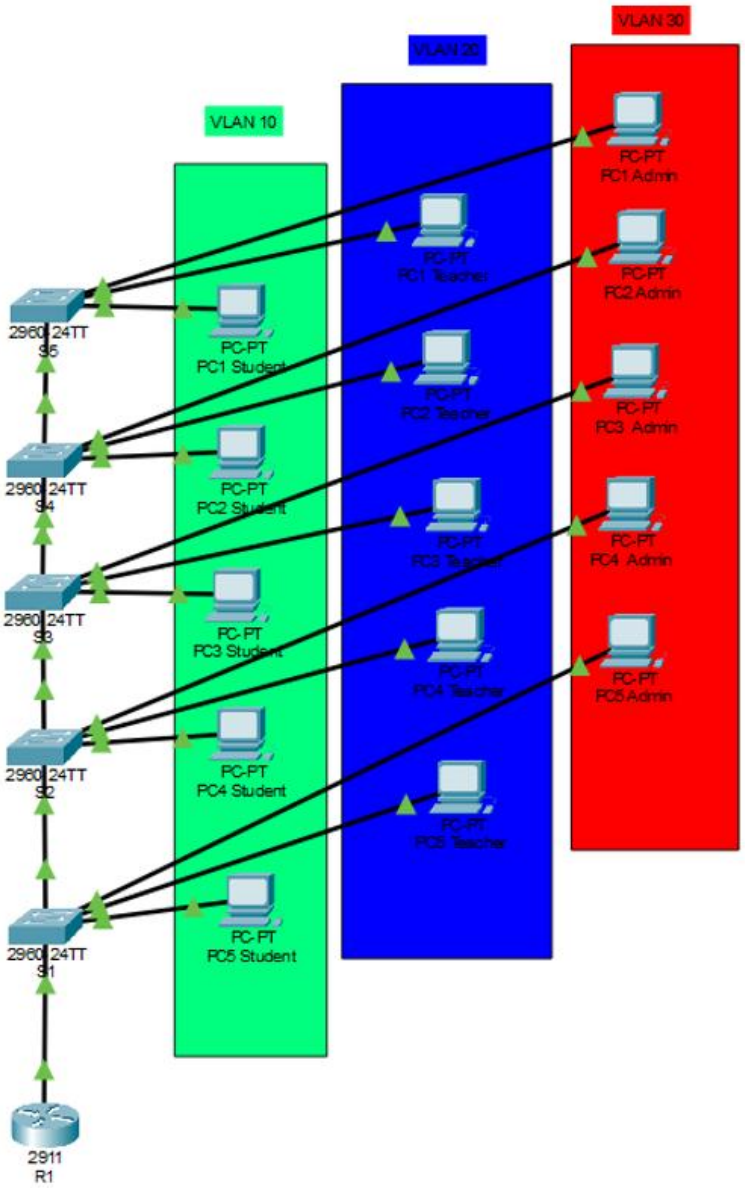

Рисунок 2.1 – Модель VLAN в програмному середовищі Cisco Packet Tracer

Оскільки в кожному сегменті використовується по п’ять комп’ютерів, IP–адреси кінцевих пристроїв було призначено послідовно. Для зручності шлюз кожної VLAN має адресу з останнім октетом *.1, а адреси комп’ютерів починаються з *.11 [9].

Таблиця 2.2 – Адресація пристроїв

Сегмент	Пристрій	IP–адреса	Шлюз
Студенти	PC1 VLAN10	192.168.10.11	192.168.10.1
Студенти	PC2 VLAN10	192.168.10.12	192.168.10.1
Студенти	PC3 VLAN10	192.168.10.13	192.168.10.1
Студенти	PC4 VLAN10	192.168.10.14	192.168.10.1
Студенти	PC5 VLAN10	192.168.10.15	192.168.10.1
Викладачі	PC1 VLAN20	192.168.20.11	192.168.20.1
Викладачі	PC2 VLAN20	192.168.20.12	192.168.20.1
Викладачі	PC3 VLAN20	192.168.20.13	192.168.20.1
Викладачі	PC4 VLAN20	192.168.20.14	192.168.20.1
Викладачі	PC5 VLAN20	192.168.20.15	192.168.20.1
Адміністрація	PC1 VLAN30	192.168.30.11	192.168.30.1
Адміністрація	PC2 VLAN30	192.168.30.12	192.168.30.1
Адміністрація	PC3 VLAN30	192.168.30.13	192.168.30.1
Адміністрація	PC4 VLAN30	192.168.30.14	192.168.30.1
Адміністрація	PC5 VLAN30	192.168.30.15	192.168.30.1

Шлюзи VLAN реалізовано на маршрутизаторі R1 за допомогою підінтерфейсів. Для VLAN_10 використовується підінтерфейс GigabitEthernet0/0.10, для VLAN_20 – GigabitEthernet0/0.20, а для VLAN_30 – GigabitEthernet0/0.30. Такий спосіб організації називається Router–on–a–Stick. Він дозволяє виконувати маршрутизацію між кількома VLAN через один фізичний інтерфейс маршрутизатора. Це показано на рис. 2.3

```
Router#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  up                    down
Router#
```

Рисунок 2.2 – Фізичний інтерфейс маршрутизатора

2.2 Налаштування VLAN, trunk–портів і маршрутизації між VLAN

Після створення фізичної топології було виконано налаштування VLAN на комутаторах. Оскільки пристрої VLAN_10, VLAN_20 і VLAN_30 розміщені на різних комутаторах, відповідні VLAN необхідно створити на всіх комутаторах, через які проходить трафік цих сегментів.

На кожному комутаторі було створено VLAN_10, VLAN_20 і VLAN_30, це показано на рис 2.3

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name students
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name teachers
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name admin
```

Рисунок 2.3 – Налаштування комутатора для створення VLAN

Після створення VLAN було налаштовано порти, до яких підключені пристрої. Такі порти працюють у режимі access. Це означає, що кожен порт належить лише до однієї VLAN. Приклад налаштування портів продемостровано на рис. 2.4

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```

Рисунок 2.4 – Налаштування access-портів на комутаторі

Оскільки комутатори S1–S5 з’єднані послідовно, міжкомутаторні з’єднання налаштовано в режимі trunk. Trunk–порти передають трафік кількох VLAN через один фізичний канал. У цій мережі через trunk–з’єднання передається трафік VLAN_10, VLAN_20 і VLAN_30.

Таблиця 2.5 – Призначення trunk–з’єднань у мережі

З’єднання	Тип порту	VLAN, що передаються
R1 ↔ S5	Trunk	VLAN_10, VLAN_20, VLAN_30
S5 ↔ S4	Trunk	VLAN_10, VLAN_20, VLAN_30
S4 ↔ S3	Trunk	VLAN_10, VLAN_20, VLAN_30
S3 ↔ S2	Trunk	VLAN_10, VLAN_20, VLAN_30
S2 ↔ S1	Trunk	VLAN_10, VLAN_20, VLAN_30

```
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

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

Switch(config-if)#switchport trunk allowed 10,20,30
                                           ^
```

Рисунок 2.6 – Приклад налаштування trunk–порту на комутаторі:

Якщо комутатор має два з’єднання з іншими комутаторами, trunk потрібно налаштувати на обох відповідних портах. По такому ж принципу як показано вище.

```
Switch#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      10,20,30
Gig0/2      10,20,30

Port        Vlans allowed and active in management domain
Gig0/1      10,20,30
Gig0/2      10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30
Gig0/2      10,20,30
```

Рисунок 2.7 – Перевірка trunk–портів

На маршрутизаторі R1 було налаштовано підінтерфейси для кожної VLAN, див. рис.1.6 [10]. Саме ці підінтерфейси виконують роль шлюзів для відповідних підмереж.

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#no shut

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

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

Router(config-if)#exit
Router(config)#int g0/0.10
Router(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/0.20
Router(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.20, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/0.30
```

```
Router(config)#int g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#ex
```

Рисунок 2.8 – Налаштування інтерфейсів

Після створення підінтерфейсів маршрутизатор R1 отримав можливість пересилати трафік між VLAN_10, VLAN_20 і VLAN_30. Якщо комп’ютер студентського сегмента звертається до комп’ютера викладацького сегмента, пакет спочатку надходить до шлюзу VLAN_10, тобто до підінтерфейсу GigabitEthernet0/0.10. Далі маршрутизатор визначає мережу призначення та пересилає пакет до відповідного сегмента. Так само з іншими комп’ютерами.

2.3 Тестування працездатності та безпеки мережі

Після завершення налаштування VLAN, trunk–портів і підінтерфейсів маршрутизатора було виконано тестування працездатності мережі. Основним способом перевірки стала команда ping, яка дозволяє визначити, чи доставляються пакети між пристроями [11].

Спочатку було перевірено зв’язок у межах кожного логічного сегмента. Для цього з одного комп’ютера VLAN_10 було виконано ping до іншого комп’ютера цієї ж VLAN. Аналогічно перевірявся зв’язок між пристроями VLAN_20 і VLAN_30. Успішна доставка пакетів у межах одного сегмента

підтверджує правильність налаштування access–портів і належність пристроїв до відповідних VLAN.

Наступним етапом було перевірено доступність шлюзів, див. Додаток А.

Успішна відповідь від шлюзів підтверджує, що підінтерфейси маршрутизатора налаштовані правильно, а trunk–з'єднання між маршрутизатором і комутатором передає трафік відповідних VLAN.

Після цього було перевірено міжвланову маршрутизацію. Для цього виконувалось передавання пакетів між пристроями різних VLAN. Наприклад, з комп'ютера студентського сегмента було виконано ping до комп'ютера викладача та до комп'ютера адміністрації. Оскільки ці пристрої належать до різних IP–підмереж, пакет передається не напряму, а через маршрутизатор R1.

Таблиця 2.6 – Тестування мережі

Перевірка	Команда	Очікуваний результат	Фактичний результат
Зв'язок між ПК у VLAN_10	ping 192.168.10.12	Пакети доставляються	Успішно
Зв'язок між ПК у VLAN_20	ping 192.168.20.12	Пакети доставляються	Успішно
Зв'язок між ПК у VLAN_30	ping 192.168.30.12	Пакети доставляються	Успішно
Доступ ПК VLAN_10 до свого шлюзу	ping 192.168.10.1	Пакети доставляються	Успішно
Доступ ПК VLAN_20 до свого шлюзу	ping 192.168.20.1	Пакети доставляються	Успішно
Доступ ПК VLAN_30 до свого шлюзу	ping 192.168.30.1	Пакети доставляються	Успішно
Зв'язок VLAN_10 з VLAN_20	ping 192.168.20.11	Пакети доставляються	Успішно
Зв'язок VLAN_10 з VLAN_30	ping 192.168.30.11	Пакети доставляються	Успішно
Перевірка trunk–портів	show interfaces trunk	Пакети доставляються	Успішно
Перевірка створених VLAN	show vlan brief	Пакети доставляються	Успішно

За результатами тестування встановлено, що створена VLAN–мережа працює коректно. Пристрої в межах одного логічного сегмента успішно обмінюються пакетами, шлюзи кожної VLAN доступні, а міжвланова маршрутизація через маршрутизатор R1 забезпечує зв’язок між VLAN_10, VLAN_20 і VLAN_30. Також перевірка команд show interfaces trunk і show vlan brief підтвердила правильність налаштування trunk–портів та створених VLAN на комутаторах. Під час тестування в режимі Simulation Mode було встановлено, що під час передавання пакета між різними VLAN трафік спочатку надходить до маршрутизатора. Наприклад, якщо комп’ютер студентського сегмента VLAN_10 надсилає пакет до комп’ютера викладацького сегмента VLAN_20, то пакет передається до шлюзу 192.168.10.1, після чого маршрутизатор пересилає його до підмережі 192.168.20.0/24. Це підтверджує правильність роботи міжвланової маршрутизації [12].

Для перевірки безпеки мережі можна застосувати список контролю доступу ACL. Наприклад, доцільно обмежити доступ студентського сегмента до адміністративного сегмента. До застосування ACL пакети між VLAN_10 і VLAN_30 доставляються успішно, що підтверджує працездатність маршрутизації. Після застосування ACL доступ із мережі студентів до адміністративної мережі блокується. Це показано на рис. 2.10

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
```

Рисунок 2.9 – Налаштування ACL

На рисунку показано створення списку контролю доступу ACL на маршрутизаторі R1. Перше правило забороняє передавання IP-трафіку зі студентської мережі 192.168.10.0/24 до адміністративної мережі 192.168.30.0/24. Друге правило дозволяє весь інший трафік, щоб не

заблокувати обмін даними між дозволеними сегментами мережі. Така ACL використовується для обмеження доступу студентського сегмента VLAN_10 до адміністративного сегмента VLAN_30.

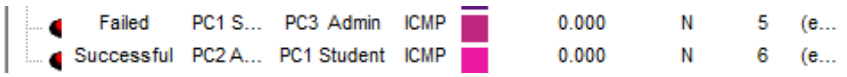

Рисунок 2.10 – Перевірка роботи ACL

Показано результат перевірки доступу між VLAN після налаштування ACL. Пакет від комп’ютера студентського сегмента до комп’ютера адміністрації не був доставлений, що підтверджує блокування доступу з VLAN_10 до VLAN_30. Водночас пакет з адміністративного сегмента до студентського комп’ютера доставлений успішно. ACL обмежує саме заданий напрямок трафіку та не блокує всю роботу мережі.

РОЗДІЛ 3 АНАЛІЗ РЕЗУЛЬТАТІВ VLAN–МЕРЕЖІ

3.1 Перевірка роботи створеної мережі

У рамках дослідження розроблено та реалізовано модель локальної мережі освітнього закладу із застосуванням технології VLAN. Архітектура створеної мережі включає маршрутизатор R1, комутатори S1–S5 та кінцеві пристрої користувачів [12].

З метою логічної сегментації мережевого середовища було конфігуровано три віртуальні локальні мережі (VLAN) [13]: VLAN 10 для студентів, VLAN 20 для викладачів та VLAN 30 для адміністрації. Кожній VLAN було призначено окрему IP-підмережу. Студентський сегмент використовує адресний простір 192.168.10.0/24, сегмент викладачів — 192.168.20.0/24, а адміністративний сегмент — 192.168.30.0/24.

Зазначений підхід забезпечує структуризацію адресного простору мережі та спрощує її адміністрування. Для функціонування VLAN на комутаторах було конфігуровано відповідні віртуальні мережі, а порти асоційовано з визначеними сегментами. З'єднання між комутаторами конфігуровано в режимі trunk, що забезпечує передачу трафіку декількох VLAN через єдиний фізичний канал зв'язку. З метою організації взаємодії між логічними сегментами реалізовано міжвланову маршрутизацію за технологією Router-on-a-Stick [12].

На маршрутизаторі R1 конфігуровано підінтерфейси для кожної VLAN, що виконують функцію шлюзів за замовчуванням. Передача трафіку між VLAN здійснюється через маршрутизатор із застосуванням стандарту IEEE 802.1Q. Проведено тестування працездатності розробленої мережі. Отримані результати підтвердили коректний обмін даними між пристроями в межах однієї VLAN, успішний доступ до шлюзів за замовчуванням, а також коректне функціонування міжвланової маршрутизації.

Додатково було підтверджено працездатність trunk-з'єднань між комутаторами. З метою підвищення рівня безпеки мережі було конфігуровано списки контролю доступу (ACL). За допомогою ACL реалізовано обмеження доступу між окремими сегментами мережі, що дало змогу продемонструвати механізми контролю мережевого трафіку та захисту службових ресурсів від несанкціонованого доступу.

3.2 Аналіз безпеки та ізоляції VLAN

У практичній моделі для цього можна створити правило, яке забороняє трафік з мережі 192.168.10.0/24 до мережі 192.168.30.0/24. Це означає, що пристрої студентського сегмента не зможуть звертатися до адміністративних комп'ютерів. Водночас, інші дозволені напрямки зв'язку можуть залишатися доступними. Наприклад, студентський сегмент може мати доступ до викладацького сегмента, якщо це передбачено архітектурою мережі. ACL доцільно застосовувати на підінтерфейсі GigabitEthernet0/0.10 у напрямку вхідного трафіку [13]. Саме через цей підінтерфейс трафік студентського сегмента надходить до маршрутизатора. Заборона небажаного трафіку на вході до маршрутизатора дозволяє ефективно відкидати пакети, які не повинні потрапляти до адміністративної VLAN.

Після застосування ACL перевірка виконується за допомогою команди ping. До налаштування ACL ping з комп'ютера VLAN_10 до комп'ютера VLAN_30 успішно проходить. Після застосування правила доступу пакети з VLAN_10 до VLAN_30 не повинні доставлятися. Якщо при цьому зв'язок з дозволеними сегментами залишається працездатним, це підтверджує правильність налаштування ACL.

Крім ACL, важливу роль у безпеці відіграє коректне налаштування портів комутаторів [2]. Порти, до яких підключені кінцеві пристрої, повинні функціонувати в режимі access і належати виключно до відповідної VLAN. Наприклад, порт студентського комп'ютера має бути призначений до

VLAN_10, порт комп'ютера викладача – до VLAN_20, а порт адміністративного комп'ютера – до VLAN_30. Помилкове призначення порту до іншої VLAN може порушити логічну структуру мережі. Також важливо правильно налаштовувати trunk-порти. У розгорнутій мережі trunk-з'єднання передають трафік VLAN_10, VLAN_20 та VLAN_30 між комутаторами S1–S5 та маршрутизатором R1.

Неправильне налаштування списку дозволених VLAN на trunk-порті, або дозвіл зайвих VLAN, може ускладнити контроль трафіку. Тому доцільно дозволяти на trunk лише ті VLAN, які активно використовуються в мережі. У розробленій мережі ізоляція VLAN забезпечує чіткий поділ студентів, викладачів та адміністрації [14].

Студентські комп'ютери функціонують у власному сегменті, викладацькі – у своєму, а адміністративні – в окремому службовому сегменті. Такий підхід спрощує адміністрування, полегшує діагностику несправностей та створює основу для подальшого впровадження правил доступу. Аналіз безпеки показав, що VLAN-сегментація підвищує керованість мережі та забезпечує базову логічну ізоляцію між групами користувачів.

Самі VLAN не є повною заміною спеціалізованих засобів захисту, але вони формують необхідну основу для контролю трафіку. У поєднанні з міжвлановою маршрутизацією та ACL така структура дозволяє обмежувати небажану взаємодію між сегментами, зокрема заборонити доступ студентського сегмента до адміністративного. Таким чином, розгорнута VLAN-мережа є не лише функціональною, а й більш керованою з погляду безпеки.

3.3 Переваги впровадження VLAN у мережі закладу

Впровадження технології VLAN у мережеву інфраструктуру установи підвищує її керованість, упорядкованість та адаптивність. У запропонованій моделі мережа сегментована на три логічні віртуальні локальні мережі:

VLAN_10 для студентів, VLAN_20 для викладачів та VLAN_30 для адміністративного персоналу. Такий розподіл відповідає організаційній структурі установи, оскільки різні групи користувачів мають відмінні функціональні завдання та потребують різного рівня доступу до мережевих ресурсів.

Основна перевага VLAN полягає у можливості логічної сегментації єдиної фізичної мережі на кілька ізольованих доменів [2]. Без використання VLAN усі пристрої функціонували б у спільному широкомовному домені. У такій конфігурації пристрої студентів, викладачів та адміністративного персоналу не мали б чіткого розмежування, що ускладнювало б адміністрування та реалізацію політик доступу.

Інтеграція VLAN дозволяє кожній групі пристроїв отримати власний логічний сегмент. У розробленій мережі комп'ютери студентів віднесені до VLAN_10, викладачів – до VLAN_20, а адміністративного персоналу – до VLAN_30. Це дозволяє оперативно ідентифікувати приналежність пристрою до конкретної групи та здійснювати диференційоване управління кожним сегментом. Такий підхід робить мережеву архітектуру більш прозорою для адміністратора та спрощує подальше технічне обслуговування.

Суттєвою перевагою VLAN є незалежність логічної структури мережі від фізичного розташування пристроїв. У практичній моделі комутатори S1–S5 з'єднані каскадно. Проте пристрої, що належать до однієї VLAN, можуть бути підключені до різних комутаторів. Наприклад, студентські комп'ютери можуть бути розподілені по різних фізичних ділянках мережі, але логічно залишатися частиною єдиного студентського сегмента. Ця особливість ілюструє гнучкість VLAN-сегментації. Ще однією перевагою є зниження обсягу широкомовного трафіку. У мережі без VLAN широкомовні повідомлення поширюються на всі пристрої у великому спільному домені. Це створює надмірне навантаження та знижує продуктивність мережі зі зростанням кількості пристроїв.

Після поділу на VLAN широкомовний трафік обмежується межами відповідного сегмента. Наприклад, службові повідомлення студентського сегмента не поширюються безпосередньо у викладацький або адміністративний сегменти. VLAN також сприяє ефективнішому використанню наявної фізичної інфраструктури. Для створення окремих сегментів не потрібно прокладати окремі кабельні мережі для студентів, викладачів та адміністрації.

Достатньо конфігурувати VLAN на комутаторах та призначити порти до відповідних сегментів. Trunk-з'єднання між комутаторами забезпечують передачу трафіку кількох VLAN через єдиний фізичний канал. У розробленій мережі через trunk-з'єднання передається трафік VLAN_10, VLAN_20 та VLAN_30. Це зберігає логічний поділ мережі навіть за умови підключення пристроїв до різних комутаторів. Такий підхід є оптимальним для мережі установи, де комп'ютери різних груп користувачів можуть бути розташовані у різних приміщеннях.

Окремою перевагою є спрощення адміністрування. У разі потреби зміни приналежності пристрою до іншого сегмента адміністратору не потрібно фізично перепідключати кабель. Достатньо змінити конфігурацію порту комутатора. Наприклад, порт може бути переведений з VLAN_10 до VLAN_20, якщо пристрій необхідно перемістити зі студентського сегмента до сегмента викладачів. Це мінімізує кількість фізичних змін у мережі та скорочує час обслуговування.

Використання окремих IP-підмереж для кожної VLAN також є перевагою. У створеній моделі студентський сегмент використовує мережу 192.168.10.0/24, сегмент викладачів – 192.168.20.0/24, а адміністративний сегмент – 192.168.30.0/24. Такий розподіл дозволяє оперативно визначати приналежність пристрою до певної VLAN за його IP-адресою. Це спрощує моніторинг функціонування мережі, діагностику несправностей та ведення документації. Впровадження VLAN створює основу для контролю доступу

між сегментами. У розробленій мережі обмін даними між VLAN здійснюється через маршрутизатор R1. Це означає, що пристрої різних сегментів не взаємодіють безпосередньо, а передають трафік через маршрутизатор. Цей механізм дозволяє визначати, які сегменти мають право обмінюватися даними, та які напрямки доступу слід обмежити.

З погляду безпеки VLAN дозволяє ізолювати адміністративний сегмент від студентського та викладацького. Адміністративні комп'ютери можуть використовуватися для обробки службової інформації, тому доступ до них не повинен бути відкритим для всіх користувачів мережі. VLAN-сегментація створює фундаментальну основу для такого розмежування, а додаткове застосування списків контролю доступу дозволяє обмежувати небажаний трафік між сегментами. Наприклад, у мережі може бути заборонений доступ зі студентського сегмента VLAN_10 до адміністративного сегмента VLAN_30. У такому випадку студенти зможуть працювати у своєму сегменті та мати доступ лише до дозволених ресурсів, а адміністративна частина мережі буде краще захищена від небажаних підключень. Це підвищує рівень керованості мережі та надає можливість впроваджувати політики доступу.

Водночас VLAN не замінює повноцінні засоби кіберзахисту. Вона не виконує функцій антивірусного програмного забезпечення, міжмережевого екрана або системи автентифікації. Проте VLAN значно оптимізує організацію мережі та створює основу для подальшого впровадження правил безпеки. Тому VLAN доцільно використовувати у поєднанні з іншими засобами захисту.

Ще однією практичною перевагою є спрощення діагностики несправностей. У разі виникнення проблеми в одному сегменті адміністратор може локалізувати перевірку відповідної VLAN, її портів, IP-адресації, шлюзу та trunk-з'єднань. Наприклад, якщо зв'язок не функціонує у студентському сегменті, спочатку перевіряється VLAN_10. Це дозволяє швидше ідентифікувати причину несправності та уникнути аналізу всієї мережі як

єдиного великого сегмента. VLAN також забезпечує можливість подальшого масштабування мережі.

Якщо в майбутньому виникне потреба додати нову групу користувачів або окремий службовий сегмент, це можна зробити шляхом створення нової VLAN та виділення для неї окремої IP-підмережі. При цьому не потрібно повністю перебудовувати фізичну інфраструктуру мережі. Практична реалізація в Cisco Packet Tracer підтвердила функціональність обраного підходу. Пристрої в межах однієї VLAN успішно обмінюються даними через комутатори, а передача пакетів між різними VLAN здійснюється через маршрутизатор R1. Trunk-з'єднання забезпечують проходження трафіку VLAN_10, VLAN_20 та VLAN_30 між комутаторами, а підінтерфейси маршрутизатора виконують роль шлюзів для відповідних підмереж. Отже, впровадження технології VLAN у мережеву інфраструктуру установи має важливе практичне значення. Воно дозволяє логічно розділити користувачів, зменшити широкомовний трафік, спростити адміністрування, покращити контроль доступу та забезпечити готовність мережі до подальшого розширення. Порівняно з мережею без логічного поділу, VLAN-мережа характеризується вищим ступенем упорядкованості, гнучкості та зручності в обслуговуванні.

ВИСНОВКИ

У кваліфікаційній роботі досліджено питання формування віртуальної мережі установи на основі технології VLAN. Проведено аналіз фізичної та віртуальної структури комп'ютерної мережі, ідентифіковано їхні характеристики, переваги та обмеження, а також здійснено практичне моделювання VLAN-мережі в середовищі Cisco Packet Tracer.

Ключовим аспектом стало логічне сегментування мережі на окремі домени для студентів, викладачів та адміністрації. У першому розділі розглянуто фізичну структуру комп'ютерної мережі. Встановлено, що фізична реалізація формує основу функціонування будь-якої локальної мережі, оскільки вона включає мережеве обладнання, кабельну систему, комутатори, маршрутизатори, точки доступу, сервери та кінцеві пристрої.

Фізична структура забезпечує реальне підключення пристроїв та передавання даних у межах мережі. Однак, фізична структура не забезпечує логічного розмежування користувачів за ролями або рівнями доступу. В умовах сучасних мереж установ першочерговим є не лише забезпечення фізичного підключення пристроїв, а й оптимальна організація їхньої взаємодії. Функціонування всіх пристроїв в єдиному широкомовному домені ускладнює адміністрування, призводить до надмірного поширення широкомовного трафіку та ускладнює керування доступом. Отже, для мереж з різними категоріями користувачів обґрунтованим є застосування логічної сегментації.

У роботі розглянуто технологію VLAN, яка дозволяє поділити одну фізичну мережу на кілька окремих логічних сегментів. Встановлено, що VLAN дає змогу групувати пристрої не лише за місцем їх фізичного підключення, а й за функціональним призначенням. Це означає, що комп'ютери однієї групи можуть бути підключені до різних комутаторів, але логічно залишатися в одному сегменті. Цей підхід є оптимальним для установ, де комп'ютери студентів, викладачів та адміністрації можуть бути розміщені в різних приміщеннях.

Під час порівняння фізичної та віртуальної структури мережі визначено, що фізична структура формує технічну основу мережі, тоді як VLAN-структура забезпечує логічну організацію трафіку. Фізична мережа забезпечує підключення пристроїв, але не створює чітких логічних меж між групами користувачів. VLAN, навпаки, дозволяє створити такі межі без необхідності повної реорганізації кабельної інфраструктури. Отже, оптимальним рішенням для мережі установи є синергія якісно розбудованої фізичної інфраструктури та логічного поділу за допомогою VLAN.

У другому розділі розроблено віртуальну мережу за допомогою симулятора Cisco Packet Tracer. Модель мережі включала маршрутизатор R1, п’ять комутаторів S1–S5 та кінцеві пристрої. Комутатори були з’єднані між собою послідовно. Це дало змогу продемонструвати функціональність VLAN як в межах окремого комутатора, так і в умовах багатокомутаторної мережі. Після конфігурації мережі здійснено її тестування.

На початковому етапі було перевірено зв’язок у межах кожної VLAN. Успішне виконання команди ping між пристроями одного сегмента підтвердило коректність конфігурації портів доступу та відповідність пристроїв їхнім VLAN-сегментам. Наступним кроком була перевірка доступності шлюзів кожної VLAN. Позитивна відповідь від шлюзів підтвердила правильність налаштування субінтерфейсів маршрутизатора R1. Додатково було перевірено міжвланову маршрутизацію. Для цього здійснювалося передавання пакетів між пристроями різних VLAN. Встановлено, що обмін даними між VLAN_10, VLAN_20 і VLAN_30 реалізується через маршрутизатор R1. Це підтвердило коректність функціонування механізму Router-on-a-Stick та правильність конфігурації транкового з’єднання між маршрутизатором і комутатором.

У третьому розділі проаналізовано результати реалізації VLAN-мережі. Встановлено, що розроблена мережа функціонує згідно із заздалегідь визначеною архітектурою. Пристрої в межах одного логічного сегмента

успішно обмінюються даними через комутатори, а пристрої різних VLAN взаємодіють через маршрутизатор. Це підтверджує коректність функціонування VLAN-сегментації, транкових портів, IP-адресації та міжвланової маршрутизації.

Окремо розглянуто аспекти безпеки та ізоляції, що забезпечуються VLAN. Визначено, що VLAN створює базову логічну ізоляцію між групами користувачів. Студентський, викладацький та адміністративний сегменти не належать до єдиного широкомовного домену. Така конфігурація мінімізує небажане поширення службового трафіку та підвищує керованість мережі.

Особливе значення має відокремлення адміністративного сегмента, що може містити службові комп'ютери та внутрішні ресурси установи. Водночас, слід зазначити, що VLAN не є самодостатнім засобом кібербезпеки. Вони не замінюють антивірусні програми, міжмережеві екрани або системи автентифікації. Однак VLAN формують основу для подальшої імплементації політик безпеки. У роботі розглянуто потенціал використання списків контролю доступу (ACL). Із застосуванням ACL можливо обмежити доступ студентського сегмента VLAN_10 до адміністративного сегмента VLAN_30. Такий підхід дає змогу не лише розмежувати мережу, а й контролювати напрямки передачі трафіку між сегментами.

Практична цінність отриманих результатів полягає в тому, що створена модель може слугувати прецедентом для проектування або модернізації локальної мережі установи. Запропонована структура дозволяє розділити користувачів за категоріями, зменшити навантаження від широкомовного трафіку, спростити адміністрування та закласти фундамент для ефективного контролю доступу. Модель також придатна для використання як навчальний приклад для пояснення принципів роботи VLAN, транкових портів, IP-адресації, міжвланової маршрутизації та ACL.

Внаслідок виконання кваліфікаційної роботи поставлену мету було досягнуто. Розглянуто структуру фізичних та віртуальних мереж, розроблено

модель VLAN-мережі з окремими сегментами, здійснено її конфігурацію та проведено тестування функціональності. Також ідентифіковано переваги застосування VLAN у порівнянні з традиційними мережами без логічного сегментування. Отже, використання VLAN у мережі установи визнано доцільним та емпірично обґрунтованим. VLAN дозволяє ефективно використовувати одну фізичну інфраструктуру для кількох логічних сегментів, забезпечує ефективний розподіл користувачів за категоріями (студенти, викладачі, адміністрація), спрощує адміністрування, підвищує ефективність контролю доступу та покращує загальну організацію мережі. Результати моделювання в Cisco Packet Tracer підтвердили, що запропонована VLAN-структура виявилася працездатною, гнучкою та масштабованою для подальшого розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Таненбаум Е. С., Везеролл Д. Дж., Фімстер Н. Computer Networks. 6th ed. Harlow : Pearson Education Limited, 2021. 960 p.

2. КОМП'ЮТЕРНІ МЕРЕЖІ Частина 1 НАВЧАЛЬНИЙ ПОСІБНИК [Електронний ресурс]. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/c4ecfaa7-73d5-498c-a63a-513137ee0aba/content (дата звернення 20.11.2025)

3. IEEE 802.1Q-2022. Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks. URL: https://standards.ieee.org/ieee/802.1Q/10323/ (дата звернення 20.12.2025).

4. IEEE 802.1Q Maintenance. URL: https://1.ieee802.org/maintenance/802-1q-2022-rev/ (дата звернення 24.12.2025).

5. Cisco Networking Academy. Cisco Packet Tracer Resource Hub [Електронний ресурс]. – Режим доступу: https://www.netacad.com/cisco-packet-tracer (дата звернення: 08.11.2025).

6. Cisco. Configuring VLAN Trunks. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_microswitches/ software/releases/15_2_8_e/configuration_guide/vlan/b_1528e_vlan_cms_cg/configuring_vlan_trunks.html (дата звернення 26.01.2026).

7. Cisco Networking Academy. Lab - Configure VLANs and Trunking. URL: https://www.netacad.com/content/srwe/1.0/courses/ content/m3/en-US/assets/3.4.6-lab---configure-vlans-and-trunking.pdf (дата звернення 28.01.2026).

8. Cisco. Configure Inter VLAN Routing with the Use of an External Cisco Router. URL: https://www.cisco.com/ c/en/us/support/docs/lan-switching/inter-vlan-outing/14976-50.html (дата звернення 30.01.2026).

9. Cisco Press. Router-on-a-Stick Inter-VLAN Routing. URL: https://www.ciscopress.com/articles/article.asp?p=3089357&seq Num=5 (дата звернення 03.02.2026).

10. Cisco. ACL Samples. URL: https://www.cisco.com/ c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html (дата звернення 06.02.2026).

11. Cisco. Configure IP Access Lists. URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html (дата звернення 09.02.2026).

12. Cisco. Configure IP Addresses and Unique Subnets for New Users. URL: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html (дата звернення 10.02.2026).

13. .Cisco Networking Academy. Cisco Packet Tracer. URL: https://www.netacad.com/learning-collections/cisco-packet-tracer (дата звернення 11.02.2026).

14. Cisco. Campus LAN and Wireless LAN Solution Design Guide. URL: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html (дата звернення 11.02.2026).

15. Cisco Press. Campus Wired LAN Designs. URL: https://www.ciscopress.com/articles/article.asp?p=2832408&seqNum=4 (дата звернення 12.02.2026).

Додатки

Додаток А – Перевірка доступності шлюзів

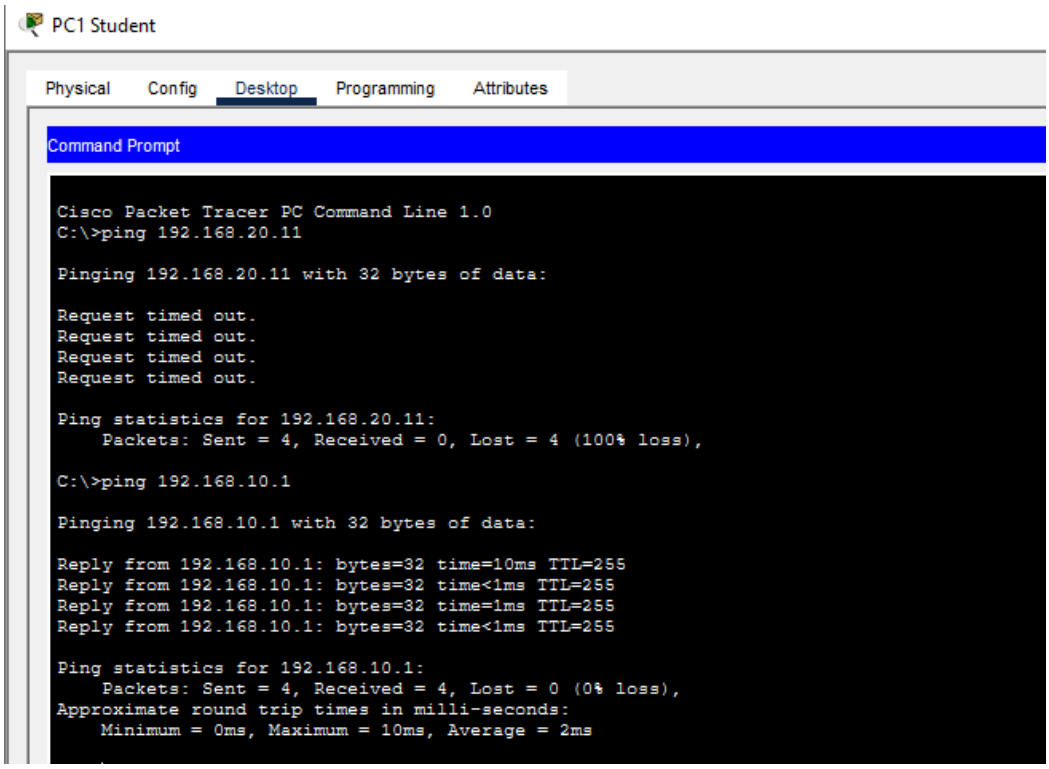

Рисунок 1 – Певірка зв’язку зі студентським ПК

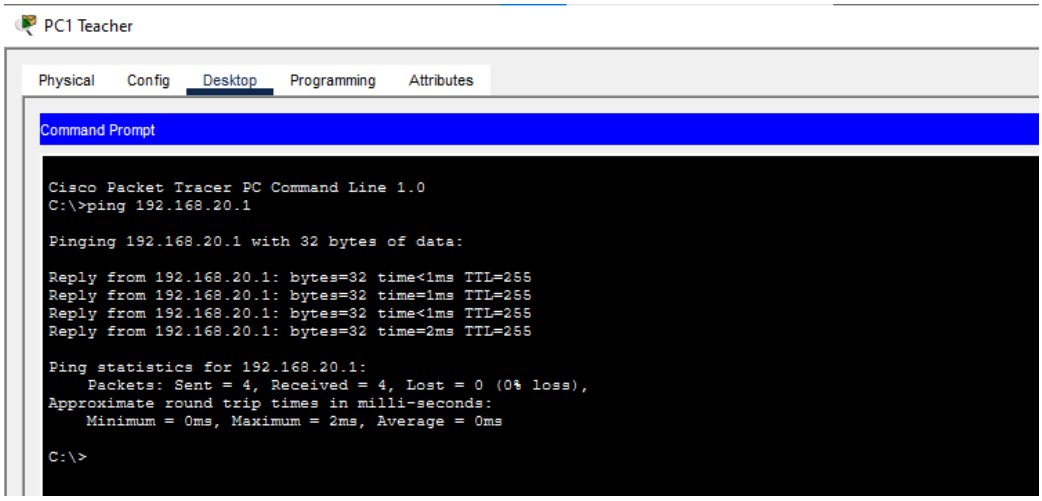

Рисунок 2 - Певірка зв’язку з викладацьким ПК

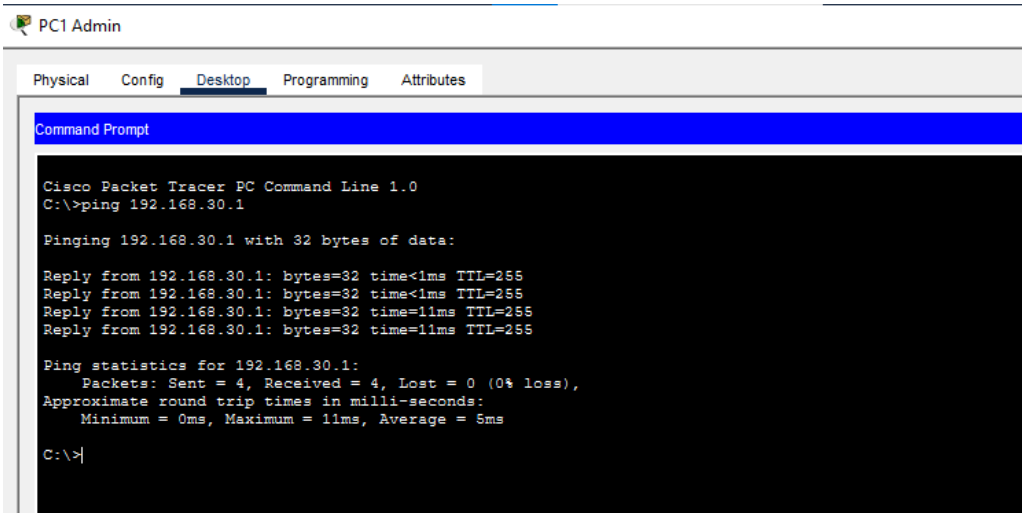

Рисунок 3 – Певірка зв’язку з ПК адміністратора мережі