Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
з передатестаційної практики

здобувача Скроботова Євгенія Олександровича
(ПІБ)

академічної групи 123-22ск-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему «Розробка безпечної мережної інфраструктури коледжу з впровадженням технологій захисту DHCP»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Молодець Б. В.			
спеціальна частина	доц. Молодець Б. В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » _____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Скроботова Є. О. **академічної групи** 123-22ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему «Розробка безпечної мережної інфраструктури коледжу з впровадженням технологій захисту DHCP»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути існуючі уразливості DHCP-сервісів та загрози, пов'язані з їх експлуатацією.	10.02.2025
Технічні вимоги та розробка апаратної частини	Сформулювати найменування й призначення комп'ютерної системи, висунути технічні вимоги до неї Виконати розробку частини комп'ютерної системи.	20.04.2025
Розробка корпоративної мережі	Побудувати в Packet Tracer типову мережну топологію коледжу з VLAN-сегментацією. Впровадити технології захисту DHCP та провести тестування та симуляцію потенційних атак	31.05.2025

Завдання видано _____ доц. Молодець Б. В.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Скроботова Є. О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 37 рис., 3 табл., 1 дод., 14 джерел.

ЗАХИСТ, МЕРЕЖА, DAI, DHCP, DNS, SPOOFING, VLAN.

Об’єкт професійної діяльності – комп’ютерна мережа навчального закладу, зокрема інфраструктура локальної мережі коледжу, її захищеність та працездатність при використанні мережних сервісів, таких як DHCP.

Мета роботи − розробка та впровадження системи безпеки мережної інфраструктури коледжу з акцентом на захист від загроз, пов'язаних із DHCP.

Актуальність теми полягає в необхідності захисту мережних сервісів освітніх установ від зовнішніх і внутрішніх атак. DHCP є критично важливим елементом, і його неправильне функціонування або зловмисне використання (наприклад, підміна DHCP-серверів, DHCP starvation) може спричинити повну втрату доступу до мережі для легітимних користувачів. Тому забезпечення цілісності та надійності цього сервісу має ключове значення для стабільної роботи IT-інфраструктури.

Серед основних завдань є реалізація технологій захисту DHCP, які зменшують ризики, пов'язані з атакою на мережні протоколи.

У результаті виконання роботи було розроблено та змодельовано безпечну мережу для коледжу з урахуванням сегментації трафіку, контролю доступу до DHCP-сервісу, а також з впровадженням базових механізмів захисту другого рівня. Запропонована модель сприяє підвищенню стійкості мережі до внутрішніх атак та забезпечує стабільне надання IP-адрес клієнтам.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

DHCP – англ. Dynamic Host Configuration Protocol;

IP – англ. Internet Protocol;

MAC – англ. Media Access Control;

VLAN – англ. Virtual Local Area Network;

ARP – англ. Address Resolution Protocol;

DAI – англ. Dynamic ARP Inspection

ACLs – англ. Access Control Lists

DNS – англ. Domain name System

SSH – англ. Secure Shell

ВСТУП

У сучасному освітньому просторі комп’ютерні системи відіграють ключову роль у забезпеченні навчального процесу та адміністративної діяльності коледжів. Вони створюють основу для організації електронного документообігу, дистанційного навчання, зберігання та обробки великих обсягів інформації, а також забезпечують доступ до мережних ресурсів як для співробітників, так і для студентського колективу.

Безпека мережної інфраструктури відіграє критичну роль в сучасному освітньому середовищі, особливо в коледжах. Вона не просто забезпечує безперебійний доступ до інформаційних ресурсів, а й гарантує конфіденційність даних студентів, викладачів та адміністрації, а також захищає від потенційних атак, які можуть призвести до серйозних збоїв в навчальному процесі.

Серед безлічі компонентів мережної інфраструктури, DHCP (Dynamic Host Configuration Protocol) відіграє важливу роль, автоматично призначаючи мережні наоалаштування пристроям, що підключаються до мережі. Ця зручність, однак, робить DHCP-сервіс вразливим до різних атак, які можуть поставити під загрозу всю мережу коледжу. Наслідки таких атак можуть бути руйнівними: від втрати доступу до Інтернету до компрометації особистих даних студентів. Впровадження методів захисту допоможе коледжам захистити свою мережну інфраструктуру, забезпечити безперебійну роботу та захистити конфіденційну інформацію, що є критично важливим для успішного функціонування навчального закладу в сучасному цифровому світі.

Основні задачі, які необхідно вирішити в рамках роботи:

– розробити концепцію мережної архітектури для навчального закладу з урахуванням логічної сегментації, рівнів доступу та впровадження захисту DHCP;

– створити модель комп’ютерної мережі коледжу у середовищі Cisco Packet Tracer, з реалізацією механізмів безпеки;

– налаштувати мережне обладнання (маршрутизатори, комутатори) та налаштувати централізований DHCP-сервер на маршрутизаторі;

– зміцнити мережну безпеку на рівні доступу, розробивши захист за допомогою механізмів DHCP Snooping, Port Security, Dynamic ARP Inspection (DAI).

– реалізувати атаки для демонстрації вразливості;

– перевірити працездатність розробленої мережної архітектури, протестувати ефективність впроваджених заходів захисту на рівні другої та третьої моделей OSI.

– оцінити доцільність та ефективність впроваджених засобів безпеки в умовах коледжу, з урахуванням можливостей масштабування та модернізації в майбутньому.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Особливості функціонування комп'ютерної мережі коледжу в умовах цифровізації та актуальні загрози DHCP-сервісу

Сучасна освітня галузь, зокрема система фахової передвищої освіти, до якої належать коледжі, перебуває в активному етапі цифрової трансформації. Коледжі відіграють ключову роль у формуванні кваліфікованих кадрів для різних галузей національної економіки. У контексті розвитку цифрової держави, розширення доступу до електронних освітніх ресурсів та дистанційного навчання, саме комп'ютерна система навчального закладу виступає критично важливою інфраструктурною складовою забезпечення якості освітнього процесу.

Коледжі зазвичай об'єднують різноманітні категорії користувачів: адміністративний персонал, викладачів, студентів, технічну службу, які працюють у межах єдиної локальної мережі, але мають відмінні рівні доступу до інформаційних ресурсів. У структурі таких закладів можна виділити кілька ключових функціональних зон: адміністративну частину (деканат, бухгалтерія, керівництво), освітній сектор (аудиторії, лабораторії, бібліотека, викладацькі), зону підтримки (серверні, мережні центри, ресурсні кімнати) тощо. Всі вони потребують безперебійного доступу до локальних та мережних сервісів: файлів, електронного журналу, баз даних студентів, відеоконференцій, вебпорталу навчального закладу, тощо.

Поширеним технічним рішенням у таких установах є створення сегментованої комп'ютерної мережі з підтримкою віртуальних локальних мереж (VLAN), централізованого керування IP-адресацією (DHCP), механізмів контролю доступу (ACL), базового моніторингу трафіку та впровадження політик безпеки. При цьому надзвичайно важливими залишаються питання захисту мережних сервісів, зокрема сервісу DHCP, який є одним із базових сервісів для підтримки IP-мереж.

Комп’ютерна система коледжу, як правило, є складною інфраструктурою, яка обслуговує різноманітні потреби: від забезпечення доступу до Інтернету та навчальних матеріалів до управління адміністративними процесами. Вона охоплює навчальні аудиторії, комп’ютерні лабораторії, бібліотеку, адміністративні офіси та гуртожитки (за наявності). Галузь застосування включає в себе: електронне навчання (LMS), системи управління студентами (SMS), мережний доступ до файлів та принтерів, а також забезпечення зв'язку (електронна пошта, відеоконференції).

Особливості впровадження комп’ютерної системи в закладі освіти обумовлюються необхідністю підтримувати постійний і якісний зв’язок між різними відділами та аудиторіями, підтримувати високу продуктивність серверів, мінімізувати простої обладнання та забезпечувати безпеку даних. Ключову роль у роботі мережі коледжу відіграє протокол DHCP (Dynamic Host Configuration Protocol). Він автоматично надає IP-адреси, маски підмереж, шлюзи за замовчуванням та DNS-сервери клієнтським пристроям, спрощуючи адміністрування мережі. Проте, використання DHCP може бути пов'язане з певними проблемами та недоліками.

Попри очевидні переваги DHCP (простота налаштування, економія часу, мінімізація людського фактора), у коледжах такий підхід має певні недоліки й проблеми:

– можливі випадки конфлікту IP-адрес або їхнє дублювання за наявності несправностей у сервері DHCP чи його неправильної конфігурації;

– уразливість до атак типу «man-in-the-middle», коли зловмисник підмінює DHCP-сервер і видає шкідливі налаштування мережі, перенаправляючи трафік через себе;

– атаки типу DHCP Starvation – загроза заповнення DHCP-пулу валідних адрес фальшивими запитами, що веде до відмови в обслуговуванні (DoS) для легітимних клієнтів

– втрата підключення пристроїв у разі тимчасової недоступності сервера DHCP, нові пристрої не зможуть підключитися до мережі, а пристрої з простроченою орендою IP-адреси втратять з'єднання.

– неавтентифікований доступ, що дозволяє будь-кому підключитися до мережі та отримати IP-адресу, що може створити проблеми з безпекою;

Для вирішення цих проблем необхідно ретельно налаштовувати DHCP-сервер, використовувати резервні DHCP-сервери, впроваджувати комплексні заходи безпеки та розглядати використання статичних IP-адрес для критично важливих пристроїв. Правильне адміністрування DHCP є критично важливим для забезпечення стабільної, безпечної та ефективної роботи комп'ютерної системи коледжу.

1.2 Аналіз фізичної та логічної структури комп'ютерної мережі коледжу як об'єкта впровадження безпечної IT-інфраструктури

Коледж обслуговує понад 800 студентів та 100 працівників, включаючи викладачів, адміністративний і технічний персонал. Усі користувачі щоденно взаємодіють із внутрішніми сервісами: електронним журналом, системою управління навчанням (LMS), електронною бібліотекою, локальними файловими сховищами, тощо. Високий рівень IT-навантаження потребує стабільної, безпечної та масштабованої комп'ютерної мережі з централізованим управлінням.

На рисунку 1.2 показано мережу освітнього закладу, що включає трьохповерхову будівлю коледжу, гуртожиток, бібліотеку, серверну і підключення до Інтернет-провайдера (ISP).

ISP (Інтернет-провайдер) забезпечує зовнішній доступ до мережі та ресурсів Інтернету.

Оптичні підключення (червоні лінії) використовуються для з'єднання маршрутизаторів між собою та з ISP. Оптика забезпечує високу пропускну здатність і стабільний швидкісний зв'язок для критично важливих каналів.

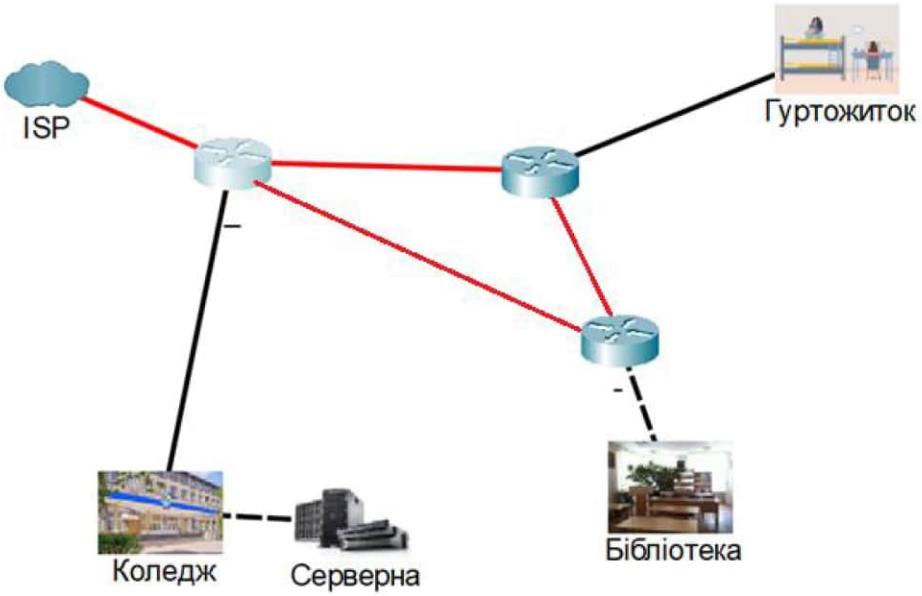

Рисунок 1.1 – Топологія локальної мережі коледжу

Fast Ethernet підключення (чорні лінії) застосовуються для підключення підрозділів до мережевих пристроїв, забезпечуючи надійне та швидке з’єднання на локальному рівні.

Об'єктом впровадження безпечної мережної інфраструктури є трьохповерхова будівля коледжу з розподіленими аудиторіями, лабораторіями, офісними приміщеннями, серверною кімнатою, а також зонами загального користування. Така структура типова для середніх навчальних закладів, де присутня значна кількість одночасно підключених користувачів і пристроїв.

На кожному поверсі будівлі розміщені різні функціональні приміщення (рис. 1.2).

Рисунок 1.2 – План 1 поверху

Перший поверх включає в себе адміністративний блок (кабінет директора, бухгалтерія, приймальня, серверна), кілька навчальних аудиторій загального призначення, а також їдальня та приміщення охорони. Тут зосереджені критично важливі обчислювальні вузли: головний комутаційний центр, міжмережний шлюз, сервери DHCP, DNS, а також системи відеоспостереження та доступу.

Другий поверх призначено здебільшого для проведення теоретичних занять. Він обладнаний комп’ютерними класами, мультимедійними аудиторіями, кабінетами викладачів. Саме тут виникає потреба в сегментації мережі, щоб забезпечити розподіл між доступом викладачів і студентів, ізоляцію лабораторій, а також гарантований пріоритет трафіку для навчальних цілей.

Третій поверх виконує змішану функцію: тут розташовані лабораторії спеціалізованих дисциплін (наприклад, електроніки, інформаційних технологій), спортивна та актова зали, зони для групових занять і дослідницької роботи студентів.

На кожному поверсі розміщені точки доступу (Wi-Fi), комутатори access-рівня, що підключають кінцеві пристрої (ноутбуки, ПК, принтери тощо).

Серверна кімната розташована в спеціальному приміщенні із контрольованим доступом, де розміщуються 1 сервер, на якому налаштовано декілька сервісів: DNS, HTTP, SMTP, FTP та інше мережне обладнання.

Ядро коледжної мережі з'єднане із зовнішніми ресурсами (інтернет-провайдером) через захищений маршрутизатор.

Із технічного боку, будівля має розгалужену структуровану кабельну систему (СКС), прокладену за принципом зірки з центральною комутаційною шафою на першому поверсі та допоміжними точками концентрації на кожному наступному рівні. Усі мережні з’єднання виконані за стандартом Cat.6 з можливістю розширення до оптичного зв’язку у разі модернізації.

Безпечна мережна інфраструктура, що впроваджується в цьому об’єкті, передбачає чіткий поділ на ізольовані віртуальні локальні мережі (VLAN) для адміністрації, викладачів, студентів, гостьового доступу та серверного сегменту. Центральна маршрутизація з підтримкою DHCP Relay забезпечує централізоване управління IP-адресацією, тоді як фільтрація трафіку, політики доступу та механізми аутентифікації користувачів гарантують дотримання вимог інформаційної безпеки.

Таким чином, будівля коледжу виступає комплексним об’єктом впровадження, в якому фізична структура простору гармонійно поєднується з логічною архітектурою мережі, створюючи передумови для ефективного,

стабільного й безпечного функціонування комп’ютерної системи навчального закладу.

З урахуванням фізичного розташування корпусів, мережна інфраструктура має бути побудована з урахуванням принципів резервування каналів зв'язку, сегментації за допомогою VLAN, централізованого надання IP-адрес через DHCP, та забезпечення міжвузлового захищеного зв’язку. Інтеграція цих елементів дозволить забезпечити захист від несанкціонованого доступу, підвищити ефективність адміністрування та створити гнучку основу для подальшого розвитку інформаційної системи коледжу.

1.3 Розробка схеми організаційної структури коледжу

Коледж, як заклад фахової передвищої освіти, є складною організацією, що потребує чіткої та ефективної структури для забезпечення якісного освітнього процесу, належного управління ресурсами та досягнення поставлених цілей. Організаційна структура коледжу – це сукупність взаємопов’язаних елементів (підрозділів, органів управління, посадових осіб) та їхніх взаємозв’язків, що визначають розподіл обов’язків, відповідальності та повноважень у закладі. Її основна мета – координація діяльності всіх структурних підрозділів для забезпечення оптимального функціонування коледжу та виконання його місії.

Діяльність коледжу регулюється законодавством України у сфері освіти, зокрема Законом України "Про фахову передвищу освіту" та іншими нормативними актами. Організаційна структура повинна відповідати вимогам цих документів.

Організаційна структура повинна враховувати наявні людські, фінансові та матеріально-технічні ресурси. Наприклад, невеликий коледж може мати більш просту структуру, ніж великий.

Типова організаційну структуру коледжу наведена на рисунку 1.3.

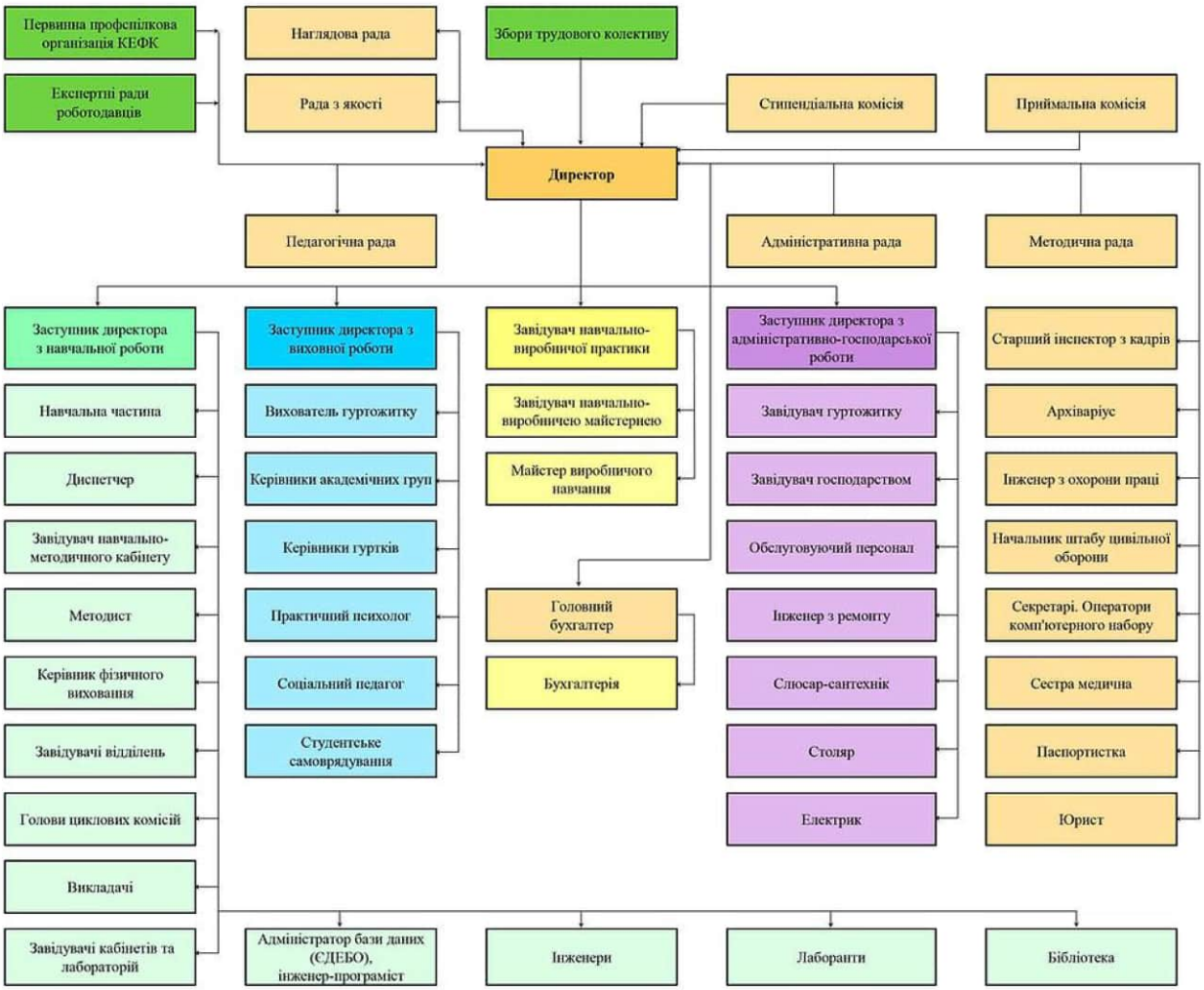

Рисунок 1.3 – Організаційна структура коледжу

Директор є керівником коледжу та здійснює загальне керівництво його діяльністю. Він несе відповідальність за організацію освітнього процесу, фінансово-господарську діяльність, забезпечення дотримання законодавства та виконання стратегічних цілей коледжу. Директор представляє ко ледж у відносинах з іншими організаціями.

Педагогічна рада є колегіальним органом управління, що розглядає та вирішує ключові питання освітньої, методичної та наукової діяльності. До складу педагогічної ради входять директор, його заступники, завідувачі відділень, голови циклових комісій, представники викладацького складу та студентського самоврядування.

Рада коледжу може існувати в коледжах, які здійснюють наукову або дослідно-конструкторську діяльність. Рада розглядає питання наукової

роботи, затверджує наукові плани та звіти, рекомендує кандидатури на наукові звання.

Наглядова рада може бути створена з метою забезпечення контролю за фінансово-господарською діяльністю коледжу, дотриманням законодавства та захистом інтересів закладу. До складу наглядової ради можуть входити представники засновника, органів державної влади, місцевого самоврядування, роботодавців та громадськості

Заступники директора здійснюють керівництво окремими напрямками діяльності коледжу, такими як навчальна робота, науково-методична робота, виховна робота, адміністративно-господарська робота:

– заступник директора з навчальної роботи відповідає за організацію та контроль навчального процесу, розробку навчальних планів та програм, графіків навчального процесу, організацію практик та державних іспитів;

– заступник директора з науково-методичної роботи відповідає за організацію та координацію методичної роботи, підвищення кваліфікації викладачів, впровадження нових освітніх технологій, організацію науково-практичних конференцій та семінарів;

– заступник директора з виховної роботи відповідає за організацію виховної роботи, створення сприятливих умов для розвитку особистості студентів, організацію культурно-масових заходів, профілактику правопорушень;

– заступник директора з адміністративно-господарської роботи відповідає за забезпечення матеріально-технічного забезпечення освітнього процесу, утримання будівель та споруд, організацію харчування та медичного обслуговування студентів.

Завідувачі відділень очолюють структурні підрозділи, що здійснюють підготовку фахівців за певними спеціальностями. Вони відповідають за організацію навчальної, методичної та виховної роботи на відділенні, комплектування навчальних груп, контроль за відвідуванням занять та успішністю студентів.

Завідувачі навчально-методичних кабінетів забезпечують методичне забезпечення навчального процесу, накопичення та систематизацію методичних матеріалів, організацію виставок методичних розробок.

Головний бухгалтер здійснює бухгалтерський облік та фінансову звітність коледжу.

Керівник відділу кадрів здійснює кадрове забезпечення коледжу, ведення кадрової документації, організацію атестації педагогічних працівників.

Циклові комісії є об'єднаннями викладачів, які викладають дисципліни одного або спорідненого профілю. Циклові комісії розробляють навчальні програми дисциплін, методичні рекомендації, організовують взаємовідвідування занять, обмінюються досвідом.

Викладачі здійснюють навчальну, методичну, наукову та виховну роботу зі студентами. Вони відповідають за якість викладання дисциплін, проведення практичних занять, організацію самостійної роботи студентів, контроль за їхніми знаннями та вміннями.

Бібліотека забезпечує інформаційне забезпечення освітнього процесу, надає студентам та викладачам доступ до навчальної та наукової літератури, періодичних видань, електронних ресурсів.

Навчальні лабораторії та майстерні забезпечують проведення лабораторних та практичних занять, надають студентам можливість отримати практичні навички за спеціальністю;

Інформаційно-обчислювальний центр забезпечує інформатизацію освітнього процесу, підтримку комп'ютерної мережі коледжу, доступ до інтернету.

Студентське самоврядування є формою організації студентів, що забезпечує їхню участь в управлінні коледжем, захист їхніх прав та інтересів, організацію культурно-масових заходів. Органи студентського самоврядування можуть брати участь у роботі педагогічної ради, ради коледжу, наглядової ради.

1.4 Стислі відомості про технології збору та передачі інформації для об’єкта впровадження

Коледжі – це середньорозмірні організації з різними потребами у доступі до мережі, що відвідують студенти, викладачі, адміністративний та технічний персонал. Сучасний освітній процес в коледжі немислимий без надійної та ефективної інформаційної інфраструктури. Технології збору та передачі даних відіграють ключову роль у забезпеченні доступу до навчальних матеріалів, комунікації між студентами та викладачами, а також підтримці адміністративних процесів. Технології, які використовуються для цих цілей, постійно розвиваються, адаптуючись до потреб і викликів цифрової епохи.

Процес збору інформації в коледжі охоплює широкий спектр даних, включаючи інформацію про абітурієнтів, студентів, викладачів, навчальні програми, фінанси та інфраструктуру. Традиційні методи, такі як паперові анкети та особисті співбесіди, поступово поступаються місцем сучасним технологіям. Онлайн-платформи для подачі заявок дозволяють абітурієнтам легко подавати документи, а адміністративному персоналу – централізовано збирати та обробляти інформацію. Системи управління навчанням (Learning Management Systems, LMS), такі як Moodle, Canvas або Blackboard, є ключовими інструментами для збору інформації про прогрес студентів, відвідуваність, результати тестувань та зворотний зв'язок. Електронні опитування та форми зворотного зв'язку, що проводяться за допомогою інструментів, таких як Google Forms або SurveyMonkey, дозволяють швидко збирати інформацію про задоволеність студентів та викладачів різними аспектами освітнього процесу.

Передача інформації в коледжі також використовує різноманітні технологічні рішення. Електронна пошта залишається важливим каналом комунікації між адміністрацією, викладачами та студентами. Інформаційні портали та веб-сайти коледжу надають централізований доступ до важливої

інформації, такої як розклад занять, академічний календар, новини та оголошення. LMS використовуються не лише для збору інформації, але й для її розповсюдження, забезпечуючи доступ до навчальних матеріалів, завдань та оцінок. Системи сповіщень та повідомлень, що інтегровані з мобільними додатками, дозволяють оперативно інформувати студентів та викладачів про важливі події, зміни в розкладі або терміни подачі документів. Нарешті, соціальні мережі та внутрішні платформи для співпраці (наприклад, Microsoft Teams або Slack) використовуються для неформального спілкування та обміну інформацією між членами академічної спільноти.

Ethernet (Fast/Gigabit) – основна технологія дротового підключення, яка забезпечує надійне та швидке передавання даних між комутаторами, серверами та клієнтськими пристроями. Ethernet залишається основою локальних мереж (LAN) в багатьох освітніх закладах. Використовуючи фізичне з’єднання через кабель, Ethernet забезпечує надійну та швидку передачу даних. Найбільш поширеними стандартами є Fast Ethernet (100 Мбіт/с) та Gigabit Ethernet (1 Гбіт/с). Gigabit Ethernet поступово замінює Fast Ethernet завдяки значно вищій пропускній здатності, що є критично важливим для обробки великих обсягів даних, необхідних для сучасних мультимедійних навчальних матеріалів та онлайн-платформ. Ethernet забезпечує стабільний зв'язок для комп'ютерних класів, лабораторій та офісів, де потрібна максимальна продуктивність мережі.

Wi-Fi (802.11ac/n) надає бездротовий доступ до мережі, що є надзвичайно зручним для студентів та викладачів, які використовують мобільні пристрої, такі як ноутбуки, планшети та смартфони. Стандарти 802.11ac та 802.11n забезпечують високу швидкість передачі даних (до декількох гігабіт на секунду в випадку 802.11ac) та широкий радіус покриття. Розгортання Wi-Fi мережі в коледжі вимагає ретельного планування, щоб забезпечити достатнє покриття та пропускну здатність в місцях з високою концентрацією користувачів, таких як бібліотеки,

кафетерії та аудиторії. Безпека Wi-Fi мережі також має першочергове значення, тому використовуються протоколи шифрування, такі як WPA2/WPA3, для захисту даних від несанкціонованого доступу.

VLAN (Virtual Local Area Network) дозволяє логічно розділити фізичну мережу на декілька віртуальних мереж. Це дозволяє ізолювати трафік різних груп користувачів, наприклад, трафік студентів від трафіку адміністрації або трафік гостьової Wi-Fi мережі від внутрішньої корпоративної мережі. VLAN підвищує безпеку мережі, зменшує широкомовний трафік та спрощує адміністрування. У коледжах VLAN може бути використана для створення окремих мереж для різних відділів, лабораторій або навіть для різних рівнів доступу до мережних ресурсів.

DHCP (Dynamic Host Configuration Protocol) є протоколом, який автоматично призначає IP-адреси, маски підмережі, шлюзи за замовчуванням та DNS-сервери клієнтським пристроям, які підключаються до мережі. Це значно спрощує адміністрування мережі, оскільки адміністраторам не потрібно вручну конфігурувати кожен пристрій. DHCP також допомагає уникнути конфліктів IP-адрес, коли декілька пристроїв намагаються використовувати одну й ту ж адресу. У коледжах з великою кількістю користувачів та динамічно змінюваним списком пристроїв, DHCP є незамінним інструментом для ефективного управління IP-адресами.

Додатково технології:

– SNMP/NetFlow/Syslog – протоколи моніторингу та збору статистики трафіку для аналізу стану мережі та виявлення інцидентів;

– MQTT/HTTP (локально для IoT) – застосовується в навчальних лабораторіях або дослідницьких проєктах для збору даних із сенсорів, розумних пристроїв та їх візуалізації;

– FTP/SMB/NFS – протоколи передачі файлів для обміну навчальними матеріалами, резервного копіювання та доступу до навчальних ресурсів;

– Cloud-сервіси та VPN – для віддаленого доступу до ресурсів коледжу із забезпеченням захищеного з’єднання.

Мережа має забезпечувати:

– бездротовий та дротовий доступ до Інтернету та внутрішніх ресурсів;

– мультимедіа-сервіси, включаючи онлайн-лекції, відеоконференції, доступ до баз даних;

– гнучкий доступ для гостей і відвідувачів без шкоди для безпеки основної мережі;

– сумісність зі стандартами нового покоління Wi-Fi 6, а також підтримку багатьох одночасних підключень.

Характерним для мереж коледжів є потреба в:

– високій доступності мережних сервісів для забезпечення безперервності навчального процесу;

– легкому масштабуванні при збільшенні кількості пристроїв;

– забезпеченні безпеки у складних середовищах з численними користувачами і пристроями, включаючи BYOD (Bring Your Own Device);

– автоматизованому управлінні мережею, з використанням сучасних інструментів для оптимізації обслуговування і захисту.

1.5 Огляд існуючих рішень для захисту DHCP-сервісів

Протокол динамічного призначення IP-адрес (DHCP) є фундаментальним компонентом сучасних IP-мереж, що дозволяє автоматизувати конфігурацію параметрів хостів. Проте відкритість цього протоколу робить його вразливим до низки атак, таких як DHCP spoofing, starvation та rogue-server атаки. Через ці загрози актуальним є впровадження захищених рішень, які забезпечують цілісність, надійність та контроль доступу до DHCP-інфраструктури.

1.5.1 DHCP Snooping

DHCP Snooping – це важлива функція безпеки, яка запобігає атакам на мережі шляхом контрольованого відстеження DHCP-повідомлень, що

дозволяє блокувати зловмисні дії [2]. Вона захищає мережу від таких загроз, як підробка IP-адрес, атаки типу "людина посередині" та атаки на відмову в обслуговуванні. Коректне налаштування та використання DHCP Snooping може суттєво підвищити загальний рівень безпеки мережі.

DHCP Snooping дозволяє блокувати зловмисні пристрої, що намагаються підробити DHCP-повідомлення. Ця функція працює на комутаторах і маршрутизаторах, що захищає мережу від підроблених серверів DHCP та атак на відмову в обслуговуванні. Захист від атак, таких як IP Spoofing, "людина посередині" і атаки на відмову в обслуговуванні, є основною метою DHCP Snooping. Використання DHCP Snooping допомагає зменшити час простою мережі та оптимізує використання пропускної здатності.

Механізм, що дозволяє комутаторам контролювати і фільтрувати повідомлення DHCP на на комутаторах другого рівня. Він дозволяє визначити, які порти мережі є довіреними (для DHCP-серверів), а які – ні (для клієнтів), що запобігає прийому неправомірних DHCP-пакетів. Ця функція аналізує DHCP-пакети, фільтрує підозрілу активність і створює так звану "базу довіри" (binding table), де фіксуються MAC-адреси, IP-адреси, інтерфейси та інші параметри, що допомагає відслідковувати законні клієнтські сесії. Налаштування DHCP Snooping вимагатиме конфігурації довірених інтерфейсів та зазначення IP-адреси сервера DHCP для коректної роботи (рис. 1.4)

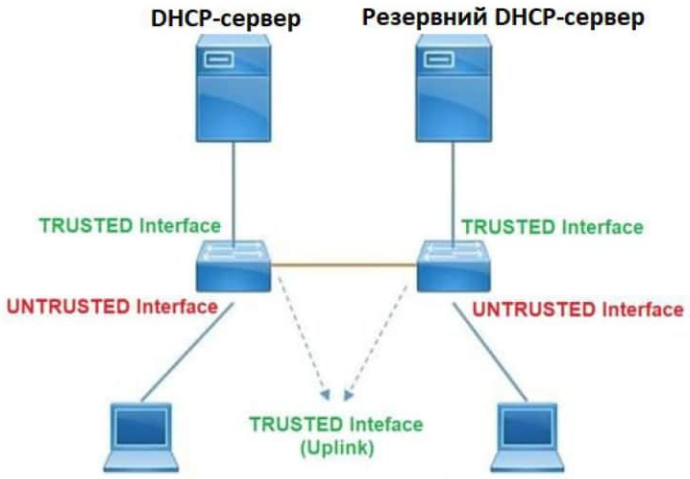

Рисунок 1.4 – DHCP Snooping

Переваги:

– блокує підключення до фальшивих (rogue) DHCP-серверів;

– запобігає DHCP starvation-атакам;

– створює базу для інших механізмів безпеки (наприклад, IP Source Guard, Dynamic ARP Inspection).

1.5.2 IP Source Guard

Комутатори Ethernet вразливі до підробки IP та MAC адрес, що може призвести до атак на відмову в обслуговуванні (DoS) [3]. Функція IP Source Guard перешкоджає подібним атакам, перевіряючи пакети на ненадійних інтерфейсах доступу. Ця технологія працює в тандемі з DHCP Snooping і дозволяє здійснювати фільтрацію трафіку на основі IP- і MAC-адреси джерела. Вона гарантує, що пристрої можуть надсилати трафік у мережу лише з дозволеними параметрами. IP Source Guard отримує дані про зв’язки IP-адрес та MAC-адрес з таблиці DHCP snooping, яка може заповнюватися динамічно або статично. Якщо заголовок пакета не відповідає дійсному запису в таблиці DHCP snooping, пакет відкидається. Функція IP Source Guard може бути налаштована з іншими функціями безпеки, такими як VLAN тегування та 802.1X автентифікація користувачів.

Переваги:

– запобігає підробці адрес джерела (spoofing);

– дає змогу застосовувати політики доступу до мережі на основі надійності пристрою.

1.5.3 Dynamic ARP Inspection (DAI)

Динамічна перевірка ARP (Dynamic ARP Inspection, DAI) є механізмом безпеки, що захищає мережу від зловмисних ARP-атак шляхом відхилення невідомих ARP-пакетів [4]. Цей процес базується на перевірці відповідностей IP-адрес та MAC-адрес, використовуючи базу даних прив'язок, яка створюється через DHCP Snooping. Конфігурація DAI включає налаштування інтерфейсів як довірених або недовірених, щоб ефективно контролювати ARP-пакети в мережі. Завдяки цьому усуваються можливості ARP-spoofing атак, які часто використовуються для створення MITM (man-in-the-middle) середовищ.

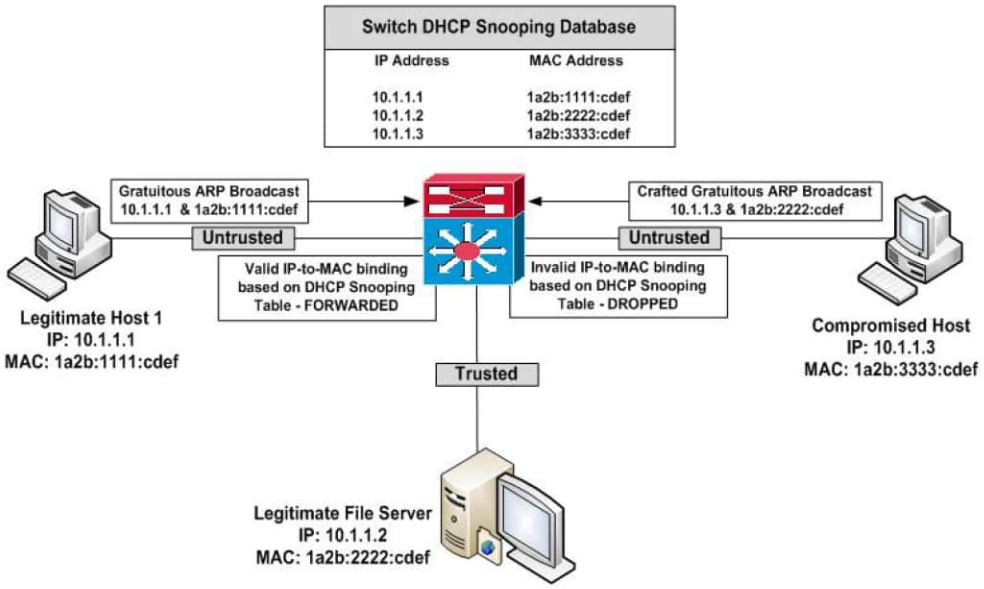

Рисунок 1.5 – Dynamic ARP Inspection

1.5.4 DHCP Rate Limiting

DHCP Rate Limiting дозволяє обмежити кількість DHCP-повідомлень, які отримує інтерфейс [5]. Ненадійні порти, підключені до сегментів мережі, де розташовані DHCP-хости, зазвичай підлягають обмеженню.

Рекомендується не перевищувати 100 пакетів на секунду для ненадійних інтерфейсів.На надійних портах може знадобитися підвищити ліміт для trunk-портів, які несуть кілька VLAN. Коли ліміт швидкості перевищено, порти переходять у стан "error-disabled". Це є простим, але ефективним методом захисту від DoS-атак або спроб масової генерації запитів.

1.5.5 ACL (Access Control List) для DHCP

Access Control Lists (ACL) – це потужний інструмент для управління доступом до ресурсів у мережі. Застосування ACL для DHCP може допомогти в забезпеченні безпеки мережі, запобігаючи несанкціонованому доступу до DHCP-серверів та контролюючи трафік DHCP. Можна вручну обмежити доступ до DHCP-серверів за допомогою списків контролю доступу, вказавши, з яких VLAN, IP або MAC-адрес дозволено обмін DHCP-повідомленнями. Це зменшує ризик атак, таких як людина посередині (Man-in-the-Middle) або отруєння DHCP (DHCP Spoofing).

1.5.6 DHCP Relay Agent Information Option (Option 82)

Функція розподілу IP-адрес DHCP за допомогою опції 82 дозволяє DHCP-серверу використовувати додаткову інформацію, надану DHCP Relay Agent, для точнішого призначення динамічних IP-адрес клієнтам. Вона розширює можливості традиційного автоматичного розподілу адрес, включаючи інформацію, таку як VLAN, що допомагає серверу ідентифікувати, які адреси слід виділяти залежно від виходу запиту. Додатково функція підтримує класи DHCP, що дозволяє групувати клієнтів за спільними характеристиками, забезпечуючи гнучкість у налаштуваннях адресного пулу. Ця опція дозволяє DHCP Relay Agent додавати інформацію про розташування клієнта в DHCP-запит, що дозволяє DHCP-серверу більш точно контролювати розподіл IP-адрес та ідентифікувати потенційні атаки [6].

Коли клієнтський пристрій надсилає запит на отримання IP-адреси через DHCP, опція 82 дозволяє надану DHCP Relay Agent (наприклад, комутатору або маршрутизатору) додавати інформацію про себе до запиту. Це включає дані, такі як VLAN або порт, що використовується для підключення.

DHCP-сервер, отримуючи ці додаткові дані, може перевірити, чи дійсно запит надходить з надійного джерела, знижуючи ризик успішної атаки з фальшивими DHCP-серверами. Наприклад, сервер може надавати адреси лише тим пристроям, що підключені до певних довірених портів, що ускладнює атаки на комп'ютери, які не мають відповідних прав. Завдяки інформації з опції 82, адміністратори можуть легше відстежувати і аналізувати DHCP-трафік. Це полегшує виявлення аномалій або підозрілих запитів, що може вказувати на спроби атак.

1.5.7 VLAN Segmentation

Одним з ефективних способів зменшення векторів таких атак є впровадження VLAN (Virtual Local Area Network). Використання VLAN дозволяє логічно сегментувати мережу та ізолювати клієнтів, сервери й інші мережеві ресурси. Зокрема, розміщення DHCP-сервера у виділеній VLAN (наприклад, VLAN 99) забезпечує фізичне та логічне відокремлення його від клієнтських пристроїв. У такій конфігурації клієнти в інших VLAN не мають прямого доступу до DHCP-сервера, що значно ускладнює запуск несанкціонованого DHCP-сервера або здійснення атаки типу Man-in-the-Middle. Крім того, VLAN сприяє зменшенню зони розповсюдження широкомовного трафіку (broadcast domain), у межах якого передаються DHCP-запити. Це ускладнює реалізацію атак типу DHCP starvation, під час яких зловмисник намагається вичерпати пул доступних IP-адрес. У поєднанні з функціональністю маршрутизатора або L3-комутатора (через механізм `ip helper-address`), мережа може централізовано передавати

DHCP-запити з клієнтських VLAN до сервера, розташованого у захищеній VLAN.

1.6 Обґрунтування вибраного напрямку інженерного рішення

Проєктування безпечної мережної інфраструктури для навчального закладу, зокрема коледжу, вимагає всебічного аналізу сучасних викликів у сфері інформаційної безпеки та оптимального вибору технологій, здатних гарантувати цілісність і доступність критичних сервісів. Одним із таких сервісів є DHCP – служба динамічного призначення IP-адрес, без якої неможливе масштабоване та централізоване адміністрування IP-мереж.

Аналіз існуючих ризиків, таких як DHCP spoofing, rogue DHCP-сервери та DoS-атаки (DHCP starvation), показує, що базові налаштування DHCP у корпоративних мережах є вразливими до порушення мережної функціональності, перехоплення трафіку та несанкціонованого доступу до ресурсів. Ці проблеми особливо актуальні для середовищ із великою кількістю користувачів і частою зміною клієнтських пристроїв, що характерно саме для навчальних закладів.

В цій кваліфікаційній роботі вибраний інженерний напрямок полягає у впровадженні комплексного захисту DHCP-сервісів шляхом поєднання таких технологій, як:

– DHCP Snooping –для створення захищеної бази даних авторизованих клієнтів і фільтрації нелегітимного DHCP-трафіку;

– IP Source Guard – для перевірки відповідності IP- та MAC-адрес клієнта під час передачі даних;

– Dynamic ARP Inspection (DAI) – як додатковий захист від атак типу ARP spoofing, які можуть супроводжувати DHCP-атаки;

– VLAN-сегментація та обмеження рівнів довіри до інтерфейсів – для ізоляції користувацьких і службових сегментів мережі;

– контроль доступу через ACL та Port Security – як механізм базової фільтрації трафіку;

– використання Cisco Packet Tracer – для моделювання, тестування та демонстрації функціональності захисних механізмів у навчальному середовищі.

Рішення базується на VLAN-архітектурі з доповненням механізмів L2-рівня, такими як DHCP snooping, DAI, що забезпечує фільтрацію недостовірних DHCP-повідомлень. У поєднанні з Access Control Lists (ACL) та Port Security, така модель створює багаторівневий захист проти типових атак на DHCP.

Враховуючи відкритість доступу до мережі у навчальному закладі, обраний підхід дає змогу забезпечити:

– централізоване управління адресацією без втрати безпеки;

– запобігання появі нелегальних DHCP-серверів;

– контроль автентичності трафіку на другому рівні моделі OSI;

– адаптацію під сучасні навчальні лабораторії та подальшу масштабованість.

Важливим чинником є також сумісність запропонованого рішення з наявним мережним обладнанням Cisco, що активно використовується в навчальних закладах для лабораторних і проєктних робіт. Вибір Cisco Packet Tracer як середовища моделювання дозволяє детально протестувати механізми безпеки до їхнього впровадження в реальну мережу.

1.7 Завдання і мета роботи

Метою даної кваліфікаційної роботи є проєктування безпечної мережної інфраструктури коледжу з акцентом на впровадження механізмів захисту служби динамічного налаштування хостів (DHCP), з метою забезпечення надійного, стабільного та захищеного функціонування комп’ютерної мережі навчального закладу.

Захист служби DHCP розглядається як один із ключових компонентів загальної політики мережної безпеки, оскільки цей сервіс відіграє важливу

роль у процесі автоматичного розподілу IP-адрес, масок підмережі, шлюзів за замовчуванням та інших параметрів TCP/IP для кінцевих користувачів.

Для досягнення поставленої мети в роботі формуються наступні завдання:

– розробити концепцію мережної архітектури для навчального закладу з урахуванням логічної сегментації, рівнів доступу та впровадження захисту DHCP;

– створити модель комп'ютерної мережі у середовищі Cisco Packet Tracer;

– налаштувати мережне обладнання (маршрутизатори, комутатори) та налаштувати централізований DHCP-сервер;

– зміцнити мережну безпеку на рівні доступу, розробивши захист за допомогою механізмів DHCP Snooping, Port Security, Dynamic ARP Inspection (DAI);

– реалізувати атаки для демонстрації вразливості;

– перевірити працездатність розробленої мережної архітектури, протестувати ефективність впроваджених заходів захисту;

– оцінити доцільність та ефективність впроваджених засобів безпеки в умовах коледжу, з урахуванням можливостей масштабування та модернізації в майбутньому.

Таким чином, мета та завдання роботи спрямовані на поєднання теоретичних знань з практичними навичками у сфері комп'ютерних мереж, інформаційної безпеки та мережного адміністрування. Результатом роботи стане реалістична та ефективна модель захищеної інфраструктури DHCP-сервісів, яка може бути впроваджена в умовах реального навчального закладу або використана для навчання майбутніх фахівців.

2 ФОРМУВАННЯ ВИМОГ І РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КС КОЛЕДЖУ

2.1 Технічні вимоги до КС коледжу

2.1.1 Найменування і призначення КС коледжу

Комп'ютерна система коледжу представляє собою багаторівневу мережну інфраструктуру з логічною сегментацією на базі VLAN та динамічним розподілом мережних адрес засобами DHCP. Система призначена для забезпечення інформаційних потреб навчального закладу, що включає надання доступу до освітніх ресурсів, підтримку адміністративних процесів та управління мережною інфраструктурою в цілому.

Система покликана вирішувати комплекс завдань з обміну даними між підрозділами коледжу, забезпечення доступу до спільних інформаційних ресурсів, організації ефективної колаборації між студентами та викладачами, а також захисту інформації через механізми логічної сегментації мережі та контролю доступу до ресурсів різного рівня конфіденційності.

Основними користувачами системи є адміністрація коледжу, викладацький склад, студенти та технічний персонал. Кожна категорія користувачів має чітко визначені права доступу та функціональні можливості в межах своєї віртуальної мережі.

2.1.2 Вимоги до структури і функціонуванню системи

Комп'ютерна система коледжу має включати взаємопов'язані підсистеми, що забезпечують цілісність функціонування освітньої установи. Архітектура повинна базуватися на сучасних мережних технологіях з врахуванням специфіки освітнього процесу.

Підсистема локальної мережі має забезпечувати високошвидкісну передачу даних між робочими станціями, серверами та іншим обладнанням

навчального закладу. Ця підсистема слугує фундаментом для забезпечення доступу до спільних ресурсів та створює базис для адміністративних і навчальних функцій. Характеристики включають швидкість передачі даних не менше 1 Гбіт/с для кінцевих користувачів і 10 Гбіт/с для магістральних з'єднань.

Підсистема бездротового доступу повинна надавати можливість мобільного підключення до ресурсів коледжу через технологію Wi-Fi. Ця підсистема має забезпечувати суцільне покриття приміщень коледжу з можливістю роумінгу між точками доступу. Характеристики включають підтримку стандартів IEEE 802.11ac/ax (Wi-Fi 5/6) та забезпечення швидкості не менше 300 Мбіт/с на користувача.

Структура комп'ютерної системи коледжу повинна базуватися на трирівневій ієрархічній моделі з використанням технології віртуальних локальних мереж (VLAN) для логічної сегментації мережного середовища. Такий підхід забезпечує модульність та масштабованість, що особливо важливо для розростання мережі у міру збільшення кількості користувачів та пристроїв.

Мережа повинна бути побудована за ієрархічною топологією, яка включає:

– access рівень відповідає за підключення кінцевих пристроїв – ноутбуків, стаціонарних комп’ютерів, мобільних пристроїв та точок доступу wi-fi. у великих коледжах можуть бути реалізовані switch stack (набір комутаторів, що працюють як один логічний пристрій) за допомогою технологій на кшталт cisco stackwise, що спрощує керування мережею;

– distribution рівень агрегує трафік з access рівня, реалізує політики безпеки, маршрутизацію внутрішнього трафіку та забезпечує зв’язок з ядром мережі.

– рівень Core (ядро) – високопродуктивні маршрутизатори та комутатори, що забезпечують маршрутизацію та швидку передачу даних

між різними сегментами мережі. Це високопродуктивний шар із подвійною резервованістю для забезпечення безперервної роботи;

У коледжах особливо важливим є підтримка сучасних бездротових стандартів (наприклад, Wi-Fi 6), що дозволяють одночасно обслуговувати багато мобільних користувачів із високою пропускною здатністю.

Система повинна використовувати технологію VLAN для логічного поділу мережі на ізольовані сегменти відповідно до функціональних та безпекових вимог:

– VLAN 10 – адміністрація (Departament): призначена для адміністративного персоналу коледжу, обробки конфіденційної інформації та управління системами. Доступ до цієї VLAN має бути строго контрольованим із застосуванням додаткових механізмів аутентифікації;

– VLAN 20 – викладачі (Teachers): призначена для викладацького складу, забезпечує доступ до освітніх ресурсів, системи управління навчанням, та засобів підготовки навчальних матеріалів. Повинен мати пріоритет трафіку для відеоконференцій та онлайн-лекцій;

– VLAN 30 – студенти (Students): призначена для студентського контингенту, забезпечує доступ до навчальних матеріалів, електронної бібліотеки та систем дистанційного навчання. Має обмежений доступ до адміністративних ресурсів та контрольований доступ до Інтернету;

– VLAN 40 – комп'ютерні класи (Lab): призначена для навчальних лабораторій та комп'ютерних класів, забезпечує доступ до спеціалізованого програмного забезпечення та навчальних симуляторів. Має особливі політики безпеки та моніторингу активності;

– VLAN 50 – гостьовий доступ (Guest): забезпечує обмежений доступ до Інтернету для відвідувачів коледжу. Має найнижчий пріоритет трафіку та жорсткі обмеження пропускної здатності, а також повну ізоляцію від внутрішніх ресурсів;

VLAN 60 – сервери (Servers): призначена виключно для серверів. Доступ до цієї VLAN повинен бути строго обмежений IT-персоналом;

Система повинна використовувати DHCP для автоматичного конфігурування мережних параметрів кінцевих пристроїв:

– централізований DHCP-сервер повинен підтримувати функціонал DHCP-релеїв для обслуговування різних VLAN. Має здійснювати видачу IP-адрес відповідно до політики коледжу з можливістю резервування (опція 82);

– окрім стандартних параметрів (IP-адреса, маска підмережі, шлюз за замовчуванням), DHCP-сервер повинен надавати додаткові параметри, такі як адреси DNS-серверів, NTP-серверів та WINS-серверів, а також домен пошуку для DNS;

– для кожної VLAN повинен бути виділений окремий пул адрес з відповідними параметрами. Розмір пулу має враховувати поточну кількість користувачів та перспективи розвитку;

– система повинна використовувати DHCP Snooping для запобігання атак з неавторизованих DHCP-серверів. IP Source Guard та Dynamic ARP Inspection мають бути активовані для запобігання спуфінгу;

– для серверів, принтерів та іншого стаціонарного обладнання має бути реалізовано механізм зарезервованих адрес на основі MAC-адрес;

– система повинна забезпечувати детальне журналювання всіх DHCP-транзакцій для аудиту та діагностики проблем.

2.1.3 Вимоги до способів і засобів зв'язку між компонентами

Для забезпечення оптимального функціонування комп'ютерної системи коледжу необхідно впровадити різноманітні технології зв'язку, що відповідають найкращим сучасним практикам у галузі мережних комунікацій.

Магістральні з'єднання між рівнями Core та Distribution повинні реалізовуватися за допомогою волоконно-оптичних ліній зв'язку з використанням стандарту не нижче 10GBASE-SR/LR. Це забезпечить високу пропускну здатність та стійкість до електромагнітних завад. Оптичні

з'єднання також слід використовувати для зв'язку між географічно розподіленими корпусами коледжу, якщо такі існують.

На рівні Distribution та Access необхідно застосовувати технологію Ethernet з пропускною здатністю від 1 до 10 Гбіт/с. Комутатори рівня Distribution повинні підтримувати функції агрегації каналів (IEEE 802.3ad), що дозволить збільшити пропускну здатність та забезпечити відмовостійкість. Доступ кінцевих користувачів має забезпечуватися через комутатори з портами Fast Ethernet (100 Мбіт/с) або Gigabit Ethernet (1 Гбіт/с), залежно від потреб конкретних підрозділів.

Бездротова інфраструктура повинна базуватися на стандартах IEEE 802.11ac/ax (Wi-Fi 5/6) з підтримкою WPA3 для шифрування. Точки доступу мають бути розміщені таким чином, щоб забезпечити повне покриття всіх навчальних та адміністративних приміщень. Контролери Wi-Fi повинні забезпечувати централізоване управління, моніторинг та налаштування точок доступу.

Для сегментації мережі та забезпечення безпеки необхідно використовувати технологію VLAN (IEEE 802.1Q), що дозволить логічно розділити мережу на окремі сегменти відповідно до функціональних груп (адміністрація, викладачі, студенти, гості).

Для управління мережним обладнанням необхідно використовувати протоколи SNMP v3, SSH та HTTPS, які забезпечують безпечне адміністрування та моніторинг мережної інфраструктури.

2.1.4 Вимоги функцій, виконуваним системою

Комплексний механізми безпеки та контролю доступу.

– Port Security: обмеження кількості MAC-адрес на портах комутаторів доступу для запобігання несанкціонованим підключенням;

– DHCP Snooping: захист від неавторизованих DHCP-серверів через перевірку DHCP-повідомлень;

– Dynamic ARP Inspection: захист від ARP-спуфінгу шляхом перевірки відповідності IP та MAC адрес;

– IP Source Guard: захист від IP-спуфінгу через фільтрацію вхідного трафіку на основі таблиць DHCP Snooping;

– Private VLAN: додаткова ізоляція в межах однієї VLAN для критично важливих систем.

Для забезпечення безпеки та ефективного управління мережними ресурсами наступні вимоги до адресації:

– статичні резервування DHCP для директора, заступників та відповідальних осіб;

– для викладацького складу та навчально-методичних кабінетів DHCP з лізингом на 14 днів;

– для студентських комп'ютерів загального призначення найбільший DHCP-пул, розрахований на одночасне підключення до 400 пристроїв;

– для комп'ютерів у навчальних лабораторіях DHCP з опцією PXE Boot для розгортання образів ОС;

– для відвідувачів коледжу DHCP з коротким терміном лізингу (4 години);

– для управління мережним обладнанням статичні IP-адреси з мінімальним використанням DHCP;

– для серверів та критично важливих систем статичні IP-адреси.

2.1.5 Вимоги до показників призначення

Пропускна здатність мережної інфраструктури є одним з ключових показників, що визначає можливість системи обслуговувати велику кількість користувачів одночасно. Магістральні з'єднання між рівнями Core та Distribution повинні забезпечувати пропускну здатність не менше 10 Гбіт/с, з можливістю масштабування до 40/100 Гбіт/с при подальшій модернізації. На рівні доступу комутатори повинні забезпечувати швидкість з'єднання не менше 1 Гбіт/с для кожного користувача. Бездротова мережа

має забезпечувати реальну пропускну здатність не менше 300 Мбіт/с для кожного активного пристрою.

Час відгуку системи є критичним показником для забезпечення комфортної роботи користувачів. Для локальних сервісів (внутрішні веб-портали, бази даних) час відгуку не повинен перевищувати 100 мс. Для зовнішніх ресурсів, доступних через Інтернет, затримка повинна бути не більше 500 мс. При роботі з системами управління навчанням (LMS) час завантаження сторінок не повинен перевищувати 2 секунди.

Масштабованість системи має забезпечувати можливість одночасної роботи всіх користувачів коледжу. Система повинна підтримувати одночасне підключення не менше 400 користувачів, з перспективою збільшення до 1000. При цьому продуктивність системи не повинна знижуватися більш ніж на 20% при максимальному навантаженні.

Надійність та доступність системи є критичними показниками для забезпечення безперервності освітнього процесу. Система повинна забезпечувати коефіцієнт готовності не менше 99,9% (що відповідає простою не більше 8,76 годин на рік). Для критичних підсистем (аутентифікація, основні сервіси) коефіцієнт готовності має бути не менше 99,95%. Середній час між відмовами (MTBF) для серверного обладнання повинен бути не менше 50000 годин, а для мережного обладнання – не менше 100000 годин.

Система аутентифікації повинна підтримувати не менше 500 одночасних сесій, з максимальною затримкою при авторизації не більше 2 секунд. Веб-сервери повинні обслуговувати не менше 1000 одночасних з'єднань без значного зниження продуктивності.

2.2 Розробка апаратної частини комп'ютерної системи

2.2.1 Розробка загальної архітектури мережі коледжу

Оптимальною архітектурною моделлю для коледжу є класична трирівнева ієрархічна схема (рис. 2.1) з логічною сегментацією на базі VLAN та динамічним розподілом мережних адрес через DHCP:

– рівень ядра (Core Layer);

– рівень розподілу (Distribution Layer);

– рівень доступу (Access Layer).

Ця архітектура дозволяє впровадити складні політики безпеки, зменшити кількість точок відмови, легко масштабуватися під зростаючу кількість користувачів і сервісів. В усіх сучасних корпоративних та освітніх мережах така топологія вважається еталонною.

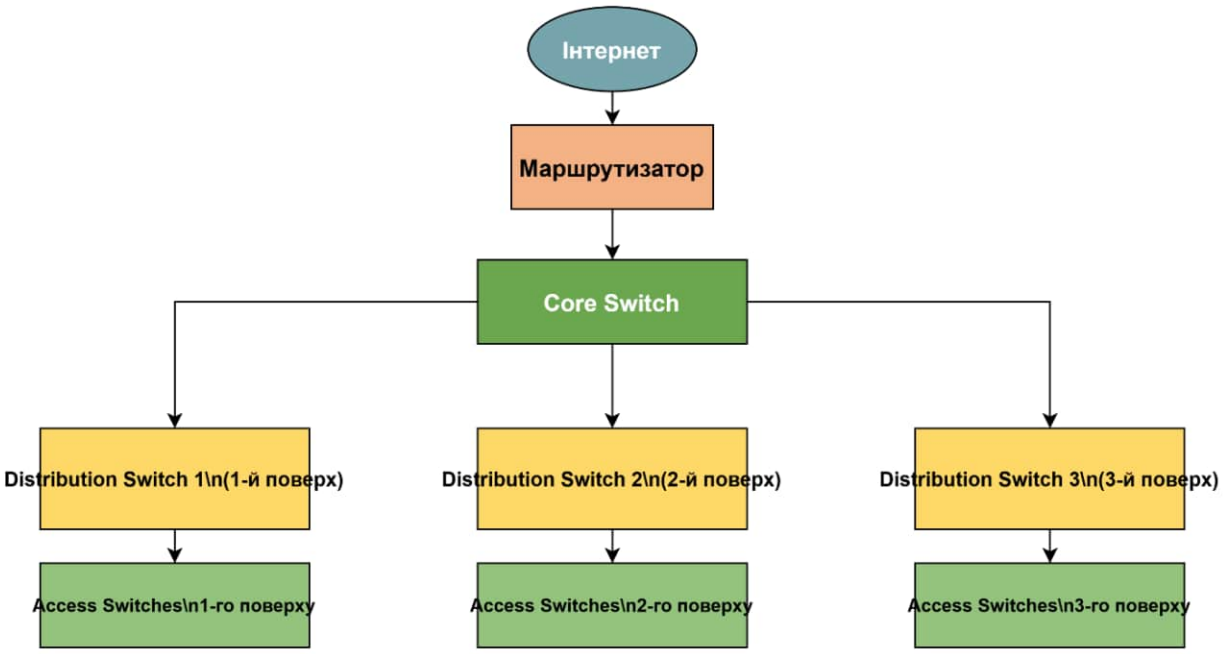

Рисунок 2.1 – Архітектура мережі коледжу

Мережа коледжу представлена у вигляді трирівневої ієрархічної структури:

а) рівень ядра (Core Layer):

1) забезпечує високошвидкісну маршрутизацію між різними VLAN;

2) складається з двох високопродуктивних комутаторів Layer 3 у відмовостійкій конфігурації;

3) підключення до зовнішньої мережі (Інтернет) через маршрутизатор;

4) взаємодія з серверною фермою, що включає два DHCP-сервери.

а) рівень розподілу (Distribution Layer):

1) агрегування трафіку з рівня доступу;

2) реалізація політик безпеки та фільтрації;

3) три комутатори Layer 3, по одному на кожен поверх коледжу;

4) підтримка DHCP Relay для передачі DHCP-запитів з різних VLAN до централізованих DHCP-серверів.

б) рівень доступу (Access Layer):

1) безпосереднє підключення кінцевих пристроїв;

2) 16 комутаторів Layer 2 з підтримкою VLAN, розподілених по поверхах і навчальних аудиторіях;

3) конфігурація портів відповідно до приналежності до конкретних VLAN;

4) впровадження механізмів DHCP Snooping, IP Source Guard та Dynamic ARP Inspection;

5) налаштування helper-address для перенаправлення DHCP-запитів з різних VLAN на централізовані DHCP-сервери та додавання опції 82 для ідентифікації джерела запиту.

Для забезпечення ефективного розподілу IP-адрес розробити централізовану систему DHCP, що складається з:

а) первинний DHCP-сервер:

– відповідає за обробку запитів з усіх VLAN;

– розташований у серверній кімнаті з контрольованим доступом;

– підключений до комутаторів рівня ядра;

– конфігурація окремих DHCP-областей для кожної VLAN.

б) вторинний DHCP-сервер:

– працює в режимі Hot Standby для відмовостійкості;

– синхронізує конфігурацію та лізинги з первинним сервером;

– автоматично приймає на себе обробку запитів у випадку відмови первинного сервера.

2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Побудова надійної та захищеної комп'ютерної мережі потребує ретельного вибору мережевого обладнання, яке не лише відповідає технічним вимогам інфраструктури навчального закладу, а й підтримує сучасні функції безпеки, необхідні для реалізації захисних механізмів, зокрема DHCP Snooping, Dynamic ARP Inspection, IP Source Guard та інших.

На основі розробленої архітектури комп'ютерної мережі коледжу було сформовано структурну схему комплексу технічних засобів, яка забезпечує масштабованість, безпеку та відмовостійкість системи на всіх її рівнях – від ядра до периферійного доступу (рис. 2.2).

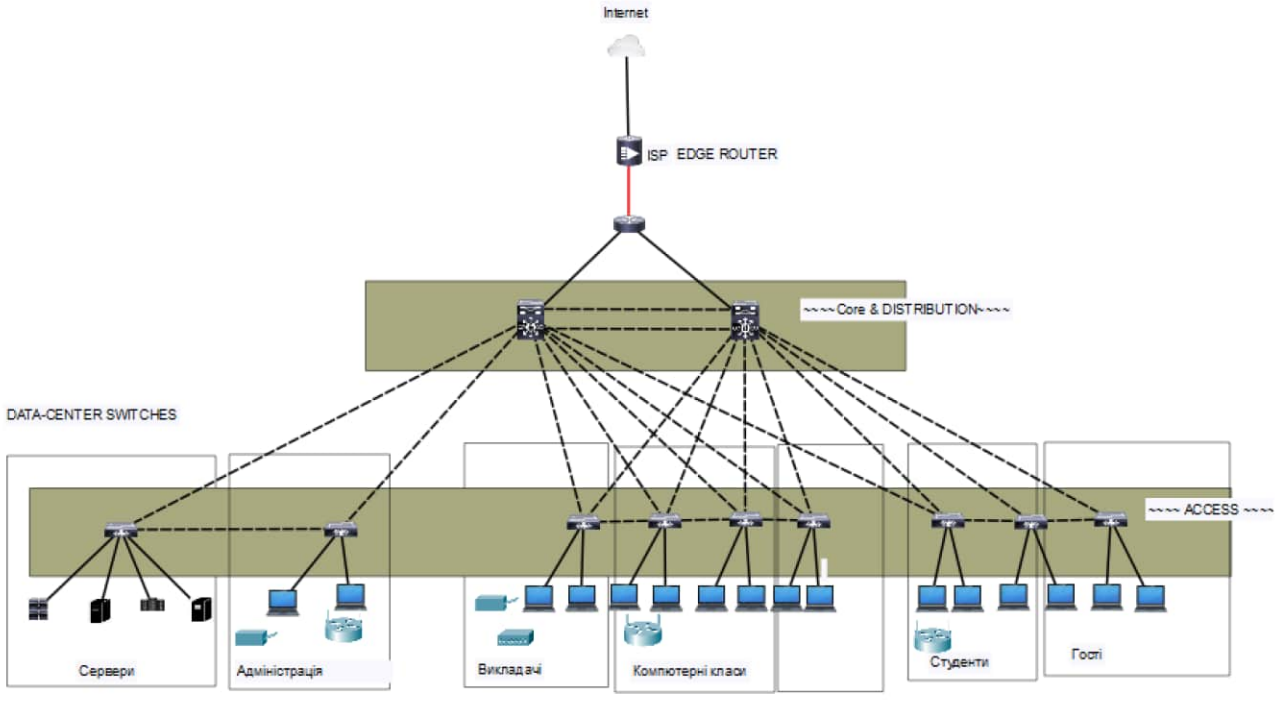

Рисунок 2.2 – Структурна схема комплексу технічних засобів колежду

З огляду на цілі проєкту, для моделювання мережної інфраструктури коледжу обрано обладнання Cisco, яке є галузевим стандартом у сфері мережевих технологій і підтримується в симуляційному середовищі Cisco Packet Tracer. Це дозволяє на практиці реалізувати необхідні функції, протестувати політики безпеки, а також створити навчальне середовище для демонстрації типових атак та механізмів протидії.

Центральним елементом виступає рівень ядра, де передбачено встановлення двох високопродуктивних комутаторів Cisco Catalyst 3650 Series з модулями 10G SFP+, об'єднаних у стек для забезпечення резервування та надійності. Ці комутатори відповідають за міжвіртуальну маршрутизацію, централізоване підключення серверної інфраструктури та взаємодію із зовнішньою мережею через маршрутизатор Cisco 2911. Останній реалізує політики безпеки, такі як ACL і Zone-Based Firewall, а також резервує канали доступу до Інтернету. Вони також виконую функцію рівня розподілу, та відповідають за агрегацію трафіку з рівня доступу, міжповерхову маршрутизацію та застосування політик безпеки. Кожен з комутаторів виконує функції DHCP Relay Agent з підтримкою опції 82, що дозволяє ідентифікувати клієнтів і застосовувати відповідні фільтри доступу.

Рисунок 2.3 – Комутатор Cisco 3560

Маршрутизатор Cisco 2911 – використовується як центральний маршрутизатор, що забезпечує маршрутизацію між VLAN, NAT, доступ до зовнішньої мережі та підтримку DHCP Relay (через функцію ip helper-address). Цей пристрій обрано за його підтримку інтегрованих сервісів, зокрема політик безпеки, фільтрації трафіку та роботи з ACL. На

маршрутизаторі використовується модуль GLC-LH-SMD для під'єднання оптичного кабелю (рис. 2.4).

Рисунок 2.4 – Маршрутизатор Cisco 2911

На рівні доступу впроваджено 16 керованих комутаторів Cisco Catalyst 2960-X Series (рис. 2.5) із підтримкою технології PoE+, що забезпечує живлення IP-телефонів, точок доступу та інших пристроїв без потреби в додаткових джерелах живлення. Порти кожного з комутаторів налаштовано у режимі access з чітким закріпленням за VLAN, відповідно до топології мережі. Реалізовано ключові функції безпеки – DHCP Snooping, IP Source Guard і Dynamic ARP Inspection, що забезпечують захист від типових мережевих атак та несанкціонованого доступу.

Рисунок 2.5 – Комутатор Cisco 2960

Серверна інфраструктура базується на двох потужних серверах Dell PowerEdge R740 з ОС Windows Server 2022. Вони виконують ролі DHCP-, DNS- та Active Directory-серверів. Як сховище даних використовується система Dell EMC Unity, що забезпечує високу продуктивність та підтримку відмовостійкості. Для захисту даних реалізовано систему резервного копіювання Veeam Backup & Replication, яка гарантує збереження критичної інформації та можливість швидкого відновлення у разі збою.

DHCP-сервер (симульований у Packet Tracer) – виступає як централізований сервер для автоматичного розподілу IP-адрес. Його розміщено в окремій захищеній VLAN (наприклад, VLAN 60), що унеможливлює прямий доступ з клієнтських VLAN;

Кінцеві пристрої (ПК, принтери) – моделюють робочі станції студентів і персоналу, з яких генеруються DHCP-запити та інші види трафіку. На цих пристроях також імітуються дії потенційного зловмисника для перевірки ефективності захисту.

Обґрунтування вибору технічних засобів базується на ряді вагомих факторів. Cisco Catalyst – це серія комутаторів, що повністю відповідає вимогам сучасної освітньої установи. Вони підтримують усі необхідні технології – VLAN, Port Security, DHCP Snooping, IP Source Guard, DAI – та забезпечують єдину централізовану платформу керування мережею. Їхня висока надійність, масштабованість та функціональні можливості роблять їх ідеальними для створення критично важливої інфраструктури.

У сукупності така архітектура забезпечує надійну, масштабовану та керовану мережеву інфраструктуру, адаптовану до потреб сучасного навчального закладу. Вона підтримує централізовану політику безпеки, високий рівень доступності сервісів, ефективне управління користувачами та ресурсами, що дозволяє створити гнучке цифрове середовище для освітнього процесу.

2.2.3 Розробка специфікації апаратних засобів

У таблиці 2.2 подано рекомендовану специфікацію основного апаратного забезпечення для мережевої інфраструктури коледжу, розрахованої на обслуговування понад 100 працівників та сотень студентів. Для апаратної складової обрано обладнання Cisco, оскільки воно повністю підтримується у середовищі Cisco Packet Tracer. Це дозволяє створювати реалістичні моделі мережі, проводити її тестування та налагодження ще до фактичного впровадження, що значно знижує ймовірність помилок,

покращує підготовку IT-персоналу й підвищує ефективність функціонування системи контролю доступу та обміну даними. Для реалізації мережі було обрано обладнання, яке забезпечує необхідну продуктивність, можливість масштабування та централізоване управління.

Таблиця 2.1 – Специфікація обладнання

№	Пристрій	Модель	Тип	Кількість	Призначення
1	Мультилейер-комутатор	Cisco 3750-24PS	L3-комутатор	1	Ядро мережі, маршрутизація між Central/Filial/DC, OSPF
2	Доступні комутатори	Cisco 2960-24TT	L2-комутатор	8	Підключення кінцевих пристроїв у Central (3 свитчі), Filial (6 свитчів, по одному на LAN-сегмент), DC (2 в Port-channel)
3	Маршрутизатор Central	Cisco 2911	L3-маршрутизатор	1	Sub-інтерфейси VLAN 10–70, WAN→ISP, OSPF, DHCP-Relay для Central
7	Точки доступу	Cisco Aironet 2800 Series	Access Point	20	Розміщені по одній у кожній підмережі коледжу
8	Сервери	Dell PowerEdge	Сервер	2	Private DHCP

3 РОЗРОБКА КАМПУСНОЇ МЕРЕЖІ КОЛЕДЖУ

3.1 Проєктування логічної топології мережі коледжу

Логічна топологія мережі коледжу, представлена на рисунку 3.1, є ієрархічною багаторанговою структурою, яка організована для підтримки різних функціональних підрозділів академічного або корпоративного середовища з розподілом мережевого трафіку за VLAN. Мережа коледжу складається з серверної, офісу адміністратора мережі, гуртожитку та бібліотеки. Оскільки кожен об'єкт знаходиться в різній мережі, створені віртуальні LAN, завдяки маршрутизації Inter-VLAN routing. Серверна зона складається з 4 серверів, а саме: DNS+HTTP, SMTP, FTP, DHCP та резервного DHCP. Сервіси, такі як DNS та HTTP, реалізовані на одному сервері.

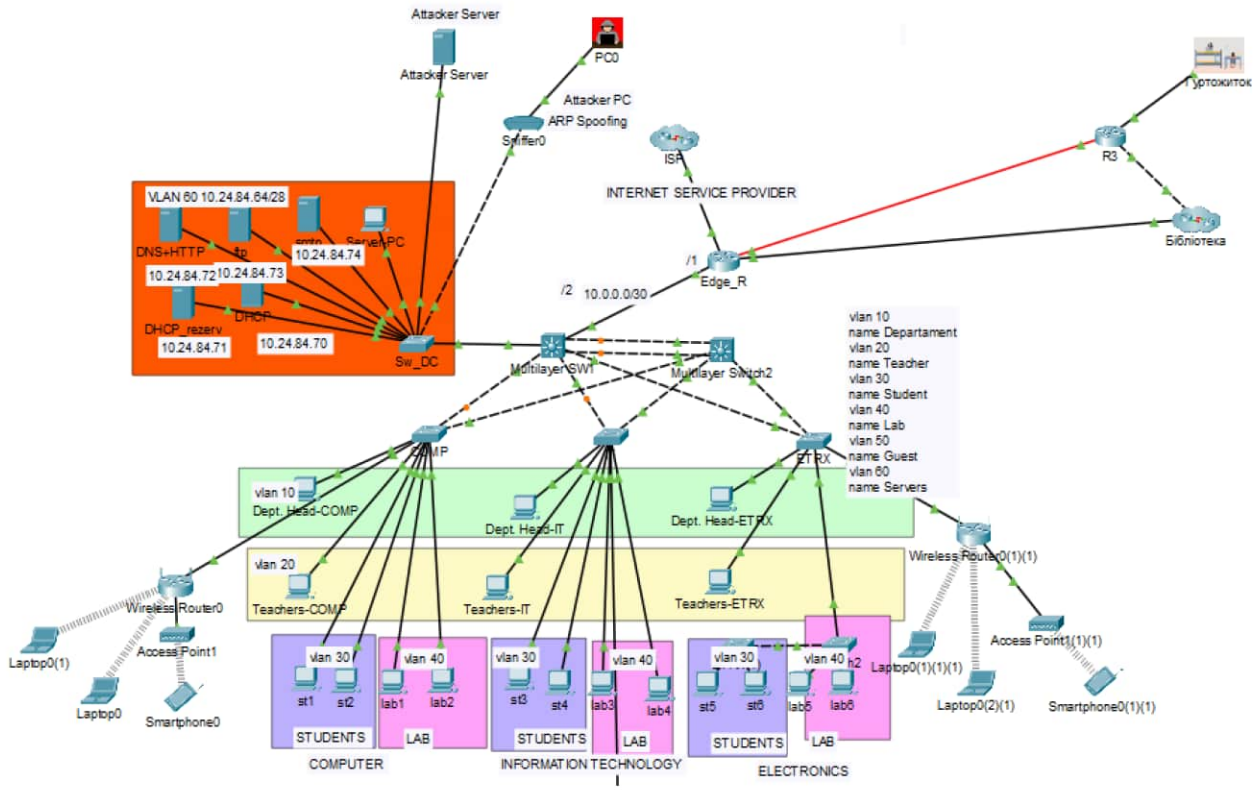

Рисунок 3.1 – Логічна топологія мережі коледжу

а) Рівень ядра та розподілу (Core & Distribution Layer).

Центральним елементом є маршрутизатор ядра (Edge_R), що

забезпечує маршрутизацію між VLAN і комунікацію з зовнішнім Інтернетом. Маршрутизатор границі мережі Edge_R змонтовано в серверній стійці. Його фізичний інтерфейс GigabitEthernet0/0/0 розділяє трафік VLAN на єдиному лінку до комутатора Multilayer SW1. Інтерфейс GigabitEthernet0/0/2 підключений до маршрутизатора провайдера по мережі 123.123.0.4/30. Такий окремий канал 1 Gbps забезпечує вихід у Інтернет і чітке розділення внутрішнього та зовнішнього трафіку

В цьому рівні також присутній другий комутатор (Multilayer_SW2), забезпечуючи резервування та балансування навантаження.

Комутатори розподілу (Dept Head-COMP, Dept Head-IT, Dept Head-ELEC) розподіляють мережевий трафік у відповідні відділи, реалізуючи доступ до підмереж VLAN для різних департаментів.

Кожен комутатор розподілу інтегрує під'єднані пристрої з певного VLAN, призначеного для конкретної категорії користувачів чи обладнання.

б) Нижній рівень (Access).

Комутатори доступу підключають кінцеві пристрої (ПК, ноутбуки, смартфони) і служать для концентрації трафіку від користувачів.

Пристрої розбиті по VLAN, кожен з яких відповідає певній групі: Department (vlan 10), Teacher (vlan 20), Student (vlan 30), Lab (vlan 40), Guest (vlan 50), Servers (vlan 60).

Підключення передбачає розмежування трафіку згідно з призначенням груп користувачів для безпеки та ефективного управління мережею.

Це критичний рівень для впровадження більшості функцій безпеки канального рівня, таких як:

– DHCP Snooping: запобігання Rogue DHCP Servers та боротьба з DHCP Starvation;

– Port Security: обмеження кількості MAC-адрес на порту для запобігання переповнення таблиць MAC та несанкціонованих підключень;

– Dynamic ARP Inspection (DAI): запобігання ARP-спуфінгу;

– IP Source Guard: запобігання IP-спуфінгу;

– Storm Control: запобігання широкомовним, багатоадресним та одноадресним штормам.

– VLAN Trunking: аплінк-порти, що з'єднують комутатори доступу з багатошаровими комутаторами, налаштовані як транкові порти для передачі трафіку всіх VLAN.

в) Серверна зона VLAN 60.

Відокремлений сегмент мережі, що містить сервери, DNS, DHCP, SMTP і забезпечує корпоративні послуги в мережі.

ServerPT DHCP (10.24.80.70): Це легітимний DHCP-сервер мережі. Він відповідає за:

– призначення IP-адрес, масок підмережі, шлюзів за замовчуванням та DNS-серверів кінцевим пристроям у різних VLAN;

– управління пулами IP-адрес, термінами оренди;

– ведення обліку орендованих адрес.

ServerPT DHCP-relay (10.24.80.71 є резервним DHCP-сервером/сервером. Якщо він є Relay Agent, то він пересилає DHCP-запити від клієнтів до ServerPT DHCP (10.24.80.70) і назад.

Attacker Server: це зловмисний елемент. Його функція -– імітувати дії атакуючого, зокрема:

– виступати як Rogue DHCP Server, щоб перехоплювати DHCP-запити та видавати шкідливі налаштування;

– бути джерелом атаки DHCP Starvation;

– виступати як цільовий пристрій для перехоплення трафіку (наприклад, MitM).

3.2 IP-адресація та DHCP

Надійна IP-адресація є базовою умовою функціонування будь-якої корпоративної мережі. У мережі коледжу, де щоденно працює понад 800 студентів і 100 співробітників, використання автоматизованих засобів

призначення IP-адрес є не лише доцільним, а й критично необхідним для забезпечення керованості, безпеки та ефективності адміністрування.

З метою забезпечення логічної ізоляції трафіку та ефективного управління адресним простором, у проєкті було використано метод VLSM (Variable Length Subnet Masking) на основі приватного блоку 10.24.80.0/20 (2046 доступних IP-адрес). Розділення мережі на підмережі здійснювалось відповідно до кількості необхідних хостів у кожній VLAN з урахуванням перспектив масштабування (табл 3.1).

Таблиця 3.1 – Адресація підмережі кампусу

VLAN	Назва	Кількість хостів	Мережа	Діапазон хостів	Broadcast
30	Студенти	400	10.24.80.0/23	10.24.80.1 – 10.24.81.254	10.24.81.255
50	Гостьовий доступ	200	10.24.82.0/24	10.24.82.1 – 10.24.82.254	10.24.82.255
40	Комп’ютерні класи	100	10.24.83.0/25	10.24.83.1 – 10.24.83.126	10.24.83.127
20	Викладачі	70	10.24.83.128/25	10.24.83.129 10.24.83.254	10.24.83.255
10	Адміністрація	50	10.24.84.0/26	10.24.84.1 – 10.24.84.62	10.24.84.63
60	Сервери	10	10.24.84.64/28	10.24.84.65 - 10.24.84.78	10.24.84.79

Залишок IP-адрес у блоці 10.24.80.0/21 зарезервовано для VPN-клієнтів та майбутнього масштабування.

Блок 10.24. 10.24.84.64/28 виділений для статичної адресації серверів коледжу (рис. 3.2).

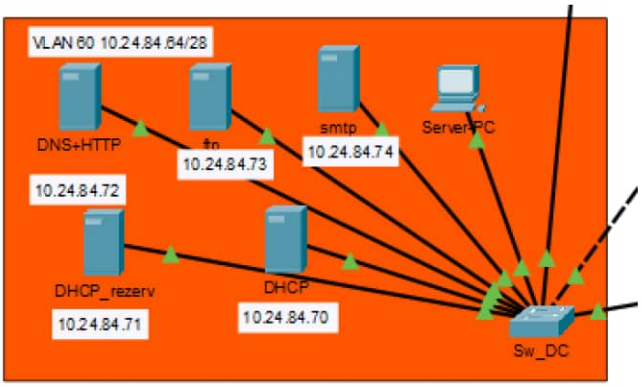

Рисунок 3.2 – Мережа серверів коледжу

На представленому рисунку 3.3 зображено інтерфейс налаштування DHCP-сервісу в мережевому симуляторі Packet Tracer. Зокрема, інтерфейс знаходиться у вкладці «Services», де обрано розділ «DHCP». Створені DHCP пули для різних VLANів, яка охоплює такі дані як ім’я пулу, шлюз за замовчуванням, DNS-сервер, початкова IP-адреса, підмережна маска, максимальна кількість користувачів, а також параметри TFTP-сервера і WLC-адреси. Значущі записи таблиці включають наступні VLAN-и з відповідними характеристиками.

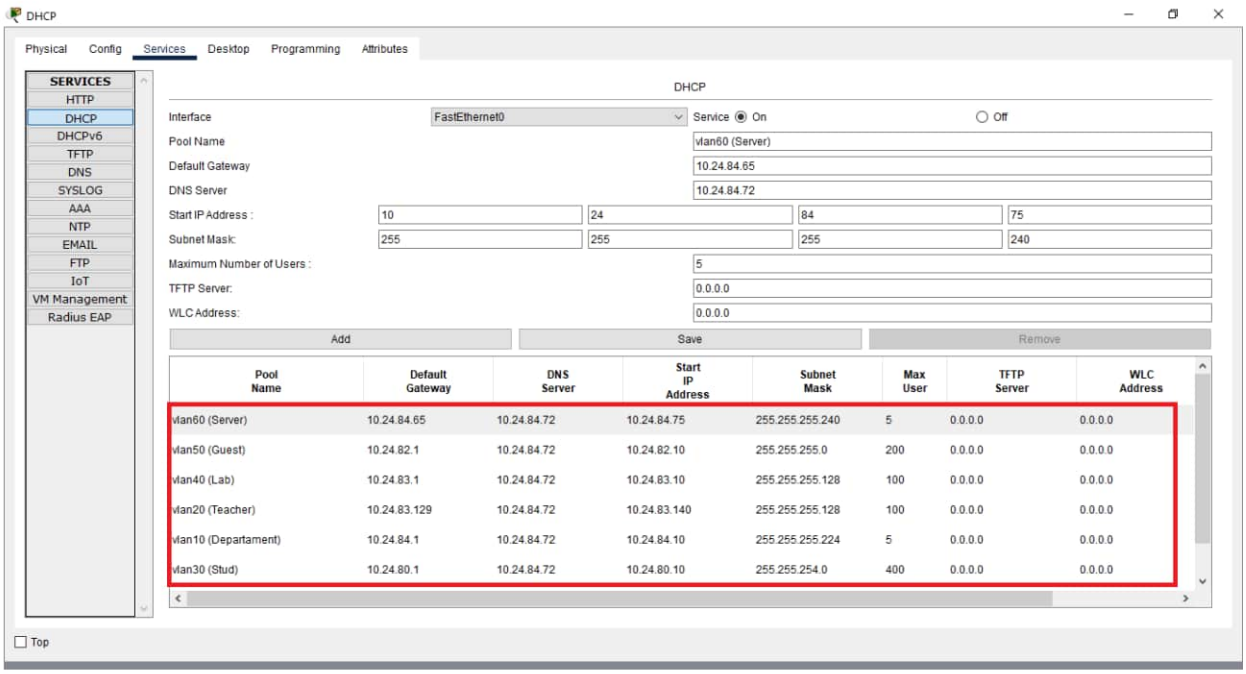

Рисунок 3.3 – Налаштування пулів DHCP

Дані в інтерфейсі дозволяють адміністраторам мережі здійснювати конфігурацію DHCP-сервера, забезпечуючи автоматичне надання IP-адрес різним пристроям у межах відповідних VLAN-мереж з різними параметрами підмережі та лімітами користувачів/

На зображенні 3.4 наведено вивід команди show ip interface brief для маршрутизатора Edge_R, що надає огляд стану його інтерфейсів.

```
Edge_R#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  10.24.84.1      YES manual up                    up
GigabitEthernet0/0.20  10.24.83.129    YES manual up                    up
GigabitEthernet0/0.30  10.24.80.1      YES manual up                    up
GigabitEthernet0/0.40  10.24.83.1      YES manual up                    up
GigabitEthernet0/0.50  10.24.82.1      YES manual up                    up
GigabitEthernet0/0.60  10.24.84.65     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     82.10.0.2       YES manual up                    up
GigabitEthernet0/1/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/2/0   unassigned      YES unset  administratively down down
GigabitEthernet0/3/0   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Рисунок 3.4 – Відомості про IP-адресацію інтерфейсів роутера Edge_R

На рисунку 3.5 наведено конфігураційні команди для двох інтерфейсів на маршрутизаторі, а саме GigabitEthernet0/0.30 та GigabitEthernet0/0.40. ip helper-address 10.24.84.70 вказує на сервер DHCP (і, можливо, інші служби), до якого пересилаються запити на отримання IP-адреси.

```
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.24.80.1 255.255.254.0
 ip helper-address 10.24.84.70
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.24.83.1 255.255.255.128
 ip helper-address 10.24.84.70
!
```

Рисунок 3.5 – Налаштування підінтерфейсів та ретрансляції DHCP

На рисунку 3.6 представлені налаштування IP-адрес для двох різних пристроїв (st5 та lab5) у мережі з VLAN 30 та VLAN 40 відповідно. Обидва

пристрої використовують протокол DHCP для отримання IP-адресів, з різними підмережами та параметрами.

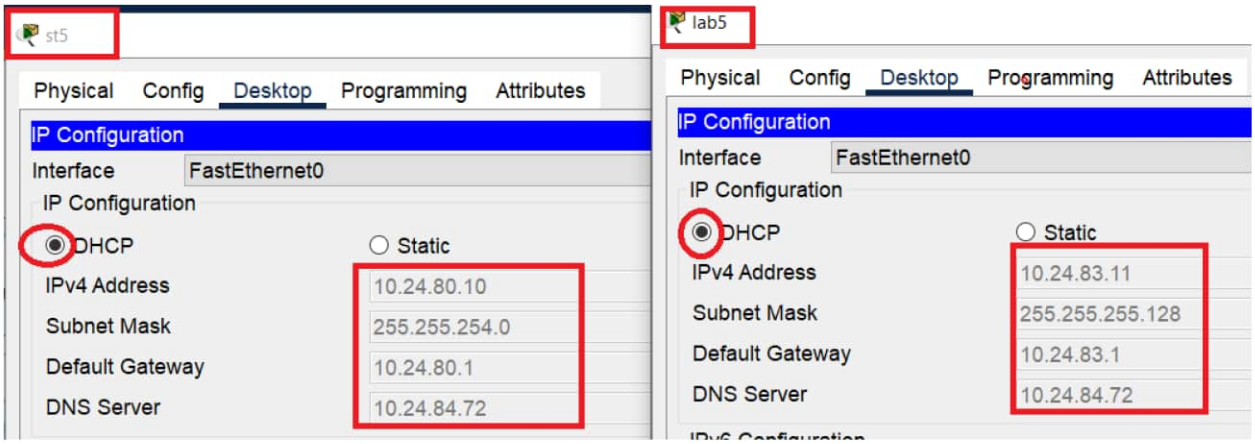

Рисунок 3.6 – Налаштування IP-адресації на ПК

Протестовано працездатність мережі за допомогою відправки icmp пакетів як ми могли спостерігати обмін пакетами між вузлами (рис.3.7). Пристрій st5 успішно взаємодіє з пристроєм lab5 у мережі на основі IP.

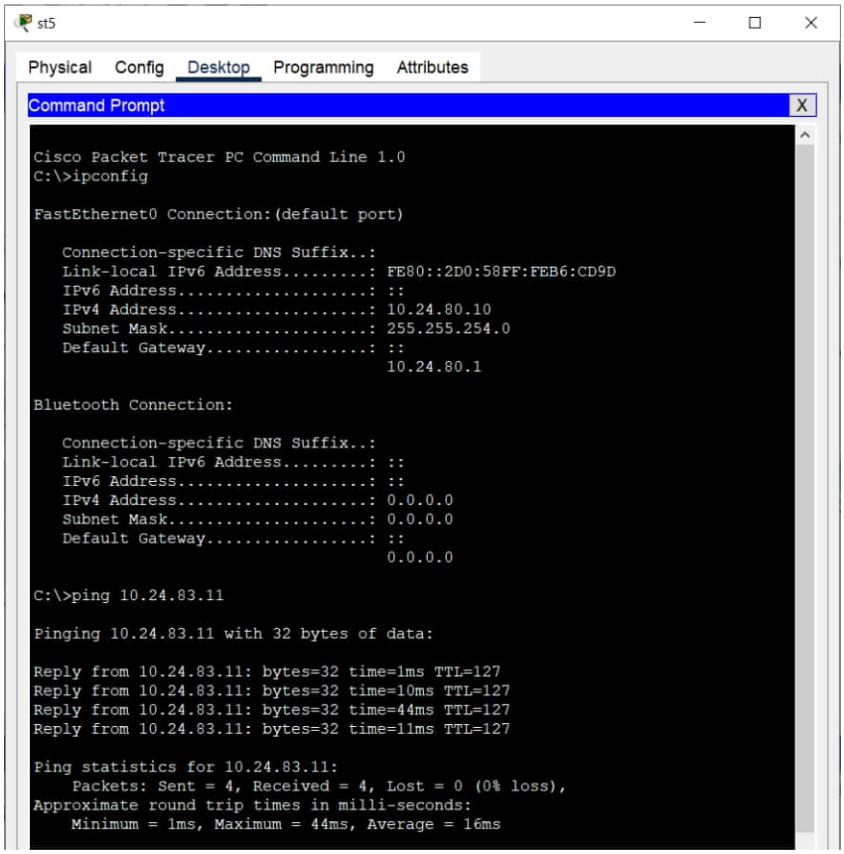

Рисунок 3.7 – Перевірка взаємодіє між ПК в різних VLAN

3.3 Налаштування доступу до мережі Інтернет

Для забезпечення виходу пристроїв внутрішньої мережі до глобальної мережі Інтернет необхідно налаштувати маршрут за замовчуванням на прикордонному маршрутизаторі (Edge Router). Цей маршрут спрямовує весь трафік, який не призначено для локальної мережі, до провайдера Інтернет-послуг (ISP).

На прикордонному маршрутизаторі було виконано таку команду конфігурації:

Edge_R(config)#ip route 0.0.0.0 0.0.0.0 82.10.0.1

Ця команда означає:

– ip route – створення статичного маршруту;

– 0.0.0.0 0.0.0.0 – універсальна адреса і маска маршруту за замовчуванням, яка охоплює весь IPv4-простір;

– 82.10.0.1 – IP-адреса наступного стрибка (next hop), тобто маршрутизатора провайдера або пристрою, що надає доступ до зовнішньої мережі.

Таким чином, якщо жоден з внутрішніх маршрутів не відповідає адресі призначення, трафік буде переспрямовано на вказану адресу шлюзу – 82.10.0.1.

На зображенні 3.8 наведено результат команди show ip route для маршрутизатора Edge_R. Цей вивід містить інформацію про маршрути, які використовуються для передачі даних, а також про їхні статуси та методи налаштування. 82.10.1.1 для мережі 0.0.0.0, що вказує на адресу, яку буде використовувати маршрутизатор для доступу до невідомих мереж.

```
Edge_R#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS i
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 82.10.0.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 12 subnets, 6 masks
C       10.24.80.0/23 is directly connected, GigabitEthernet0/0.30
L       10.24.80.1/32 is directly connected, GigabitEthernet0/0.30
C       10.24.82.0/24 is directly connected, GigabitEthernet0/0.50
L       10.24.82.1/32 is directly connected, GigabitEthernet0/0.50
C       10.24.83.0/25 is directly connected, GigabitEthernet0/0.40
L       10.24.83.1/32 is directly connected, GigabitEthernet0/0.40
C       10.24.83.128/25 is directly connected, GigabitEthernet0/0.20
L       10.24.83.129/32 is directly connected, GigabitEthernet0/0.20
C       10.24.84.0/26 is directly connected, GigabitEthernet0/0.10
L       10.24.84.1/32 is directly connected, GigabitEthernet0/0.10
C       10.24.84.64/28 is directly connected, GigabitEthernet0/0.60
L       10.24.84.65/32 is directly connected, GigabitEthernet0/0.60
     82.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       82.10.0.0/16 is directly connected, GigabitEthernet0/2
L       82.10.0.2/32 is directly connected, GigabitEthernet0/2
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/30 is directly connected, GigabitEthernet0/1/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/1/0
S*   0.0.0.0/0 [1/0] via 82.10.0.1
```

Рисунок 3.8 – Таблиця маршрутизації на Edge_R

Цей підхід є стандартною практикою для організації доступу до Інтернету в корпоративних та навчальних мережах, оскільки дозволяє централізовано контролювати трафік і забезпечити його подальшу обробку, зокрема реалізацію NAT (перетворення внутрішніх IP-адрес на публічні).

Для коректної роботи цього механізму також необхідно реалізувати перетворення адрес (NAT), яке буде описано у наступному підрозділі.

3.4 Реалізація механізму трансляції мережевих адрес (NAT)

Для забезпечення можливості доступу внутрішніх хостів до зовнішніх ресурсів мережі Інтернет, при збереженні використання приватного простору IP-адрес (згідно з RFC 1918), необхідно впровадити механізм трансляції мережевих адрес (Network Address Translation, NAT).

Механізм NAT дозволяє маршрутизатору перетворювати приватні IP-адреси внутрішньої мережі на публічну IP-адресу (або пул адрес) під час виходу у зовнішню мережу. Це забезпечує:

– збереження обмеженого пулу публічних IP-адрес;

– приховування внутрішньої топології мережі;

– додатковий рівень безпеки, оскільки зовнішні хости не можуть ініціювати з'єднання з внутрішніми пристроями без явного дозволу.

У проєктованій мережі застосовується різновид NAT: PAT (також відомий як NAT Overload). Цей механізм дозволяє багатьом хостам одночасно використовувати одну публічну IP-адресу за допомогою унікальних номерів портів.

На прикордонному маршрутизаторі було реалізовано наступну послідовність налаштувань.

Позначення внутрішнього та зовнішнього інтерфейсів:

```
Edge_R(config)#interface g0/0.10
Edge_R(config-subif)#ip nat inside
Edge_R(config-subif)#interface g0/0.20
Edge_R(config-subif)#ip nat inside
Edge_R(config-subif)#interface g0/0.30
Edge_R(config-subif)#ip nat inside
Edge_R(config-subif)#interface g0/0.40
Edge_R(config-subif)#ip nat inside
Edge_R(config-subif)#interface g0/0.50
Edge_R(config-subif)#ip nat inside
Edge_R(config-subif)#interface g0/0.60
Edge_R(config-subif)#ip nat inside
```

Налаштування списку доступу для визначення трафіку, що підлягає трансляції:

```
access-list 10 permit 10.24.80.0 0.0.15.255
```

Активація NAT з перевантаженням (PAT):

```
ip nat inside source list 10 interface GigabitEthernet1/0/24 overload
```

Після впровадження NAT пристрої внутрішньої мережі можуть надсилати пакети до Інтернету, а маршрутизатор автоматично транслює IP-адреси та порти, забезпечуючи зворотну маршрутизацію відповідей (рис 3.9)

.

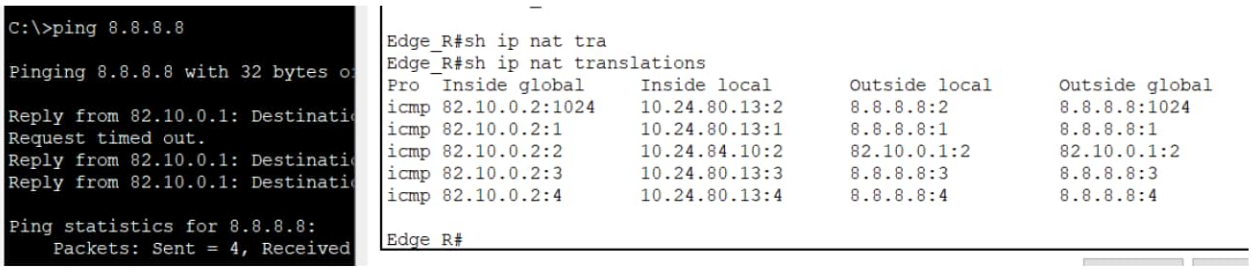

Рисунок 3.9 – Перевірка роботи NAT

Це рішення є простим, масштабованим і широко використовуваним у навчальних закладах, малому та середньому бізнесі.

3.5 Налаштування бездротової мережі

За вимогами завдання в кожному підрозділі впроваджено 2 бездротові мережі: робоча та гостьова. Застосовано методи захисту в безпровідних мережах: фільтрація MAC-адрес та паролі для підключення.

Додано по одному HomeRouter-PT-AC на кожний поверх та по два Laptop-PT до кожного HomeRouter-PT-AC . Wi-Fi для гостьової мережі та для робочої мережі показано на рисунках 3.10-3.11.

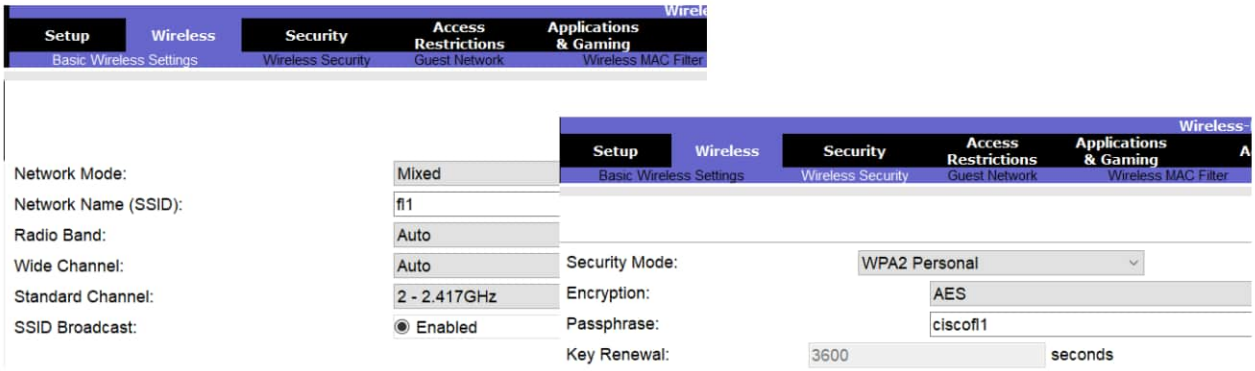

Рисунок 3.10 – Робоча мережа 1 поверху

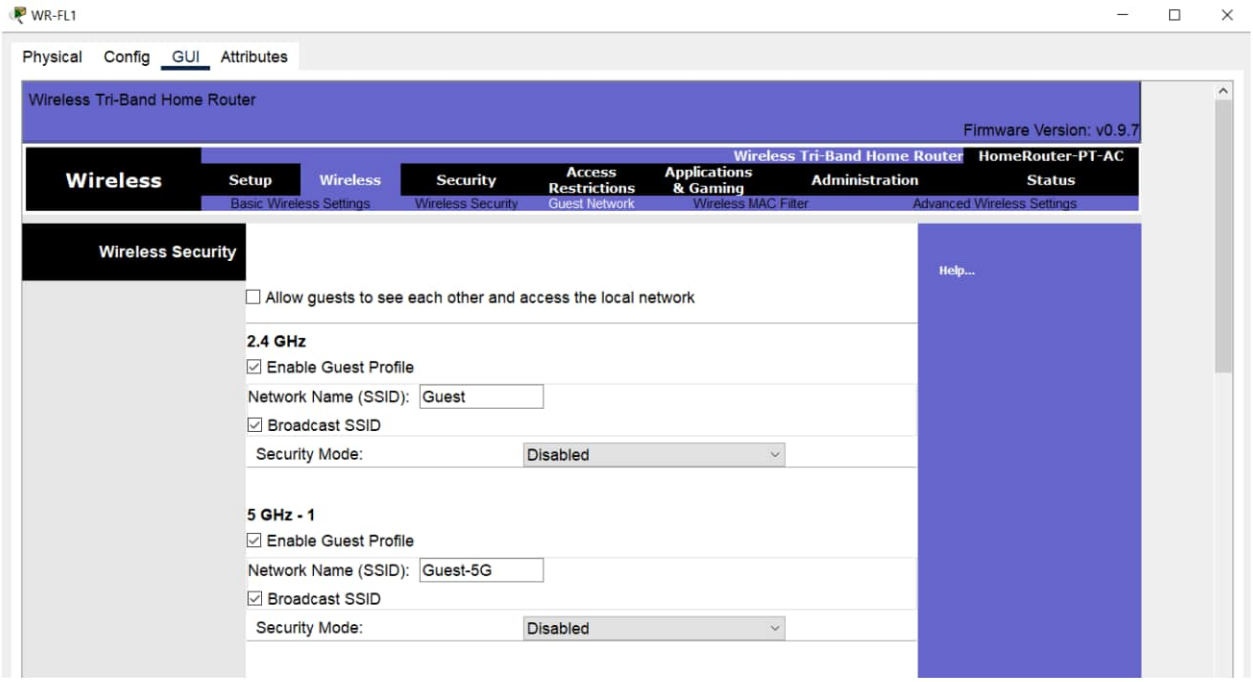

Рисунок 3.11 – Гостьова мережа Wi-Fi

Як видно на рисунку 3.12 користувач з ноутбука успішно підключився до бездротової робочої мережі.

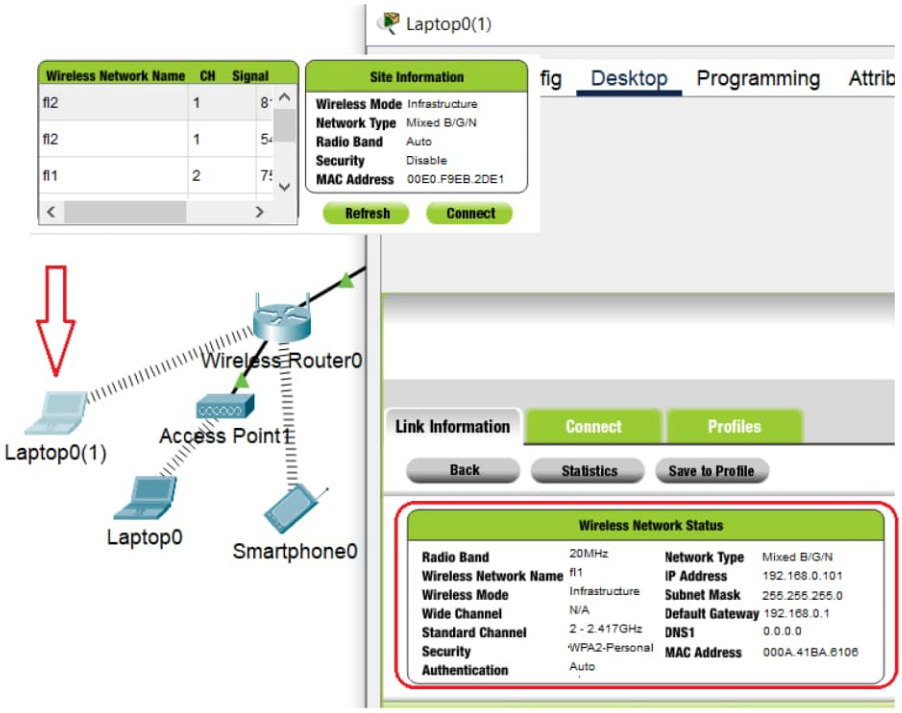

Рисунок 3.12 – Підключення по Wi-Fi

3.6 Імітація атак на DHCP

3.6.1 Імітація атаки «Виснаження DHCP»

Атака «Виснаження DHCP№ спрямована на вичерпання всього пулу доступних IP-адрес на легітимному DHCP-сервері. Зловмисник надсилає на DHCP-сервер величезну кількість DHCP Discover запитів, кожен з яких містить унікальну (підроблену) MAC-адресу. DHCP-сервер, обробляючи ці запити, резервує IP-адреси для кожної унікальної MAC-адреси, доки всі адреси в його пулі не будуть розподілені. Коли пул IP-адрес повністю вичерпаний, нові легітимні пристрої, що намагаються підключитися до мережі, не можуть отримати IP-адреси по DHCP. Це призводить до відмови в обслуговуванні (DoS) для цих пристроїв, оскільки вони або не можуть підключитися до мережі взагалі, або отримують IP-адреси з діапазону APIPA (169.254.x.x), що робить їх нефункціональними в даній мережі.

Для проведення цієї атаки використовуються спеціалізовані інструменти, такі як yersinia, dhcpstarv (у Kali Linux) або скрипти на Python з використанням бібліотеки Scapy, що дозволяють генерувати тисячі DHCP-запитів з фальшивими MAC-адресами за короткий час.

У Packet Tracer немає прямих інструментів для автоматичної генерації DHCP Starvation. Тому ми будемо використовувати імітацію шляхом ручної зміни MAC-адрес або створення безлічі віртуальних пристроїв. Атакуючий пристрій (Attacker PC) підключено до комутатора, і на цьому порту відсутні механізми захисту (DHCP Snooping, Port Security).

Припустимо, Attacker PC підключений до порту f0/3 комутатора 2960-TT у VLAN 30 (рис.3.13).

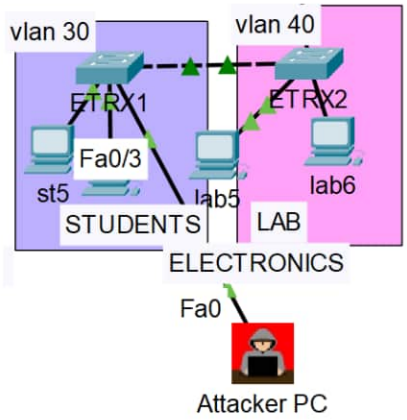

Рисунок 3.13 – ПК зловисника

Дії в Packet Tracer:

– на Attacker PC, перейти на вкладку Physical;

– натиснути на мережевий адаптер та змінити його MAC-адресу вручну (рис. 3.14):

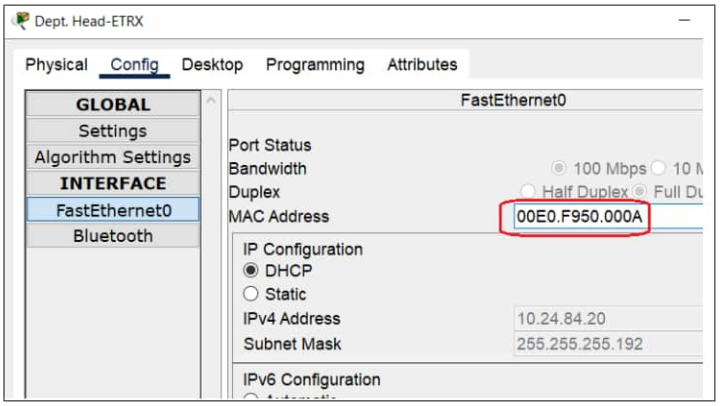

Рисунок 3.14 – Зміна MAC-адреси

– перейти на вкладку Desktop -> IP Configuration та вибрати DHCP, ПК надішле DHCP Discover з новою MAC-адресою;

– повторити ці кроки 10-20-30 разів (або більше, залежно від розміру DHCP-пулу у VLAN).

– альтернативна імітація: створити 10-20 нових ПК та підключити їх до комутатора в тому ж VLAN. На кожному ПК налаштувати отримання IP-адреси по DHCP. Кожен ПК отримає унікальну IP-адресу, виснажуючи пул.

Команда show ip dhcp binding є ключовою для адміністраторів мережі, оскільки дозволяє їм контролювати розподіл IP-адрес у мережі, а також відстежувати, які пристрої підключені до сервера DHCP. На рисунках 3.15 та 3.16 відображено статистику списку адрес, які були виділені клієнтам в мережі до атаки і після. Видно, як список Assigned Addresses заповнюється записами з різними MAC-адресами, і як зменшується кількість доступних адрес.

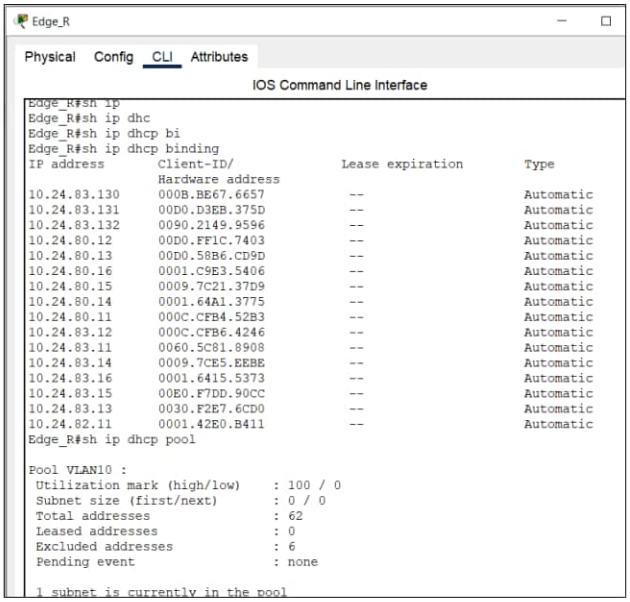

Рисунок 3.15 – Статистика DHCP до атаки виснаження IP-адрес

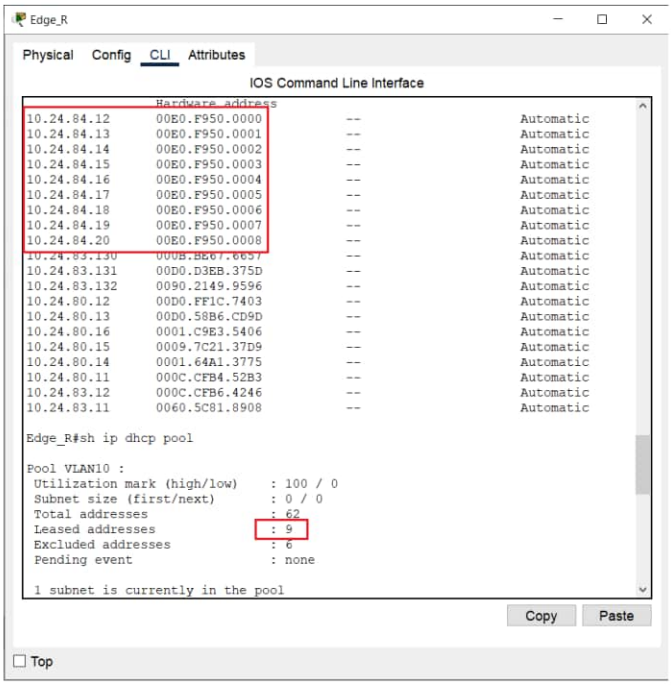

Рисунок 3.16 – Статистика DHCP під час атаки виснаження IP-адрес

В результаті пул IP-адрес для VLAN 10, до якого підключений Attacker PC, буде вичерпаний. Нові легітимні клієнти в цьому VLAN не зможуть отримати IP-адреси та залишаться з APIPA-адресами (169.254.x.x).

3.6.2 Зловмисний DHCP-сервер

Щоб зрозуміти, як DHCP-снупінг захищає мережу від несанкціонованого DHCP-сервера, додамо DHCP-сервер зловмисника до нашої мережі. На наступному зображенні показано наш приклад мережі після додавання DHCP-сервера зловминика. На рисунку 3.17 Attacker Server підключений до порту f0/4 комутатора 2960-TT ETRX1 (у VLAN 30) та встановлено статичну IP-адресу в тому ж VLAN, що й клієнти, на які буде атака, наприклад, 10.24.10.200 з маскою /24.

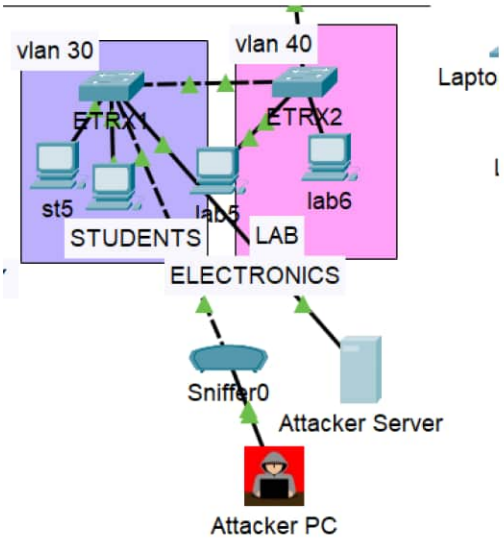

Рисунок 3.17 – Зловмисний DHCP-сервер

Суть атаки. Зловмисник розгортає в мережі свій власний DHCP-сервер. Цей «фальшивий» сервер налаштований так, щоб відповідати на DHCP Discover запити клієнтів швидше, ніж легітимний сервер, або в ситуаціях, коли легітимний сервер недоступний. Зловмисний сервер надає клієнтам шкідливі мережеві налаштування:

– некоректну IP-адресу шлюзу за замовчуванням (часто це IP-адреса самого зловмисника), що дозволяє перенаправляти весь трафік клієнта через атакуючого (Man-in-the-Middle, MitM);

– некоректну IP-адресу DNS-сервера (також часто IP-адреса зловмисника), що дозволяє здійснювати DNS-спуфінг, перенаправляючи користувача на фішингові сайти.

Наслідки: клієнти отримують невірні налаштування, їхній трафік може бути перехоплений, змінений або перенаправлений, конфіденційність та цілісність даних порушуються. Можлива також відмова в обслуговуванні, якщо налаштування будуть настільки некоректними, що пристрій не зможе взаємодіяти з мережею.

Для цієї атаки можуть використовуватися утиліти, такі як dhcpd (стандартний DHCP-сервер Linux), isc-dhcp-server, а також спеціалізовані фреймворки, як Metasploit (з модулем auxiliary/server/dhcp). Ми будемо використовувати Attacker Server для імітації зловмисного DHCP-сервера (рис.3.18).

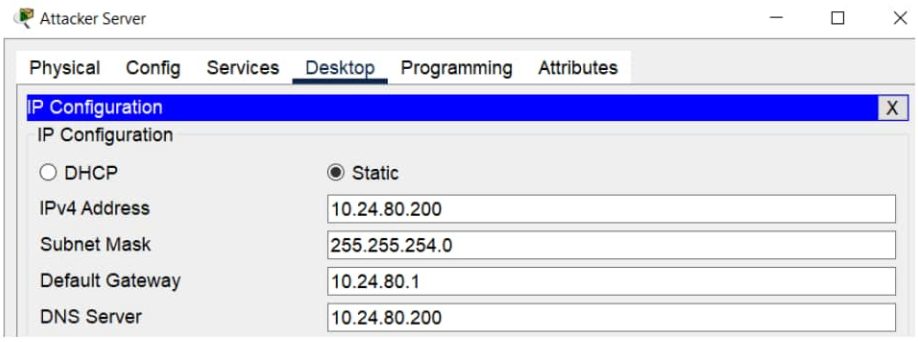

Рисунок 3.18 – Мережна адресація на Attacker Server

На вкладці Services -> DHCP налаштовано хибний DHCP-пул (рис. 3.19):

– Default Gateway: IP-адреса Attacker PC (10.24.10.8);

– DNS Server: IP-адресу Attacker Server (10.24.10.200).

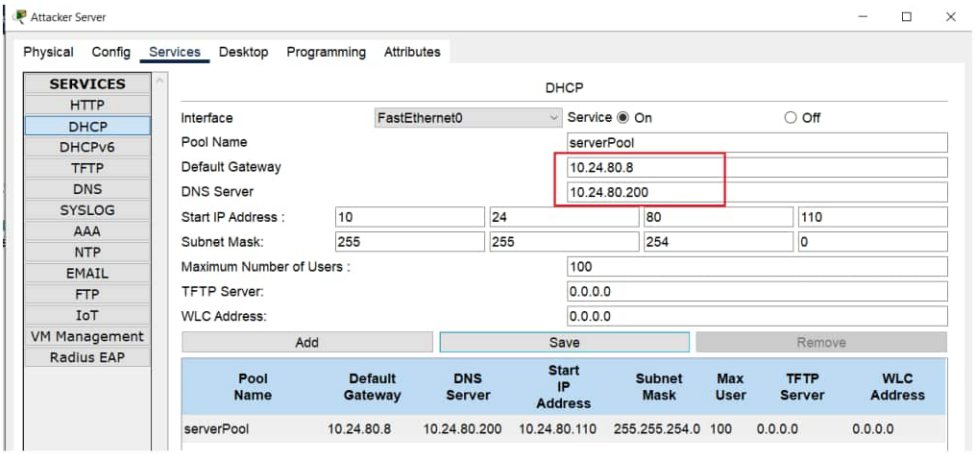

Рисунок 3.19 – DHCP-пул на Attacker Server

Спровокуємо ситуацію, коли клієнт отримує хибні налаштування. На одному з клієнтів у тому ж VLAN (наприклад, st5) переключимо з DHCP на Static, потім назад на DHCP. Це змусить клієнта надіслати новий DHCP Discover. На клієнті перевіримо отримані IP-налаштування (рис 3.18). Він отримує нову конфігурацію IP від DHCP-сервера зловмисника замість оригінального DHCP-сервера після запиту нової конфігурації IP. Клієнт отримає IP-адресу з пулу Attacker Server, а Default Gateway та DNS Server вказуватимуть на Attacker Server. Весь вихідний трафік клієнта буде спрямований на Attacker Server.

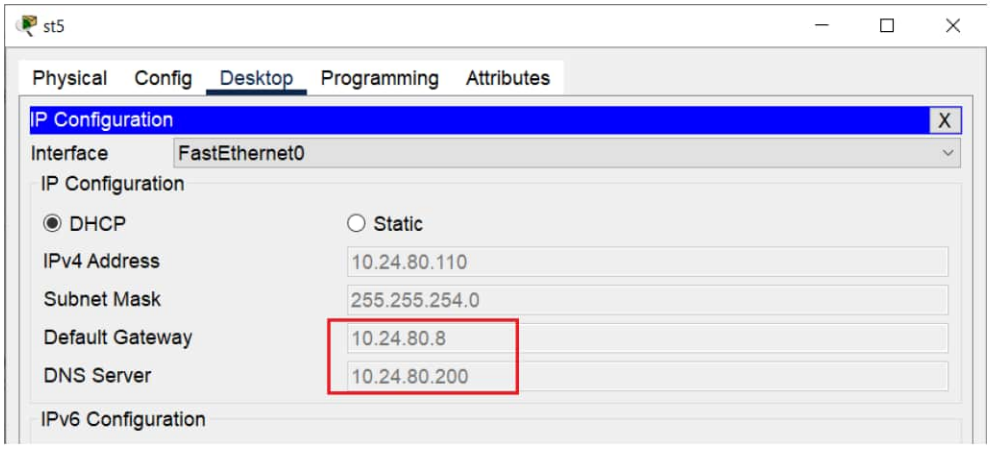

Рисунок 3.20 – IP-налаштування від зловмисного DHCP-сервера

Якщо DHCP-клієнти використовують конфігурацію IP, надану DHCP-сервером зловмисника, зловмисник може неналежним чином використати їхні дані, навіть не знаючи про них. Це відомо як атака «людина посередині»

3.7 Вровадженням технологій захисту DHCP

3.7.1 Налаштування DHCP Snooping на комутаторах

DHCP Snooping – це функція безпеки комутаторів другого рівня. Вона дозволяє фільтрувати та блокувати певні типи DHCP-трафіку. Використовуючи цю функцію, ми можемо зменшити кілька ризиків безпеки, спричинених шахрайськими DHCP-серверами та зловмисниками.

DHCP- Snooping працює для кожної окремої VLAN. За замовчуванням ця функція вимкнена. Щоб скористатися цією функцією, її спочатку потрібно ввімкнути. Після ввімкнення ми можемо налаштувати її для деяких VLAN або для всіх VLAN. Після налаштування вона активно відстежує вхідний трафік на всіх портах налаштованої VLAN. Якщо виявляє будь-який DHCP-пакет, залежно від його конфігурації, вона або дозволяє його, або відкидає.

DHCP-відстеження діє як брандмауер. Воно перевіряє всі вхідні повідомлення на порту. Якщо вхідне повідомлення не пов'язане з DHCP, DHCP-відстеження пропускає його. Якщо вхідне повідомлення пов'язане з DHCP, DHCP-відстеження використовує свою логіку. Залежно від конфігурації, DHCP-відстеження або пропускає повідомлення, або відкидає його.

В мережі коледжу функцію DHCP-сервера виконує сервер в мережі VLAN60. Було прийнято рішення налаштувати DHCP Snooping наступним чином:

– DHCP snooping вмикається на VLAN 10, 20, 30, 40 і 50;

– всі порти, до яких приєднані хости, налаштувати як ненадійні;

– для ненадійних портів встановити обмеження швидкості надсилання до шести пакетів за секунду:

– всі порти між комутаторами та до роутера, як надійні.

DHCP-відстеження розглядає всі порти зазначеної VLAN як ненадійні. Ненадійний порт – це порт, який не приймає повідомлення DHCP-сервера. Іншими словами, якщо пристрій підключено до ненадійного порту, він може

отримати IP-конфігурацію від DHCP-сервера, але не може запропонувати IP-конфігурацію. Наприклад, на ETRX1 надійним буде порт f0/23 до комутатора ETRX2, а на ETRX2 надійними будуть порти f0/23-24 (рис. 3.21).

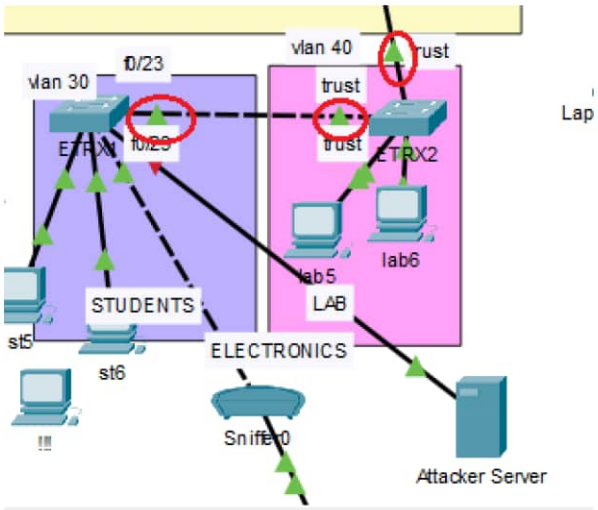

Рисунок 3.21 – Trust-порти на ETRX2 та ETRX1

У наступній таблиці наведено команди, які використовуються для налаштування та перевірки DHCP-відстеження на комутаторах Cisco.

Таблиця 3.2 – Команди для налаштування та перевірки DHCP-відстеження

Команда	**Опис**
Switch(config)# ip dhcp snooping	Щоб увімкнути DHCP-відстеження глобально.
Switch(config)# ip dhcp snooping vlan number [*number*]	Щоб увімкнути DHCP-відстеження у вказаній VLAN.
Switch(config-if)# ip dhcp snooping trust	Щоб налаштувати інтерфейс як довірений інтерфейс.
Switch(config-if)# ip dhcp snooping limit rate [*rate*]	Щоб обмежити кількість DHCP-пакетів, які інтерфейс може отримувати за секунду.
Switch# show ip dhcp snooping	Щоб переглянути конфігурацію та стан DHCP-відстеження.
Switch# debug ip dhcp snooping event	Щоб налагодити події DHCP-відстеження.
Switch# debug ip dhcp snooping packet	Щоб переглянути повідомлення та пакети DHCP.

На рисунку 3.22 налаштування dhcp snooping на ETRX1.

```
ETRX(config)#ip dhcp snooping
ETRX(config)#ip dhcp snooping vlan 10-50
ETRX(config)#interface range fa0/23
ETRX(config-if-range)#ip dhcp snooping trust
ETRX(config-if-range)#
ETRX(config-if-range)#
```

Рисунок 3.22 – Налаштування dhcp snooping на ETRX1

На наступному зображенні показано, як DHCP-відстеження блокує та дозволяє DHCP-повідомлення.

Після ввімкнення DHCP-відстеження лише DHCP-сервер, підключений до довіреного інтерфейсу, може надавати конфігурацію IP. Щоб перевірити це, надішлемо новий запит нову конфігурацію IP з ПК st5 і st5 отримує нову конфігурацію IP від легітимного DHCP-сервера.

Щоб переглянути конфігурацію та статистику DHCP snooping, командою «show ip dhcp snooping binding».

На наступному зображенні 3.23 показано результат виконання цієї команди. Ця команда відображає таблицю прив'язок DHCP Snooping інформацію про те, які IP-адреси були призначені яким MAC-адресам через DHCP і на яких інтерфейсах мережі це сталося.

```
ETRX1#show  ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:0C:CF:B4:52:B4   10.24.80.13      0           dhcp-snooping  30    FastEthernet0/2
00:D0:58:B6:CD:9D   10.24.80.14      0           dhcp-snooping  30    FastEthernet0/1
Total number of bindings: 2
```

Рисунок 3.23 – Таблиця прив'язок DHCP Snooping

3.7.2 Впровадження IP Source Guard

IP Source Guard – це механізм захисту доступу, що базується на перевірці відповідності IP-адреси та MAC-адреси пристрою на ненадійному порту. Він працює у тісній взаємодії з функцією DHCP Snooping і використовується для запобігання атакам, пов’язаним із підміною адрес (IP spoofing), що є поширеним вектором мережевих загроз.

Після активації функції DHCP Snooping на комутаторі створюється таблиця прив'язок (binding table) (рис.3.23).

IP Source Guard використовує цю таблицю для перевірки кожного IP-пакета, що надходить з клієнтського порту. Якщо IP-джерело не збігається з даними в таблиці, то пакет блокується. Приклад налаштування на f0/1.

```
interface FastEthernet0/1
ip verify source
```

3.7.3 Обмеження швидкості DHCP

За замовчуванням DHCP-відстеження не обмежує кількість DHCP-пакетів, які може отримувати інтерфейс. Оскільки ненадійні інтерфейси підключаються до DHCP-клієнтів, для підвищення безпеки можна обмежити кількість DHCP-пакетів на цих інтерфейсах.

Встановимо для кожного ненадійного порту ліміт 6 пакетів за секунду. Зазвичай обмеження швидкості застосовується до ненадійних інтерфейсів. Але за потреби його також можна налаштувати на довіреному інтерфейсі.

На наступному зображенні показано, як встановити обмеження швидкості на інтерфейсі Fa0/1 та перевірити це.

```
ETRX1(config)#int range f0/1-10
ETRX1(config-if-range)#ip dhcp snooping limit rate 6
ETRX1(config-if-range)#^Z
ETRX1#
%SYS-5-CONFIG_I: Configured from console by console

ETRX1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30,40,50
Insertion of option 82 is enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            no         6
FastEthernet0/6            no         6
FastEthernet0/4            no         6
FastEthernet0/5            no         6
FastEthernet0/2            no         6
FastEthernet0/3            no         6
FastEthernet0/9            no         6
FastEthernet0/7            no         6
FastEthernet0/8            no         6
FastEthernet0/10           no         6
FastEthernet0/23           yes        unlimited
```

Рисунок 3.24 – Команда обмеження швидкості відстеження IP DHCP

3.7.4 Налаштування VLAN та інтеграція з механізмами захисту DHCP

Віртуальні локальні мережі (VLAN) відіграють ключову роль у побудові структурованої, безпечної та масштабованої мережевої інфраструктури навчального закладу. Застосування VLAN у поєднанні з механізмами захисту служби динамічної конфігурації хостів (DHCP) дозволяє ефективно контролювати мережевий трафік, ізолювати різні категорії користувачів, а також запобігати атакам, пов’язаним із підробкою DHCP-серверів або ARP-спуфінгом.

У проєктованій мережі було створено окремі VLAN для різних підрозділів та функціональних зон навчального закладу (табл.3.1). Кожна VLAN отримує IP-адреси від окремої підмережі, що дозволяє ефективно впроваджувати політики маршрутизації та контролю доступу.

Централізований DHCP-сервер з IP-адресою 10.24.84.70 (розміщений у VLAN 60) забезпечує автоматичну видачу IP-адрес пристроям у різних VLAN. Зв'язок між VLAN і DHCP-сервером здійснюється через маршрутизатор Edge_R, на якому активовано DHCP Relay (опція IP helper-address).

Розподіл трафіку між VLAN значно знижує ризик розповсюдження атак, які базуються на широкомовних повідомленнях (broadcast). Зокрема, атаки DHCP starvation та rogue DHCP стають менш ефективними, оскільки, наприклад, зловмисник із VLAN 20 не зможе впливати на DHCP-трафік VLAN 10 без міжвланового доступу.

3.7.5 Захист на рівні доступу: Port Security

У межах забезпечення безпеки на рівні доступу в локальній мережі навчального закладу критично важливим є обмеження несанкціонованого фізичного підключення кінцевих пристроїв до мережевого обладнання. Одним з найбільш ефективних інструментів для досягнення цієї мети є механізм Port Security, реалізований на рівні комутаторів другого рівня.

Port Security дозволяє встановлювати обмеження щодо кількості та типу MAC-адрес, які можуть бути дозволені на певному фізичному порті комутатора. Таким чином, забезпечується захист від:

– підключення сторонніх пристроїв до мережі без дозволу;

– атак типу MAC flooding, при яких заповнюється таблиця MAC-адрес комутатора псевдовипадковими адресами з метою переведення його в режим широкомовної ретрансляції;

– підміни пристроїв користувачів із метою захоплення їхнього мережевого трафіку.

У рамках побудованої мережної інфраструктури Port Security було застосовано до портів, які забезпечують підключення кінцевих пристроїв студентів та працівників коледжу. Конфігурація проводилася з використанням методу динамічного прив'язування MAC-адрес (режим sticky), який автоматично реєструє адресу першого підключеного пристрою й у подальшому обмежує доступ до порту лише для цього пристрою. Приклад конфігурації:

```
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
```

У наведеній конфігурації:

– обмежується кількість дозволених MAC-адрес на порті до однієї;

– у випадку порушення — порт не вимикається повністю, але блокує підозрілу адресу та повідомляє адміністратора (режим restrict);

– автоматично зберігається MAC-адреса першого легітимного пристрою (sticky), що спрощує адміністрування.

На рис. 3.25 інформація на інтерфейсі FastEthernet 0/1 комутатора ETRX1 підтверджує, що Port Security активний і дозволяє підключати тільки один пристрій із конкретною MAC-адресою на порт FastEthernet0/1, а в разі порушення відбувається обмеження, але порт не відключається.

```
ETRX1#sh port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00D0.58B6.CD9D:30
Security Violation Count   : 0
```

Рисунок 3.25 – Стан Port Security на інтерфейсі FastEthernet 0/1 ETRX1

Для підтвердження ефективності впровадженого механізму Port Security було проведено імітацію порушення: st5 було вимкнено, замість нього до того ж порту під'єднано інший пристрій з іншою MAC-адресою. В результаті відбулася подія порушення безпеки, у відповідь комутатор відкинув трафік нового пристрою, але не вимкнув порт, зберігаючи працездатність для авторизованої адреси. У виведеному звіті (рис. 3.26) спостерігаються збільшення кількість порушень (10) і MAC-адреса-порушника не була додана до списку дозволених.

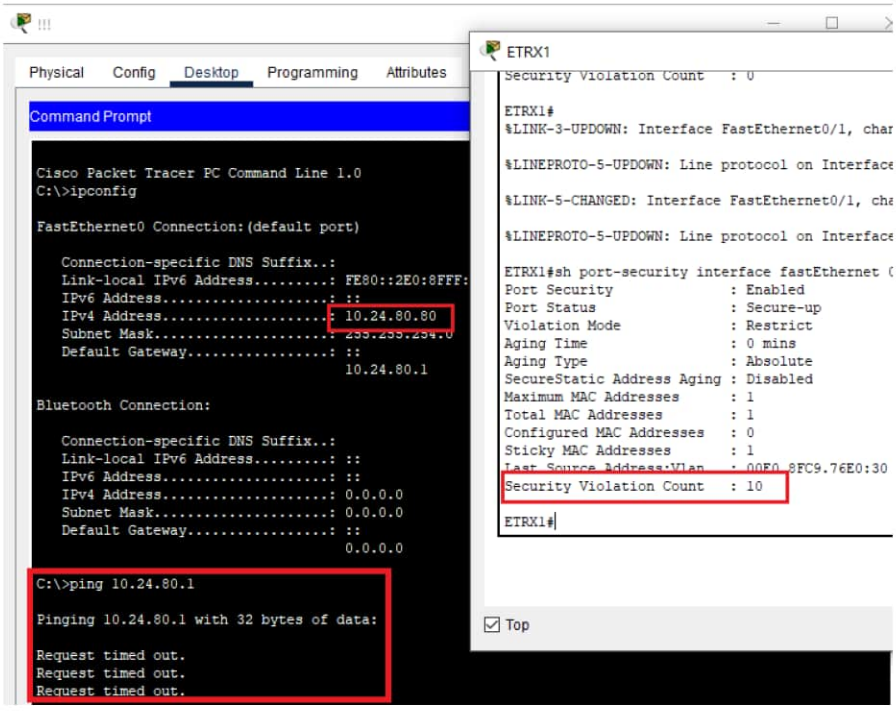

Рисунок 3.26 – Порушення безпеки на f0/1 ETRX1

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було досягнуто поставлену мету – розроблено модель безпечної мережної інфраструктури коледжу з акцентом на впровадження механізмів захисту служби динамічного налаштування хостів (DHCP). На основі аналізу актуальних загроз та особливостей архітектури локальних мереж навчальних закладів були запропоновані і реалізовані відповідні заходи безпеки.

У теоретичній частині роботи проведено аналіз основних вразливостей DHCP та обґрунтовано доцільність впровадження таких технологій захисту, як DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, а також механізмів Port Security, Access Control Lists (ACL), VLAN-сегментації та опції 82 (DHCP Relay Agent Information). Особливу увагу приділено ролі широкомовного трафіку у виникненні потенційних атак і методам його обмеження в межах сегментованої інфраструктури.

У практичній частині побудовано імітаційну модель комп'ютерної мережі навчального закладу у середовищі Cisco Packet Tracer, що включає маршрутизатори, комутатори, DHCP-сервер та клієнтські пристрої. Реалізовано логічну VLAN-сегментацію мережі, налаштовано статичну та динамічну маршрутизацію, а також впроваджено ключові захисні механізми на рівні доступу. Проведено серію тестувань щодо впливу атак, зокрема DHCP spoofing і MAC flooding, а також перевірено ефективність реалізованого захисту.

Результати дослідження засвідчили, що впроваджені механізми забезпечують підвищення рівня мережної безпеки без значного ускладнення інфраструктури. Використання технологій Cisco дозволяє адаптувати рішення до умов реального навчального закладу, з урахуванням вимог масштабованості, економічної доцільності та простоти адміністрування.

Таким чином, виконана робота поєднує теоретичне обґрунтування і практичну реалізацію сучасних підходів до побудови захищених мереж. Запропонована модель може бути використана як основа для впровадження у навчальних закладах або як навчальний приклад для підготовки майбутніх фахівців у сфері комп'ютерної інженерії та кібербезпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Про адміністративні послуги [Електронний ресурс] : Закон України № 5203-VI від 06.09.2012 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/5203-17.

2. DHCP Snooping | Junos OS | Juniper Networks. *Juniper Networks – Leader in AI Networking, Cloud, & Connected Security Solutions*. URL: https://www.juniper.net/documentation/us/en/software/junos/dhcp/topics/topic-map/dhcp-snooping.html (date of access: 28.04.2025).

3. Understanding IP Source Guard for Port Security on Switches | Junos OS | Juniper Networks. *Juniper Networks – Leader in AI Networking, Cloud, & Connected Security Solutions*.
URL: https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/port-security-ip-source-guard.html (date of access: 28.04.2025).

4. Dynamic ARP Inspection Explained. *CBT IT Certification Training*. URL: https://www.howtonetwork.com/certifications/cisco-2/dynamic-arp-inspection-explained/ (date of access: 28.04.2025).

5. DHCP snooping rate limiting best practice. *NetworkLessons Notes*. URL: https://notes.networklessons.com/dhcp-snooping-rate-limiting-best-practice (date of access: 28.04.2025).

6. DHCP Address Allocation using Option 82. *Cisco*. URL: https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/12_2sba/feature/guide/sbcpopt.html (date of access: 28.04.2025).

7. Мережева академія Cisco. URL: http://www.netacad.com (дата звернення: 15.04.25)

8. Микитишин А.Г., Митник М.М., Стухляк П.Д. Комп'ютерні мережі, книга.1. Навчальний посібник для технічних спеціальностей ВНЗ (рекомендовано МОН України): Магнолія 2023. 256 с.

9. Що таке локальна мережа і навіщо вона потрібна? URL: https://itedu.center/ua/blog/articles/lan_wan_man/ (дата звернення: 25.04.25)

10. Топології комп'ютерних мереж. URL: https://marytisna.blogspot.com/2017/10/blog-post.html (дата звернення: 26.04.25)

11. Чалый О. О. Комп'ютерні мережі: безпека та захист інформації: навч. посіб. – Київ: НАУ, 2018. – 156 с. – ISBN 978-966-598-646-5.

12. Cisco Systems. DHCP Snooping Configuration Guide [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/iosxe122_33se/configuration/guide/b_dhcp_snoop_xe.pdf

13. Wilmer Almazan / The Network Trip. Block DHCP Attacks - Deep Dive, 2024. *YouTube*. URL: https://www.youtube.com/watch?v=edguGjquol8 (date of access: 17.05.2025).

14. Jeremy's IT Lab. Free CCNA | Port Security | Day 49 | CCNA 200-301 Complete Course, 2021. *YouTube*. URL: https://www.youtube.com/watch?v=sHN3jOJIido (date of access: 17.05.2025).

Додаток А

Текст програми налаштування комутатора доступу ETRX1

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ГРАНИЧНОГО МАРШРУТИЗАТОРА

Текст програми

804.02070743.25022-01 12 01

Листів 7

2025

АНОТАЦІЯ

Дана конфігурація належить комутатору доступу мережі коледжу ETRX1 моделі Cisco WS-C2960-24TT-L та забезпечує базовий рівень захисту від атак, пов'язаних з підробкою IP та MAC адрес, шляхом використання DHCP Snooping, IP ARP Inspection і Port Security на основних портах комутатора. Також реалізовано сегментацію через VLAN 30 з підтримкою trunk-портів для міжвланової маршрутизації.

ЗМІСТ

```
Current configuration : 4381 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ETRX1
!
ip arp inspection vlan 10,20,30,40,50
!
ip dhcp snooping vlan 10,20,30,40,50
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 00D0.58B6.CD9D
!
interface FastEthernet0/2
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 000C.CFB4.52B4
!
interface FastEthernet0/3
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
```

```
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0090.0CD1.1B32
!
interface FastEthernet0/5
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/6
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/7
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/8
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/9
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
```

```
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/10
switchport access vlan 30
ip arp inspection trust
ip dhcp snooping limit rate 6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/11
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
```

```
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/23
ip dhcp snooping trust
switchport mode trunk
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```