Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комп'ютерна мережа для банківського відділу з рівнями захисту інформації
Назва теми

КвРКІ 190102.20.01.25 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія та програмування»
Назва

Виконав: студент IV курсу, група КІ2–19–1 _____ К.О. Багрій
Підпис Ініціали, прізвище

Керівник _____ П.Г. Регіда
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«31» травня 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"11" 01 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Багрій Костянтин Олександрович
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Комп'ютерна мережа для банківського відділу з рівнями захисту інформації

Керівник проекту (роботи) Регіда П.Г.,ст. викладач
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2023 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження придметної області та огляд існуючих ріщень

Програмне та апаратне забезпечення комп'терної мереж. основні комп'юненти комп'ютерної мережі

Програмно–апаратна реалізація комп'ютерної мережі

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Фізична схема ком'пютерної мережі банку

Логічна схема ком'пютерної мережі банку

Компоненти ком'пютерної мережі банку

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_11_»_____01_____2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2023	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2023	виконано
3	Робота над розділом 1 – дослідження придметної області та огляд існуючих ріщень	01.03.2023	виконано
4	Робота над розділом 2 – програмне та апаратне забезпечення комп'терної мереж. основні комп'юненти комп'ютерної мережі	01.04.2023	виконано
5	Робота над розділом 3 – програмно–апаратна реалізація комп'ютерної мережі	30.04.2023	виконано
6	Оформлення пояснювальної записки згідно вимог	11.05.2023	виконано
7	Попередній захист ВКР	26.05.2023	виконано
8	Захист ВКР на засіданні ЕК	Червень 2023 року	

Студент _____ К.О. Багрій
Підпис Ініціали, прізвище

Керівник роботи _____ П.Г. Регіда
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 190102.20.01.09 ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ 190102.19.01.25	Фізична схема комп'ютерної мережі банку	1		
3		КвРКІ 190102.19.01.25	Логічна схема комп'ютерної мережі банку	1		
4		КвРКІ 190102.19.01.25	Компоненти комп'ютерної мережі банку	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 190102.19.01.25 ВП		
Розробив		Багрій			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Регіда				У	1	1
Н. контр.		Лисенко				ХНУ, КІ2–19–1		
Затв.		Говорущенко		05.06				

АНОТАЦІЯ

Тема Комп'ютерна мережа для банківського відділу з рівнями захисту інформації

Автор роботи:Багрій Костянтин Олександрович.

Керівник роботи:Регіда Павло Генадійович.

Пояснювальна записка: 55 с., 39 рис., 7 табл., 60 джерел.

Графічна частина:3 креслення.

КОМП'ЮТЕРНА МЕРЕЖА, БАНКІВСЬКИЙ ВІДДІЛ, РІВНІ ЗАХИСТУ ІНФОРМАЦІЇ,ФІЗИЧНА ТА ЛОГІЧНА СХЕМА.

Метою дослідження полягає у проєктуванні та розробці комп'ютерної мережі для банківського відділу з рівнями захисту інформації.

Об'єктами дослідження є архітектура мережі , Захист мережевого периметру і трафіку та безпека даних

Предметом дослідження є формалізований опис та схеми локальної комп'ютерної мережі банку.

Підпис студента

01.06.2025

Дата

ЗМІСТ

ВСТУП

Комп'ютерні мережі в банках з'явилися у 1960–х роках з появою перших комп'ютерів та великих централізованих банківських операційних центрів. У цей період було створено перші мережі з використанням телефонних ліній та терміналів, які забезпечували зв'язок між різними банківськими відділеннями та операційним центром. З появою перших локальних мереж (LAN) у 1970–х роках, банки стали використовувати ці технології для забезпечення зв'язку між комп'ютерами в межах окремих відділень. У 1980–х роках з'явилися глобальні комп'ютерні мережі (WAN), що дозволили банкам об'єднувати різні відділення та операційні центри в єдину мережу. З появою Інтернету в 1990–х роках, банки стали використовувати Інтернет–технології для забезпечення зв'язку з клієнтами та обміну даними з іншими банками та фінансовими установами.

Зараз банки використовують різноманітні технології мережевої інфраструктури, такі як VPN, мережеві протоколи та безпекові механізми, щоб забезпечити надійність та безпеку зв'язку. У сучасних банках мережева інфраструктура є надзвичайно важливою, оскільки вона дозволяє забезпечувати швидкий та безпечний доступ до інформації, зменшує витрати на обслуговування та управління банком, а також допомагає підтримувати високу якість обслуговування клієнтів.

ДОСЛІДЖЕННЯ ПРИДМЕТНОЇ ОБЛАСТІ ТА ОГЛЯД ІСНУЮЧИХ РІЩЕНЬ

Аналіз предметної області

Сучасні мережні технології сприяли новій технічній революції. Створенню локальних мереж і глобальної єдиної мережі комп'ютерів надають таке ж значення, що й будівництву швидкісних автомагістралей у шістдесяті роки XX ст. Тому комп'ютерну мережу називають «інформаційною супермагістраллю».

Комп'ютерна мережа (Рисунок 1.1 – схема мережі) — це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання яких–небудь проміжних носіїв інформації.

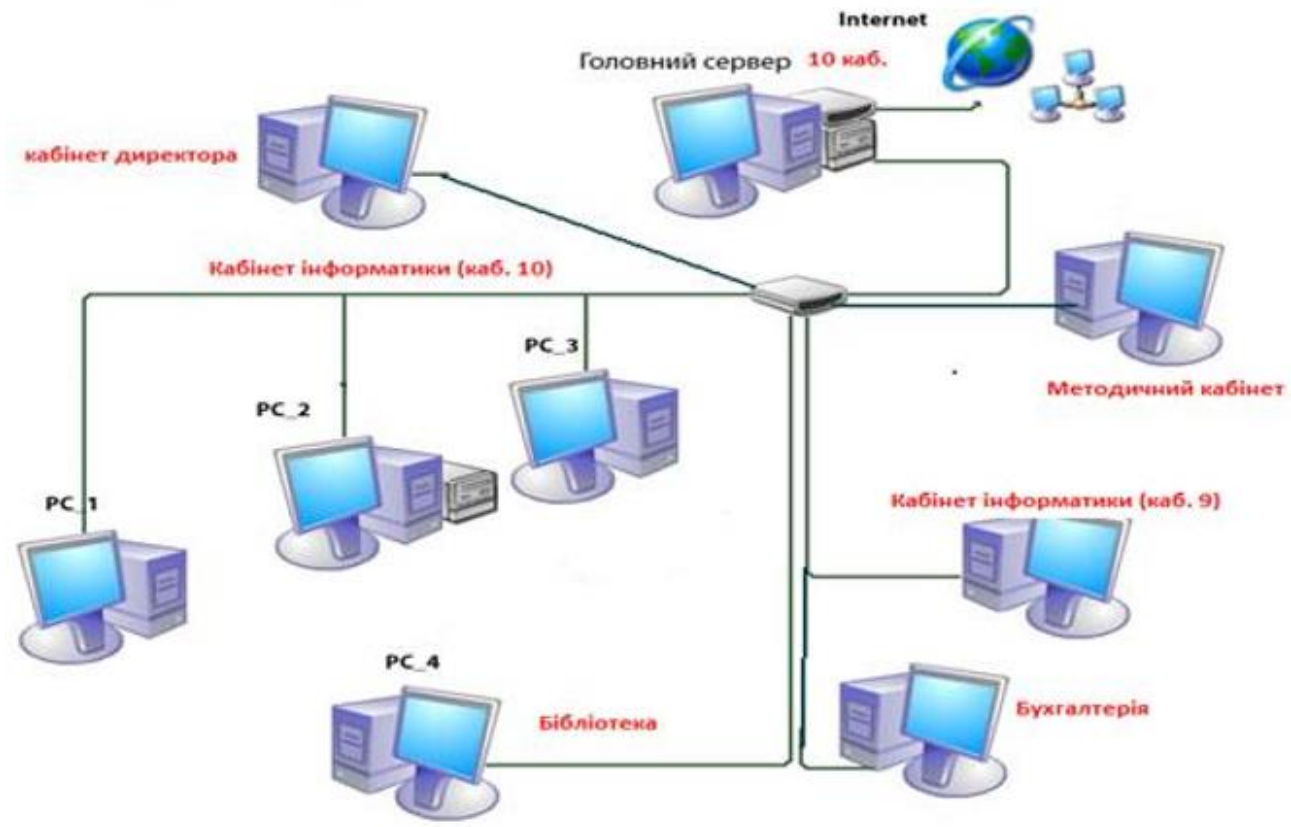


Рисунок 1.1 – Схема мережі

Ці мережі можуть бути локальними (LAN), міськими (MAN) та глобальними (WAN).

Локальні мережі (LAN) – це мережі, що охоплюють обмежену територію, зазвичай в межах однієї будівлі або офісу. Комп'ютери, принтери та інші пристрої можуть бути підключені до локальної мережі, що дозволяє їм спільно використовувати ресурси та обмінюватися даними.

Міські мережі (MAN) використовуються для з'єднання комп'ютерів у межах одного міста або регіону. Ці мережі зазвичай охоплюють більші території, ніж локальні мережі.

Глобальні мережі (WAN) – це мережі, які охоплюють велику територію, зазвичай це Інтернет. Ці мережі забезпечують зв'язок між комп'ютерами з різних країн і континентів. Приклад WAN — мережі з комутацією пакетів (Frame Relay), через яку можуть «розмовляти» між собою різні комп’ютерні мережі.

Одним з ключових елементів комп'ютерної мережі є протокол передачі даних (TCP/IP). Цей протокол визначає правила передачі даних через мережу і дозволяє комп'ютерам з'єднуватися і спілкуватися. Крім того, для побудови комп'ютерних мереж використовуються різні технології, такі як Ethernet, Wi–Fi, Bluetooth та інші. Кожна з цих технологій має свої переваги та недоліки і підходить для різних ситуацій.

Ethernet(рисунок 1.2) – це технологія побудови комп'ютерних мереж. Існує багато мережевих стандартів Ethernet. Вони відрізняються швидкістю передачі, типом кабелю та обладнанням.

Рисунок.1.2 – Зовнішній вигляд Ethernet

Історія технології Ethernet починається з 1972 року. Саме тоді з'явилися перші версії технології Ethernet. Перші експериментальні версії Ethernet могли передавати дані на швидкості до 3 Мбіт/с. Повноцінний Ethernet з'явився на початку 80–х. Таким чином, перша офіційна версія стандарту з'явилася в 1983 році. Як носій використовувався коаксіальний кабель.

Справжнім прогресом у технології став перехід до використання витої пари. Нові середовища передачі дозволили збільшити швидкість до 100 Мбіт/с. Швидша версія цієї технології отримала назву Fast Ethernet. Поява Fast Ethernet не тільки збільшила швидкість, але й зробила мережу простішою та надійнішою. Завдяки цим удосконаленням технологія Ethernet стала дуже популярною. Контролери Ethernet зараз є у всіх комп'ютерах і найчастіше використовуються для підключення до Інтернету.

Стандарти Ethernet можна класифікувати відповідно до швидкості передачі даних, яку вони пропонують:

1) 10 Мбіт/с – мережа на основі коаксіального кабелю або витої пари. Зараз не використовується.

2) 100 Мбіт/с (Fast Ethernet) — мережа на основі витої пари, наразі найпоширеніша версія мереж Ethernet, яка використовується для побудови локальних мереж у будинках і офісах і для підключення користувачів до Інтернету.

3) 1 Гбіт/с (Gigabit Ethernet) — мережі на основі витої пари або волоконної оптики. Вита пара Gigabit Ethernet тепер підтримується більшістю сучасних контролерів, тому цей варіант мережі Ethernet також популярний для побудови домашніх і офісних локальних мереж. Він рідко використовується для підключення користувачів до Інтернету.

4) 10 Гбіт/с – оптоволоконна мережа, яку використовують інтернет–провайдери.

Wi–Fi – це технологія передачі даних через радіохвилі, яка використовується для бездротового підключення до Інтернету та інших мережевих пристроїв. Зазвичай використовується в локальних мережах (LAN) з метою надання бездротового доступу до Інтернету або до інших мережевих пристроїв, таких як принтери, маршрутизатори та мережеві сховища.

Технологія Wi–Fi може працювати на різних частотах та швидкостях передачі даних, включаючи стандарти 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac та 802.11ax (Wi–Fi 6). є дуже популярною технологією, оскільки вона дозволяє підключатися до Інтернету та мережевих пристроїв з будь–якої точки в межах діапазону дії радіосигналу. Також використовується в багатьох пристроях, включаючи смартфони, планшети, ноутбуки, телевізори та інші розважальні системи.

Bluetooth – це технологія бездротового зв'язку, яка дозволяє передавати дані між електронними пристроями на невеликій відстані, зазвичай до 10 метрів. Ця технологія була розроблена з метою створення простого та зручного засобу зв'язку між різними електронними пристроями, такими як мобільні телефони, ноутбуки, планшети, годинники, акустичні системи та інші. Він використовує радіохвилі в діапазоні 2,4 ГГц для передачі даних між пристроями.

Ця технологія дозволяє обмінюватися даними між пристроями, такими як музика, фотографії, відео та інші файли, а також використовувати різноманітні функції, такі як голосовий зв'язок та передача даних між пристроями. Також має кілька версій, включаючи Bluetooth 1.0, Bluetooth 2.0, Bluetooth 3.0, Bluetooth 4.0, Bluetooth 5.0 та Bluetooth 5.1. Кожна нова версія має покращені характеристики, такі як підвищення швидкості передачі даних, зменшення споживання енергії та підвищення точності геолокації.

Термін «корпоративна мережа» також використовується в літературі для позначення об’єднання кількох мереж, кожна з яких може бути побудована на Різних технічних, програмних та інформаційних принципах. Розглянуті види мереж є мережами закритого типу, доступ до них дозволений тільки обмеженому

колу користувачів, для яких робота в такій мережі безпосередньо пов’язана з їхньою професійною діяльністю. Глобальні мережі орієнтовані на обслуговування будь–яких користувачів.

1.2 Засоби захищеного обміну даних в комп’ютерних мережах

Коли користувач намагається отримати доступ до захищеного веб–сайту з використанням HTTPS, відбувається так зване SSL/TLS з'єднання між веб–браузером користувача і веб–сервером. Під час цього з'єднання SSL/TLS виконує наступні дії:

1) Аутентифікація сервера: сервер надсилає свій цифровий сертифікат, який містить підпис від надійної третьої сторони, такої як сертифікаційний орган. Браузер перевіряє підпис ідентифікаційного сертифіката, щоб переконатися, що він дійсний, та переконується, що він співпадає з іменем сервера, до якого з'єднується браузер.

2) Встановлення обміну ключами: після того, як браузер перевірив ідентифікаційний сертифікат сервера, він та сервер обмінюються криптографічними ключами. Ці ключі використовуються для шифрування і розшифрування даних, що передаються між браузером та сервером.

3) Захист даних: після того, як було встановлено з'єднання SSL/TLS та обмінено криптографічні ключі, всі дані, які передаються між браузером та сервером, шифруються та захищаються від перехоплення та зловживання.

4) SSL/TLS можна застосовувати і для інших цілей, наприклад, для захисту електронної пошти, телеконференцій

Для віддаленого захищеного доступу використовується SSH(рисунок 1.5). За допомогою SSH можна здійснювати різноманітні дії, такі як віддалений запуск програм, налаштування системних параметрів та інше. Крім того, SSH використовується для захисту віддалених FTP–з'єднань, веб–з'єднань та інших мережевих протоколів.

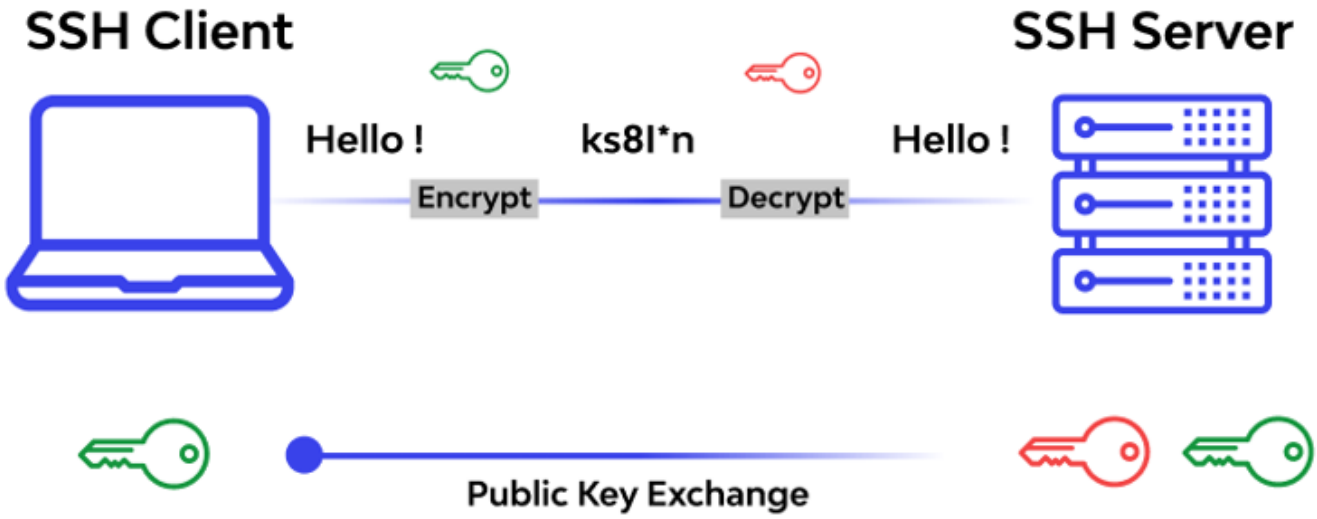


Рисунок 1.5 – Протокол SSH

Основні переваги використання SSH полягають у тому, що він забезпечує безпеку з'єднання, включаючи автентифікацію користувача та шифрування всієї передачі даних між комп'ютерами. Завдяки цьому з'єднання SSH є надійним та захищеним від перехоплення та зламу.

SSH також може бути використаний для безпечного копіювання файлів з одного комп'ютера на інший. Для цього використовується SCP (Secure Copy), який є розширенням SSH. SCP дозволяє безпечно копіювати файли з одного комп'ютера на інший через мережу Інтернет з використанням криптографічного захисту.

SSH є незамінним інструментом для системних адміністраторів та інших фахівців з IT–безпеки, які потребують віддаленого доступу до комп'ютерів та серверів, зберігаючи при цьому високий рівень безпеки та конфіденційності.

Альтернатива протоколу SSH є Telnet – це протокол мережевої комунікації, який дозволяє віддалено керувати та взаємодіяти з іншими комп'ютерами або мережевими пристроями через IP–мережу, зокрема через TCP/IP–протокол. Використовуючи Telnet, можна віддалено зайти на віддалений комп'ютер або пристрій і виконувати команди, надсилати та отримувати дані.

Telnet працює на основі клієнт–серверної архітектури. Клієнтська програма Telnet встановлює з'єднання з віддаленим сервером, який слухає на певному порту, і передає команди та дані через це з'єднання. Серверна програма Telnet, в свою чергу, отримує команди від клієнта і виконує їх на віддаленому комп'ютері або пристрої. За замовчуванням, Telnet використовує порт 23 для з'єднання.

Протокол Telnet є старішим і менш безпечним у порівнянні з іншими протоколами, такими як SSH (Secure Shell). Трафік, передаваний через Telnet, не шифрується, тому дані, включаючи паролі та іншу чутливу інформацію, можуть бути отримані зловмисником.

У сучасних мережевих середовищах рекомендується використовувати більш безпечні альтернативи, такі як SSH, які шифрують трафік та забезпечують безпеку під час віддаленого доступу до комп'ютерів або мережевих пристроїв.

IPsec може бути застосований для захисту різноманітних мережевих протоколів, таких як IPv4, IPv6, TCP, UDP та інші. Основні застосування IPsec включають:

Віддалений доступ IPsec може бути використаний для створення захищеного віддаленого з'єднання з мережевим пристроєм, таким як віддалений сервер або мережевий шлюз. Захищене з'єднання дозволяє користувачам безпечно отримувати доступ до віддалених ресурсів інтернету, включаючи файли, друк, бази даних та інші ресурси.

VPN (Virtual Private Network): IPsec є одним з найбільш поширених протоколів для забезпечення безпеки в VPN–мережах. Використання IPsec дозволяє створювати захищені канали передачі даних між віддаленими мережами або між віддаленими користувачами. Використовується для шифрування трафіку між мережевими пристроями на рівні IP–пакетів. Це забезпечує безпеку передачі даних між мережевими пристроями та дозволяє уникнути перехоплення трафіку та інших мережевих атак.

Захист VoIP–трафіку: IPsec може бути використаний для шифрування голосового трафіку, що передається по мережі Інтернет в системах VoIP (Voice over

Internet Protocol). Захист голосового трафіку забезпечує конфіденційність та надійність.

Також для захисту безпровідного зєднання підійде протокол WPA2 (Wi–Fi Protected Access 2), який захищяє від несанкціонованого доступу та перехоплення даних. WPA2 є наступником протоколу WPA і є одним з найбільш безпечних протоколів бездротової мережевої безпеки.

Захист бездротових мереж Wi–Fi: WPA2 забезпечує безпеку бездротових мереж Wi–Fi шляхом шифрування трафіку між бездротовими пристроями та точками доступу. WPA2 використовує алгоритми шифрування AES (Advanced Encryption Standard), які забезпечують високий рівень безпеки передачі даних.Захист користувачів: WPA2 дозволяє захистити користувачів від несанкціонованого доступу до бездротових мереж Wi–Fi. Це забезпечує конфіденційність інформації, яка передається між бездротовими пристроями та точками доступу.

Розширена аутентифікація: WPA2 використовує протокол EAP (Extensible Authentication Protocol) для підтвердження ідентичності користувачів, що дозволяє забезпечити високий рівень безпеки підключення до бездротових мереж Wi–Fi.

Використання WPA2 дозволяє підвищити безпеку мережі Wi–Fi і зменшити ризик несанкціонованого доступу та перехоплення даних. WPA2 є рекомендованим протоколом бездротової мережевої безпеки і використовується більшістю організацій для захисту бездротової мережі.

Мережеві екрани(firewalls) є важливою складовою частиною захисної інфраструктури комп'ютерних мереж. Вони використовуються для забезпечення безпеки та контролю доступу до мережевих ресурсів. Основна функція мережевих екранів полягає в фільтрації мережевого трафіку, що протікає через них, та блокуванні небажаних або шкідливих з'єднань як зображено на рисунку 1.6.

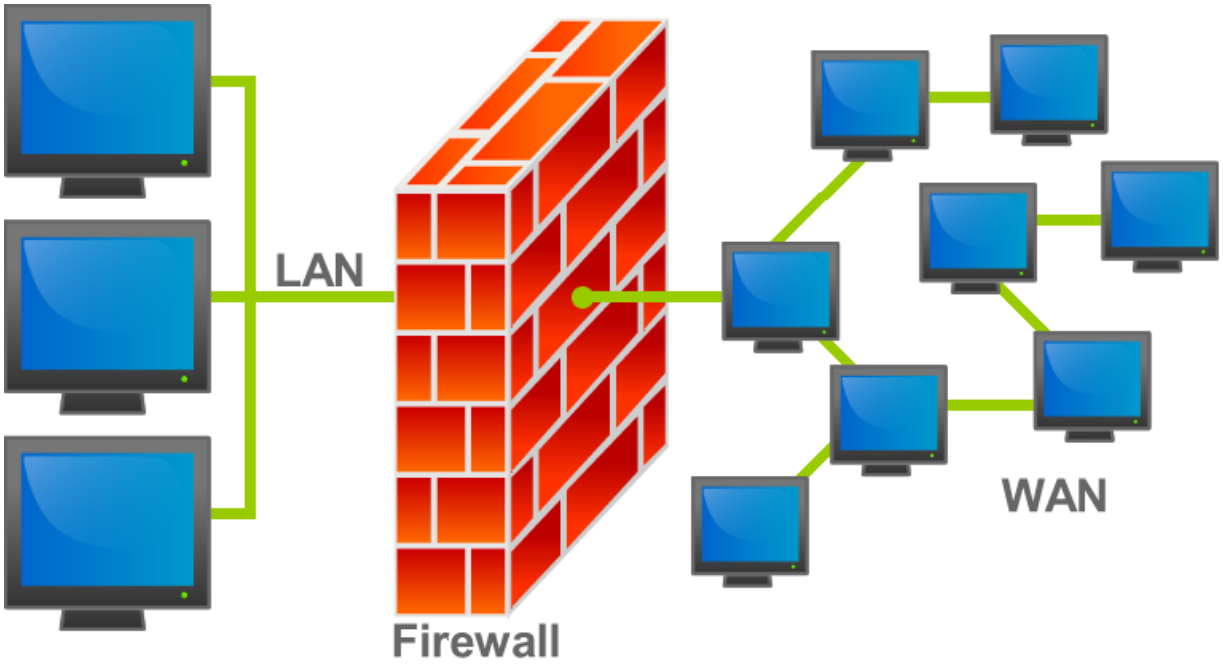


Рисунок 1.6 – Принцип роботи Firewall

Загалом, комп'ютерні мережі є невід'ємною частиною сучасного світу і дозволяють швидко та ефективно обмінюватися інформацією між комп'ютерами та пристроями.

1.3 Емуляція комп'ютерних мереж

Емуляція комп'ютерних мереж – це процес віртуального моделювання поведінки комп'ютерних мереж за допомогою програмного забезпечення. Це може бути корисно для тестування нових мережевих конфігурацій, аналізу впливу нових алгоритмів на мережу, а також для навчання студентів і фахівців у галузі комп'ютерних мереж.

Існують різні інструменти для емуляції комп'ютерних мереж, такі як GNS3, Packet Tracer, ns–3 та інші. Зазвичай ці інструменти дозволяють користувачам створювати віртуальні мережі, встановлювати в них різні типи обладнання, налаштовувати параметри мережі, запускати тестові сценарії і бачити, як комп'ютерна мережа поводиться в різних умовах. Наприклад, емуляція мережі може бути корисною у багатьох випадках:

Тестування нових конфігурацій мережі. Перш ніж впроваджувати нову мережеву конфігурацію, ви можете Також ця мережа складається з різних протоколів наприклад SSH, яка забезпечує безпечний віддалений доступ до комп'ютера або мережевого пристрою через незахищену мережу, таку як Інтернет. її, щоб побачити, як мережа поводиться за різних умов і які проблеми можуть виникнути.

Тестування безпеки мережі: емуляція може бути корисною для тестування безпеки мережі, наприклад, дозволяє інженерам банку тестувати нові мережеві рішення без встановлення обладнання в реальному середовищі. Це зменшує ризик негативного впливу на реальну мережу і може заощадити час і гроші. емуляція може бути корисною для навчання персоналу банку тому, як керувати мережею. Це також знижує ризик збоїв, які можуть виникнути під час навчання персоналу. Також може бути використана для тестування безпеки мережі та виявлення потенційних загроз, не впливаючи на вже створену мережу.

Оптимізація мережі завдяки емуляції дозволяє інженерам аналізувати мережу та виявляти потенційні проблеми зі швидкістю передачі даних, пропускною здатністю мережі, маршрутизацією даних та іншими параметрами. Це може допомогти вдосконалити мережу та підвищити її продуктивність.

Таким чином, емуляція комп'ютерних мереж може принести користь банківським системам, якщо використовувати її належним чином і з відповідною оцінкою ризиків

GNS3 і Cisco Packet Tracer (Рисунок 2.2 – GNS3 vs Cisco Packet Tracer) – це дві різні програми, які можна використовувати для моделювання віртуальних мереж і тестування мережевих конфігурацій. Нижче наведено порівняння цих програм за деякими ключовими характеристиками

GNS3 або Graphical Network Simulator–3 – це єдиний у своєму роді емулятор мережевого програмного забезпечення, який був вперше випущений у 2008 році. Ключова функція цього емулятора – створити комбінацію реальних і віртуальних пристроїв, щоб змоделювати безперебійне функціонування складних мереж.

Він використовує програмне забезпечення емуляції Dynamips для успішної симуляції Cisco IOS.

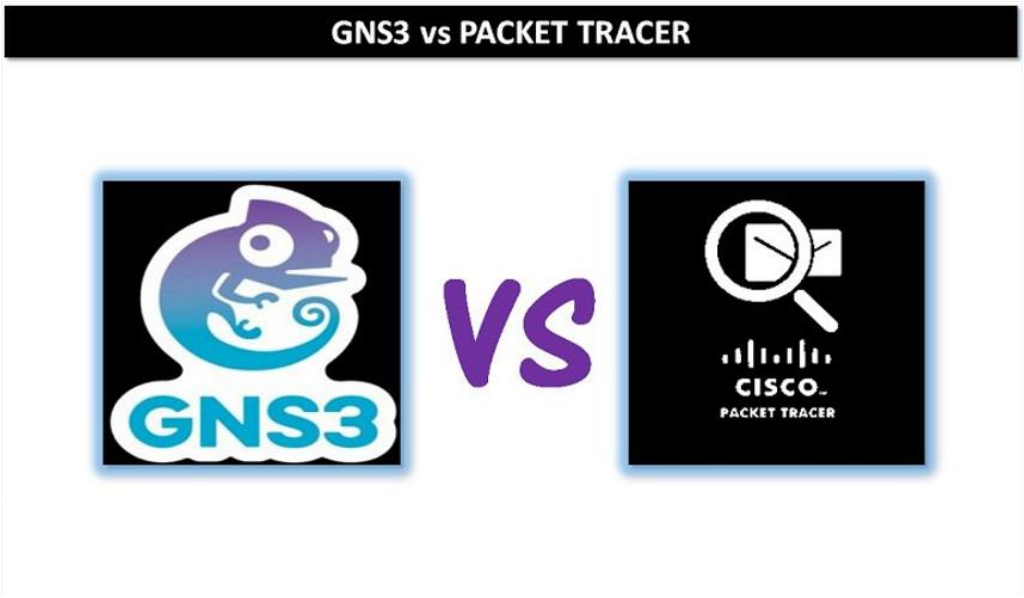


Рисунок 2.2 – GNS3 vs Cisco Packet Tracer

З іншого боку, Packet Tracer – популярний крос–платформний інструмент візуального моделювання, розроблений компанією Cisco Systems. Інструмент дозволяє користувачам будувати мережеві топології, а також відтворювати сучасні комп'ютерні мережі.

Таблиця.1.1 – GNS3 vs Packet Tracer

FEATURE	PACKET TRACER	GNS3
Перевага для новачків	Якщо ви новачок у сфері мережевих технологій, рекомен–дується почати свій шлях з Packet Tracer, оскільки його простіше встановити і він	Що до легкості у використані GNS3 для новачків, то найкраще переходити на нього лише після того, як ви набудете певного досвіду.

Кінець таблиці 1.1.– GNS3 vs Packet Tracer

	простіший у використанні.	
Cisco Firepower Threat Defence Virtual NGFW	Незважаючи на те, що це популярний кросплатформний інструмент візуального моделювання, розроблений компанією Cisco, він не має такої функції.	Популярний емулятор мережевого програмного забезпечення містить Cisco Firepower Threat Defence Virtual NGFW.
Відкритий вихідний код	Це не кросплатформний інструмент візуального моделювання з відкритим вихідним кодом.	Це емулятор мережевого програмного забезпечення з відкритим кодом.
Повністю функціональне IOS.	Імітація IOS.Часткові функції	Реальні образи IOS запускаються у віртуальному середовищі.
Підтримка конфігурації ASDM ASA	Не підтримує конфігурації ASDM ASA	Підтримує конфігурації ASDM ASA
Wi–Fi	моделюється з підтримкою протоколів LWAPP, WLC, а також CAPWAP.	не моделюється жодними подібними функціями.
3G/ 4G	Імітує функції підтримки 3G/4G.	не імітує функції підтримки 3G/4G.

З огляду на ці особливості, обидві програми мають свої переваги і недоліки, тому вибір між ними буде залежати від потреб і цілей користувача. Cisco Packet

Tracer більше підходить для навчальних цілей, тоді як GNS3 підходить для професійного використання.

Cisco Packet Tracer є популярним інструментом серед студентів, викладачів та мережевих спеціалістів. Основними перевагами використання Cisco Packet Tracer є:

Зручний інтерфейс – програма має інтуїтивно зрозумілий інтерфейс, який дозволяє швидко і легко створювати і налаштовувати мережі. Імітація різних типів мереж – програма дозволяє імітувати різні типи мереж, включаючи LAN, WAN, WLAN та інші.

Підтримка мережевих протоколів – програма підтримує багато мережевих протоколів, таких як TCP/IP, DHCP, DNS, OSPF та багато інших. Зручні інструменти мережевого аналізу – програма включає в себе різноманітні інструменти мережевого аналізу, такі як Wireshark, які можна використовувати для аналізу мережевого трафіку та вивчення протоколів.

Також це програмне забезпечення є безкоштовним і може бути завантажене з офіційного веб–сайту Cisco Systems.

Таким чином, Cisco Packet Tracer – це ефективний і зручний інструмент для моделювання мереж, який дозволяє користувачам вивчати і досліджувати мережеві технології безкоштовно і без реального обладнання.

1.4 Висновки

Тож комп’ютерна мережа це сукупність різних пристроїв, що забезпечують інформаційний обмін між комп’ютерами в мережі без використання яких–небудь проміжних носіїв інформації. Також ця мережа складається з різних протоколів наприклад SSH, яка забезпечує безпечний віддалений доступ до комп'ютера або мережевого пристрою через незахищену мережу, таку як Інтернет. Для бездротового з’єднання з мережою використовується технологія Wi–Fi. За захист бездротового з’єднання відповідає протокол WPA2 який забезпечує безпеку

бездротових мереж Wi–Fi шляхом шифрування трафіку між бездротовими пристроями та точками доступу. WPA2 використовує алгоритми шифрування AES (Advanced Encryption Standard), які забезпечують високий рівень безпеки передачі даних.

Також є мережеві екрани(firewalls) які є складовою частиною захисної інфраструктури комп'ютерних мереж. Основна функція мережевих екранів полягає в фільтрації мережевого трафіку, що проходить через них, та блокуванні небажаних або шкідливих з'єднань. Для “спілкування” усіх цих складових використовується Ethernet які відрізняються швидкістю передачі, типом кабелю та обладнанням. Їх історія починається з 1972 року. Повноцінний Ethernet з'явився на початку 80–х. Таким чином, перша офіційна версія стандарту з'явилася в 1983 році. Як носій використовувався коаксіальний кабель. Самі кабелі поділяють за рівнем пропускної здатності на 10 Мбіт/с мережа на основі коаксіального кабелю або витої пари. На 100 Мбіт/с мережа – на основі витої пари, наразі найпоширеніша версія мереж Ethernet, яка використовується для побудови локальних мереж у будинках і офісах і для підключення користувачів до Інтернету.

Також потрібне середовище де це усе можна об’єднати, налаштувати, протестувати. Ідеально підходить безкоштовна програма емулятор Cisco Packet Tracer. Воно достатньо легка у використані для новачків та є безкоштовна. Надає можливість змоделювати мережу та прослідкувати роботу мережі при різних налаштуваннях.

ПРОГРАМНЕ ТА АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ТЕРНОЇ МЕРЕЖ. ОСНОВНІ КОМП'ЮНЕНТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Топологія мережі

Мережі можна класифікувати за різними критеріями, такими як масштаб, топологія, засіб передачі даних та функціональне призначення. Ось кілька топологій мереж, які використовуються для організації комп'ютерних систем:

За масштабом:

Локальна мережа (LAN): обмежена географічна область, така як будинок, офіс або кампус.

Місцева мережа (MAN): охоплює більшу територію, таку як місто або регіон.

Глобальна мережа (WAN): охоплює великі відстані, зазвичай використовується для підключення розташованих в різних місцях локальних та місцевих мереж.

За топологією:

Одним з найважливіших відмінностей між різними типами мереж є їх топологія.

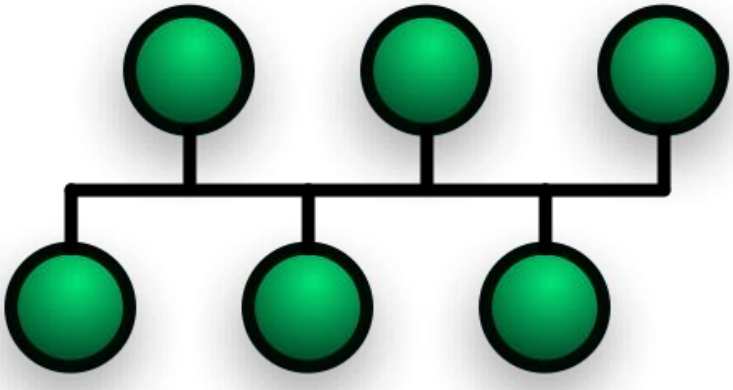
Під топологією звичайно розуміють взаємне розташування один щодо одного вузлів мережі. До вузлів мережі в даному випадку відносяться комп'ютери, концентратори, комутатори, маршрутизатори, точки доступу тощо

Топологія – це конфігурація фізичних зв'язків між вузлами мережі. Характеристики мережі залежать від типу встановлюваної топології. Зокрема, вибір тієї чи іншої топології впливає:

1) на склад необхідного мережевого обладнання;
2) на можливості мережевого обладнання;
3) на можливості розширення мережі;
4) на спосіб управління мережею.

Розрізняються такі основні види топологій як шина, кільце, зірка, коміркова топологія і решітка. Решта є комбінаціями основних топологій і називаються змішаними або гібридними.

Шина як зображено на рисунку 2.1. Мережі з шинної топологією використовують лінійний моноканал (коаксіальний кабель) передачі даних, на кінцях якого встановлюються спеціальні заглушки – термінатори (terminator). Вони необхідні для того, щоб погасити сигнал після проходження по шині. До недоліків шинної топології слід віднести наступне:



Рисунку 2.1 – Топологія шина

1) дані, передані по кабелю, доступні всім підключеним комп'ютерам;
2) в разі пошкодження шини вся мережа перестає функціонувати.

Кільце(рис.2.2) – це топологія, у якій кожен комп'ютер з'єднаний лініями зв'язку з двома іншими: від одного він отримує інформацію, а іншому передає. Тобто мається на увазі наступний механізм передачі даних: дані передаються послідовно від одного комп'ютера до іншого, поки не досягнуть комп'ютера–одержувача. Недоліки топології "кільце" тіж, що і у топології "шина":

1) загальнодоступність даних;
2) нестійкість до пошкоджень кабельної системи.

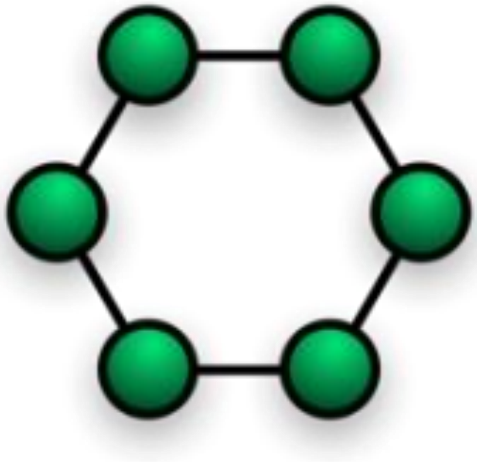


Рисунок 2.2 – Кільцева топологія

Зірка(рисунок 2.3) – це єдина топологія мережі з явно виділеним центром, званим мережевим концентратором або "хабом" (hub), до якого підключаються всі інші учасники мережі. Функціональність мережі залежить від стану цього концентратора. У топології "зірка" прямі з'єднання двох комп'ютерів в мережі відсутні. Завдяки цьому є можливість вирішення проблеми загальнодоступності даних, а також підвищується стійкість до пошкоджень кабельної системи.

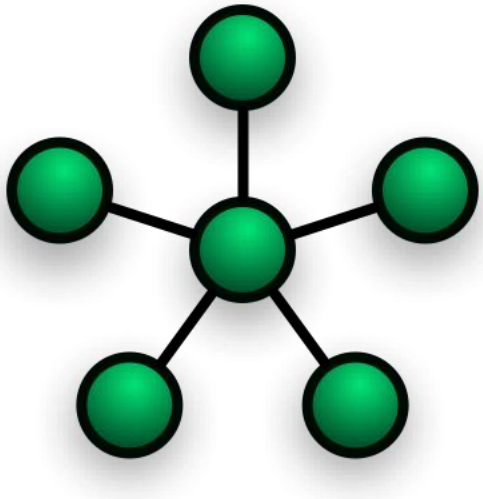


Рисунок 2.3 – Топологія типу "зірка"

Сітчаста топологія(рисунок 2.4) – це топологія комп'ютерної мережі, в якій кожна робоча станція мережі з'єднується з декількома робочими станціями цієї ж

мережі. Характеризується високою відмовостійкістю, складністю налаштування і надлишковою витратою кабелю. Кожен комп'ютер має безліч можливих шляхів з'єднання з іншими комп'ютерами. Обрив кабелю не спричинить до втрати з'єднання між двома комп'ютерами.

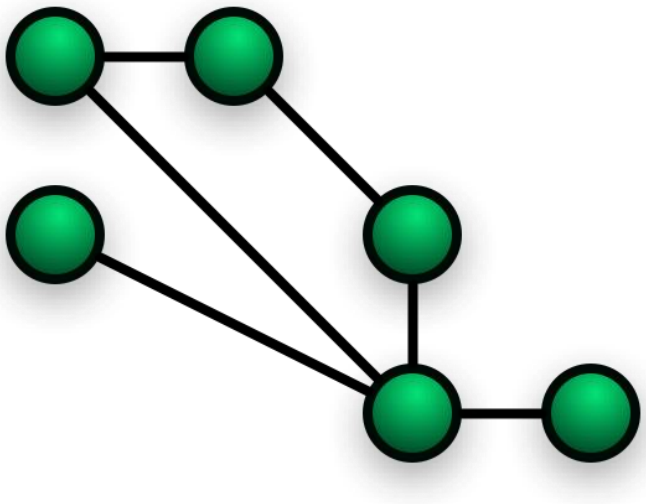


Рисунок 2.4 – Сітчаста топологія

Решітка – це топологія, у якій вузли утворюють багатовимірну решітку. При цьому кожне ребро решітки паралельно її осі і з'єднує два суміжних вузла вздовж цієї осі. Одновимірна решітка – це ланцюг, що з'єднує два зовнішніх вузла (що мають лише одного сусіда) через деяку кількість внутрішніх (у яких по два сусіди – ліворуч і праворуч). При з'єднанні обох зовнішніх вузлів виходить топологія "кільце".

Мережі, засновані на FDDI, використовують топологію "подвійне кільце", досягаючи тим самим високої надійності і продуктивності. Багатовимірна решітка, поєднана циклічно в більш ніж одному вимірі, називається "тор".

Змішана топологія (рисунок 2.5) – топологія, що переважає в великих мережах з довільними зв'язками між комп'ютерами.

Для підключення великої кількості вузлів мережі застосовують мережеві підсилювачі і (або) комутатори. На практиці використовують два види комутаторів, що забезпечують підключення 8 або 16 ліній.

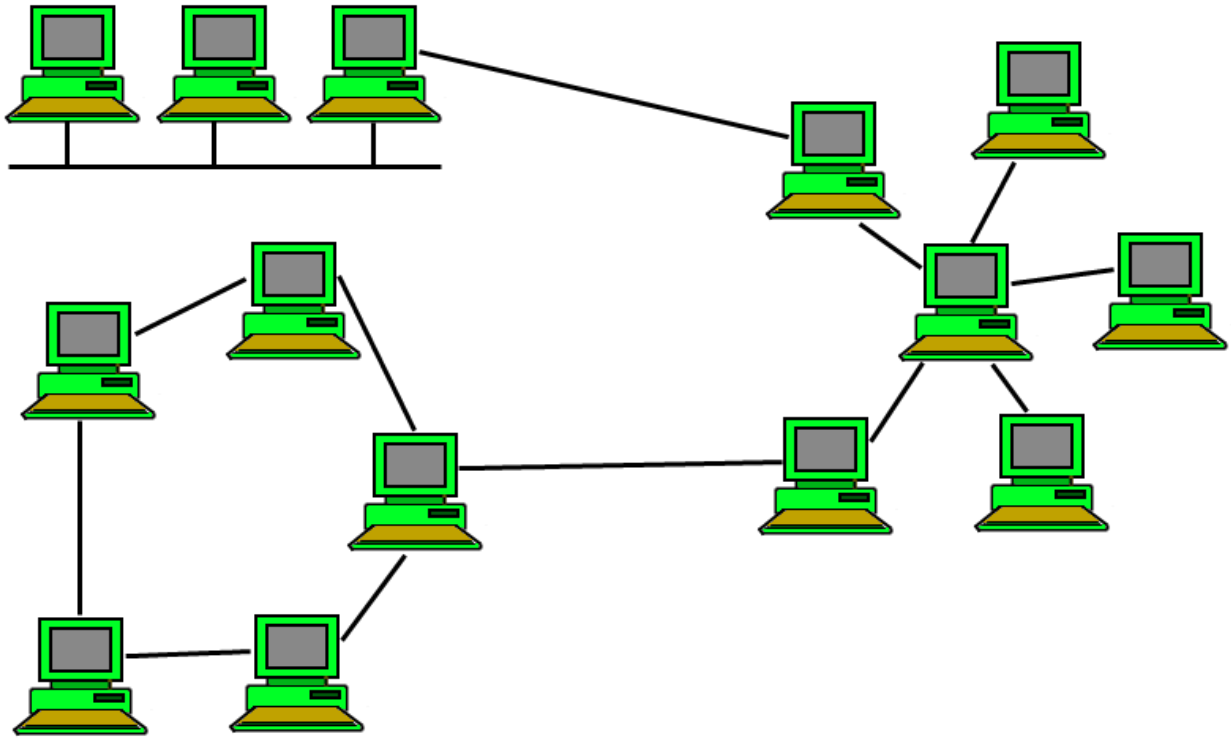


Рисунок 2.5 – Змішана топологія

Інший тип комутаційного пристрою – пасивний концентратор, який дозволяє організувати розгалуження мережі для трьох робочих станцій. Мале число приєднаних вузлів означає, що пасивний концентратор не потребує підсилювачі. Такі концентратори застосовуються в тих випадках, коли відстань до робочої станції не перевищує декількох десятків метрів.

У порівнянні з шинної або кільцем, змішана топологія є більш надійною. Вихід з ладу одного з компонентів мережі в більшості випадків не впливає на загальну працездатність мережі.

Розглянуті вище топології локальних мереж є основними. Реальні обчислювальні мережі будують, ґрунтуючись на завданнях, які покликана вирішити дана локальна мережа, і по структурі її інформаційних потоків. Таким чином, на практиці топологія обчислювальних мереж являє собою синтез традиційних типів топологій.

2.2 Вимоги до мережі

Комп'ютерні мережі в банках є важливим елементом інфраструктури, що забезпечує ефективну та безпечну обробку фінансової інформації та надійний доступ клієнтів до банківських послуг. Однак, як і в будь–якій предметній області, тут існують певні проблеми та виклики, які потребують вирішення. Ось деякі з них:

1) Безпека: Банки зберігають конфіденційну фінансову інформацію про клієнтів, що робить їх мішенню для кіберзлочинців. Щоб запобігти крадіжкам і злому, банки повинні забезпечити високий рівень безпеки своїх комп'ютерних мереж.

2) Висока доступність: Банки повинні надавати клієнтам доступ до своїх послуг у будь–який час. Для забезпечення високої доступності банки повинні мати мережі з резервними маршрутизаторами та обладнанням, яке автоматично перемикається на резервне обладнання у разі виходу з ладу основного.

3) Швидкість: Банки повинні забезпечувати швидкий доступ до даних, щоб клієнти могли здійснювати транзакції в режимі реального часу. Швидкість мережі залежить від обсягу інформації, яку потрібно передати, та технології, що використовується.

4) Банки повинні забезпечити сумісність своїх комп'ютерних мереж з іншими мережами, наприклад, з мережами інших банків, щоб мати можливість проведення транзакцій між ними.

5) Масштабованість: Банки повинні мати мережі, які можна масштабувати вгору та вниз.

Для комп'ютерної мережі банку необхідно мати належну мережеву інфраструктуру, яка забезпечує надійне та безперебійне з'єднання між комп'ютерами, серверами та іншими мережевими пристроями. банк повинен мати достатню кількість комп'ютерів для роботи співробітників.

Комп'ютери повинні відповідати вимогам банку щодо продуктивності та безпеки. Також мати мережеві пристрої такі як маршрутизатори, комутатори та інші пристрої, які забезпечують з'єднання між комп'ютерами та іншими мережевими пристроями. Для централізованого управління, збереження даних та

захисту потрібні сервери. Самі пристрої мають бути підключені через кабелі а також для роботи персоналу потрібні бездротові засоби зв’язку. Ще потрібні камери відео нагляду для спостереження за персоналом та приміщенням у випадку якоїсь крадіжки чи схожих не передбачуваних обставин. Також камери мають бути підключенні до локальної мережі. Для цього є два способи пряме підключення по проводам це наддасть змогу швидкого та безперешкодної передачі даних але проведення проводу може задати певних незручностей а саме демонтаж стін і кошти на довжину кабелю.

Окрім прямого підключення існує також дистанційне через Wi–Fi та Bluetooth. Завдяки такому підключенню не потрібно купляти та проводити кабелі до відео камер, що дасть зберегти кошти, але тут є певні недоліки , велика товщина стін та сукупність приладів створює перешкоди для передачі сигналу. Тому спосіб підключення камер потрібно вибирати у залежності від планування приміщення

Адміністрація повинна мати можливість доступу до інших комп’ютерів чи пристроїв по локальній мережі, а самі працівники тільки могли переносити дані між собою також через локальну мережу. Має бути окрема кімната для доступу серверної частини з якої буде зручний доступ до серверної частини інженерам та іншим фахівця у цій сфері.

У банківській мережі юридична зона – це сегмент мережі, призначений для обробки та збереження конфіденційних і чутливих даних, пов'язаних з юридичними аспектами банківської діяльності.

Основна мета юридичної зони – забезпечити високий рівень безпеки, конфіденційності та доступності даних, що стосуються юридичних питань банку. У цьому сегменті мережі застосовуються додаткові заходи безпеки, такі як фаєрволи (firewalls), виявлення та запобігання вторгнень (intrusion detection and prevention systems), системи шифрування, системи контролю доступу та інші заходи, що допомагають захистити дані від несанкціонованого доступу, витоку чи пошкодження.

В юридичній зоні також можуть бути розміщені робочі станції адвокатів, юристів та інших співробітників, які мають доступ до важливих юридичних документів та систем для виконання своїх обов'язків.

Враховуючи конфіденційний характер інформації, яка зберігається в юридичній зоні, важливо забезпечити належний рівень безпеки, використовуючи технології шифрування, резервне копіювання даних, контроль доступу та моніторинг системи, щоб уникнути можливих порушень безпеки та збитків.

Касова зона в банківській мережі відноситься до області, де знаходяться касові термінали або термінали обслуговування клієнтів. Це місце, де проводяться фінансові транзакції, обробляються платіжні операції та здійснюється обмін фінансовою інформацією між банком і клієнтами.Касова зона зазвичай обладнана спеціальними пристроями, такими як касові апарати, термінали оплати, карт–рідери та інші пристрої для обробки платежів. Вона може бути підключена до центральної банківської системи або сервера для авторизації та обробки транзакцій.

Безпека в касовій зоні має велике значення, оскільки вона включає обробку фінансових даних і особистої інформації клієнтів. Застосовуються заходи безпеки, такі як шифрування даних, захищений доступ до мережі, використання фаєрволів для захисту від несанкціонованого доступу та зловживань.

2.3 Апаратне забезпечення

Для реалізації поставленої задачі, обрано банківську систему, яка буде складись з певних зон, у які буть входити потрібне апаратне забезпечення. Сам план приміщення зображений на рисунку 2.6.

Так у юридичну зона входить:

1) 4 комп’ютери
2) 1 принтери

В адміністративну зону входять

1) 3 комп’ютери
2) 2 маршрутизатори

Касова зона:

1) 2 комп’ютери
2) 1 принтер

Серверна зона складається

1) 1 сервера
2) 1 комутатор
3) 1 Cisco ASA 5050

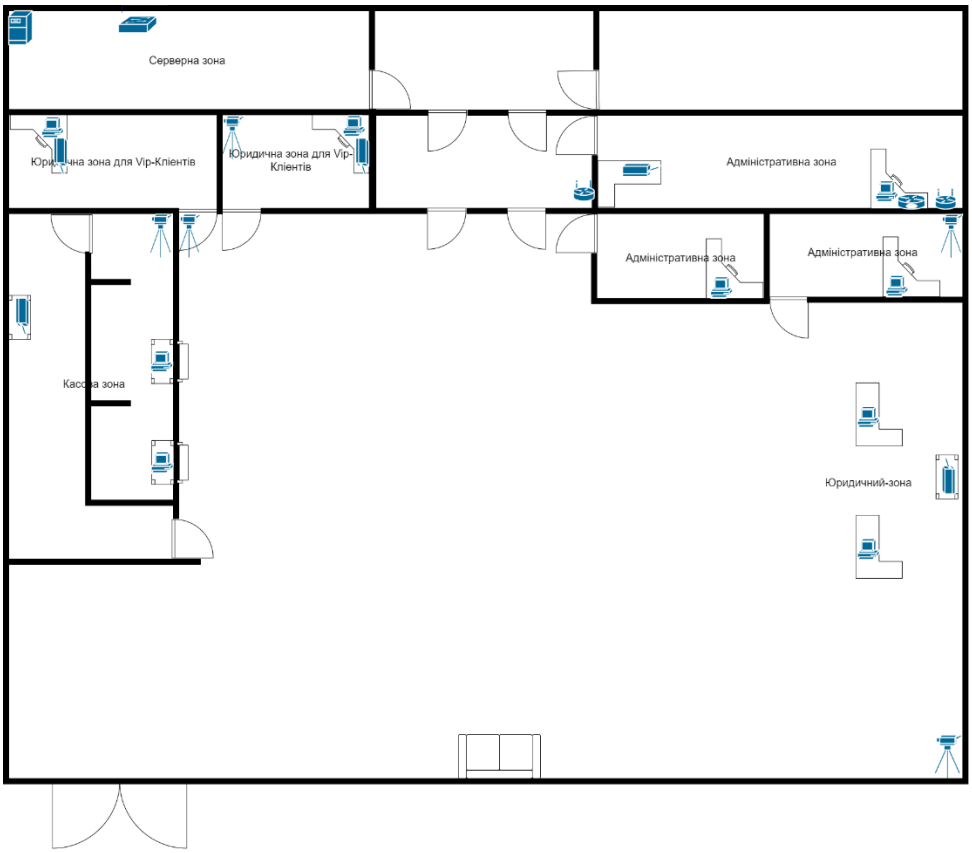


Рисунок 2.6 – План приміщення

Також у коридорі між Адміністративною та юридичною зонах стоїть 1 маршрутизатор, який роздає інтернет мережу для клієнтів.

Кожне вище перечисленні приладів виконує певні функції у мережі. Наприклад маршрутизатор як зображано на рисунку 2.7 відіграє важливу роль у

банківських системах і забезпечує ефективну комунікацію між різними мережевими пристроями, такими як комп'ютери, сервери, термінали, банкомати та інші пристрої.

Рисунок 2.7 – Маршрутизатор D-LINK DIR-820 AC1200

Основне застосування маршрутизатора в банківській системі включають. Підключення до інтернету, маршрутизатори використовуються для підключення банківської системи до зовнішнього Інтернету. Вони забезпечують шлюз між внутрішньою мережею банку і глобальною мережею, дозволяючи здійснювати комунікацію з іншими банками, клієнтами, платіжними системами та іншими зовнішніми ресурсами. Відділення та філії: Багато банків мають розподілену мережу філій та відділень. Маршрутизатори використовуються для підключення цих розподілених мереж та забезпечення безпечного та надійного обміну даними між ними та центральними серверами банку. Внутрішня мережа банку: Маршрутизатори використовуються для створення та керування внутрішньою мережею банку. Вони дозволяють розподіляти мережевий трафік, маршрутизувати пакети між різними підрозділами, встановлювати правила безпеки та контролювати доступ до ресурсів мережі. Маршрутизатори можуть підтримувати VPN–з'єднання для забезпечення безпечного та приватного доступу до банківської

мережі з віддалених місць. Тому мною був обраний маршрутизатори моделі D–Link DIR–820 характеристики якого зображені на таблиці 2.1.

Таблиця 2.1 – Технічні характеристики машрутизатора

Швидкість Wi–Fi	До 1167 Мбіт/с
Частота роботи Wi–Fi	2,4 ГГц,5 ГГц
Інтерфейс	Rj45–LAN, WAN
Швидкість LAN–портів	100 Мбіт/с
Кількість LAN–портів	3
WAN–порт	Ethernet
USB–порт	Hi
Розміри	30 x 190 x 120 мм

Також за планом потрібен один сервер моделі ARTLINE Business R35 v30, який зображений на рисуноку 2.8 і характеристики якого записані в таблиці 2.2. Він є не від'ємною складовою банківської мережі. Основне його застосування це централізоване зберігання даних. Сервер використовується для зберігання та керування великим обсягом даних банку, включаючи інформацію про клієнтів, транзакції, рахунки тощо. Це дозволяє забезпечити централізований доступ та управління даними, забезпечувати їх безпеку та резервне копіювання. Обробка транзакцій банківські сервери відповідають за обробку транзакцій клієнтів, включаючи перекази коштів, платежі, зняття грошей з банкоматів та інші операції. Ці сервери забезпечують швидку та надійну обробку транзакцій, забезпечуючи високу доступність та низьку затримку.

Мобільний банкінг сервери використовуються для підтримки мобільних банкінгових додатків та послуг. Вони забезпечують безпечний доступ клієнтів до їх банківських рахунків через мобільні пристрої, дозволяючи здійснювати платежі, перевіряти стан рахунків, заморожувати картки та багато іншого.

Рисунок 2.8 – Сервер RTLINE Business R35 v30

Таблиця 2.2 – Технічні характеристики серверних

Тип процесора	Восьмиядерний Intel Xeon E–2388G (3.2 – 5.1 ГГц)
Оперативна пам’ять	8 GB DDR4 оперативной памяти
CD/DVD	Оптичний привід LG DVD±R/RW SATA Super Multi
HDD	SSD: 3 x 500 ГБ

Для під’єднання усіх пристрої було обрано комутатор моделі TP–Link TL–SF1024D характеристики якого записані на таб 2.3 та зображений на рис 2.1.

Комутатори відіграють важливу роль у банківських системах, забезпечуючи швидке та надійне перемикання мережевого трафіку між різними пристроями в мережі. Для цієї цілі було обрано комутатор моделі TP–Link TL–SF1024D характеристики якого записані на таблиці 2.3 та зображений на рисунку 2.9.

Рисунок 2.9 – Комутатор TP–Link TL–SF1024D

Основні способи використання комутаторів у банківських системах:

1) Локальна мережа (LAN): Комутатори використовуються для підключення комп'ютерів, серверів, принтерів та інших пристроїв до локальної мережі банку. Вони забезпечують швидку передачу даних в межах мережі, дозволяючи ефективну комунікацію та спільний доступ до ресурсів.

2) Віртуальна локальна мережа (VLAN): Комутатори дозволяють створювати та управляти віртуальними локальними мережами. Це дозволяє розділити фізичну мережу на логічні сегменти, що мають власні правила доступу та політики безпеки. VLAN дозволяє контролювати комунікацію між різними групами пристроїв у мережі банку.

3) Безпека мережі: Комутатори можуть виконувати функції безпеки на рівні мережевого доступу. Вони підтримують функцію аутентифікації пристроїв, контролю доступу та виявлення шкідливого трафіку. Комутатори здатні розпізнавати та блокувати недозволений доступ до мережі та виявляти аномалії в мережевому трафіку.

4) Висока доступність: Комутатори можуть працювати в режимі резервування (redundancy) для забезпечення надійності та високої доступності мережі. Вони підтримують технології, такі як Spanning Tree Protocol (STP) або Rapid Spanning Tree Protocol (RSTP), які дозволяють уникати петель у мережі.

Таблиця 2.4 – Технічні характеристики комутатора

Кількість портів	24
Стандарт мережі	IEEE 802.3i 10 BASE–T, IEEE 802.3u 100 BASE–TX, IEEE 802.3x Управління потоком, IEEE 802.3af PoE
Максимальний струм навантаження	450Вт (48В, 9.3А)
Потужність на канал (Вт)	15.4
Напруга в зоні	48В

Камери відеоспостереження(рисунок.2.9) є ще однією частиною в захисті банку. Вони використовуються для нагляду, контролю та захисту приміщень, активів і персоналу банку. Основні застосування камер відеоспостереження у банках включають:

1) Безпека приміщень: Камери будуть встановлені у важливих зонах банку, таких як каси, адміністративній, юридичній, та серверній зонах. Вони дозволяють відстежувати дії співробітників та клієнтів, а також реагувати на будь–які підозрілі або небажані події, такі як крадіжки, вторгнення або інциденти безпеки.

2) Моніторинг транзакцій: Камери встановлюються неподалік від кас та банкоматів для відеозапису транзакцій клієнтів. Це допомагає вирішувати спірні ситуації, встановлювати відповідальність і забезпечувати відстеження фінансових операцій.

3) Виявлення і запобігання шахрайству: Камери допомагають виявляти та запобігати шахрайству, такому як фальшиві заявки, підроблення документів або шахрайство з платіжними картками. Вони можуть бути сполучені з системою розпізнавання обличчя та іншими технологіями, щоб виявляти підозрілу активність та автоматично сповіщати відповідних служб безпеки.

4) Забезпечення доказової бази: Відеозаписи з камер відеоспостереження можуть служити як докази в разі виникнення правових питань, розслідування інцидентів або вирішення спорів.

Рисунок 2.9 – Камера VLC–1128WM

Принтери в банках використовуються для друку різних документів та матеріалів, що стосуються банківських операцій та обслуговування клієнтів. Основні застосування принтерів у банках включають:

1) Друк банківських документів: Принтери використовуються для друку банківських документів, таких як чеки, виписки з рахунку, банківські заяви, платіжні доручення тощо. Це дозволяє клієнтам отримувати фізичні копії документів та забезпечує зручність та надійність у проведенні банківських операцій.

2) Друк документів для клієнтів: Принтери використовуються для друку різних документів для клієнтів, таких як квитанції про зняття грошей, підтвердження транзакцій, розрахункові виписки та інші документи. Це дозволяє клієнтам мати фізичні копії важливих документів, які можуть бути потрібні для обліку та подальшого використання.

3) Друк внутрішніх матеріалів: Принтери використовуються для друку внутрішніх матеріалів банку, таких як внутрішні документи, звіти, меморандуми, наклейки, брошури тощо. Це забезпечує внутрішню комунікацію та обмін інформацією між співробітниками банку.

Для комп'ютерної мережі банку необхідно мати потужні комп'ютери з відповідними характеристиками, які забезпечують ефективну роботу мережевих додатків та обробку великого обсягу даних. Основні вимоги до комп'ютерів для банківської мережі включають:

1) Процесор: Рекомендується використовувати процесори з високою швидкістю та багатоядерними можливостями, що дозволяють ефективно обробляти завдання в мережі. Наприклад, Intel Core i5 або i7, AMD Ryzen 5 або Ryzen 7.

2) Оперативна пам'ять (RAM): Важливо мати достатню кількість оперативної пам'яті для запуску багатьох програм і процесів одночасно. Рекомендована мінімальна кількість RAM – 8 ГБ, але для більш вимогливих завдань може бути потрібно 16 ГБ або більше.

3) Жорсткий диск: Відповідно до потреб банківської мережі може використовуватись жорсткий диск (HDD) або твердотільний накопичувач (SSD). SSD забезпечує швидший доступ до даних і виконання завдань, тому рекомендується його використання для більшої продуктивності.

4) Графічна карта: У банківській мережі графічні вимоги зазвичай не є основними, тому використання інтегрованої графічної карти буде достатнім.

5) Операційна система: Зазвичай в банківській мережі використовується операційна система Windows

Тому зважаючи написаного вище було вибрано відповідний комп'ютер з додатковим обладнням яке описано в таблиці. 2.5.

Таблиця 2.5 – Технічні характеристики комп'ютера.

Тип процесора	AMD Ryzen 5 3600 3.6GHz/32MB
Материнська плата	Socket AM4 (AMD A320 Chipset, 2 x DDR4, mATX)
Оперативна пам'ять	16 GB DDR4 оперативной памяти
CD/DVD	Оптичний привід LG DVD±R/RW SATA Super Multi
Відеоадаптер	AMD Radeon R Graphic
HDD	TB TOSHIBA Hard Drive – 64MB Cache, 7200RPM, 6.0Gb/s
Монітор	22" Samsung S22B420BW – Class B

2.4 Мережевий екран(Cisco ASA)

Cisco ASA 5505 (рисунок 2.10 – Зовнішній вигляд) – це сучасний багатофункціональний пристрій для захисту локальних мереж від зовнішніх атак і вторгнень. Основною функцією брандмауера Cisco є захист мережі від вторгнень, вірусів, спаму, шпигунського програмного забезпечення та фільтрації вмісту

трафіку користувачів. Створений на апаратній платформі мережевий екран Cisco ASA забезпечує високу надійність і продуктивність для безпеки локальної мережі від зовнішніх атак. Брандмауер Cisco ASA 5505 забезпечує високий рівень безпеки з достатньою гнучкістю.

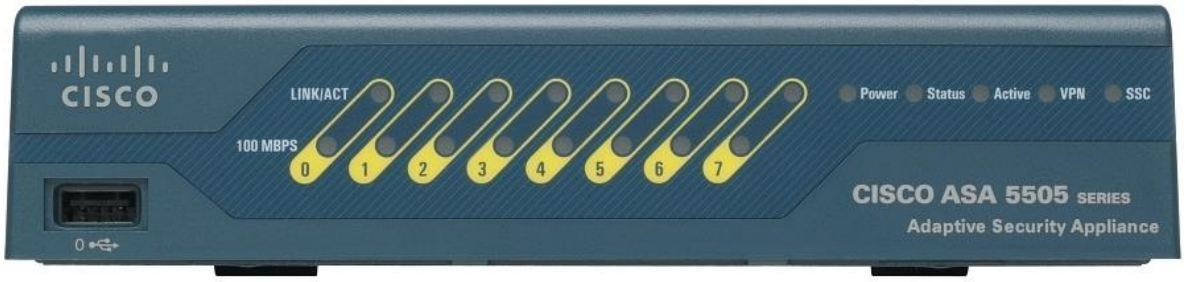


Рисунок 2.10 – Зовнішній вигляд Cisco ASA 5505

Багатофункціональний пристрій безпеки Cisco ASA серії 5505 — це перша та найкраща лінія захисту. Забезпечення безпеки та надійності корпоративної мережі означає, що співробітники завжди можуть довіряти мережі.

Брандмауер Cisco ASA 5505 забезпечує до 150 Мбіт/с транзитного трафіку. При налаштуванні VPN–доступу він працює на швидкості до 100 Мбіт/с*. В першу чергу, завдяки простоті використання пристрій спрямований на забезпечення безпеки мережі для користувачів у сегменті малого та середнього бізнесу. На додаток до функції брандмауера, ASA 5505 виконує трансляцію NAT для спільного доступу до Інтернету та є сервером IPSec VPN для безпечного віддаленого доступу до локальних ресурсів. Великою перевагою є вбудований 8–портовий комутатор з 2 портами, які підтримують PoE. Він дозволяє легко підключати IP–камери, точки доступу WI–FI або IP–телефони.

Функціональні можливості ASA 5505:

1) підтримка двох мереж VPN для зв'язку між офісами та партнерами з розширенням до 25 (ASA 5505);

2) підтримка від 5 (ASA 5505) користувачів локальної мережі будь–якої точки;

3) безліч варіантів високошвидкісних мережевих з'єднань, залежно від ваших потреб у продуктивності;

4) заздалегідь налаштовані пакети для спрощення замовлення та налаштування.

2.5 Висновки

Можна зробити висновок що перед створенням комп’ютерної мережі потрібно визначитись із топологією. Після перегляду усіх варіантів було обрана топологія Зірка. Далі потрібно обрати апаратне забезпечення для комп’ютерної мережі банку. З початку потрібно підрахувати кількість техніки яка буде використовуватись. Адже від цього буде вибраний комутатор. Він забезпечить швидке та надійне перемикання мережевого трафіку між різними пристроями в мережі. Маршрутизатор потрібен для ефективної комунікацію між різними мережевими пристроями, такими як комп'ютери, сервери, термінали, банкомати та інші пристрої. Сервер у мережі виконує одну із важливих найважливіших завдань .Він дозволяє забезпечити централізований доступ та управління даними, і також їх безпеку та резервне копіювання. Cisco ASA використовується як firewoll, VPN–концентратор, система виявлення та запобігання вторгнення, а також забезпечує можливість керування трафіком в мережі. Камери надають можливість фізично захистити мережу від шахраїв та призначені для моніторингу приміщень.

3 ПРОГРАМНО–АПАРАТНА РЕАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Налаштування сегментів мережі та маршрутизаціїі

По–перше, сегменти слід розташувати відповідно до обраної типології. В даному випадку форма зірки є однією з найпростіших і поширених. Після визначення типу логічної мережі необхідно налаштувати комп'ютер для встановлення IP–адреси, маски підмережі та шлюзу за замовчуванням. Потрібно зайти на свій комп'ютер або принтер по шляху «Config» → «Global Settings» та поставити галочку біля DHCP. Це показано на рисунку 3.1.

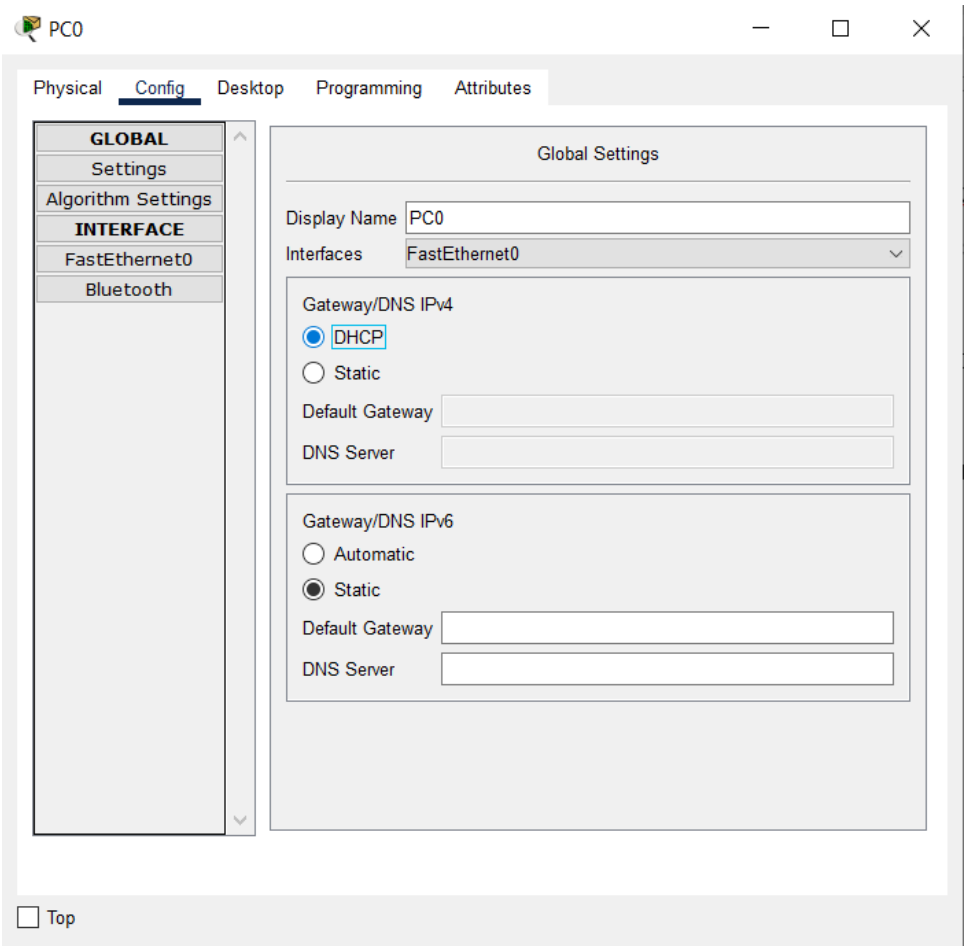


Рисунок 3.1 – Встановлення IP–адресу, маску підмережі та шлюзи за замовченням.

IP–адреси потрібні для ідентифікації та адресації комп'ютерів у комп'ютерній мережі. Ці адреси використовуються для встановлення з'єднань і обміну даними між комп'ютерами в мережі.

Маска підмережі (subnet mask) використовується в поєднанні з IP–адресою комп'ютера, щоб визначити, до якої підмережі він належить і які мережеві адреси він може використовувати.

Шлюз за замовчуванням (default gateway) визначає шлях до іншої мережі або Інтернету за допомогою комп'ютера, коли немає конкретної мережі чи підмережі для надсилання пакетів даних.

Використовуючи протокол DHCP, комп'ютер може отримати її IP–адресу, маску підмережі, адресу шлюзу за замовчуванням та інші параметри мережі від свого DHCP–сервера автоматично та централізовано. Усі адреси наведено в таблиці 3.1.

Таблиця 3.1 – Таблиця адресів

Пристрій	Інтерфейс	IP –адреса	Маска підмережі	Шлюз за замовчуванням
PC0	Fa0/1	192.168.1.0	255.255.255.0	192.168.1.1
PC1	Fa0/2	192.168.1.2	255.255.255.0	192.168.1.1
PC2	Fa0/3	192.168.1.3	255.255.255.0	192.168.1.1
PC3	Fa0/4	192.168.2.0	255.255.255.0	192.168.2.1
PC4	Fa0/5	192.168.2.2	255.255.255.0	192.168.2.1
PC5	Fa0/6	192.168.3.0	255.255.255.0	192.168.3.1
PC6	Fa0/7	192.168.3.2	255.255.255.0	192.168.3.1
PC7	Fa0/8	192.168.2.3	255.255.255.0	192.168.2.1
PC8	Fa0/9	192.168.2.4	255.255.255.0	192.168.2.1
Printer0	Fa0/10	192.168.2.5	255.255.255.0	192.168.2.1
Printer1	Fa0/11	192.168.3.3	255.255.255.0	192.168.3.1

Кінець таблиці.3.1– Таблиця адресів

Camera2	Fa0/15	192.168.1.6	255.255.255.0	192.168.1.1
Camera3	Fa0/16	192.168.1.7	255.255.255.0	192.168.1.1
Sever	Fa0/17	192.168.4.0	255.255.255.0	192.168.4.1
ASA0	Fa0/18		255.255.255.0	
R	Fa0/19		255.255.255.0	
R1	Fa0/20	192.168.1.9	255.255.255.0	192.168.1.1
R2	Fa0/21	192.168.1.10	255.255.255.0	192.168.1.1
Printer3	Fa0/22	192.168.1.8	255.255.255.0	192.168.1.1
Printer4	Fa0/23	192.168.2.3	255.255.255.0	192.168.2.1
Printer2	Fa0/12	192.168.2.5	255.255.255.0	192.168.2.1
Camera	Fa0/13	192.168.1.4	255.255.255.0	192.168.1.1
Camera1	Fa0/14	192.168.1.5	255.255.255.0	192.168.1.1

Після налаштування адрес потрібно налаштувати VLAN у зонах обладнання комутатора. VLAN дозволяють створювати групи комп'ютерів або мережевих пристроїв, які програмно належать до цієї мережі незалежно від їх фізичного розташування.

У старіших версіях CISCO Packet Tracer, щоб створити новий vlan, потрібно було прописувати команду в ручну через GLI, Для цього потрібно було використовувати такі команди як switchport access vlan N–встановлював чисельне значення vlan; switchport mode access – встановлював вид каналу; interface range ports – встановлював який порти під'єднані до vlan.

Але з новішою версією CISCO Packet Tracer є можливість встановити новий vlan без написання коду потрібно зайти switch–>Config–>Vlandatabase

Вести число та ім'я і додати до інших підмереж. Далі потрібно призначити vlan на певні порти потрібно зайти в switch–>Config–>interface і вибрати відповідний порт. Потім потрібно встановити відповідний vlan в меню і показати який з каналу зв'язку ми обираємо потрібний для зв'язку однієї мережі, а канал

trunk для декількох зазвичай його ставлять між маршрутизаторами та комутаторам для доступу усім пк до інтернета.

Приклад створення vlan на рисунку 3.1, діаграма підключення портів до VLAN на рисунку 3.2 та налаштування типу каналу на рисунку 3.3.

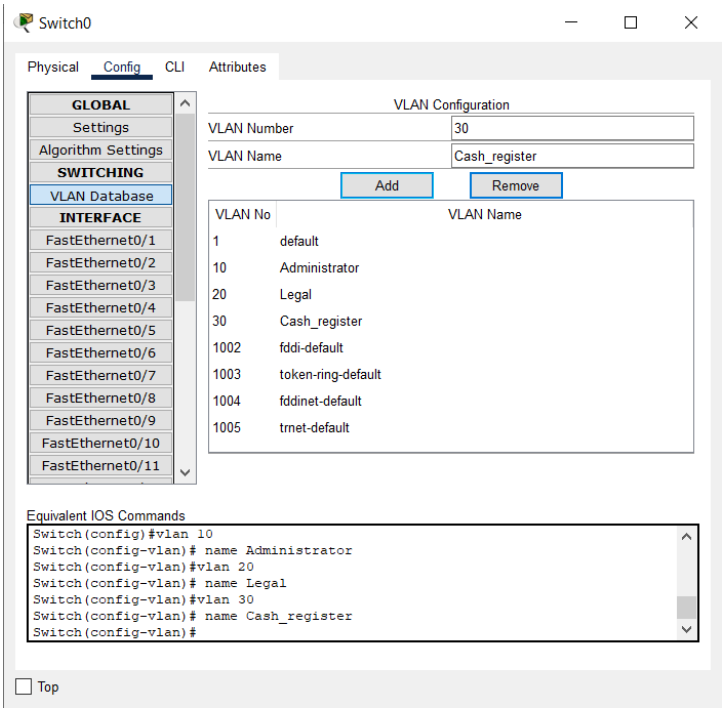


Рисунок 3.1 – Створення vlan "Admistrator", " legal", " cash register" на маршрутизаторі S1

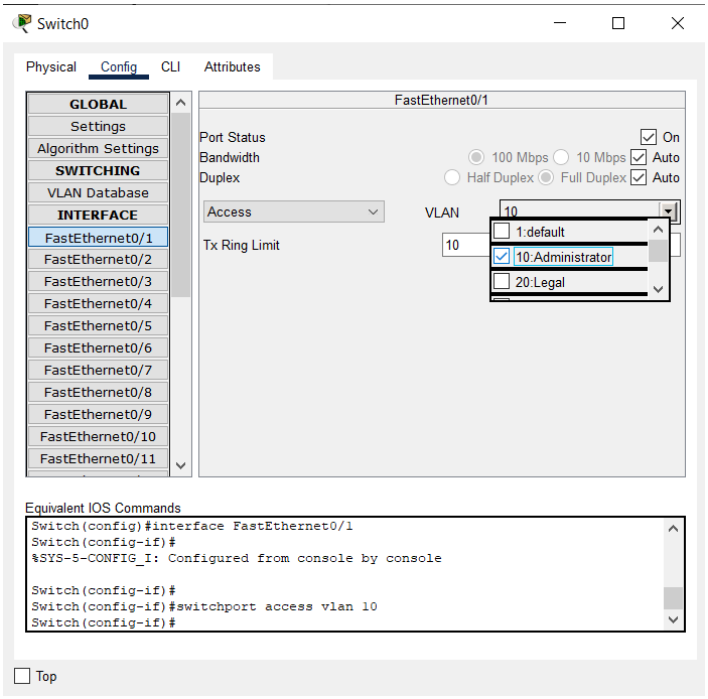


Рисунок 3.2 – Призначення vlan портам на S1

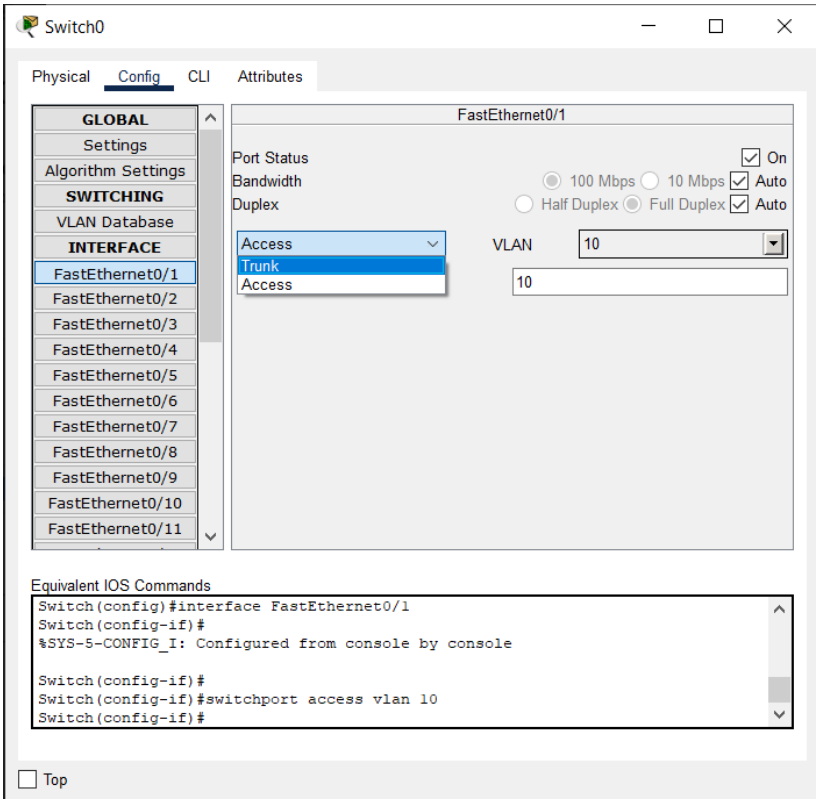


Рисунок 3.3 – Створення trunk каналів на S1

У маршрутизаторі потрібно налаштувати IP–адресу для цього порту як на рисунку 3.4.

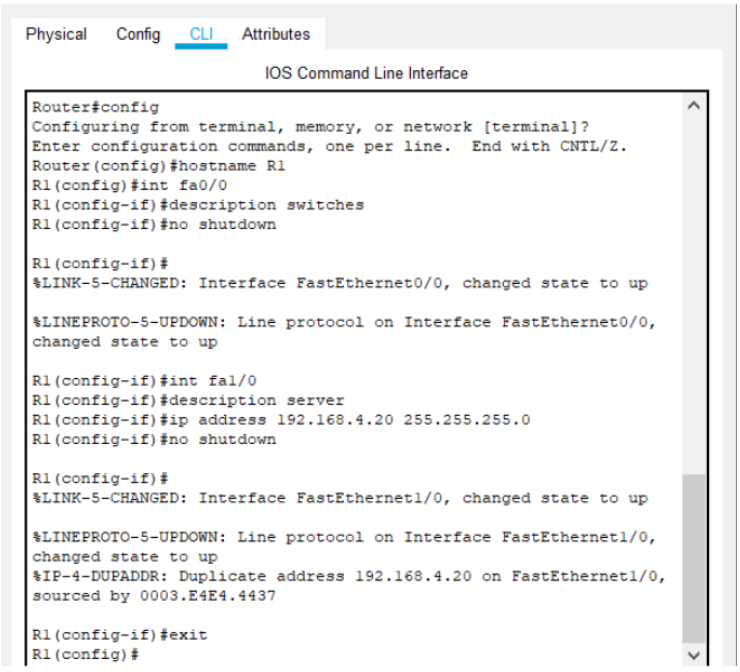


Рисунок 3.4 – Увімкнення портів на маршрутизаторі, назначення IP адреси

Для цього підходить команда int Interface Number. Interface – це ім’я порту/інтерфейсу відповідно, а Number – номер інтерфейсу. Використовуйте команду description description для опису інтерфейсу. де description – це опис інтерфейсу. Потім встановіть IP–адресу. Це робиться за допомогою команди ip–адреси Address Mask. де Address — це введена вами адреса, а Mask — маска підмережі. Щоб мати можливість підключитися до порту, потрібно відкрити порт на маршрутизаторі. Для цього не потрібна команда відключення.

Потім створіть sub–interface. Для цього потрібно написати команду int Interface Number.Number. Після створення sub–interface потрібно призначити нову VLAN за допомогою команди інкапсуляції dot1Q Number. де Number – це номер VLAN. Також потрібно вказати, які інтерфейси зовнішні, а які внутрішні. Ви повинні написати ip nat inside для внутрішнього та ip nat external для зовнішнього як зображено на рисунку 3.7.

Далі потрібно створити саб інтерфейси для кожного vlan як на рисунку 3.5:

Рисунок 3.5 – Створення sub–interface.

Після приписання sub–interface для кожного vlana потрібно перевірити, чи вони були створені на маршрутизаторі для цього підходить команда show run результат виконання на рисунку 3.6.

Рисунок 3.6 – Результат виконання.

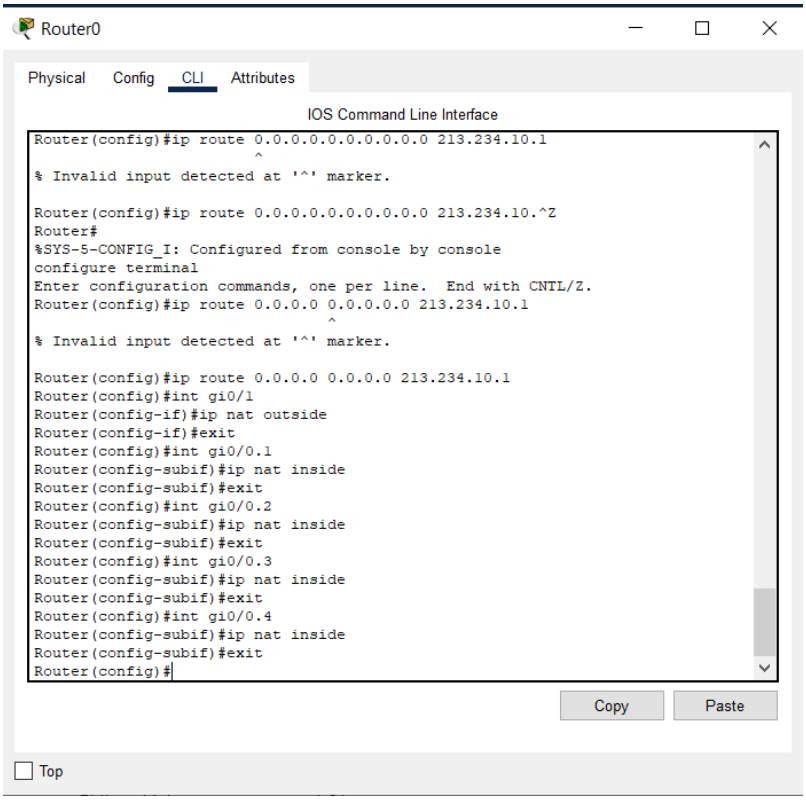


Рисунок 3.7 – налаштування NAT

Далі потрібно створити access–list він потрібний в маршрутизаторі для керування трафіком на основі різних критеріїв, таких як IP–адреси, порти транспортного рівня, протоколи тощо. ACLs встановлюються на маршрутизаторі для фільтрації пакетів даних, керування доступом та захисту мережі. Для створення access–list використовують команду ip access–list standard Name, де Name це назва access–list. Щоб додати до access–list потрібно прописати permit Adress Mask, як зображано на рисунку 3.8.

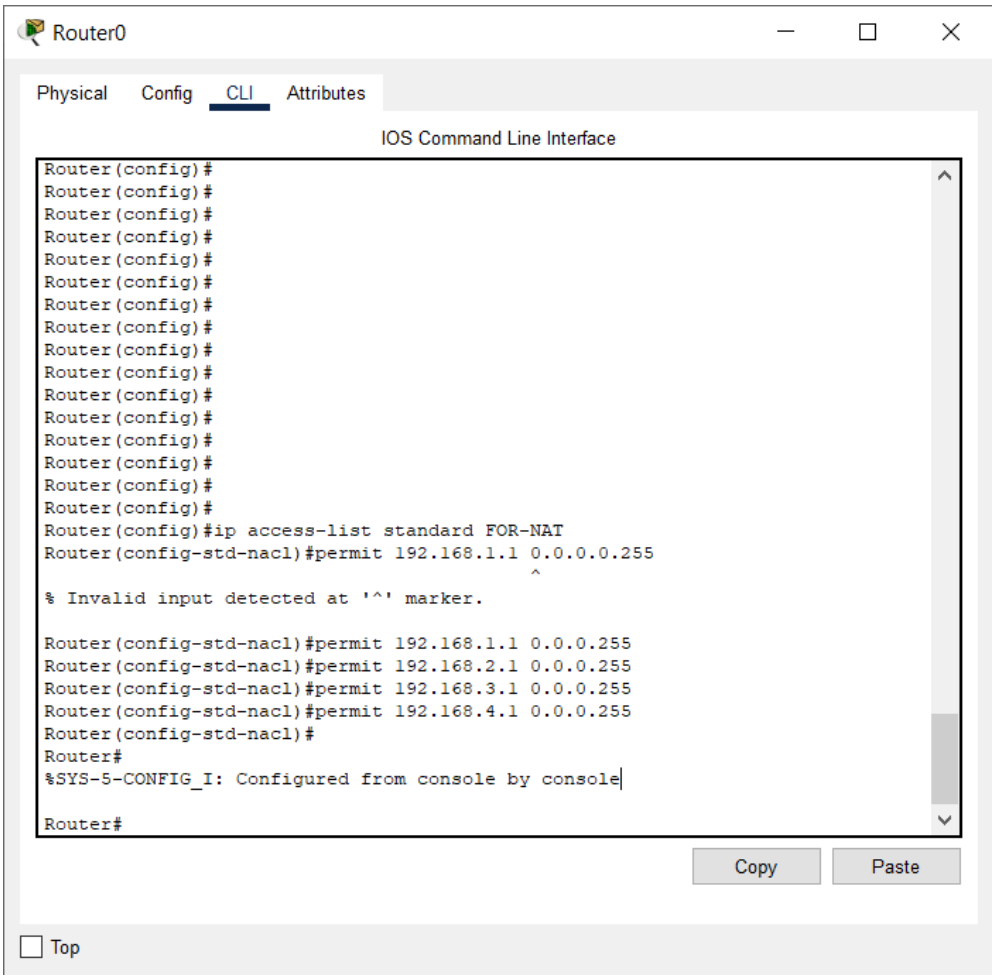


Рисунок 3.8 – Налаштування access–list на маршрутизаторі

3.2 Налаштування серверу, служби dhcp та підключення.

Для налаштування dhcp потрібен сервер завдяки ньому ми зможемо надавати динамічні ip для кожного пристрою, який підключений до мережі, але для початку потрібно задати статичний ip для сервера. Натиснемо на серевер в Cisco Packet

Tracer перейдемо на вкладку Desktop зайдемо в IP–configuration, де припишемо адрес 192.168.4.1 з шлюзом 255.255.255.0 і шлях до sub–interfase 192.168.4.1 це має виглядати як на рисунку 3.9.

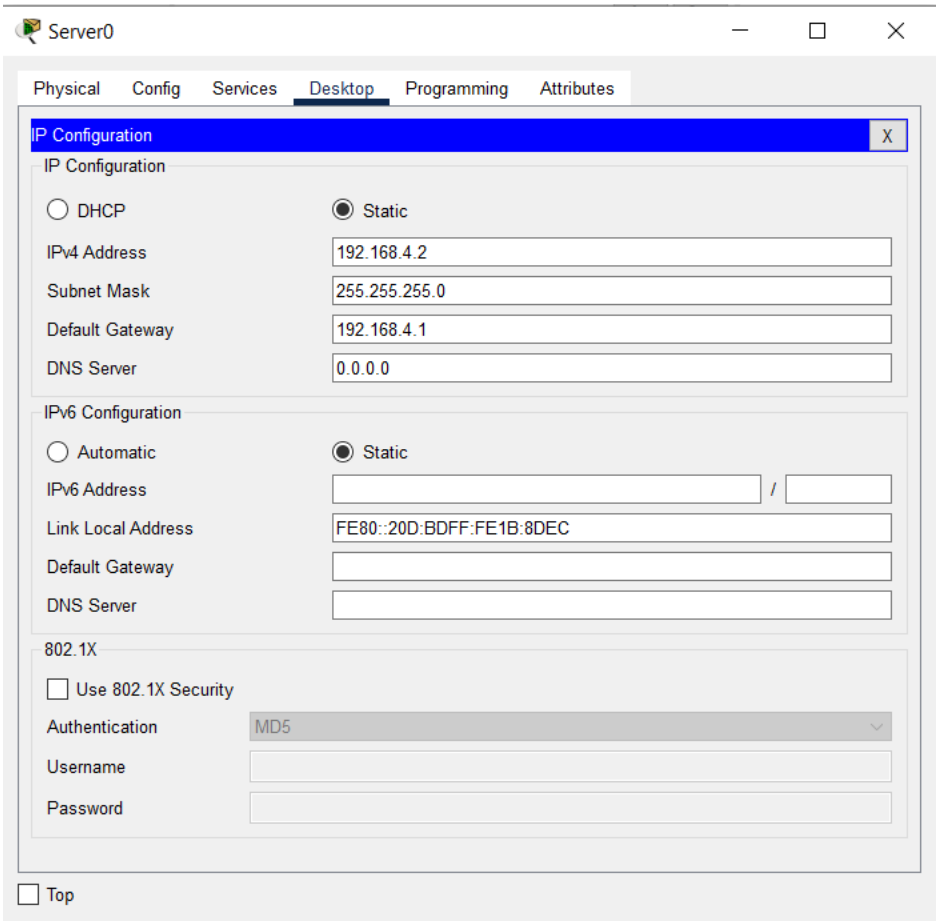


Рисунок 3.9 – Налаштування IP сервера.

Після того як було прописано налаштування ip. Можна переходити до створення dhcp на сервері для подальшої передачі адресації на пристрої мережі. Насамперед перейдемо на вкладку Config–>DHCP, де буде створений один стандартний Pool ip. У полі Pool Name ведемо потрібне ім’я для ідифікації pool, далі припишемо шлях до sub–interface на маршрутизатор для певного vlan. Після того як було встановлено ім’я та шлях, потрібно вести від якого адреса буде динамічного створюватись ip для пристроїв підкочених на пряму до мережі, результат зображений на рисунку 3.10.

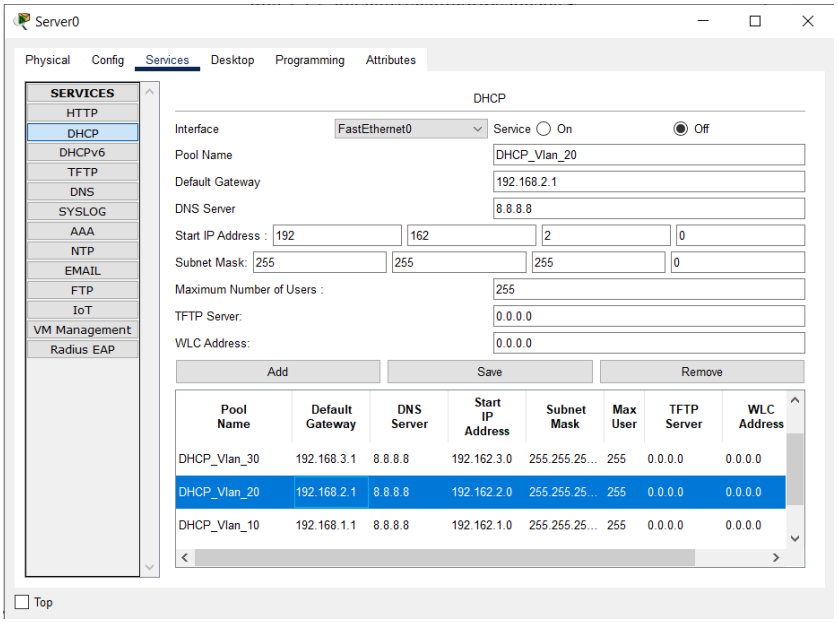


Рис.3.10 – налаштування DHCP на сервері

Але сервер знаходиться в окремому сегменті і коли пристрої будуть надсилати широкомовний запит при пошуку dhcp–сервера, він через маршрутизатор не пройде оскільки пристрої знаходяться у різних vlan. Тому потрібно перейти на маршрутизатор і використати команду helper–address(рисунок 3.11), її потрібно прописати для кожного sub–interface. Завдяки цьому запит буде надходити до сервера у якому зберігаються згенеровані ip.

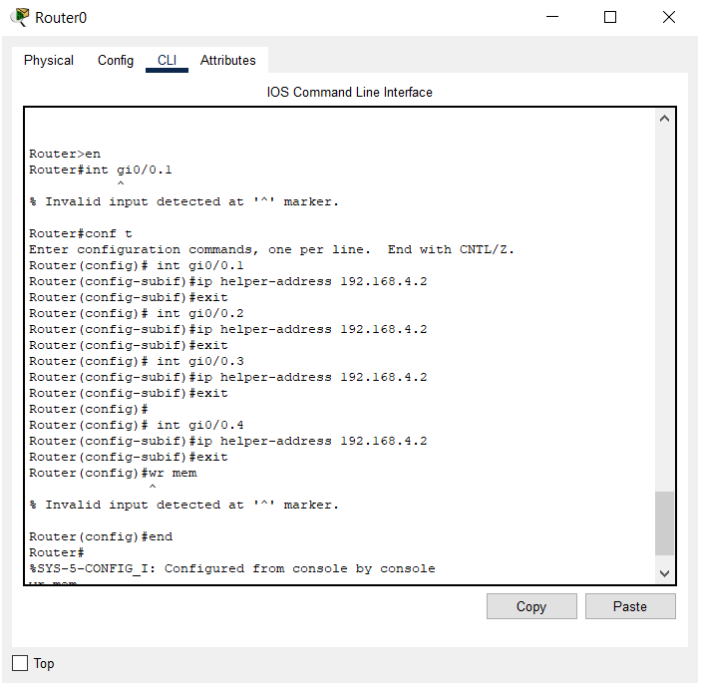


Рисунок 3.11 – Налаштування маршрутизатора для роботи dhcp–сервера

Після налаштування маршрутизатора можна перейти до налаштування бездротового з’єднання для початку потрібно встановити статичний ip, маску, та шлях до маршрутизатора як зображено на рисуноку 3.12.

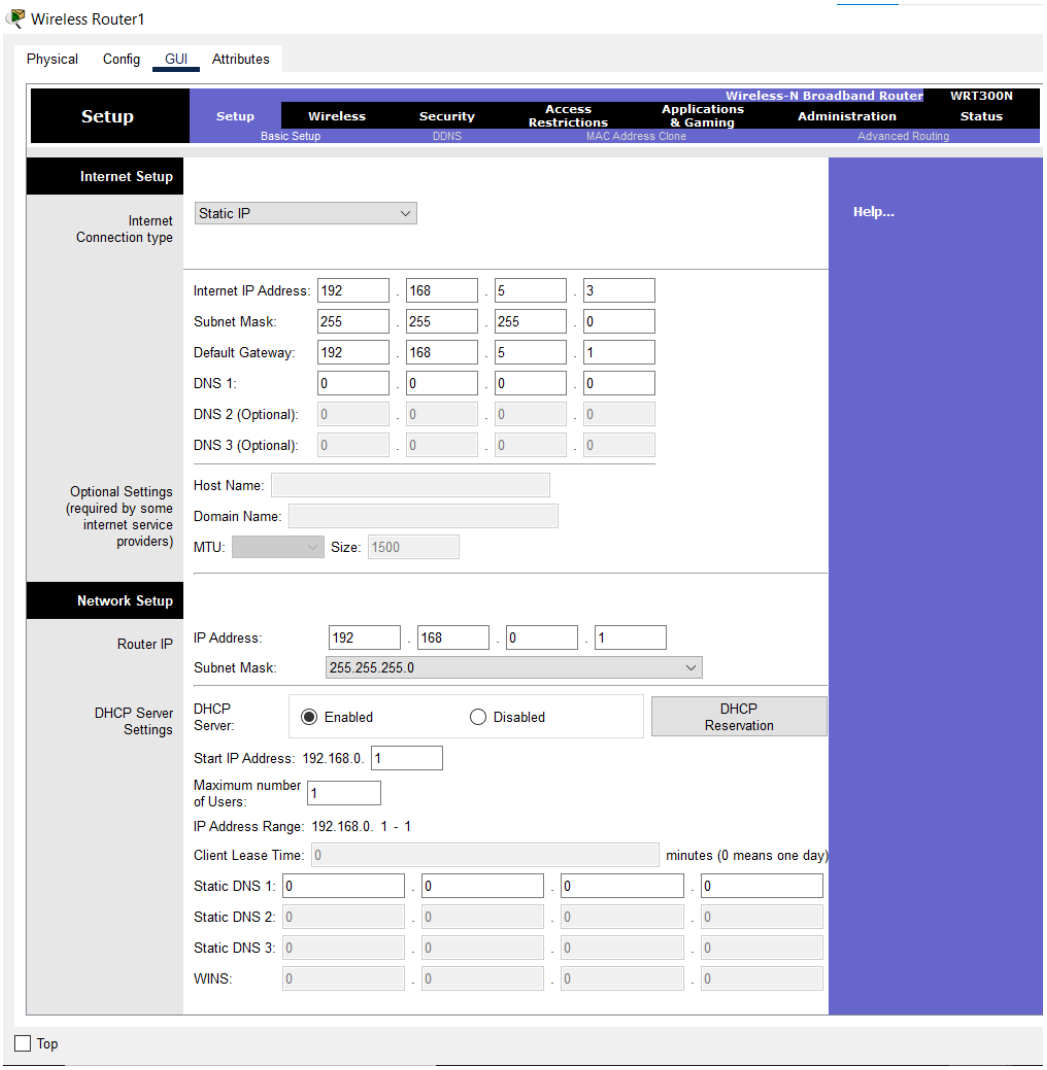


Рисунок 3.12 – Налаштування бездротового з’єднання.

Далі встановимо SSID ім’я яке буде відображатись для наших приладів. Його можна встановити на вкладці Wireless–>Basic Wireless Settings та в строчці Network Name (SSID) встановимо потрібне ім’я, як зображано на рис.3.13. Після встановлення ім’я також потрібно обрати протокол за яким буде відбуватись захист бездротового з’єднання. Для перейдемо до вкладки Wireless–> Wireless Security. У ній переходимо до строчки Security Mode і обираємо тип захисту WPA2 Personal як зображено на рис.3.14.

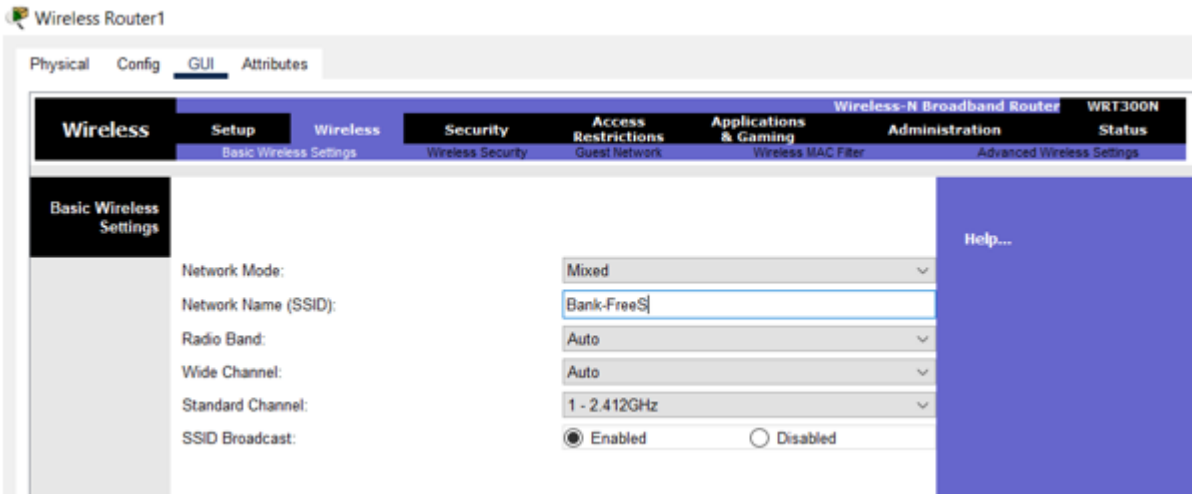


Рис.3.13 – Встановлення ім’я для бездротової мережі.

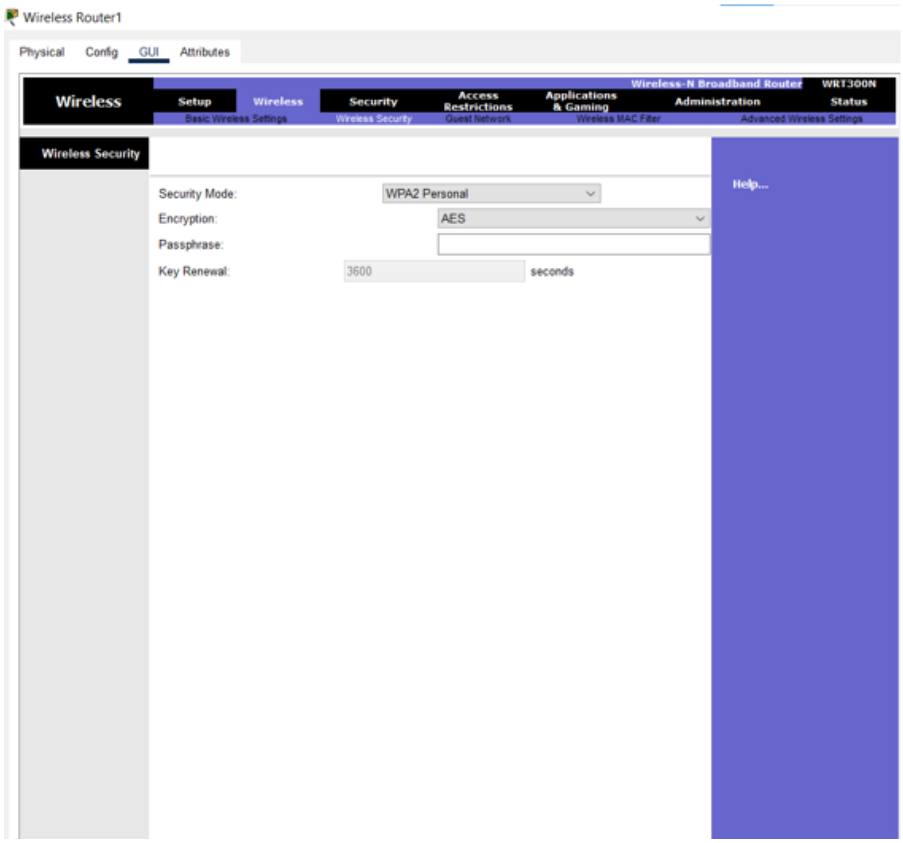


Рисунок 3.14 – Налаштування захисту бездротового з’єднання.

3.3 Налаштування безпеки.

Для встановлення безпеки на мережі щоб ніхто з постороніх не мав можливості доступу до комутатора. Спочатку потрібно створити пароль для цього

потрібно прописати line console 0, потім написати пароль за допомогою команди Password password, де password – ваш пароль який ви зазначаєте він потрібний для входу в конфігураційний режим. Далі прописати login. Також є можливість встановлення банерного повідомлення за допомогою команди banner motd “Message”, де Message– цк наше повідомлення яке ми прописуємо для сповіщення

Встановлення паролів та банерного повідомлення на комутатор S1 як на рисунку 3.15:

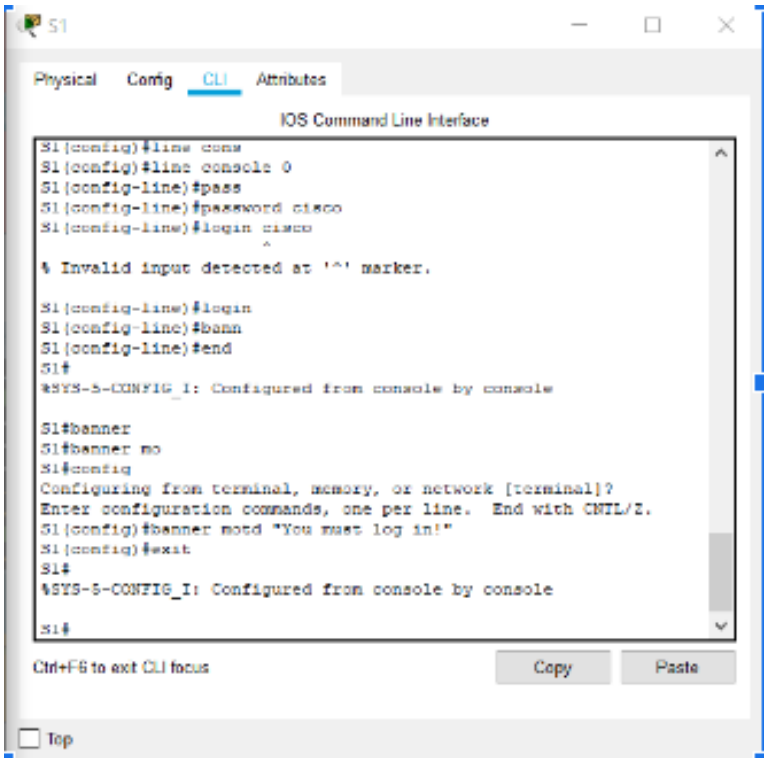


Рисунок 3.15 – Встановлення паролів та банерного повідомлення на комутатор S1.

Перед тим як створювати DMZ потрібно налаштувати Cisco ASA. Перейдіть у CLI, та спробуйте зайти в привілейований режим із командою enable, пристрій запитає про пароль для входу. Поки даний пристрій має налаштування за замовчуванням – пароль не визначений, або пустий. Далі налаштуємо можливість виконувати конфігурування екрану за допомогою логіну та паролю, тому створимо відповідний запис на стороні екрану як на рис.3.16

Тепер перейдемо на налаштування Security Level яке встановлює рівень довіри до інтерфейсу, і визначається наступним чином – чим більше його значення, тим більший і рівень довіри. Повертаючись до цих налаштувань, можна помітити що інтерфейс, який відповідає за трафік мережі з середини – має налаштований рівень в 100, тоді як інтерфейс для зовнішнього – 0. Тут діє правило, трафік з інтерфейсу з більшим рівнем security level може передавати пакети на інтерфейс з меншим рівнем security level, але не навпаки.

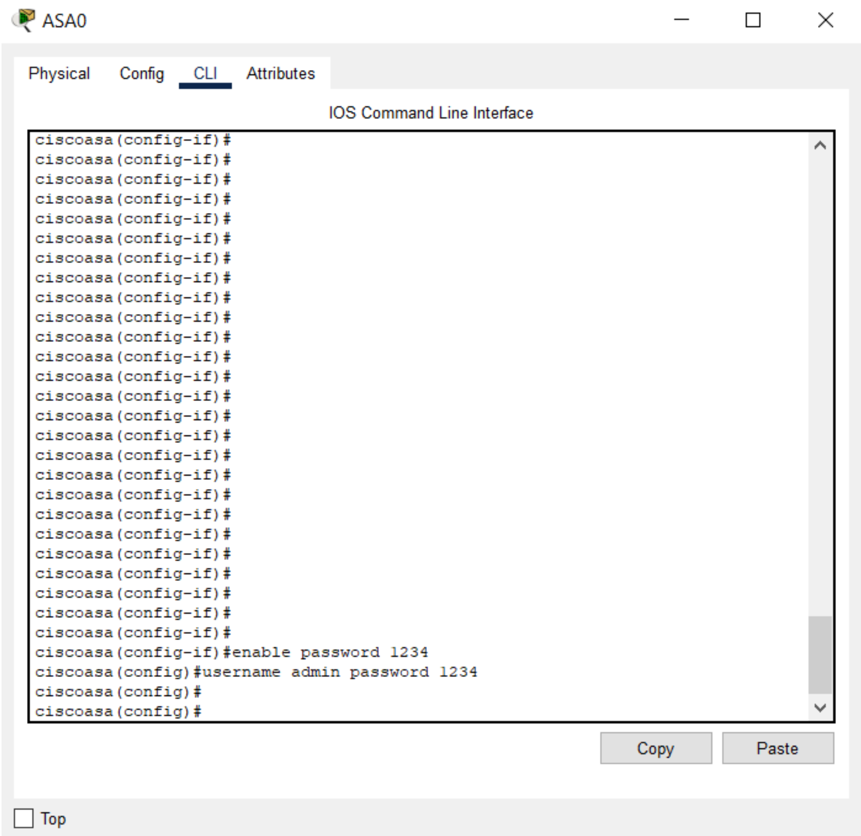


Рис.3.16 – Встановлення пароля та користувача на Cisco ASA.

Тому, із налаштуваннями за замовчуванням – трафік із внутрішньої мережі може виходити за його межі (бо 100 більше за 0), а от зовнішній входити не зможе (бо 0 менше за 100).

Щоб змінити цей рівень доступу потрібно перейти до interface та вести комаду security–level як це зображено на рис.3.17.

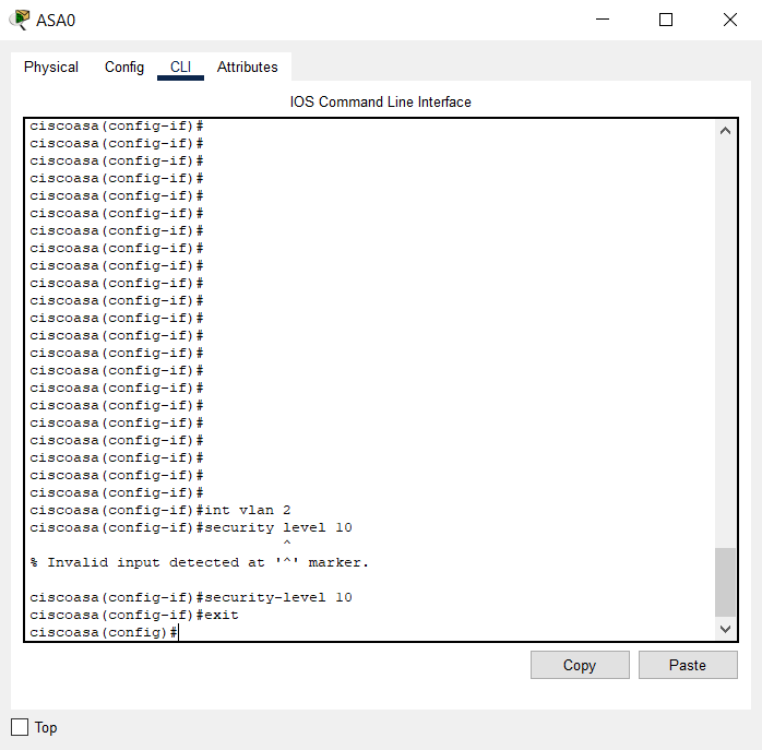


Рис.3.17 – призначення рівень доступу для зовнішнього vlan.

Далі перейдемо до налаштування DMZ зони в мережі. Для початку налаштуємо NAT з боку Cisco ASA. Для цього потрібно знову вернутися до CLI. У ньому ми припишемо команди як зображені на рис.3.18.

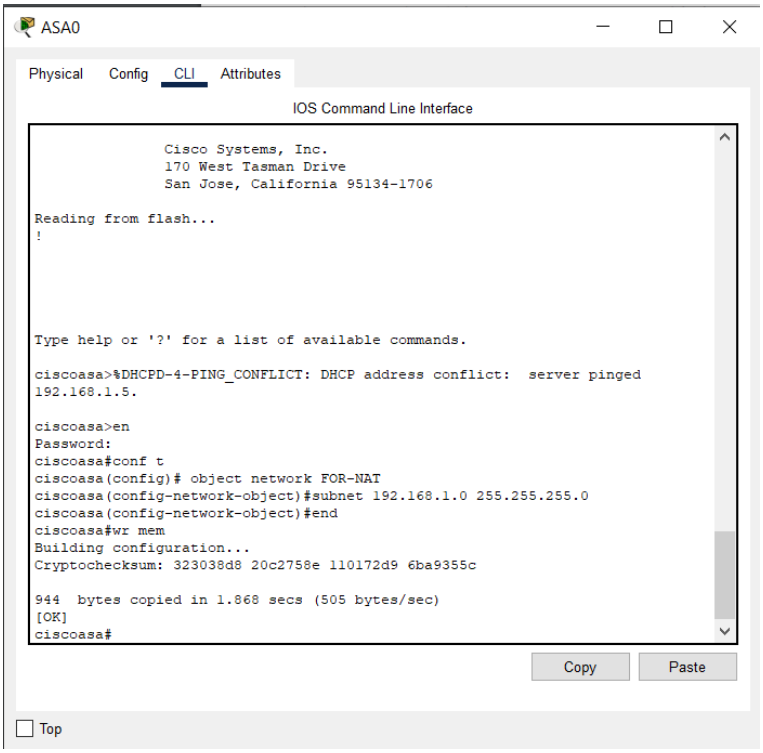


Рис.3.18 – Налаштування NAT на Cisco ASA.

Тепер перейдемо до налаштування самого DMZ опираючись на вище написане про security level. Для демілітаризованої зони потрібно виставити рівень захисту 50. Но перед цим потрібно додати новий сегмент до Cisco ASA. Адже у нього за замовчуванням стоять vlan на вихід та вхід у мережу. Це усе потрібно зробити як зображено на рис.3.19.

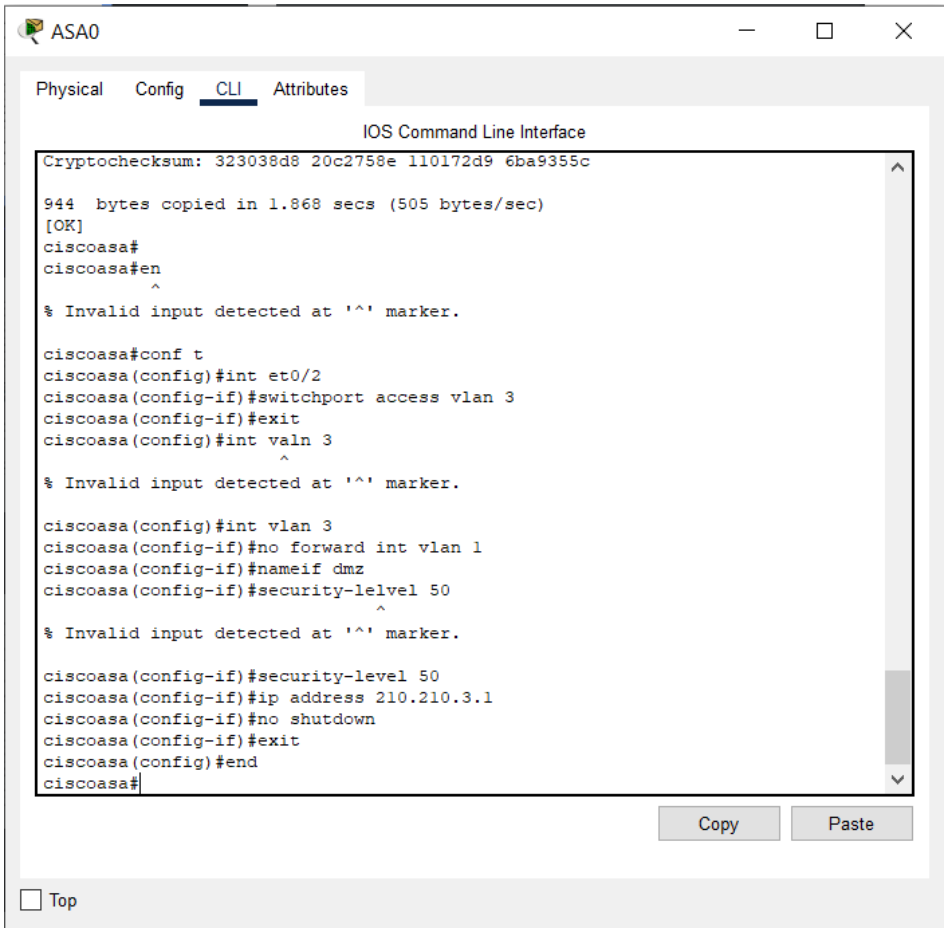


Рис.3.19 – Налаштування DMZ.

Так як ми формуємо загальнодоступний сервер, то спробуємо перевірити підключення до нього з маршрутизатора. І цей сервер буде не доступний, усе через правило рівня довіри між сегментами. Коли звертаємось до серверу , він входить в сегмент із рівнем довіри 50, але запит іде з сегменту із рівнем довіри 0. Тому ASA відкине такі запити. ASA за замовчуванням забороняє увесь трафік, і ми можемо використати правила доступу, щоб надати дозвіл саме до тих сервісів які потрібні. Для цього ми припишемо команду access–list FROM–OUTSIDE extended permit icmp any host address. Де address – це номер ip якому ми дозволяємо трафік. Прописати маємо як на рис.3.20.

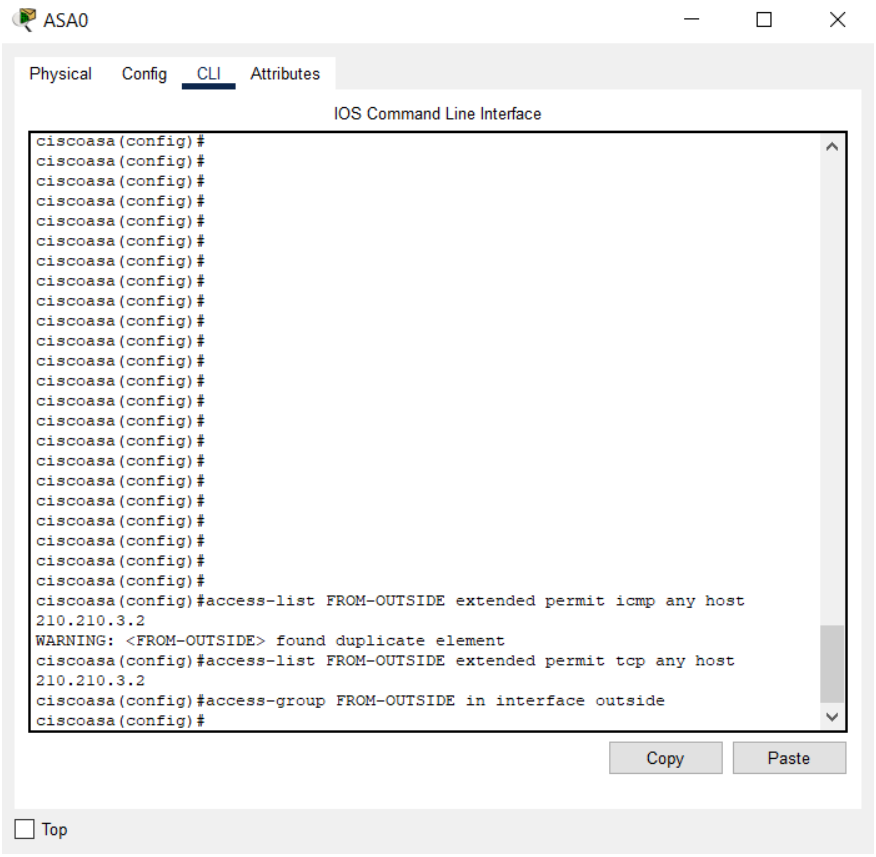


Рисунок 3.20 – Налаштування трафіку на Cisco ASA.

3.4 Налаштування відео спостереження.

На сам перед відео спостереження потрібне для моніторинга та фіксування усіх процесів у банку це можна віднести до фізичного захисту мережі. Це надасть можливість уникнути незручних ситуацій такі як крадіжка, мілке шахрайство, також є можливість спостерігання за процесом роботи працівників для подальшого їхнього мотивування. Камери можуть бути оснащені звуко записним пристроєм. Після перечислення переваг відео камер можна перейти до їх налаштування.

Спочатку потрібно їм призначити статичний ip адрес до якого буде звертатись мережа як зображено на рисунку 3.21.

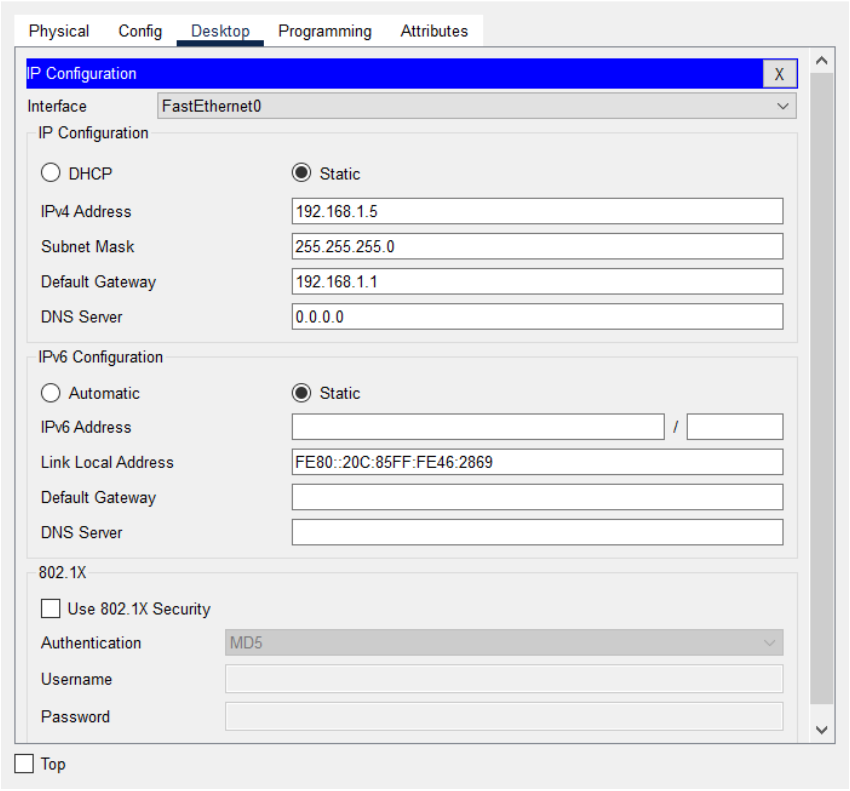


Рисунок 3.21 – Налаштування ip для камер.

Потім зайдемо до камери у меню нажмемо advanced і у меню виберемо I/O та Network Adapter обрати відповідне підключення як на рисунку 3.22.

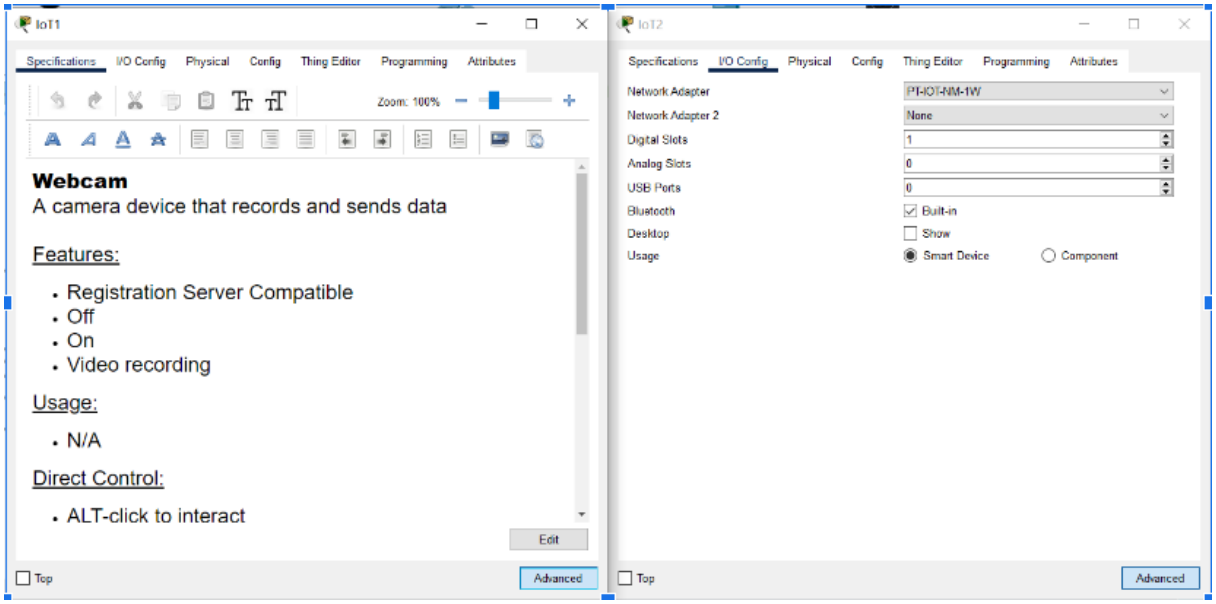


Рисунок 3.22 – Налаштуваня камери

Далі перевіримо чи все працює коректо. Для цього перейдемо до вкладки Desktop і там виберемо IoT Monitor. Далі нас зустріне вікно авторизації як на рисунку 3.23. Після того як авторизація виконана успішно, відкриється вікно на якому можна спостерігати роботу камер як на рисунку 3.24.

Рисунок 3.23 – Відображення входу на камери

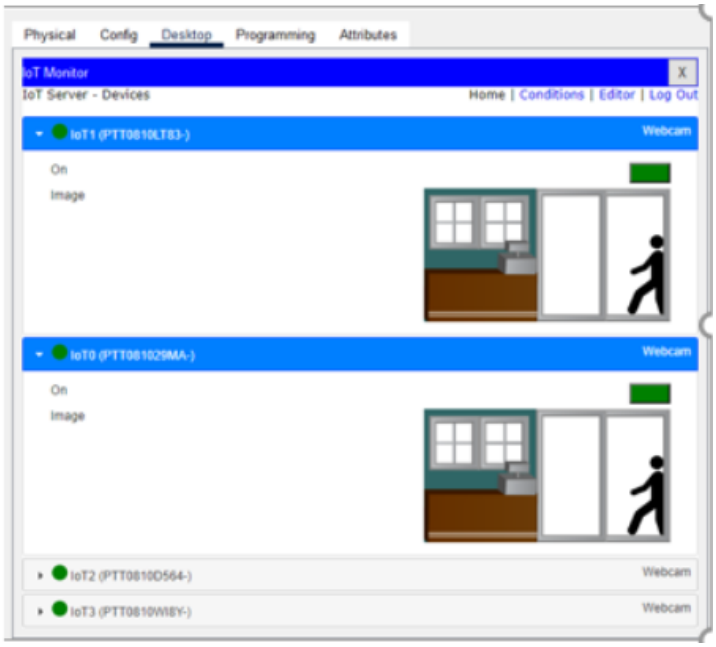


Рисунок 3.24 – Відображення роботи камери на пк

3.5 Висновки

Тож налаштування мережі починається з призначення ip–адресів усім пристроям мережі. Потім створюємо vlan для групування цих пристроїв. Далі маршрутизатор у якому налаштовуємо NAT. Він діє як бар'єр між зовнішньою мережею Інтернет і внутрішньою приватною мережею. Він приховує приватні IP–адреси комп'ютерів внутрішньої мережі, що забезпечує певний рівень безпеки, оскільки зовнішні мережі не можуть прямо звертатися до комп'ютерів з приватними IP–адресами.

Далі потрібно налаштувати захист мережі. Для цього встановлюється логін та пароль на комутатор і маршрутизатор, щоб ніхто хто має прямий доступ до мережі не зміг завдати їй шкоди. Також для захисту трафіку у мережі потрібно налаштувати CISCO ASA.Він аналізує інформацію про пакети даних, що переходять через нього, та застосовує правила безпеки для блокування небажаного трафіку та захисту від атак

Потім потрібно налаштувати сервер у якому будуть зберігатись дані мережі.Налаштування камер наддасть можливість запису та зберіганню відео.

ВИСНОВКИ

Згідно поставленого завдання мною була розроблена комп’ютерна мережа банку з рівнями захисту.

У першому розділі було розглянуто та проаналізовано основи комп’ютерних мереж, дослідження предметної області та огляд існуючих рішень щодо комп'ютерної мережі в банку. Це дало змогу зрозуміти потреби та вимоги банку, а також ознайомився з наявними технологічними рішеннями та методами, що застосовуються у банківській сферах для її захисту .

У другому розділі розглянув програмне та апаратне забезпечення комп’ютерної мереж. А саме для чого потрібна топологія, яку краще обрати. Також для чого використовується такі прилади як маршрутизатор, комутатор, сервер, відеокамера, комп’ютер, принтер і так далі у мережі банку і відповідно від тих потреб які були поставлені перед мережею, обрав відповідні апаратні характеристики

Після того як було розглянуто перший і другий розділ приступив до написання третього розділу. У якому провів налаштування апаратного забезпечення а саме налаштував сервер DHCP який створює та роздає ip на апаратне забезпечення комп’ютерної мережі банку. Також створив vlan на комутаторі для кожної зони банку. Налаштував маршрутизатор який веде контроль трафіку у мережі. Для безпеки було налаштовано мережевий екран Cisco ASA.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Larry L. Peterson.Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition. 2021. 848 с.
2. Quinn Kiser. Computer Networking: An All–in–One Beginner's Guide to Understanding Communications Systems, Network Security, Internet Connections, Cybersecurity and Hacking. 2020. 122 с.
3. Andrew Tanenbaum.Computer Networks, Global Edition 6th Edition. 2021. 230 с.
4. Doug Lowe. Networking All–in–One For Dummies (For Dummies (Computer/Tech)) 8th Edition. 2021. 1056 с.
5. Andrew S. Tanenbaum.Computer Networks 5th By Andrew S. Tanenbaum (International Economy Edition). 2020. 960 с.
6. ASA – Security Levels. URL: https://networkdirection.net/articles/firewalls/asa–securitylevels/ (дата звернення 08.05.2023).
7. William James Dally. Principles and Practices of Interconnection Networks (The Morgan Kaufmann Series in Computer Architecture and Design). 2021. 576 с.
8. Benjamin Walker. Computer Networking: The Complete Beginner’s Guide to Learning the Basics of Network Security, Computer Architecture, Wireless Technology and Communications Systems: Including CISCO, CCENT, and CCNA. 2019. 226 с.
9. Benjamin Walker. Computer Networking: The Complete Beginner’s Guide to Learning the Basics of Network Security, Computer Architecture, Wireless Technology and Communications Systems: Including CISCO, CCENT, and CCNA. 2019. 226 с.
10. GNS3 vs Packet Tracer – Know difference between GNS3 & Packet Tracer. URL: https://ipwithease.com/gns3–vs–packet–tracer/ (дата звернення 01.04.2023).
11. Mike Meyers. CompTIA Network+ Certification All–in–One Exam Guide, Seventh Edition (Exam N10–007). 2020. 960 с.
12. Ramon Nastase. Computer Networking: The Beginner’s guide for Mastering Computer Networking, the Internet and the OSI Model. 2022. 189 с.

13. Chwan–Hwa (John) Wu. Introduction to Computer Networks and Cybersecurity. 2023. 1336 с.

14. Jill West. Data Communication and Computer Networks: A Business User's Approach. 2022. 456 с.

15. Joseph Migga Kizza. Guide to Computer Network Security (Texts in Computer Science). 2020. 542 с.

16. Cisco ASA: Security Levels and Zones Explained. URL: https://www.iptrainer.net/cisco–asa–security–levels–and–nameif/ (дата звернення 06.05.2023).

17. Seth Enoka. Cybersecurity for Small Networks: A Guide for the Reasonably Paranoid. 2022. 224 с.

18. Magnus Ekman. Learning Deep Learning: Theory and Practice of Neural Networks, Computer Vision, Natural Language Processing, and Transformers Using TensorFlow. 2021. 752 с.

19. Jason Gooley. Cisco Software–Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD–WAN (Networking Technology). 2020. 608 с.

20. Cisco Networking Academy. Scaling Networks v6 Companion Guide. 2019. 672 с.

21. Andrew Mason. Cisco Secure Virtual Private Networks. 2021. 388 с.

22. Craig Berg. Cisco Networking Essentials: Complete Guide To Computer Networking For Beginners And Intermediates. 2020. 85 с.

23. James Boney. Cisco IOS in a Nutshell: A Desktop Quick Reference for IOS on IP Networks. 2019. 798 с.

24. Топологія комп'ютерних мереж. URL: https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh (дата звернення 21.04.2023).

25. Kevin Dooley and Ian Brown. Cisco IOS Cookbook: Field–Tested Solutions to Cisco Router Problems (Cookbooks (O'Reilly)). 2019. 1192 с.

26. Cisco. Cisco Networking Academy Program CCNA 1 And 2 Lab Companion. 2020. 428 с.

27. Omar Santos. Cisco CyberOps Associate CBROPS 200–201 Official Cert Guide. 2020. 688 с.

28. Hazim Dahir. Cisco Certified DevNet Professional DEVCOR 350–901 Official Cert Guide. 2022. 752 с.

29. Avinash Shukla. Cisco Cloud Infrastructure (Networking Technology). 2023. 448 с.

30. Srilatha Vemula. Software–Defined Access (Networking Technology).2020.352 с.

31. Ethernet Protocol : Architecture, Types, Working & Its Applications. URL: https://www.elprocus.com/ethernet–protocol/ (дата звернення 07.05.2023)

32. Wendell Odom. CCNA Routing and Switching Icnd2 200–105 Official Cert Guide. 2019. 992 с.

33. Jason C. Neumann.The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More. 2021. 274 с.

34. Daniel P. Newman.Penetration Testing and Network Defense. 2020. 626 с.

35. Data Communication and computer network question bank. URL: https://gfgc.kar.nic.in/raibag/FileHandler/270–bc3e95c5–12fe–4141–b848–0086967d1af4 (дата звертання 13.05.2023).

36. James Henry Carmouche. IPsec Virtual Private Network Fundamentals. 2021. 260 с.

37. Walter J. Goralski.Juniper and Cisco routing policy and protocols for multivendor IP networks. 2021. 689 с.

38. Jeff Doyle. Routing TCP/IP, Volume 1. 2019. 234 с.

39. Wendell Odom. CCNA Routing and Switching 200–125 Network Simulator. 2021. 192 с.

40. Cisco Networking Academy. Routing Protocols Companion Guide. 2022. 789 с.

41. Russ White. Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks. 2021. 832 с.

42. Mike Chapple. Access Control, Authentication, and Public Key Infrastructure: Print Bundle (Jones & Bartlett Learning Information Systems Security). 2019. 400 с.

43. Banking Computers Science Networking Computer Networks. URL: https://www.studyadda.com/notes/ssc/computers–science/network–ing/computer–networks/15471 (дата звереннння 28.04.2023).

44. Evan Gilman. Zero Trust Networks: Building Secure Systems in Untrusted Networks. 2021. 240 с.

45. Daniel Drescher. Blockchain Basics: A Non–Technical Introduction in 25 Steps. 2019. 270 с.

46. Marlon Buchanan. The Home Network Manual: The Complete Guide to Setting Up, Upgrading, and Securing Your Home Network (Home Technology Manuals). 2022. 185 с.

47. Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. 2019. 376 с.

48. Andreas Antonopoulos. Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. 2021. 464 с.

49. Three Different Approaches to Managing Your Bank's WAN. URL: https://www.safesystems.com/blog/2016/02/three–different–approaches–to–managing–your–banks–wan/ (дата звертання 13.05.2023).

50. Alan T. Norman. Computer Hacking Beginners Guide: How to Hack Wireless Network, Basic Security and Penetration Testing, Your First Hack. 2023. 167 с.

51. Quinn Kiser. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats Kindle Edition. 2020. 194 с.

52. J. Michael Stewart. Network Security, Firewalls, and VPNs (Issa). 2020. 481 с.

53. Adam Woodbeck. Network Programming with Go: Code Secure and Reliable Network Services from Scratch. 2021. 348 с.

54. Chris Sanders. Applied Network Security Monitoring: Collection, Detection, and Analysis. 2019. 496 с.

55. David Kim. Fundamentals of Information Systems Security. 2021. 550 с.

56. Computer Network – Types and Topologies – Bank PO Coaching. URL: https://po.hitbullseye.com/Hardware–and–Networking.php (дата звертання 09.05.2023).

57. COMPUTER NETWORK DESIGN FOR BUILDING OF THE BANK. URL: https://www.studocu.com/vn/document/dai–hoc–quoc–gia–thanh–pho–ho–chi–minh/network/computer–network–design–for–building–of–the–bank/19103834 (дата звертання 12.05.2023).

58. Douglas E. Comer.Computer Networks and Internets. 2021. 633 с.

59. Norman Fenton. Risk Assessment and Decision Analysis with Bayesian Networks. 2019.660 с.

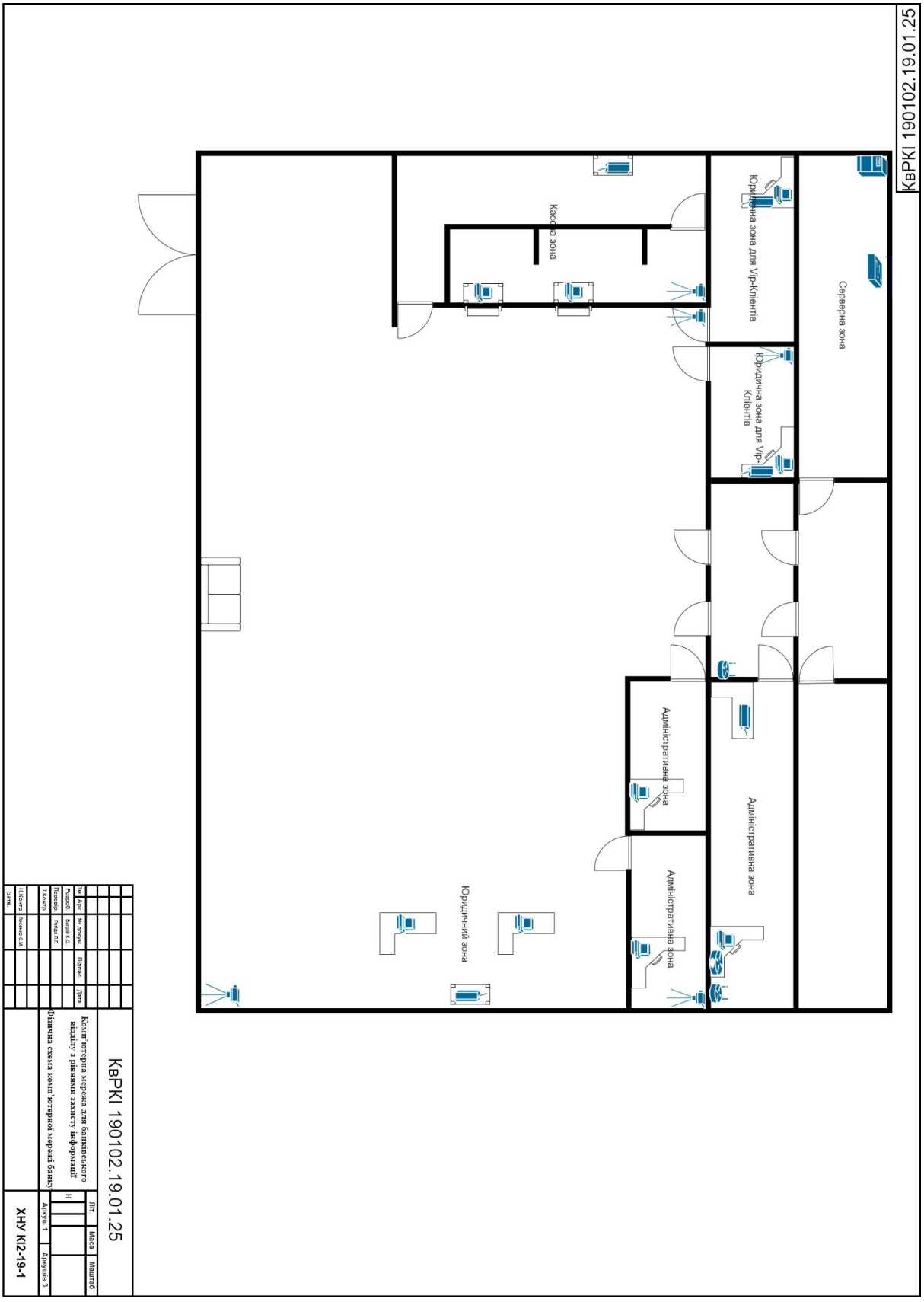
60. Design and Simulation of a Banking Network System. URL: https://www.ajer.org/papers/v4(11)/K0411079091.pdf (дата звертання 16.05.2023).

.

Додаток А

(обов’язковий)

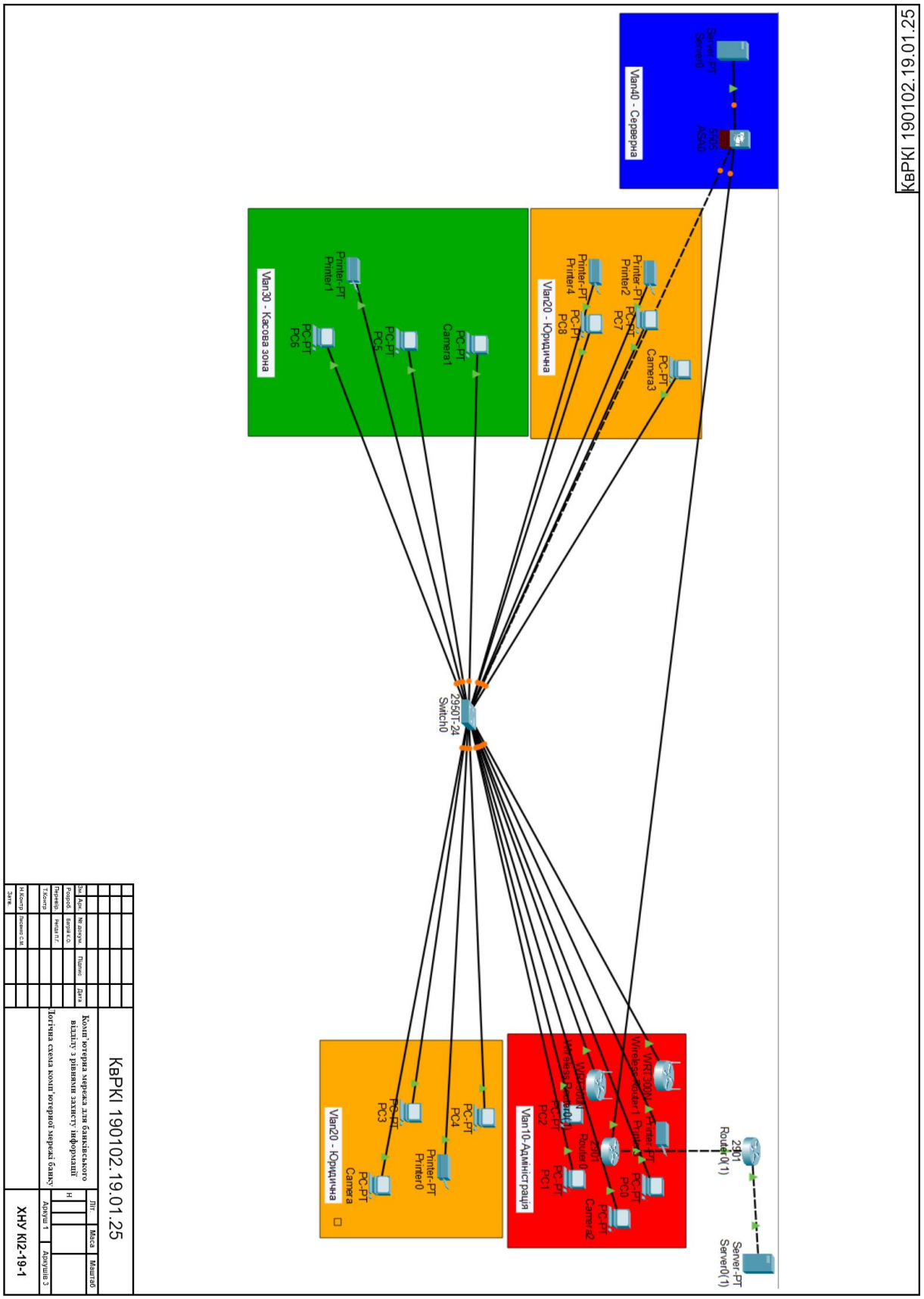
Копія креслення “Фізична схема комп’ютеної мережі банку”



Додаток Б

(обов’язковий)

Копія креслення “Логічна схема комп’ютеної мережі банку ”



Додаток В

(обов’язковий)

Копія креслення”Компоненти комп'ютерної мережі банку”

КвРКІ 190102.19.01.25

Маршрутизатор D-LINK DIR-820 AC1200

Кількість портів	24
Стандарт мережі	IEEE 802.3i 10 BASE-T, IEEE 802.3u 100 BASE-TX, IEEE 802.3x Управління потоком, IEEE 802.3af PoE
Максимальний струм навантаження	450Вт (48В, 9.3А)
Потужність на канал (Вт)	15.4
Напруга в зоні	48В
Розміри	440x290x44

Комутатор TP–Link TL–SF1024D

Швидкість Wi-Fi	До 1167 Мбіт/с
Частота роботи Wi-Fi	2,4 ГГц,5 ГГц
Інтерфейси	Rj45-LAN, WAN
Швидкість LAN-портів	100 Мбіт/с
Кількість LAN-портів	3
WAN-порт	Ethernet
USB-порт	Ні
Розміри	30 x 190 x 120 мм

Сервер RTLINE Business R35 v30

Тип процесора	Восьмиядерний Intel Xeon E-2388G (3.2–5.1 ГГц)
Оперативна пам’ять	8 GB DDR4 оперативной памяти
CD/DVD	Оптичний привід LG DVD±R/RW SATA Super Multi
HDD	SSD: 3 x 500 ГБ

Зм.	Кіл.	Арк.	№ докум.	Підпис	Дата	Комп’ютерна мережа для банківського відділу з рівнями захисту інформації		Літ	Маса	Масштаб
Розроб.							Н			
Перевір.						Компоненти комп’ютерної мережі банку		Аркуш 1	Аркушів 3	
Т.контр.										
Н.контр.				Затв.				ХНУ КІ2-19-1		

Fri Jun 02 14:31:42 EEST 2023, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 3.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 14%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114584 Назва: БКР Багатокомп'ютерна повнозв'язна топологія для паралельних систем Додано в БД: 2023-06-02 Автора: К. О. Багрій Керівники: П. Г. Регіда Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	59982	539	2891 (5%)	37 (7%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1015396116

Дата перевірки:
02.06.2023 15:30:31 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
02.06.2023 15:43:23 EEST

ID користувача:
100005591

Назва документа: **Багрій_Багатокомп'ютерна повнозв'язна топологія для паралельних систем**

Кількість сторінок: **65** Кількість слів: **9441** Кількість символів: **72076** Розмір файлу: **2.61 MB** ID файлу: **1015060362**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

8.08%
Схожість

Найбільша схожість: **1.71%** з Інтернет-джерелом (http://antibotan.com/file.html?work_id=485589)

7.41% Джерела з Інтернету	231	Сторінка 67
1.84% Джерела з Бібліотеки	84	Сторінка 68

0% Цитат

Цитати	11	Сторінка 69
Посилання	1	Сторінка 69

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	17
Підозріле форматування	10 сторінок

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Комп'ютерна мережа для банківського відділу з рівнями захисту інформації

Автор: Багрій Костянтин Олександрович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна «Комп'ютерна інженерія та програмування»

Науковий керівник: Регіда П.Г, ст. викладач

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформлені посилання;
3) найбільшу схожість встановлено з одним документом і становить вона 3% в частині загальноприйнятої термінології.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 8,08% і адресується до 231 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи П. Г. Регіда

Гарант ОПП С. М. Лисенко

Завідувач кафедри КІС Т. О. Говорущенко

Завідувачу кафедри КІС
д-р.техн.наук, проф. Говорущенко Т. О.

Багрій Костянтин Олександрович
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-19-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

05.06.2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Багрій Костянтин Олександрович

Тема: Комп'ютерна мережа для банку

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 55

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розробка мережевої топології для банку засобами Packet Tracer.

2. Висновок про відповідність роботи дипломному завданню: Дипломний проєкт відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі наведено засоби функціонування сучасних комп'ютерних мереж, та способи захищеної передачі даних в комп'ютерних мережах. Другий розділ присвячено аналізу предметної області та обґрунтованого вибору апаратних засобів для реалізації поставленої задачі, окремо розглянуто клас апаратних засобів для захисту комп'ютерних мереж. У третьому розділі представлено створення мережі в емуляторі, та її налаштування.

4. Позитивні сторони роботи: У роботі приділено увагу особливостям захисту комп'ютерних мереж за допомогою апаратних засобів.

5. Негативні сторони роботи: У роботі наявні певні недоліки із використанням усталеної термінології.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка та листи креслення оформлені коректно згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: ---

9. Оцінка дипломної роботи: Розглянувши роботу в повному обсязі, та зваживши позивні та негативні сторони, вважаю що робота заслуговує оцінки «добре» 3.75 (С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Сеник Микола Васильович доктор філософії, старший викладач, кафедра кібербезпеки.

"05" червня 2023 р. _____ (підпис)