

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комп'ютерна мережа організації з віддаленим доступом до ресурсів
Назва теми

КвРКІ. 180229.18.04. ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва


Освітня програма «Комп'ютерна інженерія»
Назва

Виконав: студент IV курсу, група КІ-18-2


Підпис


П.І.Дола
Ініціали, прізвище

Керівник

 14.06.22
Підпис, дата

С.В. Мостовий
Ініціали, прізвище

Нормоконтролер

 14.06.22
Підпис, дата

С.В. Мостовий
Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки


Підпис

Ю.П. Кльоц
Ініціали, прізвище

« 15 » червня 2022 р.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Кібербезпеки

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЯ ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри Ю. П. Кльоц

“ 01 ” 03 2022 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Долі Павлу Ігоровичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Комп'ютерна мережа організації з віддаленим доступом до ресурсів

Керівник проекту (роботи) Мостовий Сергій Володимирович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2022 № 18

2. Строк подання студентом проекту (роботи) на кафедру 30.05.2022

3. Вихідні дані до проекту (роботи) Розробити логічну та фізичну топології мережі. В логічній топології передбачити розподіл мережі на підмережі. Вибрати обладнання налаштувати обладнання (пристрої безпеки, комутатори, маршрутизатори, кінцеві пристрої) для забезпечення проходження дозволеного та блокування забороненого трафіку.

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

дослідити предметну область, проаналізувати отриману теоретичну інформацію, спроектувати та змоделювати комп'ютерну мережу згідно технічного завдання, розрахувати вартість та характеристики компонентів

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

Логічна топологія мережі (E8)

Фізична топологія мережі (E8)

Результати тестування трафіку в мережі (E8)

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	П р и м і т к а
			Текстові документи			
1		КВРКІ. 180229.18.02.04 ПЗ	Пояснювальна записка	76		
			Графічні матеріали			
2		КВРКІ. 180229.18.02.04 E8	Логічна топологія мережі	1		
3		КВРКІ. 180229.18.02.04 E8	Фізична топологія мережі	1		

КВРКІ. 180229.18.02.04 ВІІ

Зм	Арк	№ докум	Підпис	Дата	Відомість проекту	Літера	Аркуш	Аркушів
Розробив		Дола П.І.	<i>Doла</i>	14.06.22		У	1	1
Перевір.		Мостовий С.В.	<i>С.В. Мостовий</i>	14.06.22	ХНУ, КІ-18-2			
Н. контр.		Мостовий С.В.	<i>С.В. Мостовий</i>	14.06.22				
Затв.		Сльощ Ю.П.	<i>Ю.П. Сльощ</i>	15.08.22				

Дола
или, пр...
Мостовий
или, пр...

АНОТАЦІЯ

Тема кваліфікаційної роботи: *«Комп'ютерна мережа організації з віддаленим доступом до ресурсів».*

Автор роботи: *Дола Павло Ігорович*

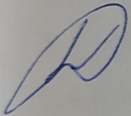
Керівник роботи: *Мостовий Сергій Володимирович.*

Пояснювальна записка: *76 с., 36 рис., 14 табл., 25 джерел.*

Графічна частина: *2 креслення.*

Метою даної роботи є розробка комп'ютерної мережі організації з віддаленим доступом до ресурсів.

Під час виконання кваліфікаційної роботи, було спроектовано комп'ютерну мережу для організації із можливістю доступу до ресурсів із зовнішніх мереж. Для реалізації мережі було обрано та налаштовано відповідне обладнання (реалізовані конфігураційні файли). Мережа була змодельована та протестована у програмному середовищі Packet Tracer.



14.06.2022

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ.....	3
ВСТУП.....	4
1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ.....	5
1.1 ХАРАКТЕРИСТИКА ТА АНАЛІЗ ФУНКЦІОНАЛЬНОЇ СТРУКТУРИ ПРЕДМЕТНОЇ ОБЛАСТІ	5
1.2 КЛАСИФІКАЦІЯ ТА ВИБІР ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	9
1.3 ОСНОВНІ ПОНЯТТЯ ПРО МЕРЕЖЕВІ ПРИСТРОЇ, АДРЕСАЦІЮ В МЕРЕЖІ ТА ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ	12
1.4 ПРОТОКОЛИ МАРШРУТИЗАЦІЇ ДЛЯ РЕАЛІЗАЦІЇ МЕРЕЖІ	21
1.5 ПОСТАНОВКА ЗАДАЧІ	22
2 ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ	23
2.1 ОЦІНКА ПЕРЕВАГ ТА ПІДХОДІВ ДО МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ	23
2.2 ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ І СИМУЛЯЦІЇ ПЕРЕДАЧІ МЕРЕЖЕВОГО ТРАФІКУ	25
2.3 ДЕТАЛЬНИЙ ОПИС СИМУЛЯТОРА CISCO PACKET TRACER.....	33
2.4 ВИСНОВКИ	40
3 МОДЕЛЮВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ	41
3.1 ПРОЕКТУВАННЯ ТА СЕГМЕНТАЦІЯ ЛОКАЛЬНИХ МЕРЕЖІ	41
3.2 РОЗРОБКА ФІЗИЧНОЇ ТОПОЛОГІЇ МЕРЕЖІ В PACKET TRACER	46
3.3 РОЗРОБКА ЛОГІЧНОЇ ТОПОЛОГІЇ МЕРЕЖІ В PACKET TRACER	49
3.4 РОЗРАХУНОК ВАРТОСТІ МЕРЕЖІ	60
3.5 ВИСНОВКИ	61
ВИСНОВКИ	62
ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ.....	63
ДОДАТОК А (ОБОВ'ЯЗКОВИЙ) КОПІЯ ГРАФІЧНОЇ ЧАСТИНИ.....	66
ДОДАТОК Б (ОБОВ'ЯЗКОВИЙ) НАЛАШТУВАННЯ МЕРЕЖНИХ ПРИСТРОЇВ	68

КВРКІ. 180229.18.02.04 ПЗ								
Зм.	Арк.	№докум.	Підпис	Дата	Комп'ютерна мережа організації з віддаленим доступом до ресурсів	Літера	Аркуш	Аркушів
Виконав		Дола П.І.		14.06.17				
Перевір.		Мостовий С.В.		14.06.17			2	76
Н.контр.		Мостовий С.В.		14.06.17	Пояснювальна записка	ХНУ, КІ-18-2		
Затвер.		Кльоц Ю.П.		15.06.17				

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

DMZ – демілітаризована зона

LAN – локальна мережа

NAT – перетворення мережевих адрес

SSH – мережевий протокол рівня застосунків

WAN – глобальна мережа

ОС - операційна система

ПЗ - програмне забезпечення

ПК – персональний комп'ютер

					КвРКІ. 180242.18.02.15 ПЗ	Арк.
						3
Зм.	Арк.	№докум.	Підпис	Дата		

ВСТУП

В наші дні виникає все більше і більше компаній, в яких постійно збільшується кількість працівників та пристроїв, якими вони користуються для виконання свої обов'язків. Ці пристрої утворюють собою мережу для передачі даних між іншими пристроями та доступу в Інтернет. Також для обмеження доступу працівників до певних ресурсів та забезпечення пристроїв від втрати даних і проникнень в систему з мережі Інтернет.

Інформаційні мережі надають можливість об'єднувати різні комп'ютери, сервери та IoT пристрої. Мережні пристрої ж дозволяють проводити комунікацію між ними, об'єднувати кінцеві пристрої в підмережі, віртуальні мережі та обмежувати трафік між ними і мережею Інтернет.

З ростом кількості техніки, зріс попит на послуги мережевих спеціалістів. Рівні складності мережевих систем збільшуються з неймовірною швидкістю. Корпоративні, приватні, публічні та державні мережі. Усі вони потребують налаштування та технічної підтримки для уникнення збоїв у роботі програмного забезпечення, покращення програмних та апаратних компонентів і забезпечення безпечного з'єднання.

Актуальність теми кваліфікаційної роботи полягає у аналізі та виборі прийнятних засобів для побудови мережі, що забезпечить її захищеність та інформаційну безпеку при віддаленій роботі підприємства.

Завданнями роботи є:

1. Провести аналіз предметної області
2. Навести приклади існуючих підходів до побудови захищених мереж, зробити аналіз і висновки щодо їх недоліків і переваг.
3. Визначити необхідний рівень захисту даних в мережі та запропонувати прийнятний підхід до вирішення задачі.

					КвРКІ. 180242.18.02.15 ПЗ	Арк. 4
Зм.	Арк.	№докум.	Підпис	Дата		

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Характеристика та аналіз функціональної структури предметної області

Комп'ютерна мережа — це система зв'язку між декількома комп'ютерами. Розглядаючи комп'ютерну мережу більше детально можна виявити, що це система різних пристроїв, які з'єднанні між собою кабельним чи бездротовим способом, призначені для різноманітних потреб. Також до цього поняття входить мережеве обладнання, яке забезпечує з'єднання та комунікацію між одиницями мережі. Для передачі інформації використовують різні способи, як правило — різноманітні електричні сигнали чи електромагнітне випромінювання. Для поширення трафіку у комп'ютерних мережах можуть використовуватися телефонні кабелі, та спеціальні мережеві кабелі: виті пари, коаксіальні кабелі, радіохвилі, світлові сигнали, волоконно-оптичні кабелі[1].

Мережева модель OSI — це абстрактна модель, яка використовується для визначення різних рівнів взаємодії систем. Кожен рівень відповідальний за свою частину роботи у ланцюзі взаємодії всіх шарів моделі. Така структура спільної роботи апаратного й програмного забезпечення є набагато простішою, зручнішою й зрозумілішою.

Усі протоколи моделі OSI повинні використовувати або протоколи свого рівня, або протоколи на одиницю вище або нижче за свій рівень. Усі протоколи моделі OSI мають права на виконання лише функцій свого рівня і їм не дозволено виконувати функцій іншого рівня. Модель складається з 7-ми рівнів, які розташовані вертикально один над одним.

Призначення комунікаційних мереж:

1. Можливість передачі інформації (електронна пошта, месенджери);
2. Використання спільної техніки та послуг (мережні принтери, сховища даних, сервери);

					КвРКІ. 180242.18.02.15 ПЗ	Арк. 5
Зм.	Арк.	№докум.	Підпис	Дата		

3. Розподілення навантаження;
4. Можливість віддаленого керування;
5. Забезпечення надійності, безпеки та відмовостійкості.

Основні можливості комп'ютерних мереж:

- Швидка передача інформації на великих відстанях;
- Пошук інформації;
- Обмін даними в режимі offline;
- Збереження інформації на серверах Internet та на локальному

комп'ютері з можливістю її подальшої обробки.

Виділяються такі типи мереж:

- персональна мережа (PAN);
- локальна мережа (LAN);
- кампусна мережа (CAN);
- міська мережа (MAN);
- глобальна мережа (WAN).

На сьогоднішній день основним використовуваним стеком протоколів є TCP/IP. На протязі існування моделі OSI вона не була реалізована в повному обсязі, і, очевидно, не буде реалізована ніколи. Сьогодні використовується тільки декілька різновидів моделі OSI (рис.1.1). Модель занадто складна, а її реалізація займе занадто багато часу та ресурсів.

TCP/IP-модель — це набір протоколів мережі Інтернет. Фактично це систематизований стек протоколів, який розділений на чотири рівні: прикладний, транспортний, міжмережевий та каналний (мережний інтерфейс) (рис.1.2).

					КвРКІ. 180242.18.02.15 ПЗ	Арк.
						6
Зм.	Арк.	№докум.	Підпис	Дата		



Рисунок 1.1 – Рівні моделі OSI[2]

Концептуальні рівні
стека TCP/IP

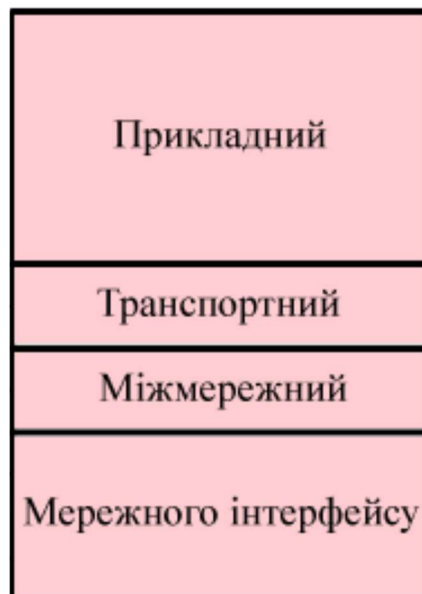


Рисунок 1.2 – Рівні моделі TCP/IP

Прикладний рівень. Протоколи прикладного рівня TCP/IP організують взаємодію програм різних мережевих комп'ютерів і форми даних, які використовуються за такої взаємодії. Програма-клієнт - це застосунок, який встановлюється безпосередньо на комп'ютер користувача, а програма-сервер - комплекс утиліт для задоволення потреб (запросів) програми-клієнта, яка звертається до першого за деякою інформацією, це основні види прикладного програмного забезпечення. Протоколи прикладного рівня зорієнтовано на конкретні прикладні завдання. Найпопулярнішими протоколами цього рівня є: SMTP та POP3, FTP та TFTP, TELNET, HTTP.

Транспортний рівень. Основними протоколами транспортного рівня є протокол керування передачею TCP і протокол користувальницьких дейтаграм UDP. Ці протоколи використовуються для передачі інформації, але їхня реалізація відрізняється. При доставці дейтаграм, протокол UDP не встановлює з'єднання, тому він не гарантує їхнього повного доставлення. В свою чергу, протокол TCP встановлює транспортне дуплексне з'єднання і гарантує доставлення сегментів.

Міжмережевий рівень. Протоколи мережевого рівня TCP/IP забезпечують взаємодію мереж різної архітектури. Основним протоколом мережного рівня є міжмережевий протокол IP та його допоміжні протоколи: ARP, RARP, ICMP тощо.

Канальний рівень. Функціями цього рівня є: відображення IP-адреси в MAC-адреси, інкапсуляція IP-дейтаграм в кадри для передачі по фізичному каналу і передачі кадрів.

Головним завданням протоколу IP є — маршрутизація пакетів даних між різними комп'ютерними мережами. Для цього протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації пакетів, виконує фрагментацію та дефрагментацію цих пакетів, якщо потрібно.

MAC-адреса — це унікальний фізичний ідентифікатор, який присвоюється кожному фізичному пристрою в мережі. Майже всі мережеві протоколи каналного рівня використовують один з трьох просторів MAC-адрес,

стандартизованих IEEE: MAC-48, EUI-48 і EUI-64. Адреси, в кожному з просторів, мають бути унікальними.

1.2 Класифікація та вибір топології комп'ютерної мережі

Комунікаційні мережі також можуть класифікуватися за топологією з'єднання пристроїв. Базовими є такі топології:

– шина (bus), при якій всі комп'ютери паралельно підключаються до однієї лінії зв'язку, а інформація від кожного комп'ютера одночасно передається усім іншим комп'ютерам;

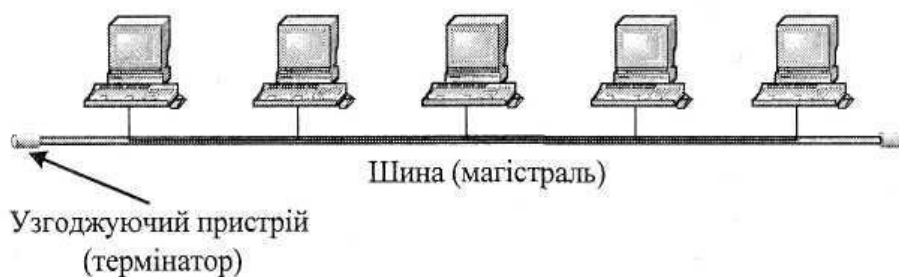


Рисунок 1.3 – Топологія мережі «шина»

– зірка (star), при якій до якогось одного центрального комп'ютера приєднуються усі інші периферійні комп'ютери, використовуючи при цьому для підключення свою окрему лінію зв'язку. На мережевий сервер, окрім основних функцій, також без проблем можуть бути приєднані додаткові функції, які допоможуть з узгодженням швидкостей роботи станцій і перетворенням протоколів обміну. Завдяки цьому, в рамках однієї робочої мережі можна об'єднувати різнотипні робочі станції.

Разом з певними перевагами, подібні локальні мережі мають низку недоліків. Зокрема, при підключенні великої кількості робочих станцій підтримання високої швидкості комутації вимагає досить великих апаратних витрат. Окрім того, більша частина функціонального навантаження центрального вузла зумовлюється його складністю, що не може залишити свої

наслідки на його надійності. У зв'язку з цим недоліком у більшій частині сучасних зіркоподібних мереж функції комутації робочих станцій та керування мережею розподілені між мережевим сервером і комутатором.

Мережевий сервер підключається до комутатора, як сама робоча станція, проте з максимальним пріоритетом. В такому випадку структура центрального вузла значно спрощується, що разом із високошвидкісними каналами дозволяє розвинути досить високу швидкість передачі даних. Так, наприклад, у зірчастій мережі ІЛіга №1 швидкість передачі даних становить 1,4 Гбіт/с.



Рисунок 1.4 – Топологія мережі «зірка»



Рисунок 1.5 – Топологія мережі «зірка» з розподіленим керуванням

Зм.	Арк.	№докум.	Підпис	Дата

– кільце (ring), при якій кожний комп'ютер передає інформацію завжди тільки одному комп'ютеру, наступному в ланцюжку, а одержує інформацію тільки від попереднього комп'ютера в ланцюжку, і цей ланцюжок замкнутий в «кільце».

Одним із значних мінусів кільцевих мереж є вихід її з ладу при розірванні кільця, який звичайно, можливо усунути за допомогою використання так званого "подвійного" кільця. Для цього до складу локальної мережі підключають додаткові лінії зв'язку і пристрої реконфігурації — спеціальні пристрої для перемикавання, надійні та прості. На рис. 1.7 показано схему переключення з одного кільця на інше у випадку його виходу з ладу на одному із сегментів кільця.



Рисунок 1.6 – Топологія мережі «кільце»

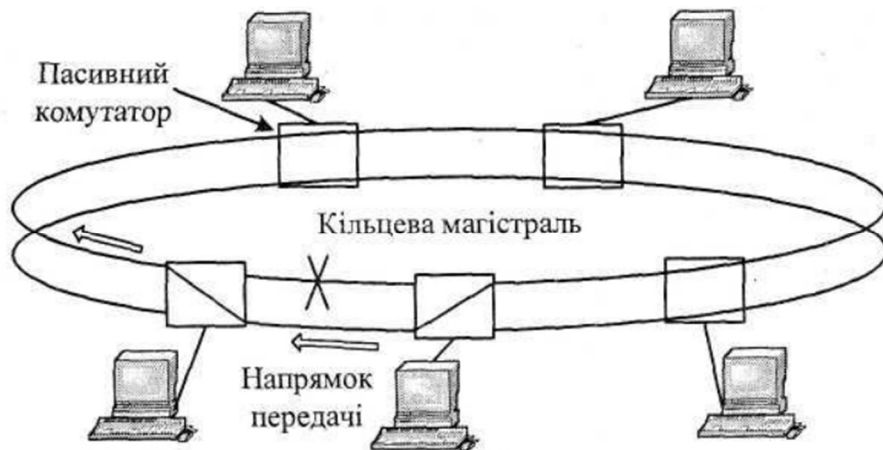


Рисунок 1.7 – Перемикавання кільце у топології «подвійного кільця»

Зм.	Арк.	№докум.	Підпис	Дата

Розглянуті вище мережеві топології є базисом. Саме на їх основі і формується конкретна структура реальних мереж, яка частіше всього, не є сильно вираженою топологією, які були представлені та описані вище, а являють собою об'єднання різноманітних базових топологій. Досить звично, що оптимальною буде та структура мережі, яка відображає більш чітко внутрішню структуру самої організації або підприємства, які обслуговуються цією мережею. Опираючись на це, фірми-виробники мережевого обладнання розробляють і постачають на ринок доволі широкий набір пристроїв, які дозволяють без проблем об'єднувати між собою мережі різноманітних топологій.[3, 4]

1.3 Основні поняття про мережеві пристрої, адресацію в мережі та протоколи передачі даних

Мережеве обладнання, їх ще називають мережевими пристроями — це пристрої, які необхідні для роботи комп'ютерної мережі. До них можна віднести: маршрутизатор, комутатор, концентратор, патч-панель та ін. Зазвичай мережеве обладнання розділяють на дві категорії: активне мережеве обладнання і пасивне.

Активне мережеве обладнання має певні «інтелектуальні» можливості, тобто те, яке можна налаштувати згідно потрібних вимог, задати певні правила та прописати певні маршрути для пакетів інформації. До цього типу належать маршрутизатор, комутатор (світч).

Під пасивним мережним устаткуванням розуміють те обладнання, яке не наділене «інтелектуальними» особливостями. Таким обладнанням вважається кабельна система, вилка, розетка, повторювач, патч-панель, концентратор (хаб), монтажні шафи, стійки, тощо.

Мережеві пристрої забезпечують транспортування пакетів з інформацією між пристроями користувача. Вони подовжують та об'єднують кабельні з'єднання, перетворюють дані із одного формату у інший та керують передачею даних.

					КвРКІ. 180242.18.02.15 ПЗ	Арк. 12
Зм.	Арк.	№докум.	Підпис	Дата		

Декілька слів про основне мереже обладнання, без котрих тяжко уявити собі навіть найпростішу комп'ютерну мережу.

Повторювач (англ. repeater) — це пристрій, призначений для того, щоб підсилити мережевих сигналів, що дозволяє переправляти їх середовищем на більшу відстань, аніж було можливо. Причому повторювач не має прав доступу на читання інформації, яка міститься в пакеті, що робить неможливим крадіжку важливих пакетів даних.



Рисунок 1.8 - Cisco Repeater для бізнесу

Концентратор (англ. hub) — це один із видів мережевого обладнання, яке можна встановлювати на рівні доступу до мережі Ethernet. Він має декілька портів для під'єднання вузлів до мережі. Концентратор не визначає, якому вузлу призначено те чи інше повідомлення. Він приймає електронні сигнали одного порту та відтворює їх для всіх інших портів. Для передачі та отримання повідомлень усі порти концентратора Ethernet під'єднують до одного і того ж самого каналу.



Рисунок 1.9 - Концентратор Cisco SRW2008-K9-G5

Міст (англ. bridge) — це пристрій, задачею якого є фільтрування потоків даних у локальній мережі, щоб локалізувати передачу даних і, у той же час, зберегти можливість зв'язку з іншими частинами мережі для перенаправлення туди потоків даних. Міст збирає інформацію, у вигляді таблиці, про те, на якому конкретно порті знаходиться конкретна MAC-адреса, після чого приймає рішення про передачу даних на підставі відповідного списку MAC-адрес. Мости виконують фільтрацію потоків даних, маючи в собі лише список MAC-адресів і відповідних їм вузлів, тому можуть досить швидко пересилати дані в вузькій мережі.



Рисунок 1.10 – Міст для камер Cisco, Vaddio 999-9660-000

Зм.	Арк.	№докум.	Підпис	Дата

Комутатор (англ. switch) — це пристрій, по своїй суті, є більш «розумним» концентратором, так як він передає дані лише тому, кому вони були безпосередньо відправлені.



Рисунок 1.11 - Комутатор Cisco 2960

Маршрутизатори (англ. router) — це пристрої об'єднаних мереж, які займаються пересилкою пакетів між мережами на основі конкретних адрес. Маршрутизатор здатний вибрати найкращий, тобто найкоротший, шлях у мережі для передання даних, тим самим збільшуючи швидкість обміну інформацією. Маршрутизатор може приймати рішення на основі мережевих адрес замість використання індивідуальних MAC-адрес другого рівня. Завдяки цій здатності маршрутизатори стали основною магістраллю глобальної мережі Internet. [5].



Рисунок 1.12 – Маршрутизатор Cisco 2901

Тепер потрібно зрозуміти, що таке адресація в мережі і як вона відбувається.

Адресація в мережі це один із найбільших обов'язків мережевого рівня.

Мережеві адреси завжди логічні, іншими словами, базуються на програмному забезпеченні. Хост, також відомий як кінцевий користувач, який має одне посилання на мережу. Зв'язок між хостом та посиланням називається інтерфейсом, а звідси можна зробити висновок, що хост може мати лише один інтерфейс.

Роутер відрізняється від хоста тим, що може містити в собі два, або більше, послань Коли маршрутизатор пересилає датаграму, він пересилає пакети з інформацією на одне із цих послань. Зв'язок між маршрутизатором і посиланням, його ще називають каналом, відома як інтерфейс, і маршрутизатор може мати декілька інтерфейсів. Кожен інтерфейс має змогу надсилати і отримувати IP-пакети, тому IP вимагає, щоб кожному інтерфейсу відповідала певна адреса.

Кожна IP-адреса має довжину в 32 біти, і вони представлені у вигляді «десяткової системи індексу», де кожен байт записується в десятковій формі, і вони розділені між собою крапкою. IP-адреса буде виглядати як 193.32.216.9, де 193 являє собою десятковий запис перших 8 біт адреси, 32 являє собою десятковий запис других 8 біт адреси.

					КвРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		16

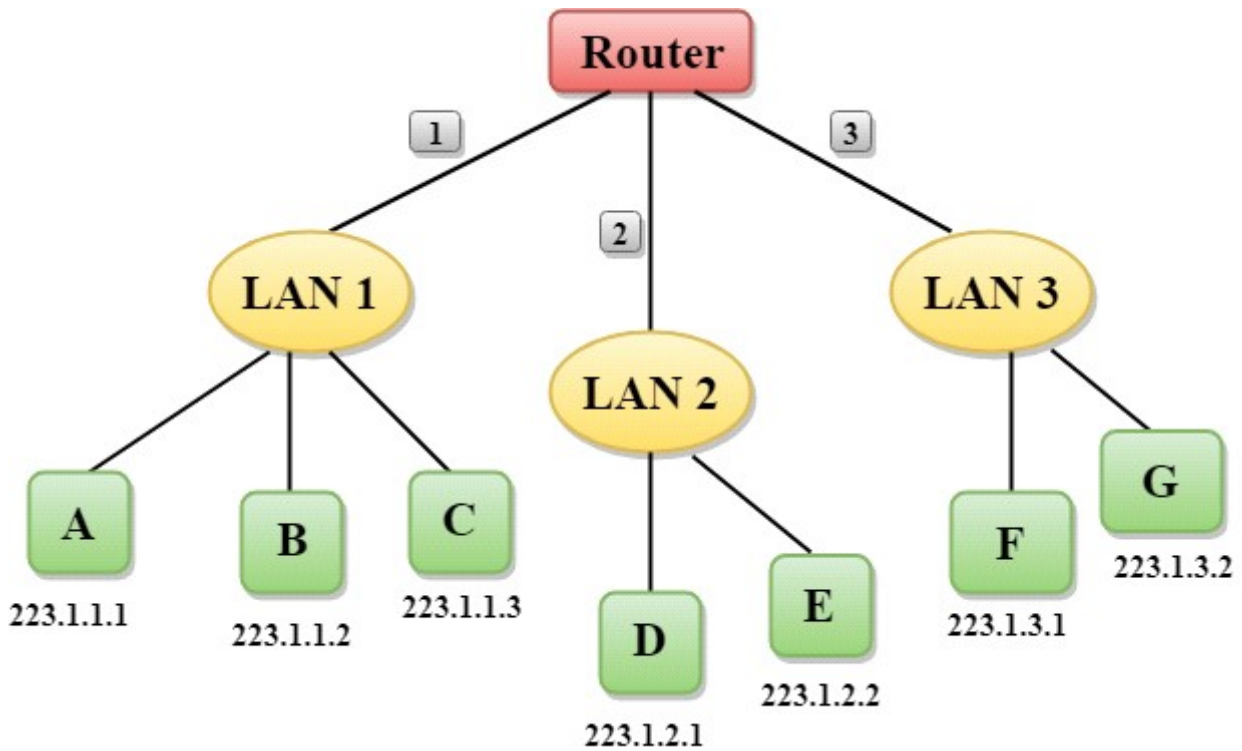


Рисунок 1.13 – Приклад адресації в мережі

На рисунку 1.13 ми бачимо маршрутизатор, який в свою чергу має три інтерфейси (LAN1, LAN2, LAN3), і кожен з цих інтерфейсів має свою ір-адресу, так само як і кожен хост має свій інтерфейс і адресу. Усі інтерфейси, які прив'язані до LAN1 має адресу 223.1.1.xxx, інтерфейси LAN2 мають адресу 223.1.2.xxx, а LAN3 - 223.1.3.xxx. Кожна адреса складається з двох частин: перша частина, тобто перших три байти, вказує мережу, а друга частина, яка являє собою останні байти адреси, визначає адресу кінцевого пристрою в даній мережі.

ІР-адреси довжиною в 32 біти розділяють на класи:

- Class A
- Class B
- Class C
- Class D
- Class E

Адресу також можна розділити на дві частини:

- Ідентифікатор мережі – яка вказує на кількість мереж
- Ідентифікатор хоста – який вказує на кількість кінцевих пристроїв

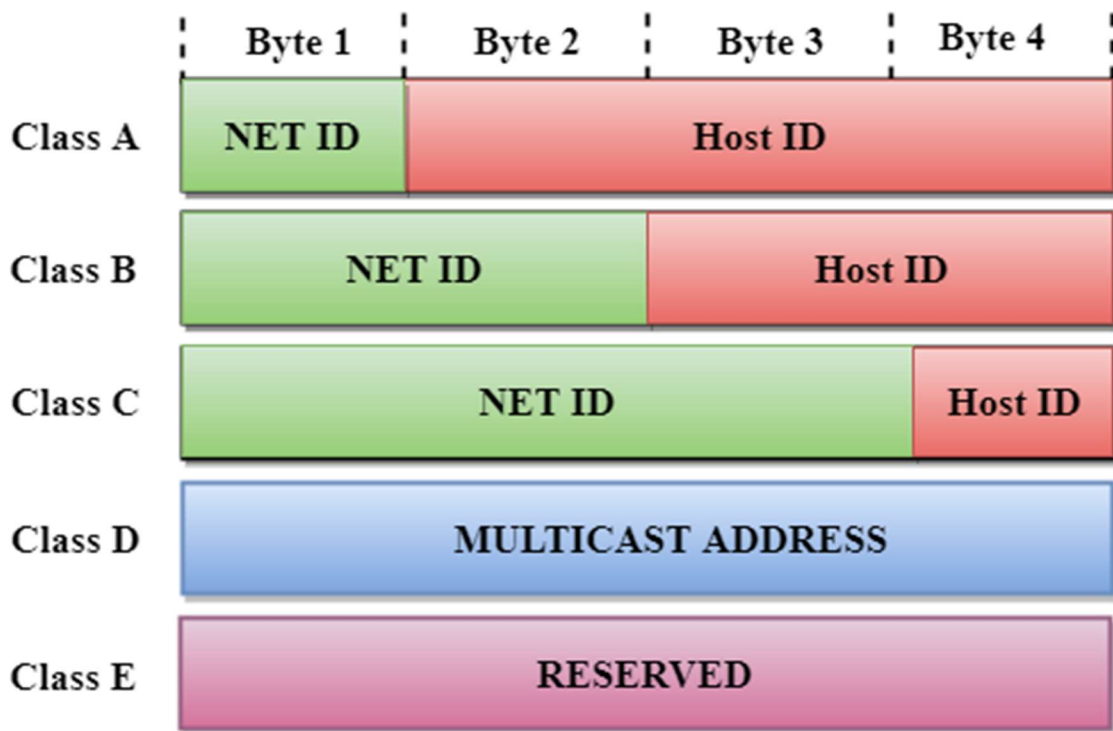


Рисунок 1.14 – Розподіл адреси по класам

IP-адреси, які належать до класу А, призначаються мережам, котрі містять в собі велику кількість хостів.

IP-адреси, котрі належать до класу В, призначаються мережам, які розмір яких варіюється від середніх до великих мереж.

IP-адреси, що належать до класу С, призначаються невеликим мережам.

IP-адреси, що належать до класу D, зарезервовані для багаторазової передачі.

IP-адреси, що належать до класу Е, зарезервовані для експериментальних та дослідницьких цілей.

Також є діапазон спеціальних IP-адрес, котрі не можна присвоювати кінцевим пристроям:

- 169.254.0.0 – 169.254.0.16 : посилання на локальні адреси
- 127.0.0.0 – 127.0.0.8 : loop-back адреси
- 0.0.0.0. – 0.0.0.8 : використовується для зв'язку в межах поточної мережі.

Існують правила призначення ідентифікатора хостам. ID хостів використовуються для того, щоб ідентифікувати кінцевого користувача в мережі. Ідентифікатор хоста призначається на основі того, що у будь-якій мережі, незалежно від її розмірів чи кількості пристроїв, ID хоста має бути унікальним і неповторним для цієї мережі. Не можна вказати таку адресу, в якій всі біти встановлені на 0, не може бути призначений, оскільки цей ідентифікатор хоста використовується для представлення ідентифікатора мережі IP-адреси. Адресу хоста, у якій всі біти встановлені на 1, не може бути призначена, оскільки ця адреса зарезервована як широкомовна, яка в свою чергу використовується для надсилання пакетів усім хостам, присутнім у цій конкретній мережі.

Правила призначення ідентифікатора мережі також є і їх варто пам'ятати. Усім кінцевим пристроям, які знаходяться, фізично, у одній і ті ж самій мережі присвоюється один і той самий ідентифікатор. Ідентифікатор мережі не може починатися з числа 127, оскільки 127 належить до адреси класу А і зарезервованій для внутрішніх функцій loop-back зв'язку. Усі біти адреси мережі, встановлені на 1, зарезервовані для використання як адреса широкомовної IP-адреси, і тому не можуть бути використані. Усі біти мережі, встановлені на 0, використовуються для позначення конкретного хоста в локальній мережі і не маршрутизуються, а отже, їх неможливо використовувати.

Мережеві протоколи — це визначений набір певних правил, які визначають як саме інформація і дані пересилаються між різними пристроями в мережі.

Процес передачі даних від одного комп'ютера на інший складається з декількох рівнів. Цей процес передбачає виконання таких операцій: отримання даних від користувача, їх стиснення, шифровку, формування пакетів із розбитих бітів повідомлення, встановлення зв'язку між тим комп'ютером, котрий відправляє дані, і тим, що приймає, транспортування цих шифрованих пакетів по каналам зв'язку, вибір найбільш ефективного, тобто найбільш короткого, маршруту передачі, та формування вихідного повідомлення з пакетів даних.

					КвРКІ. 180242.18.02.15 ПЗ	Арк. 19
Зм.	Арк.	№докум.	Підпис	Дата		

На кожному з цих етапів використовуються окремі протоколи, котрі в сукупності мають таку назву TCP/IP, і розшифровуються як:

– TCP (англійською Transmission Control Protocol — протокол керування передачею даних, відповідає за організацію сеансу зв'язку між двома комп'ютерами у мережі.

– IP (англійською Internet Protocol — відповідає за маршрутизацію, тобто за те, щоб пакет був доставлений на попередньо задану адресу. За допомогою цього протоколу комп'ютер перевіряє, чи було отримано всі частини повідомлення. При отриманні всіх порцій TCP розміщує їх в потрібному порядку і збирає в одне ціле і розшифровує.

Найвідоміші протоколи, які використовують у мережі Інтернет:

– HTTP (Hyper Text Transfer Protocol) — протокол передачі гіпертексту. Його використовують для пересилання Web-сторінок з одного персонального комп'ютера на інший.

– FTP (File Transfer Protocol) — протокол передачі файлів зі спеціального файлового сервера на комп'ютер користувача. Дає змогу користувачу обмінюватися двійковими або текстовими файлами з будь-яким комп'ютером мережі.

– SMTP (Simple Mail Transfer Protocol) — протокол, який задає певний набір правил для передавання пошти. Сервер SMTP повертає або підтвердження про прийом даних, або повідомлення про помилку передачі даних, або запитує додаткову інформацію у користувача.

– IRC (Unix to Unix Copy Protocol) — протокол, який відповідає за забезпечення інтерактивного спілкування.

– Telnet — протокол віддаленого доступу, котрий дає можливість без перешкод працювати на будь-якому пристрої, котрий має підключення до мережі Інтернет, дистанційно, як на своєму власному, тобто запускати там програми, змінювати режим роботи, редагувати, записувати і читати файли, тощо. На практиці така можливість обмежена тим рівнем доступу, який присвоїв адміністратор віддаленої машини.

					КвРКІ. 180242.18.02.15 ПЗ	Арк. 20
Зм.	Арк.	№докум.	Підпис	Дата		

– DTN — протокол, який забезпечує стабільний зв'язок із наддалекого космічного простору. Розповсюджений це протокол, зазвичай, на різноманітних космічних станціях і в приватних компаніях, котрі займаються запусками ракет, або інших машин, у космос. [6, 7].

1.4 Протоколи маршрутизації для реалізації мережі

Для реалізації безпечної і правильно структурованої мережі слід використовувати мережеві протоколи. Це набір правил, які використовуються для визначення пристроїв у мережі, також визначається принцип керування різноманітних програм, мережевих вузлів та систем, для створення єдиного цілісного простору передачі.

Було досліджено безліч мережевих протоколів та обрано, які найбільш підходять для реалізації заданої комп'ютерної мережі підприємства:

- DHCP;
- RIP;
- OSPF;
- SSH.

DHCP (Dynamic Host Configuration Protocol) – це протокол динамічної конфігурації вузла, забезпечує призначення та керування IP-адресами із визначених пулів адрес у маршрутизаторі для клієнтів DHCP [1].

RIP (Routing Information Protocol) – це протокол маршрутизації, досить розповсюджений завдяки своїй стабільності, який використовує алгоритм відстань-вектор для обчислення маршрутів [2-4].

OSPF (Open Shortest Path First) – це протокол динамічної маршрутизації, був розроблений з метою використання спеціально для IP-мереж, для підтримання IP-підмережі та тегування інформації про маршрутизацію, яку було отриману ззовні [5-6].

SSH (Secure Shell) – мережевий протокол прикладного рівня, який забезпечує безпечне підключення віддаленого доступу до мережевих пристроїв [7].

1.5 Постановка задачі

Щоб створити захищену мережу офісу, потрібно визначити структуру та розташування робочих місць, потоки даних, що будуть передаватись мережею, рівень та права доступу користувачів. Далі необхідно визначити мінімальний перелік мережного обладнання для реалізації функціоналу мережі та відповідно налаштувати всі пристрої. Після чого необхідно протестувати мережу.

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
						22
Зм.	Арк.	№докум.	Підпис	Дата		

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Оцінка переваг та підходів до моделювання комп'ютерних мереж

Використання моделювання комп'ютерних систем має деякі переваги та недоліки порівняно з емпіричним чи реальним тестуванням. Однією з переваг моделювання є гнучкість, оскільки час і темп моделювання можна адаптувати, щоб користувач міг прискорити або уповільнити переходи чи події, що сприяє точному аналізу.

Моделювання передачі трафіку дає можливість приймати більш надійні рішення, засновані на імітації широкого спектра операційних сценаріїв, що дозволяє тестувати кожен аспект комп'ютерної системи, передбачувани зміни в мережі або конкретні обставини. Користувачі можуть оцінити виникнення або поведінку конкретного сценарію, реконструюючи та уважно вивчаючи його, таким чином вони розвивають розуміння процесів, що проходять у мережі, спостерігаючи за роботою системи.

Моделювання сьогодні є обов'язковим під час проектування мережі, воно дозволяє визначити вимоги до мережі в деталях; діагностувати проблеми, що виникають у результаті взаємодії між компонентами системи.

Також незамінною перевагою моделювання перед емпіричним експериментом є дешевизна першого. Моделювання мережі допомагає уникнути збоїв у роботі реальної комп'ютерної системи. Існує тенденція до моделювання комп'ютерних мереж за допомогою дискретно-подійного моделювання [22].

Причини за якими мережі моделюються таким чином у тому, що дискретно-подійне моделювання краще адаптується для презентації поведінки комп'ютерних мереж, оскільки протоколи передачі комп'ютерних мереж можуть бути змодельовані як кінцеві стани.

Моделювання продуктивності мережі дозволяє оцінити її працездатність. За такого типу моделювання система абстрагується через правильно деталізовану модель, яка відтворює поведінку системи під впливом робочих навантажень. Основною метою моделювання продуктивності мережі є отримання набору показників продуктивності, таких як пропускна здатність досліджуваних ділянок мережі та її час відгуку у стійкому стані системи.

Моделювання мережевих протоколів відображає важливими аспектами роботи стека мережевих протоколів. При такому моделюванні основна увага звернена на мережевому, каналному та фізичному рівнях передачі даних.

Моделювання робочого навантаження на мережу дозволяє дати оцінку на поведінку навантаженої трафіком мережі та отримати точні та достовірні результати перебуваючи у програмі-симуляторі. Модель трафіку розглядає останній рівень деталізації, рівень пакетів з такими параметрами, як розподіл розмірів пакетів та час між прибуттям пакетів.

Моделювання топології мережі визначає, як вузли комп'ютерної мережі пов'язані між собою і, як може проходити інформація. Можна розглядати моделювання топологій як фізичного, і логічного рівня.

Мережеві топології моделюються за допомогою графів, де вершини відповідають вузлам мережі, а ребра – зв'язкам. Властивості моделей графів, такі як кількість зв'язків вузла, середня довжина шляху між вузлами та завантаження вузлів, дозволяють отримувати інформацію про продуктивність топології. Топологія мережі сильно впливає на продуктивність протоколу і поведінку маршрутизації, тому моделювання топології мережі є важливим.

Основними недоліками моделювання залишаються складність, висока трудомісткість і вартість розробки моделей, а іноді і велика затратність моделей при реалізації на електронних обчислювальних машинах. Хоча існуючі сьогодні продукти моделювання здатні допомогти моделювати та планувати мережу вони часом неадекватно моделюють обчислювальне середовище.

2.2 Порівняльна характеристика програмного забезпечення для моделювання і симуляції передачі мережевого трафіку

Симулятор – це частина програмного забезпечення, яка, як впливає з назви, імітує топологію мережі, що складається з одного або кількох мережних пристроїв. Імітовані мережні пристрої не є реальними мережевими пристроями і не здатні пропускати мережевий трафік так само, як реальні мережеві пристрої. Натомість кожен мережевий пристрій є частиною програмного забезпечення, яке в міру своїх можливостей є відповідним реальному мережевому пристрою. Мережевий симулятор реалізує модель комп'ютерної мережі за допомогою алгоритмів, процедур та структур відповідно до заданої мови програмування.

На ринку представлено кілька продуктів для моделювання мультимедійної комп'ютерної мережі. Одним із найбільш поширених є Microsoft Visio, який дає змогу моделювання установки, додає різні елементи та пристрої в інтерфейс, схожий на вміст. Хоча це може працювати для невеликих мультимедійних мереж, рисування кожного додаткового вузла є складним завданням, якщо моделювання проходить з великої кількості пристроїв і топологій, розподілених по всій компанії. Інші варіанти, такі як Cisco Packet Tracer і NetSim, або безкоштовні, або пропонують безкоштовні пробні версії, і хоча вони є неможливими варіантами, особливо якщо їхня вартість є проблемою, вони не надаються повним набором першокласних інструментів мережевого моделювання, щоб забезпечити більш просте управління.

Через варіативність задач у мультимедійних мережах, беручи до уваги їх унікальні проблеми, точки тиску та проблеми управління, часто корисно автоматизувати конфігурацію завдань та управління за допомогою мережевого програмного забезпечення.

Для успішного моделювання комп'ютерної мережі необхідно мати можливість використання інструменту управління конфігураційною мережею. Такий інструмент допомагає особі, що моделює мережу, правильно налаштувати і автоматизувати повторювані задачі, щоб в майбутньому зняти навантаження із мережевого адміністратора. Завдяки зростанню організації, що містить

мультимедійну мережу, вона може стати більш багаторівневою або більш складною, і може стати важко впевнено розвернути конфігурації у всій мережі. Однак інструменти керування конфігурацією складної локальної корпоративної мережі не є проблемою: інструменти зазвичай можуть автоматично визначати кожен вузол мережі, дозволяючи розглянути стандартні конфігурації, які можуть знадобитися для відповідних нормативних вимог, або відзначити будь-які конфігурації, що виходять за рамки очікуваних.

Основна перевага симуляторів полягає в тому, що вони зазвичай дуже легкі. Програмне забезпечення симулятора може працювати практично на будь-якому сучасному комп'ютері, не турбуючись про вимоги до процесора, пам'яті чи сховища. Внаслідок цього мережні пристрої у симуляторі обмежені командами та функціями (рис. 2.1), запрограмованими у симуляторі. З цієї причини багато розширених функцій.

Функції інструментів для моделювання роботи комп'ютерної мережі

Можливість конфігурації пристроїв



Відображення мапи мережі і її процесів в реальному часі

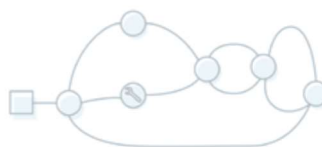


Рисунок 2.1 – Можливості сучасних інструментів для моделювання комп'ютерних мереж

Інструменти керування конфігураційними мережами також можуть виявляти вразливість, щоб ви могли усунути ці проблеми та зробити свою установку більш безпечною. Після цього ці інструменти повинні також відображати життєвий цикл пристроїв у мультимедійній мережі, повідомляючи, які пристрої підходять до кінця терміну служби, щоб надати можливість

повідомити про застарілий стан того чи іншого пристрою локальної мультимедійної мережі [23].

Для того щоб попередньо змоделювати мережу, інструмент NetworkTopologyMapper пропонує користувачам його функціонал. Цей інструмент автоматично виявляє і створює детальні топологічні карти комп'ютерної мережі і може створювати кілька типів карт без необхідності повторного сканування мережі.

2.2.1. NetworkSimulator -NS3

NS – це назва серії дискретно-подійних мережевих симуляторів, зокрема ns-1, ns-2 та ns-3. Мережевий симулятор NS-3 – це дискретно-подійний симулятор, призначений для дослідження мереж. Інструмент NetworkSimulator - NS3 забезпечує суттєву підтримку моделювання (рис. 2.2) протоколів TCP, маршрутизації та багатоадресного розсилання у дротових та бездротових (локальних та супутникових) мережах. Він загальнодоступний для досліджень, розробок та використання.

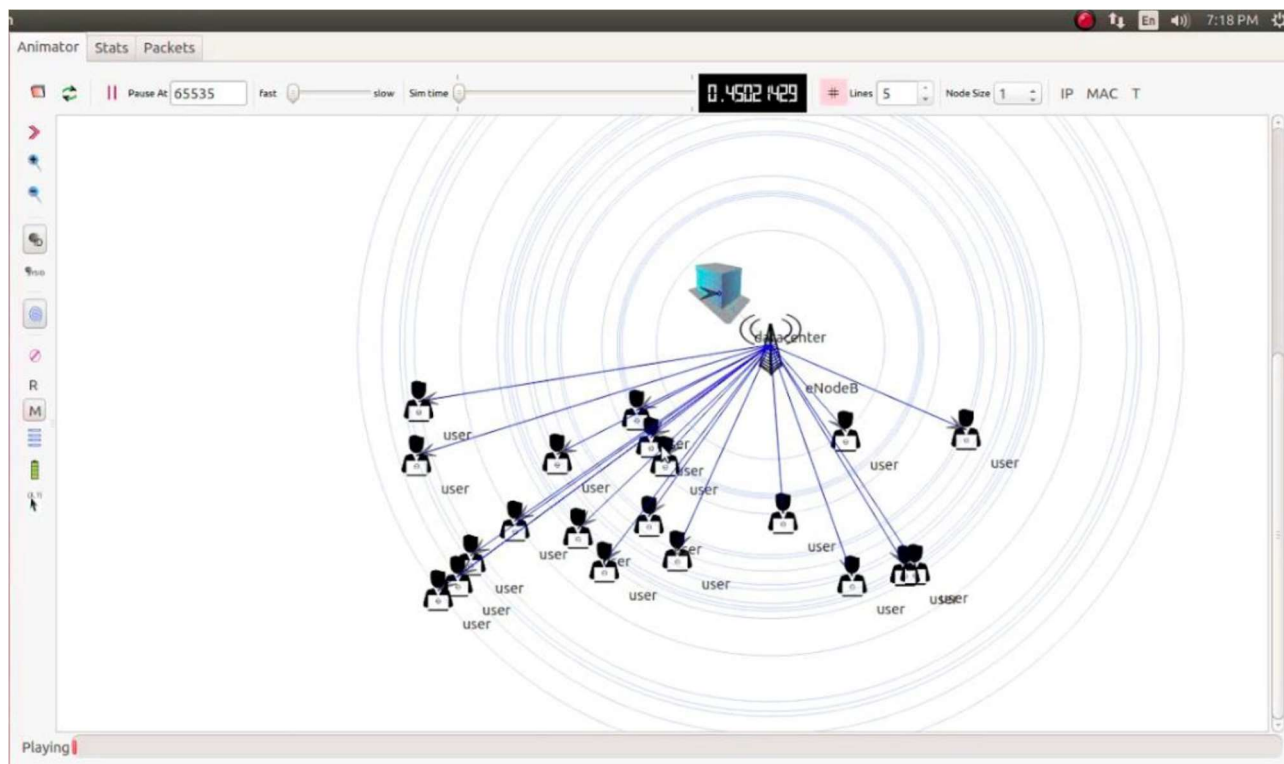


Рисунок 2.2 Інтерфейс NS3

Зм..	Арк.	№докум.	Підпис	Дата

Цей інструмент мережного моделювання дозволяє користувачам створювати мережеві топології та імітувати топології сучасних комп'ютерних мереж. PacketTracer – програму для моделювання мереж для початківців. Воно активно використовується під час навчання із сертифікації Cisco CCNA.

2.2.3. Microsoft Visio

Microsoft Visio – програма для створення діаграм та векторної графіки, розроблена компанією Microsoft. За допомогою програми Visio можна розробляти діаграми мережної архітектури, низькорівневого проектування (LLD) та високорівневого проектування (HLD).

Microsoft Visio (рис. 2.4) дозволяє створення діаграм, працювати візуально для побудови всіх видів діаграм, і є провідним у галузі з більш ніж 12 мільйонами користувачів. Visio полегшує визначення дизайну мережі, документування передового досвіду, візуалізацію майбутнього стану ініціатив із перетворення, а також дозволяє залишатися на вершині оперативної інформації у вашій компанії.

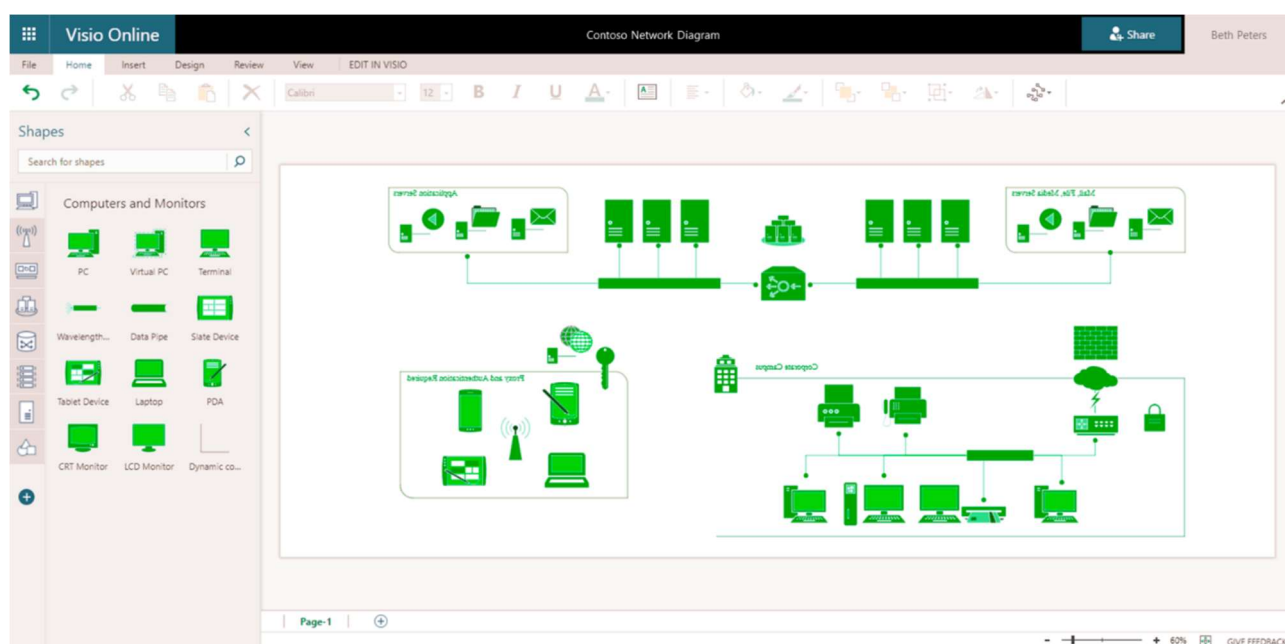


Рисунок 2.4 – Інтерфейс Microsoft Visio

Одним із основних недоліків даного програмного пакета є те, що він не має можливості сканування мережі на наявність вузлів мережі, якими можуть бути як нетбуки, так і ПК, Wi-Fi роутери, пристрої маршрутизації тощо. Функціонал

Microsoft Visio не є орієнтованим на проектування топології або моделювання процесів всередині комп'ютерних мереж. Призначенням програми є побудова схем, структур та графіків.

Переваги Visio:

- простота використання, відмінний графічний інтерфейс;
- Visio має інтерфейс Drag-n-Drop, який дозволяє переносити об'єкти з меню, а потім використовувати лінії/конектори для з'єднання всіх пристроїв.
- крім додаткових функцій, Visio поставляється з 1000 шаблонів, іконок, фігур, тем тощо, що дозволяє створювати професійні презентації;
- деякі з цих функцій інтеграції включають з'єднання декількох джерел даних з інших продуктів Microsoft. Автономне ПЗ не має функції автоматичного перегляду мережі та створення мережної діаграми, це можна зробити лише за допомогою сторонніх програм.

Якщо Visio підходить до потреб споживача він справді може створювати елегантні, корисні діаграми всіх типів, які можуть забезпечити професійний вигляд, необхідний для презентацій, звітів, аудиту, планів будівель, поверхових планів, документації та моделювання найкращих способів виконання роботи. Visio включає велику бібліотеку фігур/символів, що використовуються в десятках типів діаграм.

Ці символи представляють спеціалізовані частини діаграм, такі як діаграми потоків процесів, моделювання бізнес-процесів, діаграми потоків даних та багато інших.

2.2.4. GNS3 – GraphicalNetworkSystem 3

GraphicalNetworkSystem 3 (GNS 3) – це інструмент та програмне забезпечення для моделювання мереж. GNS3 може моделювати складні мережі та сценарії та підтримує комбінацію віртуальних та реальних мережевих пристроїв. GNS3 - це один із інструментів мережевого моделювання для створення, проектування, налаштування та тестування мережевих сценаріїв у віртуальному середовищі без ризику. Інструмент мережного моделювання GNS3 (рис. 2.5) доступний для Windows, Linux та Mac.

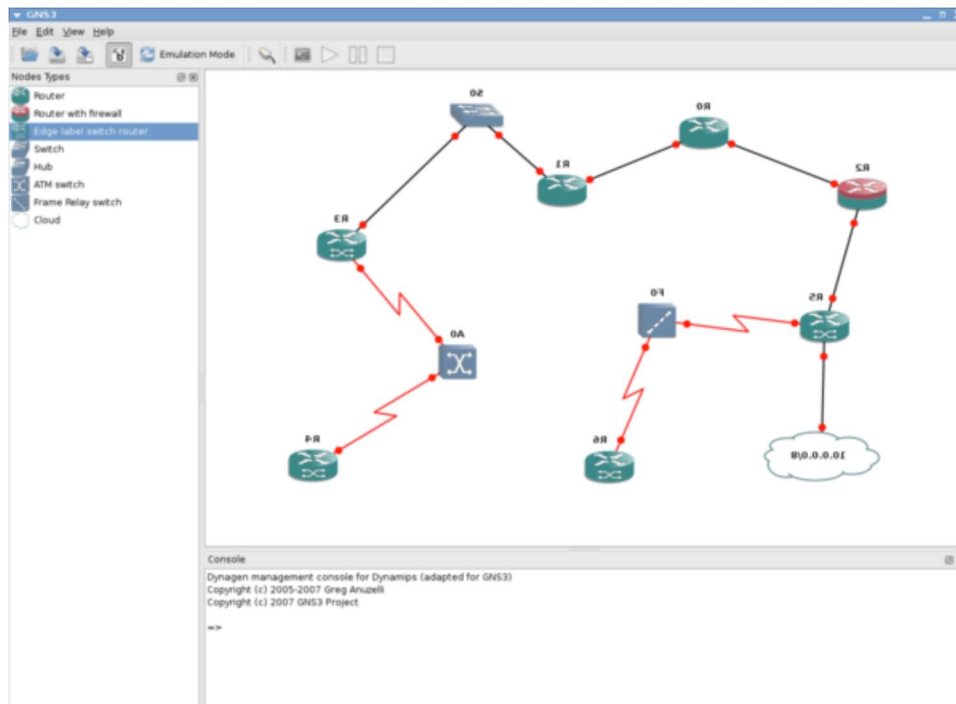


Рисунок 2.5 – Інтерфейс GNS 3

GNS3 може бути використаний для емуляції деяких апаратних продуктів CISCO на комп'ютерах. GNS3 надає студенту уникнути проблем зберігання комплектів мережевого обладнання у будинку. GNS3 запускає справжню симуляцію без похибок чи несподіваної поведінки.

Інструментарій програми дозволяє мати під рукою сотні топологій, що не потребує встановлення реального обладнання. Оскільки деякі вбудовані проекти мережі ліцензовані компанією Cisco Systems, вони не можуть бути вільно розповсюджені та потребують попереднього завантаження в програму.

GNS3 пропонує простий спосіб проектування та створення мереж будь-якого розміру без необхідності використання апаратного забезпечення [25]. Програма Graphical Network System 3 має наступний перелік функцій:

- моделювання мережі у реальному часі для попереднього тестування без необхідності використання мережного обладнання ;
- тестування різних постачальників мережного обладнання у віртуальному середовищі без ризику;

- створення динамічних мережеских карт для пошуку та усунення помилок в роботі мережі;
- має функцію запуску оперативної системи, яка емулює реальну поведінку мережного обладнання;
- надає можливість використання існуючого обладнання та розширення лабораторію, за допомогою підключення топології GNS3 безпосередньо до неї.
- тестування мережі до їх створення, щоб скоротити час, необхідний для запуску виробничої мережі;
- функція підключення GNS3 до будь-якої реальної мережі;
- швидкий запуск та тестування обладнання кількох виробників без необхідності використання апаратного забезпечення.

2.2.5. NetCracker Professional

NetCracker – інструмент для автоматизованого проектування, моделювання та аналізу комп'ютерних мереж. Він дозволяє проводити експерименти, за результатами яких можна обґрунтувати вибір типу мережі, середовища передачі, мережеских апаратних компонентів і програмно-математичного програмного забезпечення.

NetCracker дозволяє розробляти багаторівневі проекти зі ступенем деталізації, заданим дизайнером; має досить зручний інтерфейс та засоби швидкого перегляду всіх рівнів проекту. Програмне забезпечення NetCracker містить потужну базу даних мережеских пристроїв від провідних виробників: робочі станції, сервери, носії передачі, мережескі адаптери, ретранслятори, мости, комутатори, маршрутизатори, що використовуються для різних типів мереж і мережеских технологій.

Для реалізації функцій моделювання NetCracker (рис. 2.6) надає інструменти для встановлення характеристик трафіку різних протоколів; засоби для візуального контролю заданих параметрів; інструменти для накопичення статистичної інформації та звітності про експерименти.

можливість створювати мережеві топології з широкого безлічі маршрутизаторів і комутаторів компанії Cisco, робочих станцій і мережних з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Функції симулятора можуть бути придатні як для навчання, так і для роботи, настройки мережі ще на етапі планування.

Packet Tracer включає наступні особливості:

- Робочий простір для створення мережі будь-якого розміру і складності;
- Моделювання в режимі реального часу;
- Моделювання в режимі симуляції;
- Графічний інтерфейс для взаємодії з користувачем під час налаштування мережевих пристроїв;
- Зображення мережевого обладнання з підтримкою додавання, видалення, переміщення різних компонентів.

Даний симулятор дозволяє студентам проектувати свої власні мережі, створюючи і відправляючи різні пакети даних, зберігати і коментувати свою роботу. Надається можливість вивчати і використовувати такі мережеві пристрої, як комутатори, маршрутизатори, робочі станції, визначати типи зв'язків між ними і з'єднувати їх.

Відмінною особливістю даного симулятора є наявність в ньому режиму симуляції (рис. 2.7). В даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє студентам наочно продемонструвати, за яким інтерфейсу в дані момент переміщається пакет, який протокол використовується. Працюючи в симуляторі в іншому режимі, режимі реального часу, не можна простежити за переміщенням пакетів, відразу відображається кінцевий результат виконаних дій.

– Serial DCE / DTE

Кожен пристрій в програмному продукті Cisco Packet Tracer може бути налаштоване через вікно властивостей, яке викликається по подвійному кліку на пристрої. Перша вкладка Physical (рис. 2.8) відповідає за фізичні параметри пристрою. Під час налаштування маршрутизаторів і комутаторів в них можна додавати нові модулі, в робочі станції і сервери – вставляти мережеві адаптери.

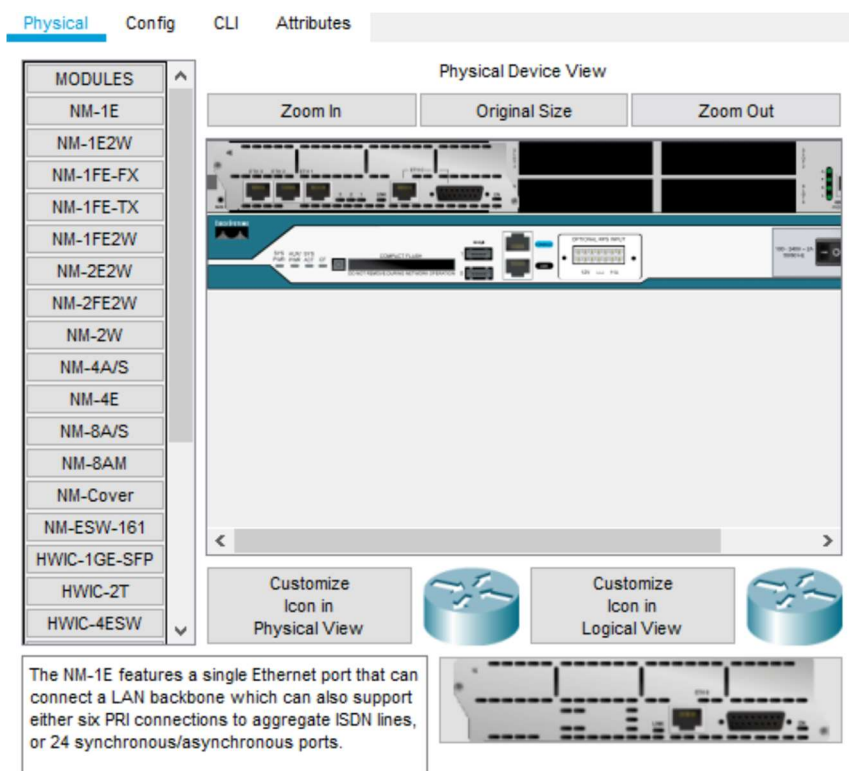


Рисунок 2.8 – Фізичний вигляд пристрою (маршрутизатора)

На вкладці Config (рис. 2.9) можна задавати основні параметри мережевих інтерфейсів (IP-адреси, маски підмережі, параметри бездротової мережі та ін.) У мережевих пристроях також можна конфігурувати маршрутизацію – статичну або динамічну, у серверів – конфігурувати служби.

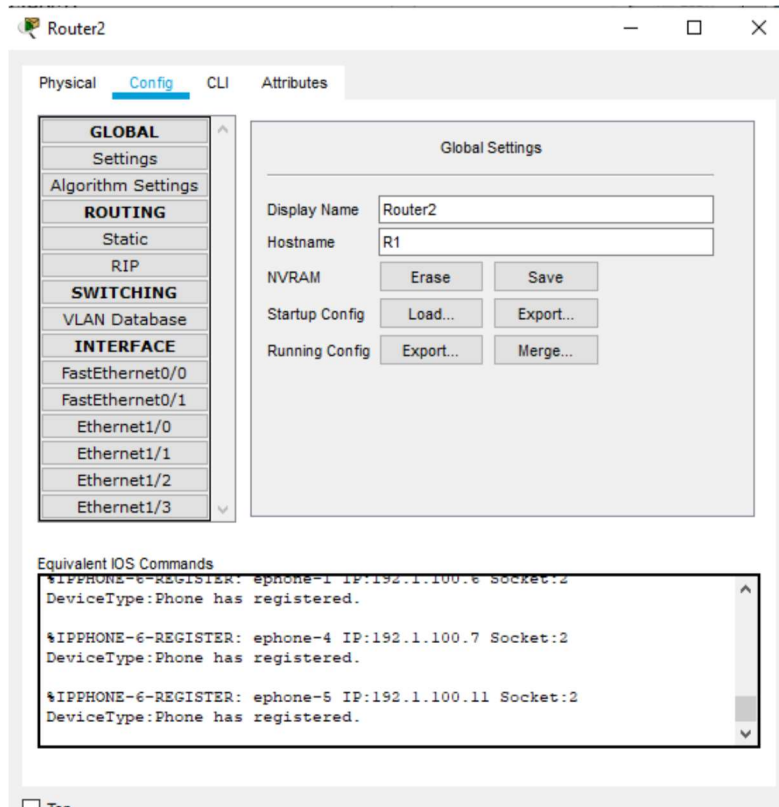


Рисунок 2.9 – Конфігурація сервера

При запуску програми відкривається головне вікно симулятора (рис. 2.10):

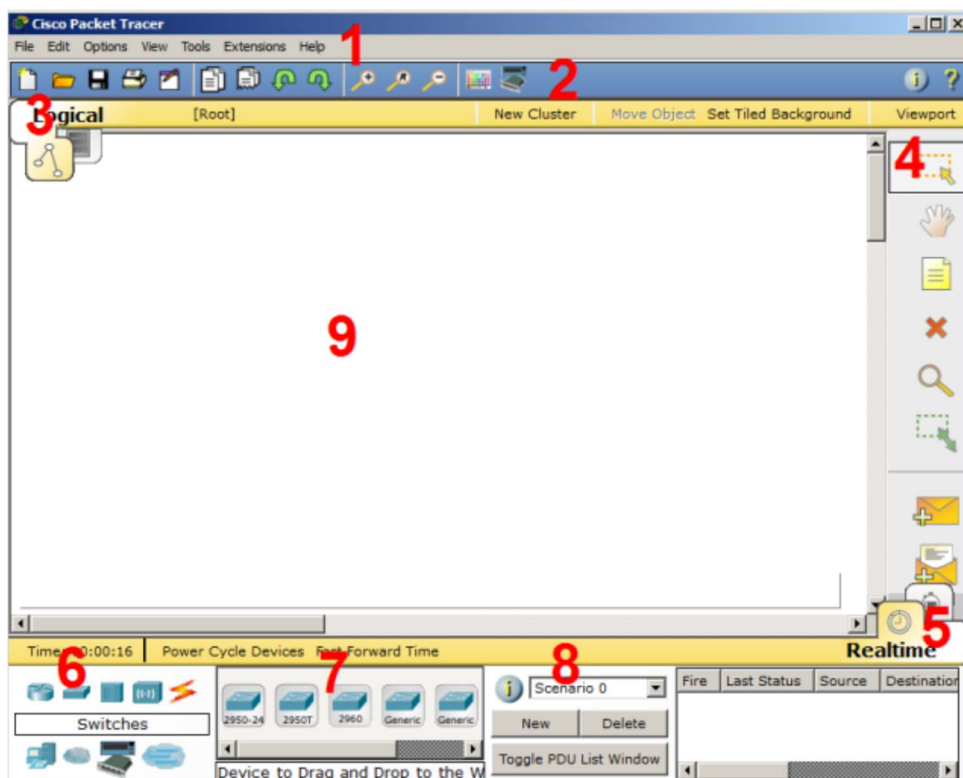


Рисунок 2.10 – Інтерфейс програми Cisco Packet Tracer

Зм..	Арк.	№докум.	Підпис	Дата

1) Головне меню програми з наступним змістом:

- Файл – містить операції відкриття / збереження документів;
- Виправлення – стандартні операції "копіювати / вирізати, скасувати / повторити";
- Налаштування - говорить сама за себе;
- Вид - масштаб робочої області і панелі інструментів;
- Інструменти - колірна палітра і кастомізація кінцевих пристроїв;
- Розширення - майстер проектів, розрахований на багато користувачів режим і кілька прибуд, які з СРТ (так я іноді буду ласкаво називати Cisco Packet Tracer) можуть зробити цілу лабораторію;
- Допомога – містить інформацію про програму та містить посилання на додатки допомоги в використанні програми;

2) Панель інструментів, частина яких просто дублює пункти меню;

3) Перемикач між логічного і зниження фізичної організацією;

4) Ще одна панель інструментів, містить інструменти виділення, видалення, переміщення, масштабування об'єктів, а так само формування довільних пакетів;

5) Перемикач між реальним режимом (Real-Time) і режимом симуляції;

6) Панель з групами кінцевих пристроїв і ліній зв'язку;








7) Самі кінцеві пристрої, тут містяться всілякі комутатори, вузли, точки доступу, провідники.

8) Панель створення призначених для користувача сценаріїв;

9) Робочий простір.

Симулятор Packet Tracer підтримує широкий діапазон мережевих з'єднань (таблиця 2.1). Кожен тип кабелю може бути з'єднаний лише з певним типом інтерфейсу.

Таблиця 2.1 – Типи кабелів в Cisco Packet Tracer

№	Тип кабелю	Опис
1	2	3
1	Консоль 	Консольне з'єднання може бути виконано між ПК і маршрутизаторами або комутаторами. Повинні бути виконані деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднань з обох сторін повинна бути однаковою, має бути 7 біт даних (або 8 біт) для обох сторін, контроль парності повинен бути однаковий, має бути 1 або 2 степових бита (але вони не обов'язково повинні бути однаковими), а потік даних може бути чимось завгодно для обох сторін.
2	Мідний прямий 	Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв, який функціонує на різних рівнях OSI. Він повинен бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet).
3	Мідний кросовер 	Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях OSI. Він може бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet)
4	Оптика 	Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт / с або 1000 Мбіт / с).
5	Телефонний 	З'єднання через телефонну лінію може бути здійснено тільки між пристроями, що мають модемні порти. Стандартне подання модемного з'єднання – це кінцевий пристрій (Наприклад, ПК), додзвонюється в мережеве хмара.
6	Коаксиальний 	Коаксиальне середовище використовується для з'єднань між коаксиальними портами, такі як кабельний модем, з'єднаний з хмарою Packet Tracer.
7	Серійний DCE Серійний DTE 	З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристроїв. Синхронізація DTE виконується за вибором.

Packet Tracer є зручним засобом моделювання мереж передачі даних. Робота з симулятором дає вельми правдоподібне відчуття настройки реальної мережі, що складається з різних пристроїв. Налаштування мережевого обладнання можна проводити як за допомогою команд операційної системи Cisco IOS, так і за допомогою графічного інтерфейсу. Завдяки режиму симуляції можна простежити переміщення даних по мережі, поява і зміна параметрів пакетів при проходженні даних через мережеві пристрої, швидкість і шляхи переміщення пакетів. Аналіз подій, що відбуваються в мережі, дозволяє зрозуміти механізм її роботи і виявити несправності.

2.4 Висновки

В розділі проаналізовано засоби та методи моделювання комп'ютерних мереж. За результатами аналізу програмного забезпечення для моделювання комп'ютерних мереж було обрано пакет Packet Tracer від компанії Cisco Systems. Серед іншого аналізувалися програми NetworkSimulator, CiscoPacketTracer, MicrosoftVisio, GraphicalNetworkSystem 3, NetCrackerProfessional.

Packet Tracer дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори та комутатори, взаємодіяти між кількома користувачами (через хмару).

У симуляторі реалізовані серії маршрутизаторів Cisco 2900 і комутаторів Cisco Catalyst 2950, а також міжмережевий екран ASA 5505, що будуть використовуватись фізично при побудові мережі. Крім того є імітації серверів DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP та EMAIL, робочі станції, різні модулі до комп'ютерів та маршрутизаторів, IP-фони, смартфони, хаби, а також хмара, що емулює WAN.

Це дає змогу успішно створювати складні макети мереж, перевіряти на працездатність топологію мережі та переносити готові конфігураційні файли на реальні пристрої.

					КвРКІ. 180242.18.02.15 ПЗ	Арк. 40
Зм.	Арк.	№докум.	Підпис	Дата		

3 МОДЕЛЮВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ

3.1 Проектування та сегментація локальних мережі

Згідно із поставленою задачею та результатами проведеного аналізу необхідно розробити мережу для підприємства, до складу якого входить три будівлі, а саме офіс, магазин та склад. Загальна кількість кімнат обрана 21 кімната, тобто в кожній будівлі 7 кімнат.

Загальна площа офісної будівлі складає 188,5 квадратних метрів (1300 см x 1450 см). Площа першої, другої, четвертої і п'ятої кімнат співпадають і дорівнюють 18 квадратних метрів (300 см x 600 см), третьої кімнати становить 20 квадратних метрів (250 см x 800 см), шостої 12 квадратних метрів (400 см x 300 см), а сьомої 18 квадратних метрів (600 см x 300 см).

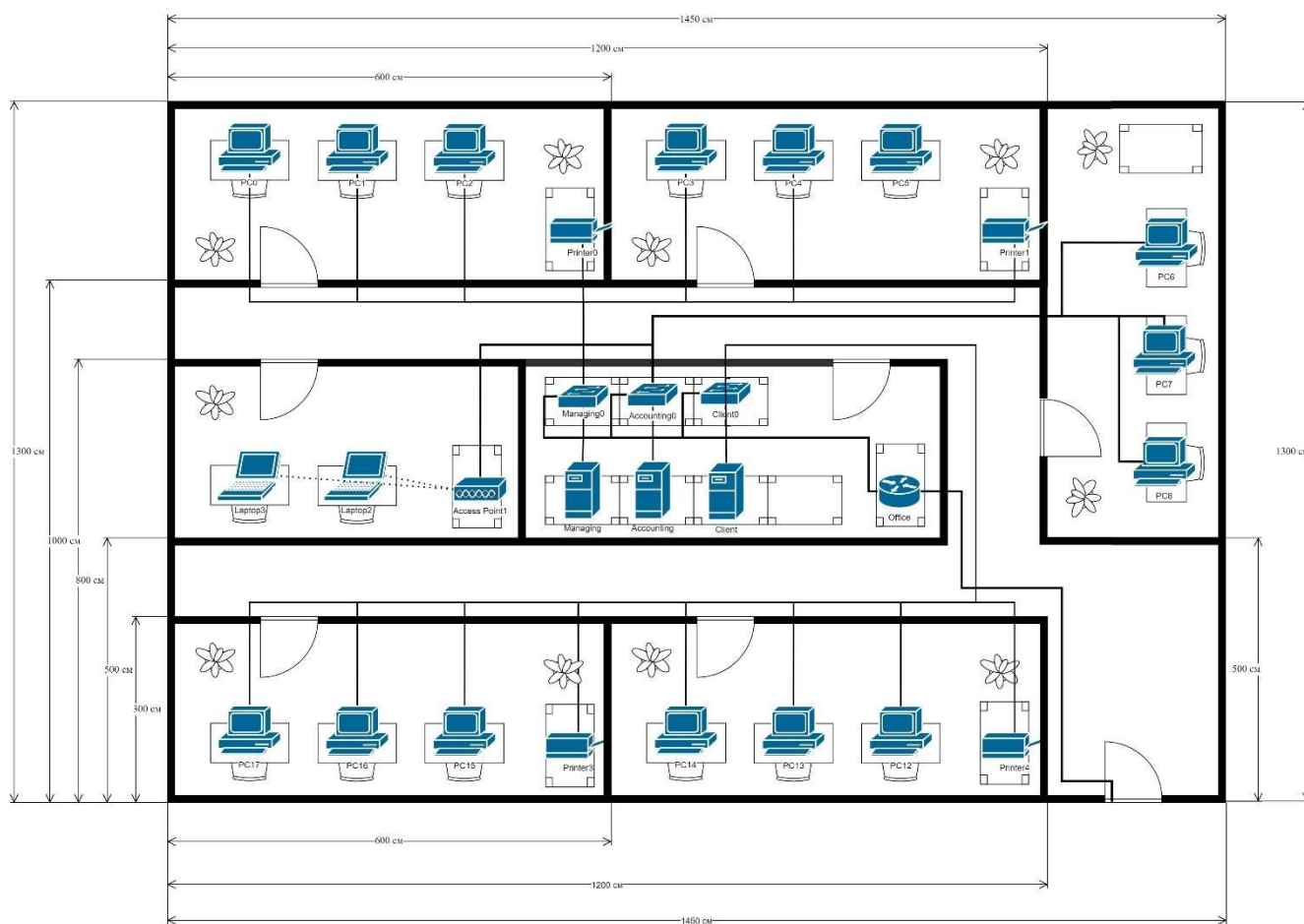


Рисунок 3.1 – Фізична топологія мережі офісної будівлі

Отже для офісної будівлі було розраховано кількість обладнання, яке необхідне для реалізації мережі, що вказано в таблиці 3.1. Фізична топологія мережі зображено на рисунку 3.1.

Таблиця 3.1 – Розрахунок кількості обладнання для офісної будівлі

Обладнання	Кількість
ПК (персональний комп'ютер)	15
Ноутбук	2
Принтер	4
Комутатор	3
Маршрутизатор	1
Сервер	3
Точка доступу	1
Загальна кількість приладів	29

Мережа підприємства повинна мати три відділи, а саме бухгалтерія, менеджери та клієнтська. Вони розміщені в кожній будівлі. В офісі для відділів було виділено по дві кімнати. В відділі для менеджерів було виділено шість комп'ютерів, два принтери, один сервер, один комутатор. А в бухгалтерію було виділено три персональних комп'ютери, два ноутбуки, точку доступу, сервер та комутатор. Клієнтський відділ обладнаний шістьма персональними комп'ютерами, двома принтерами, сервером та комутатором. Для комутаторів, серверів та маршрутизатора було виділено окрему – серверну кімнату.

В трьох приміщеннях зберігаються товари для продажу, також пристрої для контролю, а саме в першій, другій та третій кімнаті, а їх площа кожної становить 32,5 квадратних метрів (500 см x 650 см). Площа серверної кімнати становить 19,25 квадратних метрів (350 см x 550 см). Площа кімнат інших відділів, а саме четвертої, п'ятої та шостої дорівнює 19,25 квадратних метрів (350 см x 550 см). Згідно з параметрами будівлі було розраховано кількість приладів, що вказано в таблиці 3.2. А фізична топологія мережі складу зображено на

рисунку 3.2.

Таблиця 3.2 – Розрахунок кількості приладів для складу

Назва приладу	Кількість
ПК (персональний комп'ютер)	9
Ноутбук	2
Принтер	3
Комутатор	3
Маршрутизатор	1
Точка доступу	1
Загальна кількість приладів	19



Рисунок 3.2 – Фізична топологія мережі складу

Відділи містяться також і в складі, кожному було виділено по дві кімнати. В бухгалтерії містяться три персональних комп'ютери, принтер, точка доступу, комутатор. Для менеджерів розраховано три комп'ютери, принтер та комутатор. А в клієнтському відділі містяться також три комп'ютери, принтер та комутатор.

Зм.	Арк.	№докум.	Підпис	Дата
-----	------	---------	--------	------

Для комутаторів, маршрутизатора виділено окремо кімнату, в яку також помістили точку доступу і ноутбуки, які належать до відділу бухгалтерії.

До складу підприємства входить магазин, в якому теж слід також налаштувати для підключення до мережі підприємства. Площа магазину становить 252 квадратних метрів (1800 см x 1400 см). Через нестандартну форму слід відняти 35 квадратних метрів, тому загальна площа дорівнює 217 квадратних метрів. Але також слід врахувати форму будівлі і відняти 18 квадратних метрів, що дорівнюватиме 234 квадратних метрів. Площа основного приміщення магазину складає 98 квадратних метрів (700 см x 1400 см), площі другої, третьої, четвертої, п'ятої, шостої кімнат рівні і дорівнюють 13,5 квадратних метрів (450 см x 300 см).

Таблиця 3.3 – Розрахунок кількості приладів для магазину

Назва приладу	Кількість
ПК (персональний комп'ютер)	16
Ноутбук	2
Принтер	3
Комутатор	3
Маршрутизатор	1
Точка доступу	1
Загальна кількість приладів	26

Згідно з попередніх розрахунків, можна виконати розрахунок приладів для будівлі магазину, що вказано в таблиці 3.3. Фізична топологія мережі магазину зображено на рисунку 3.3.

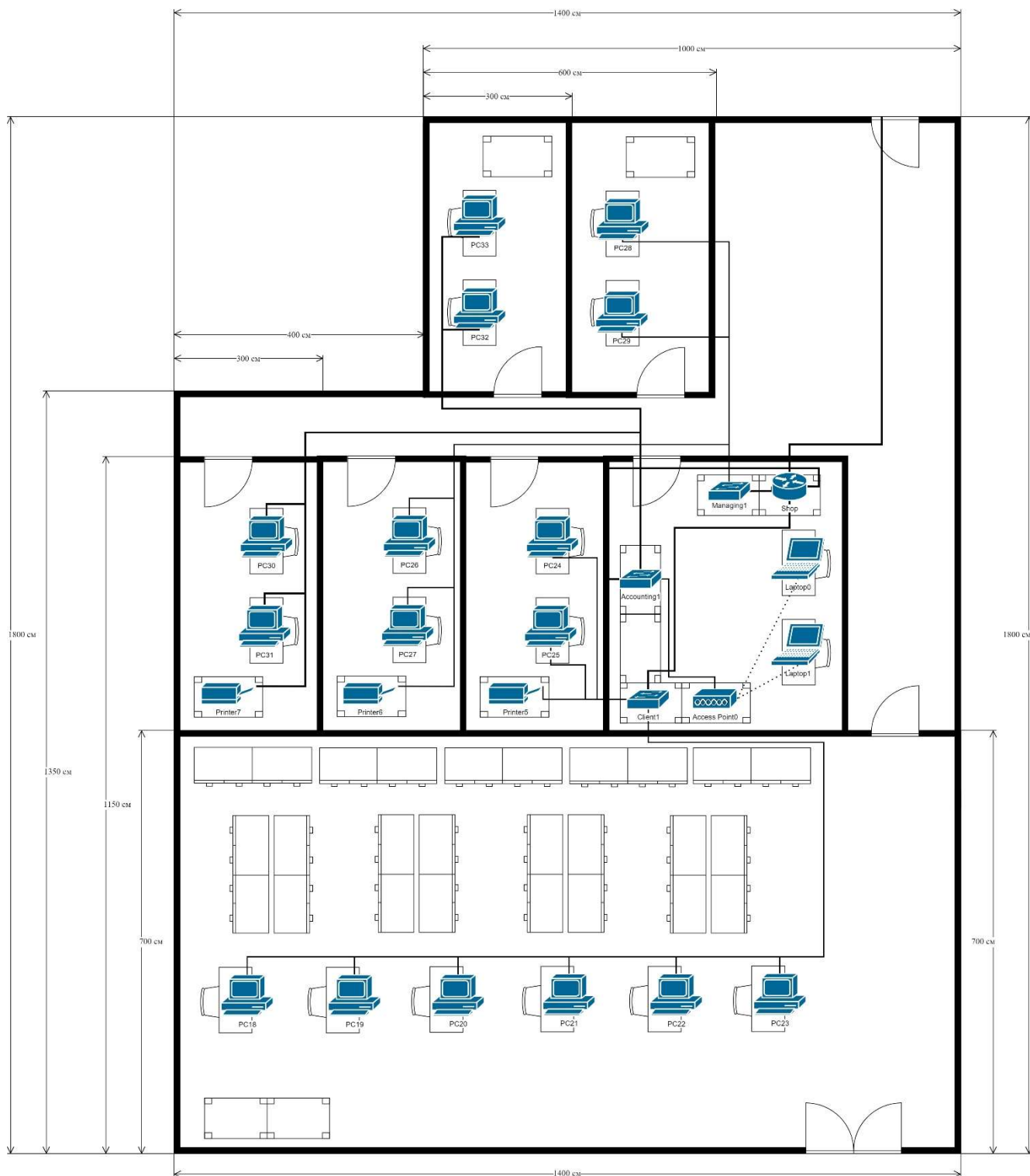


Рисунок 3.3 – Фізична топологія мережі магазину

В магазині також присутні три відділи, кожному було виділено по дві кімнати. Для клієнтського відділу було розраховано вісім персональних комп'ютерів, принтер та комутатор. В відділі для менеджерів містяться чотири персональних комп'ютери, принтер та комутатор. А у бухгалтерії розміщені

Зм.	Арк.	№докум.	Підпис	Дата

чотири персональних комп'ютери, два ноутбуки, принтер, точка доступу та комутатор. Виділено спеціальну серверну кімнату для комутаторів, маршрутизатора.

3.2 Розробка фізичної топології мережі в Packet Tracer

Для зручності налаштування логічної топології мережі було створено ще одну фізичну топологію мережі, але в Packet Tracer. У фізичному моді можна налаштувати фізичну локацію, де присутні різні рівні, а саме міжміський, міський та рівень будівель з кімнатами.

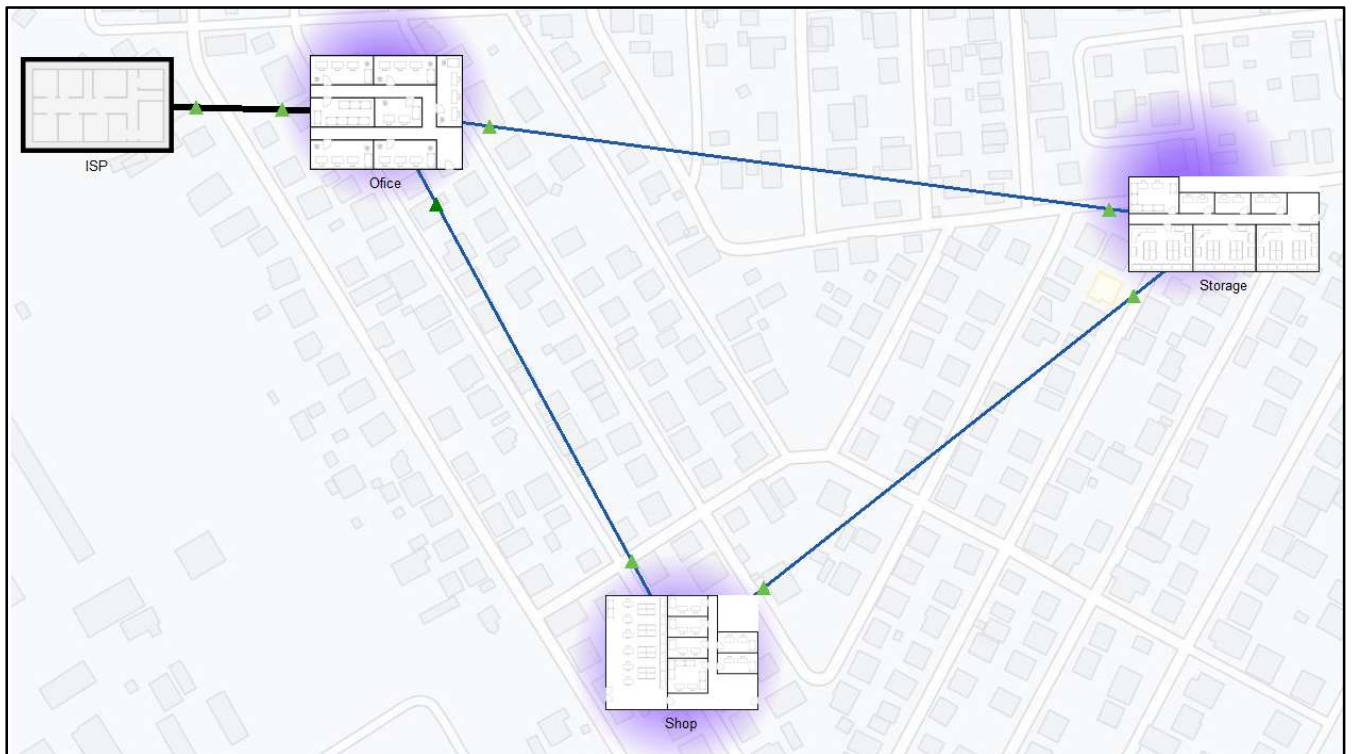


Рисунок 3.4 – Міжміський рівень фізичної топології

На міжміському рівні немає ускладненої топології, адже будівлі компанії перебувають на міському рівні, на відстані 500 метрів одна від одної. Але на даному рівні можна показати локацію, для даного завдання було обрано країну – Україну, а місто – Хмельницький, що зображено на рисунку 3.4.

Зм.	Арк.	№докум.	Підпис	Дата

На міському рівні було встановлено приблизну локацію споруд, які розміщені приблизно на відстані 500 метрів одна від одної. На рисунку показано також будівлю ISP – це Інтернет сервіс провайдер, який надає доступ до Інтернету. Вигляд міського рівня фізичної топології в Packet Tracer зображено на рисунку 3.5.



Рисункок 3.5 – Міський рівень фізичної топології

Далі можна перейти в кожну будівлю і налаштувати кожну кімнату. На рисунках 3.6-3.8 показано фізичну топологію офісу, магазину та складу. Було змінено стандартний фон відповідно до будови кожної будівлі компанії. Також можна переглянути та налаштувати з'єднання. Прилади розміщені відповідно до розрахунків в попередньому розділі, для цього створено полицки і столи. Можна увійти в кімнату і змінити розміщення пристроїв, а також можна провести налаштування без участі логічного моду. Блакитним кольором позначено ділянку дії точку доступу і можна перевірити радіус дії, чи прилади зможуть підключитися до неї.

Зм.	Арк.	№докум.	Підпис	Дата

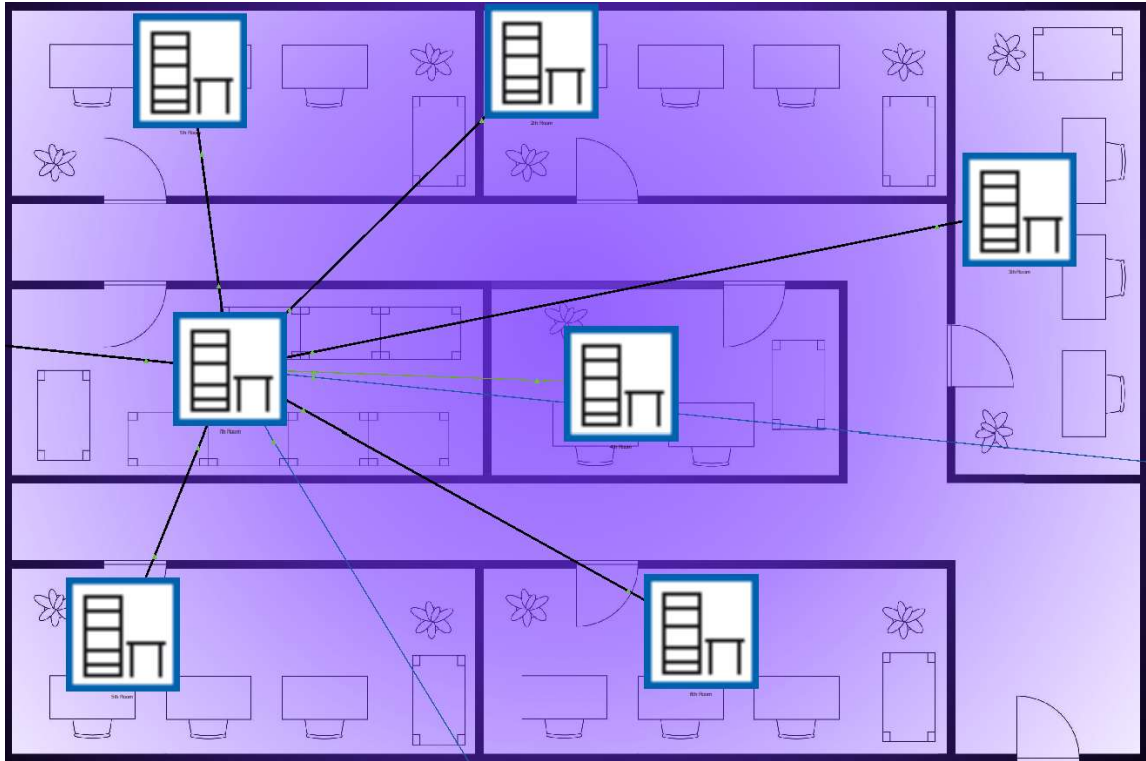


Рисунок 3.6 – Фізична топологія мережі офісної будівлі в Packet Tracer

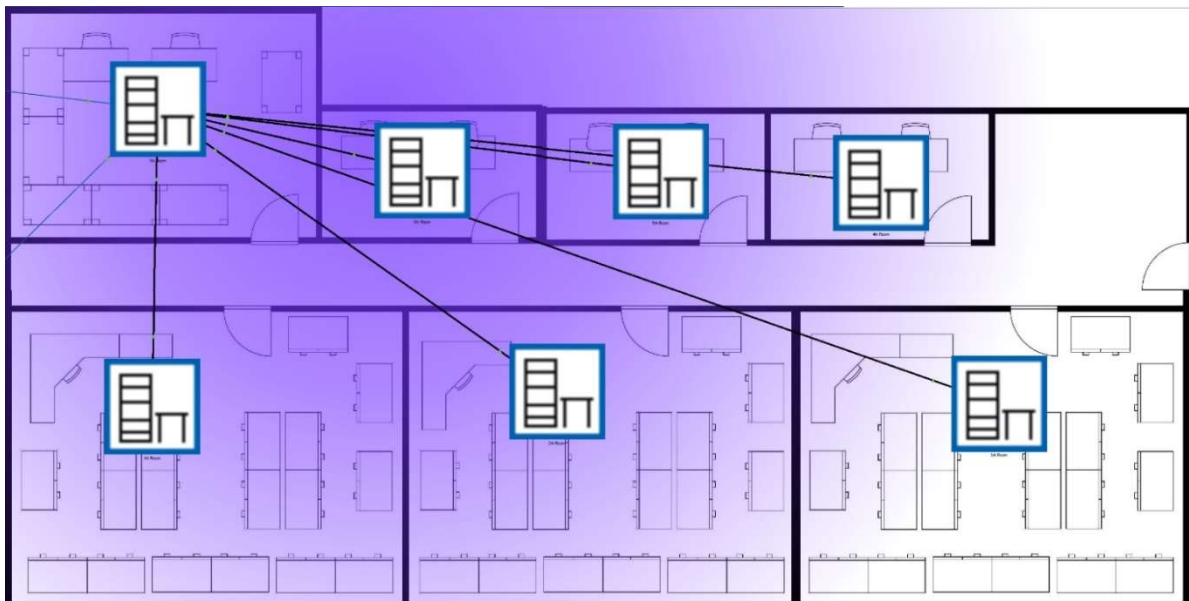


Рисунок 3.7 – Фізична топологія мережі складу в Packet Tracer

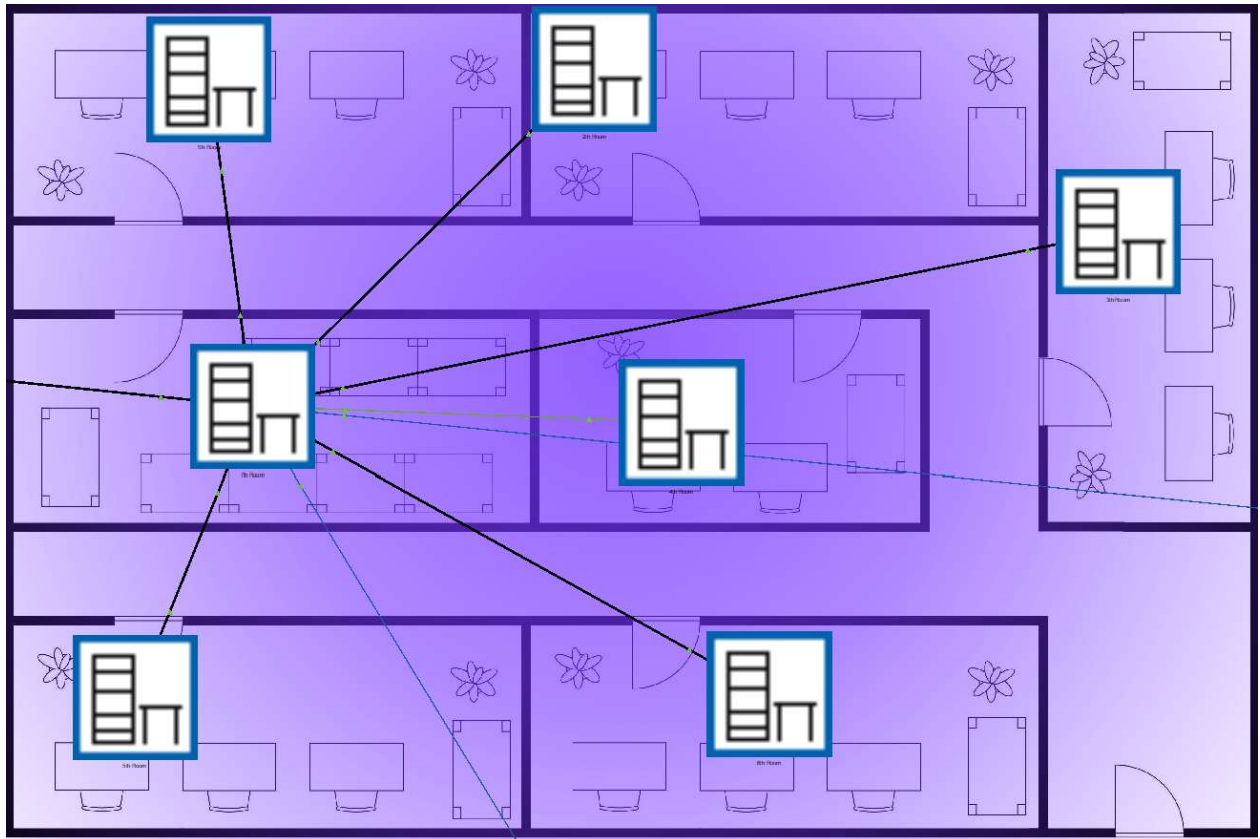


Рисунок 3.8 – Фізична топологія мережі складу в Packet Tracer

3.3 Розробка логічної топології мережі в Packet Tracer

Логічну топологію мережі було розроблено і налаштовано в програмному забезпеченні Packet Tracer. В кожній будівлі було створено три відділи, а саме три підмережі (VLAN), даний список наведено в таблиці 3.4. На рисунку 3.9 зображено частину топології мережі, а саме для офісної будівлі.

Таблиця 3.4 – Список VLAN для будівлі офісу

№VLAN	Назва VLAN	Примітка
1	default	Управління
10	Managing	Менеджмент
20	Accounting	Бухгалтерія
30	Client	Клієнтська

замовчуванням.

```
ip dhcp pool Managing0-pool
network 192.168.1.0 255.255.255.0
dns-server 192.168.1.11
default-router 192.168.1.1
```

При налаштуванні протокол DHCP потрібно обов'язково налаштувати виключення, для того щоб певні адреси не призначалися автоматично пристроям. Це здійснюється для того щоб зарезервувати окремим хостам. Для цього потрібно використати команду `ip dhcp excluded-address` і ввести відповідну IP-адресу.

Після даного налаштування можна перейти у будь-який пристрій перейти до налаштувань IP та увімкнути DHCP.

Таблиця 3.5 – Список IP-адрес для офісної будівлі

IP-адреса	Примітка	VLAN
192.168.1.0 / 24	Менеджмент	10
192.168.1.1	шлюз	
192.168.1.1-254	пристрої	
192.168.1.11	сервер	
192.168.2.0 / 24	Бухгалтерія	20
192.168.2.1	шлюз	
192.168.2.1-254	пристрої	
192.168.2.11	сервер	
192.168.2.0 / 24	Клієнтська	30
192.168.2.1	шлюз	
192.168.2.1-254	пристрої	
192.168.2.11	сервер	

Таблиця 3.6 – Таблиця адресації пристроїв для будівлі офісу

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
Office (модель 2911)	GigabiteEthernet0/0	192.168.1.0/24	255.255.255.0
	GigabiteEthernet0/1	192.168.2.0/24	255.255.255.0
	GigabiteEthernet0/2	192.168.3.0/24	255.255.255.0
	Serial0/1/0	20.0.0.1/30	255.255.255.252
	Serial0/2/0	10.10.10.6/30	255.255.255.252
	Serial0/2/1	10.10.10.2/30	255.255.255.252
PC0-PC5 Printer0- Printer1	FastEthernet0	192.168.1.2-9/24	255.255.255.0
PC6-PC8	FastEthernet0	192.168.2.2-4/24	255.255.255.0
Laptop0- Laptop1	Wireless0	192.168.2.2-4/24	255.255.255.0
PC12- PC17 Printer3- Printer4	FastEthernet0	192.168.3.2-9/24	255.255.255.0
Managing (Server- PT)	FastEthernet0	192.168.1.11/24	255.255.255.0
Accounting (Server- PT)	FastEthernet0	192.168.2.11/24	255.255.255.0
Client (Server- PT)	FastEthernet0	192.168.3.11/24	255.255.255.0

В підсумку, пристрій отримає автоматичні налаштування, а саме IP-адресу, маску підмережі, IP-адресу за замовчуванням, DNS-сервер. Таким самим чином

					КвРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		52

налаштовуються і інші VLAN. Було отримано список IP-адрес де вказані VLAN, для офісної будівлі розміщені в таблиці 3.5. Також було отримано таблицю адресації пристроїв вказаних в таблиці 3.6.

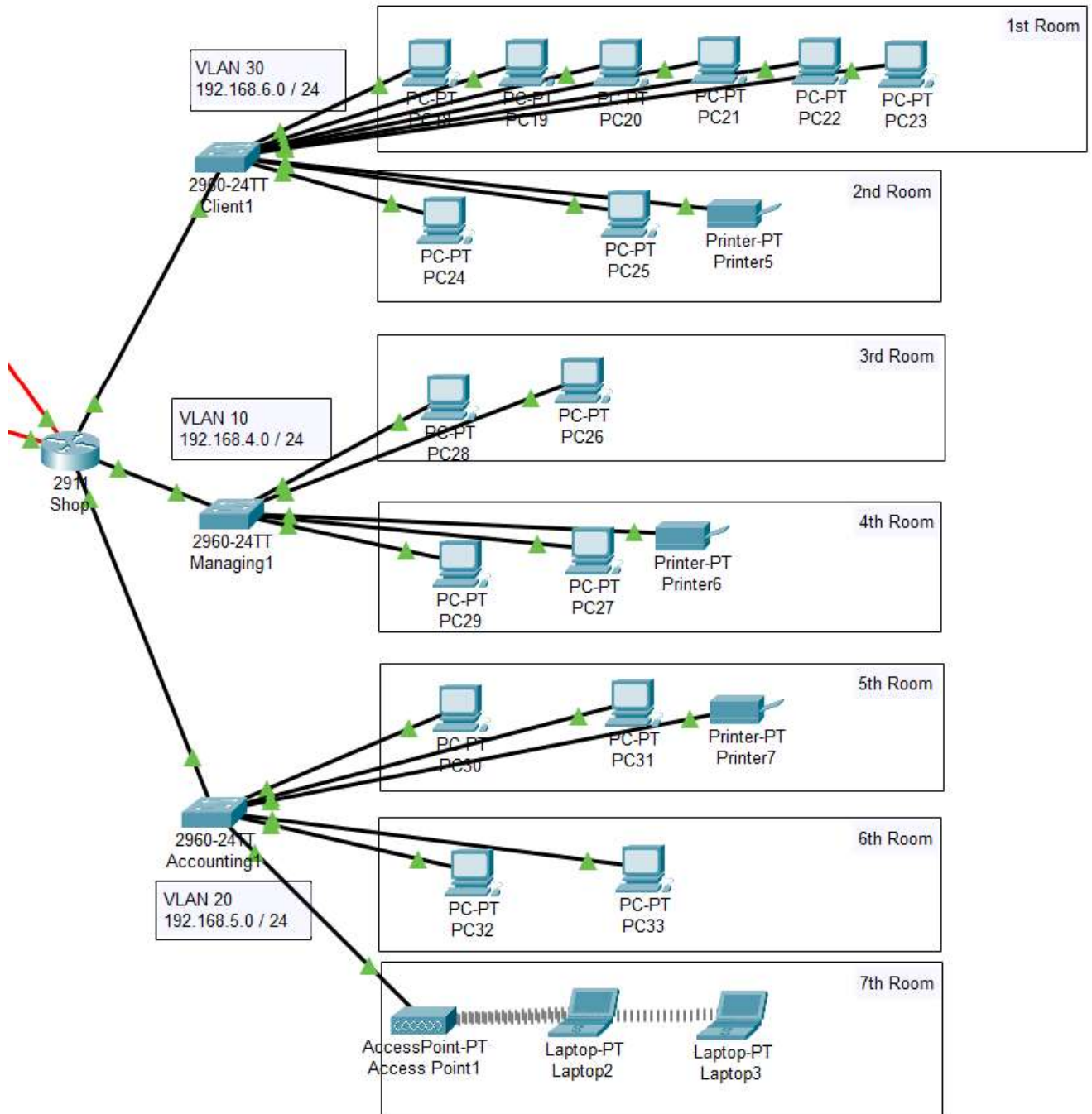


Рисунок 3.10 – Логічна топологія мережі магазину

Наступним кроком потрібно налаштувати також і інші будівлі у мережі підприємства. На рисунку 3.10 зображено логічну топологію мережі магазину.

Тут також присутні три відділи, а саме три VLAN 10-30, тому слід провести їх налаштування. Для даних пристроїв було використано протокол DHCP.

Крім тих самих пристроїв, в магазині присутня точка доступу, яку слід також налаштувати. Отож потрібно дати назву і встановити пароль. Для того щоб виконати підключення ноутбуків для даної точки доступу потрібно вимкнути пристрій та замінити вбудований модуль на WPC300N. А потім у налаштуваннях знайти потрібну точку доступу та ввести правильний пароль.

У підсумку було отримано дві таблиці, а саме таблицю 3.7 з адресацією пристроїв для магазину та таблицю 3.8 з IP-адресами, де вказані VLAN.

Таблиця 3.7 – Таблиця адресації пристроїв для магазину

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
Shop (модель 2911)	GigabiteEthernet0/0	192.168.5.0/24	255.255.255.0
	GigabiteEthernet0/1	192.168.4.0/24	255.255.255.0
	GigabiteEthernet0/2	192.168.6.0/24	255.255.255.0
	Serial0/2/0	10.10.10.5/30	255.255.255.252
	Serial0/2/1	10.10.10.9/30	255.255.255.252
PC18- PC25 Printer5	FastEthernet0	192.168.6.6- 11/24	255.255.255.0
PC26- PC29 Printer6	FastEthernet0	192.168.4.2-6/24	255.255.255.0
Laptop2-3	Wireless0	192.168.5.7-8/24	255.255.255.0
PC30- PC33 Printer7	FastEthernet0	192.168.5.2-6/24	255.255.255.0

Таблиця 3.8 – Список IP-адрес для магазину

IP-адреса	Примітка	VLAN
192.168.4.0 / 24	Менеджмент	10
192.168.4.1	шлюз	
192.168.4.1-254	пристрої	
192.168.5.0 / 24	Бухгалтерія	20
192.168.5.1	шлюз	
192.168.5.1-254	пристрої	
192.168.6.0 / 24	Клієнтська	30
192.168.6.1	шлюз	
192.168.6.1-254	пристрої	

Для того щоб можна було здійснити підключення з одного комп'ютера або пристрою офісної будівлі до іншого комп'ютера або пристрою в магазині потрібно налаштувати протокол RIP. Але перед тим необхідно налаштувати з'єднання між маршрутизаторами маршрутизатори. Для цього слід прописати IP-адресу та маску підмережі для інтерфейсів, за допомогою яких підключенні маршрутизатори один до одного. Наприклад для маршрутизатора офісу для порту Serial0/2/0 припишемо IP-адресу та маску підмережі який з'єднаний з портом маршрутизатора магазину.

in se0/2/0

ip address 10.10.10.5 255.255.255.0

Аналогічним чином слід прописати IP-адресу та маску підмережі для інтерфейсів маршрутизаторів. І лише після того можна налаштовувати протокол RIP, для обчислення маршрутів. Потрібно увійти в налаштування RIP за допомогою спеціальної команди та скористатися ефективною другою версією, а після того ввести мережі, які братимуть участь у процесі RIP.

router rip

version 2

network 192.168.1.0

Таким самим чином слід налаштувати мережу складу, логічна топологія якої зображено на рисунку 3.11.

В результаті налаштування якої було отримано таблицю 3.9 список IP-адрес, де вказана відповідна VLAN та таблицю 3.10, де вказано адресацію пристрої.

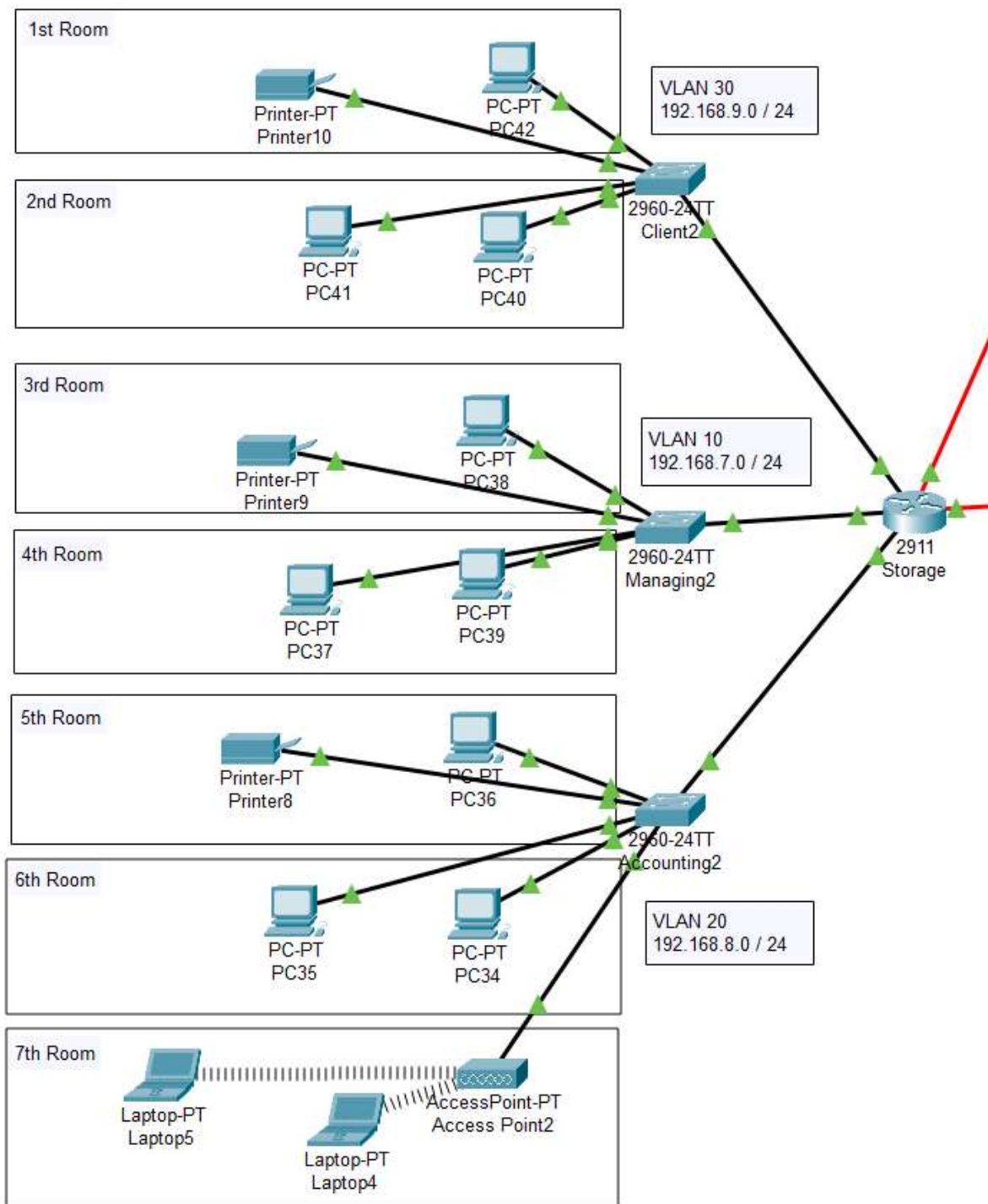


Рисунок 3.11 – Логічна топологія мережі складу

Зм.	Арк.	№докум.	Підпис	Дата

Таблиця 3.9 – Список IP-адрес для складу

IP-адреса	Примітка	VLAN
192.168.7.0 / 24	Менеджмент	10
192.168.7.1	шлюз	
192.168.7.1-254	пристрої	
192.168.8.0 / 24	Бухгалтерія	20
192.168.8.1	шлюз	
192.168.8.1-254	пристрої	
192.168.9.0 / 24	Клієнтська	30
192.168.9.1	шлюз	
192.168.9.1-254	пристрої	

Таблиця 3.10 – Таблиця адресації пристроїв для складу

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
Storage (модель 2911)	GigabiteEthernet0/0	192.168.9.0/24	255.255.255.0
	GigabiteEthernet0/1	192.168.7.0/24	255.255.255.0
	GigabiteEthernet0/2	192.168.8.0/24	255.255.255.0
	Serial0/1/0	10.10.10.1/30	255.255.255.252
	Serial0/1/1	10.10.10.10/30	255.255.255.252
PC40-PC42 Printer10	FastEthernet0	192.168.6.2- 5/24	255.255.255.0
PC37-PC39 Printer9	FastEthernet0	192.168.7.2- 5/24	255.255.255.0
Laptop4-5	Wireless0	192.168.5.7- 8/24	255.255.255.0
PC34-PC36 Printer8	FastEthernet0	192.168.5.2- 6/24	255.255.255.0

Для того щоб підключити мережу підприємства до Інтернету потрібно з'єднатися з Інтернет сервіс провайдером. Для даного моделювання використано маршрутизатор моделі 2911 та названо ISP. А також підключено до нього сервер і названо `www.cisco.com` для моделювання підключення пристроїв мережі в подальшому. Дане з'єднання маршрутизаторів показано на рисунку 3.12.

Маршрутизатор ISP було підключено до маршрутизатора офісної будівлі, шляхом встановлення IP-адреси та маски підмережі до їх інтерфейсів. Так само як і інші сервери слід налаштувати сервер `www.cisco.com`, а також налаштувати підключення до веб-сторінки. Після виконання всіх налаштувань було отримано наступну таблицю 3.11 з адресацією пристроїв.

Також для провести налаштування протоколу OSPF. Слід перейти до налаштувань одного з роутерів та вказати відповідні IP-адреси мережі, з якими він пов'язаний, та маску підмережі.

```
router ospf 10
network 10.10.10.1 255.255.255.252 area 0
```

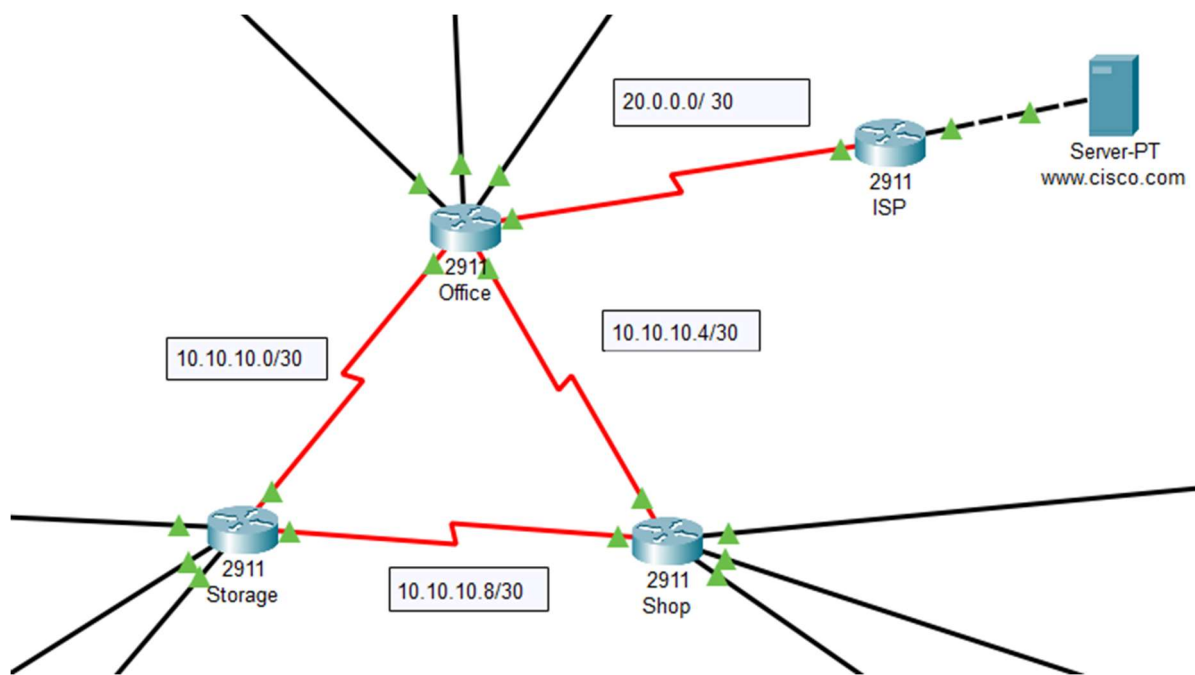


Рисунок 3.12 – З'єднання між трьома будівлями та підключення інтернет сервіс провайдером

Таблиця 3.11 – Таблиця адресації пристроїв після підключення ISP

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
Office (модель 2911)	Serial0/1/0	20.0.0.1/30	255.255.255.252
	Serial0/2/0	10.10.10.6/30	255.255.255.252
	Serial0/2/1	10.10.10.2/30	255.255.255.252
ISP	Serial0/2/0	20.0.0.2/30	255.255.255.252
	GigabiteEthernet0/0	192.168.50.1/ 24	255.255.255.0
www.cisco.com (Server-PT)	FastEthernet0	192.168.3.11/ 24	255.255.255.0

Для фільтрування трафіку потрібно прописати списки контролю доступу IP для кожного маршрутизатора і налаштувати їх для відповідного інтерфейсу. А для захисту сеансів слід налаштувати протокол SSH. Спочатку слід налаштувати доменне-ім'я.

ip domain-name office.com

Далі слід створити користувача з максимально можливим рівнем повноважень і паролем.

username admin privilege 15 secret cisco

Далі налаштувати VTY, де значення 0-4 означає, що пристрій може дозволити п'ять одночасних віртуальних з'єднань, які можуть бути SSH та дозволити тільки SSH з'єднання.

vty 0 4

login local

transport input ssh

Для того щоб згенерувати пару ключів шифрування RSA з модулем 1024 слід використати наступну команду.

crypto key generate rsa

Паролі встановлені для пристроїв вказані в таблиці 3.12.

Таблиця 3.12 – Паролі для пристроїв мережі

Назва пристроїв	Пароль
Office	cisco
Storage	cisco1
Shop	cisco2
Client0	client0
Accounting0	accounting0
Managing0	managing0
Client1	client1
Accounting1	accounting1
Managing1	managing1
Client2	client2
Accounting2	accounting2
Managing2	managing2

3.4 Розрахунок вартості мережі

Було проведено дослідження цін в інтернет-магазинах і створено таблицю 3.13 з розрахунками пристроїв і в підсумку загальної вартості створення мережі підприємства.

Таблиця 3.13 – Розрахунки вартості мережі підприємства

Пристрій	Модель	Кількість	Ціна, грн. (за 1 шт.)	Загальна ціна, грн.
1	2	3	4	5
Маршрутизатор	Cisco 2911/K9	3	15 000	45 000

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи проведено дослідження та аналіз предметної області про проектування комп'ютерних мереж. В результаті проведеного аналізу обрано засоби та підходи для розробки мережі. Як результат, була спроектована, розроблена та реалізована комп'ютерна мережа організації з віддаленим доступом до ресурсів, яка забезпечує доступ до внутрішніх ресурсів компанії із зовнішньої мережі із достатнім рівнем захисту даних.

Було здійснено огляд та аналіз засобів для моделювання та дослідження мереж та обрано в якості такого пакет Packet Tracer від компанії Cisco. За допомогою цього середовища розроблено фізичну та логічну схеми мережі, виконано налаштування пристроїв безпеки, налаштування комутаторів, маршрутизаторів, кінцевих пристроїв, для забезпечення проходження дозволеного та блокованого трафіку.

Результати тестування мережного трафіку показали коректність та правильність налаштування пристроїв для забезпечення параметрів безпеки мережі.

Вимоги до мережі виконано у повному обсягу. Розроблена мережа має широкий простір для удосконалення, доповнення, розширення та модернізації згідно з побажаннями замовника.

					КвРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		62

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ

1 Yaibuates M. Implementing of IP address Recovery for DHCP Service. / M. Yaibuates, R. Chaisricharoen, C. Rai // International Journal of Applied Engineering Research, 2018. – Pp. 2659-2662.

2 Dumitrache C. G. Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer / C. G. Dumitrache, G. Predusca, L. D. Circiumarescu, N. Angelescu, D. C. Puchianu, // In 2017 5th International Symposium on Electrical and Electronics Engineering, 2017. – Pp. 1-6.

3 Ajani, A. A. Comparative performance evaluation of open shortest path first, OSPF and routing information protocol, RIP in network link failure and recovery cases / A. A. Ajani, B. J. Ojuolape, A. A. Ahmed, T. Aduragba, M. Balogun // In 2017 IEEE 3rd International Conference on Electro-Technology for National Development, 2017. –Pp. 280-288.

4 Wai K. K. Analysis of RIP, EIGRP, and OSPF Routing Protocols in a Network / Wai K. K. // International Journal of Trend in Scientific Research and Development, 2019. – p. 5.

5 Jati W. S. Perbandingan Kinerja Protocol Routing Open Shortest Path First (OSPF) dan Routing Information Protocol (RIP) Menggunakan Simulator Cisco Packet Tracer / W. S. Jati, H. Nurwasito, M. Data // Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, 2018. –p. 258

6 Gyi, M. M., & San San Naing, P. E. S. (2019). Performance of Best Route Selection using RIP and OSPF Routing Protocols. time out, 9, 11.

7 McLaren P. Decrypting live SSH traffic in virtual environments / P. McLaren, G. Russell, W. J. Buchanan, Z. Tan, // Digital Investigation, 2019 – Pp. 109-117.

8 Gu M. M. On component connectivity of hierarchical star networks / M. M. Gu, J. M. Chang, R. X. Hao // International Journal of Foundations of Computer Science, 2020. – Pp. 313-326

9 Канальний рівень моделі OSI [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Канальний_рівень. – Назва з екрана. (електронне джерело).

10 Мережевий рівень моделі OSI [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Мережевий_рівень. – Назва з екрана. (електронне джерело).

11 Демілітаризована зона [Електронний ресурс] Режим доступу: http://nickshevtsov.blogspot.com/2017/11/blog-post_86.html. – Назва з екрана. (електронне джерело).

12 Stateful inspection [Електронний ресурс] Режим доступу: <https://www.techtarget.com/searchnetworking/definition/stateful-inspection>. – Назва з екрана. (електронне джерело).

13 Мережева модель OSI [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Мережева_модель_OSI. – Назва з екрана. (електронне джерело).

14 Канальний рівень моделі OSI [Електронний ресурс] Режим доступу: <https://static-course-assets.s3.amazonaws.com/ITE50UK/course> – Назва з екрана. (електронне джерело).

15 Комутатор [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/Мережевий_комутатор. – Назва з екрана. (електронне джерело).

16 Боршевніков, А. Е. Мережеві атаки. Види. Способи боротьби (2011)

17 Информационная безопасность : учебное пособие. – Москва : РГ- Пресс, 2020. – 144 с.

18 Диогенес Ю., Озкая Э. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.: ил.

19 Адресс Джейсон. Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с

20 Aditya Mukherjee. Network_Security_Strategies 2020. - 390с.

					КВРКІ. 180242.18.02.15 ПЗ	Арк. 64
Зм.	Арк.	№докум.	Підпис	Дата		

21 Sai Huda. Next Level Cybersecurity. Detect the Signals, stop the Hack. 2021.
– 220с.

22 Офіційний сайт компанії Cisco Packet Tracer (Електронний ресурс) Режим доступу: [www/ URL: https://www.cisco.com/](http://www.cisco.com/)

23 У. Одом "Офіційне керівництво Cisco по підготовці до сер-тіфікаційним іспитів CCNA ICND2 200-101. Маршрутизація і комутація" (2016)

24 Офіційний сайт емулятора GNS 3 (Електронний ресурс). Режим доступу: [www/ URL: https://gns3.com/](http://www.gns3.com/)

25 Офіційний сайт емулятора SNMP Agent Simulator (Електронний ресурс). Режим доступу: [www/ URL: https://veraxsystems.com/](http://www.veraxsystems.com/)

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		65

ДОДАТОК Б
(обов'язковий)

Налаштування мережних пристроїв

Маршрутизатор Shop:

Current configuration : 4280 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Office

!

enable password cisco

!

!

ip dhcp excluded-address 192.168.1.1

ip dhcp excluded-address 192.168.1.254

ip dhcp excluded-address 192.168.1.11

ip dhcp excluded-address 192.168.2.1

ip dhcp excluded-address 192.168.2.254

ip dhcp excluded-address 192.168.2.11

ip dhcp excluded-address 192.168.3.1

ip dhcp excluded-address 192.168.3.254

ip dhcp excluded-address 192.168.3.11

ip dhcp excluded-address 192.168.1.10

ip dhcp excluded-address 192.168.2.10

ip dhcp excluded-address 192.168.3.10

!

ip dhcp pool Managing0-pool

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 192.168.1.11

ip dhcp pool Accounting0-pool

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

dns-server 192.168.2.11

ip dhcp pool Client0-pool

network 192.168.3.0 255.255.255.0

default-router 192.168.3.1

dns-server 192.168.3.11

!

!

!

no ip cef

no ipv6 cef

!

username admin privilege 15 password 0 cisco

					КВРКІ. 180242.18.02.15 ПЗ	Арк. 68
Зм.	Арк.	№докум.	Підпис	Дата		

```

!
!
license udi pid CISCO2911/K9 sn FTX1524V8IB-
!
ip domain-name oficesecurity.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group From-SCisco in
ip access-group OAL010 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
ip access-group From-SCisco in
ip access-group AAL020 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.3.1 255.255.255.0
ip access-group From-SCisco in
ip access-group CAL030 out
duplex auto
speed auto
!
interface Serial0/1/0
ip address 20.0.0.1 255.255.255.252
ip access-group From-outside in
clock rate 64000
!
interface Serial0/1/1
no ip address
clock rate 2000000
!
interface Serial0/2/0
ip address 10.10.10.6 255.255.255.252
ip access-group From-SCisco in
clock rate 64000
!
interface Serial0/2/1
ip address 10.10.10.2 255.255.255.252
ip access-group From-SCisco in
clock rate 64000
!
interface Vlan1
ip address 192.168.100.2 255.255.255.0
shutdown
!

```

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		69

```

router ospf 10
log-adjacency-changes
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
! router rip
version 2
network 10.0.0.0
network 20.0.0.0
network 192.168.1.0
network 192.168.2.0
network 192.168.3.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard OAL010
deny 192.168.2.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
ip access-list standard AAL020
deny 192.168.1.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list extended From-SCisco
permit tcp 192.168.1.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.2.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.3.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.4.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.5.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.6.0 0.0.0.255 host 192.168.50.2 eq www
deny ip 192.168.1.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.2.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.3.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.4.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.5.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.6.0 0.0.0.255 host 192.168.50.2
permit ip any any
ip access-list extended From-outside
deny ip any 192.168.1.0 0.0.0.255
deny ip any 192.168.2.0 0.0.0.255

```

					КВРКІ. 180242.18.02.15 ПЗ	Арк. 70
Зм.	Арк.	№докум.	Підпис	Дата		

```

deny ip any 192.168.3.0 0.0.0.255
deny ip any 192.168.4.0 0.0.0.255
deny ip any 192.168.5.0 0.0.0.255
deny ip any 192.168.6.0 0.0.0.255
deny tcp any host 20.0.0.2 eq telnet
permit ip any host 20.0.0.2
ip access-list standard CAL030
deny 192.168.1.0 0.0.0.255
deny 192.168.2.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
!
no cdp run
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
!
!
end

```

Маршрутизатор Shop:

Building configuration...

```

Current configuration : 2769 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Shop
!
!
!
enable password cisco2
!
!
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.4.254
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.5.254
ip dhcp excluded-address 192.168.6.1
ip dhcp excluded-address 192.168.6.254
ip dhcp excluded-address 192.168.6.10

```

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		71

```

ip dhcp excluded-address 192.168.5.10
ip dhcp excluded-address 192.168.4.10
!
ip dhcp pool Managing1-pool
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
dns-server 192.168.1.11
ip dhcp pool Accounting1-pool
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
dns-server 192.168.2.11
ip dhcp pool Client1-pool
network 192.168.6.0 255.255.255.0
default-router 192.168.6.1
dns-server 192.168.3.11
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$yG9qv7LLYVv0YzwRYtdTM/
!
!
license udi pid CISCO2911/K9 sn FTX1524D21C-
!
ip domain-name shopsecurity.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.5.1 255.255.255.0
ip access-group AAC120 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.4.1 255.255.255.0
ip access-group MAL110 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.6.1 255.255.255.0
ip access-group CAC130 out
duplex auto
speed auto
!
interface Serial0/2/0
ip address 10.10.10.5 255.255.255.252

```

					КВРКІ. 180242.18.02.15 ПЗ	Арк. 72
Зм.	Арк.	№докум.	Підпис	Дата		

```

!
interface Serial0/2/1
ip address 10.10.10.9 255.255.255.252
!
interface Vlan1
ip address 192.168.100.3 255.255.255.0
shutdown
!
router ospf 10
log-adjacency-changes
network 10.10.10.4 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
!
router rip
version 2
network 10.0.0.0
network 192.168.4.0
network 192.168.5.0
network 192.168.6.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard MAL110
deny 192.168.2.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard AAC120
deny 192.168.1.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard CAC130
deny 192.168.1.0 0.0.0.255
deny 192.168.2.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
!

```

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		73

```
line con 0
!  
line aux 0
!  
line vty 0 4
login local
transport input ssh
!  
end
```

Маршрутизатор Storage:

```
Current configuration : 2810 bytes
!  
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!  
hostname Storage
!  
!  
enable password cisco1
!  
!  
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.9.254
ip dhcp excluded-address 192.168.8.254
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.7.1
ip dhcp excluded-address 192.168.7.254
ip dhcp excluded-address 192.168.7.10
ip dhcp excluded-address 192.168.8.10
ip dhcp excluded-address 192.168.9.10
!  
ip dhcp pool Managing2-pool
network 192.168.7.0 255.255.255.0
default-router 192.168.7.1
dns-server 192.168.1.11
ip dhcp pool Accounting2-pool
network 192.168.8.0 255.255.255.0
default-router 192.168.8.1
dns-server 192.168.2.11
ip dhcp pool Client2-pool
network 192.168.9.0 255.255.255.0
default-router 192.168.9.1
dns-server 192.168.3.11
!  
!  
!  
no ip cef
no ipv6 cef
!
```

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		74

```

!
!
username admin privilege 15 secret 5 $1$mERr$q.MA2tj.WFptzvbifq/1i.
!
!
license udi pid CISCO2911/K9 sn FTX1524Q23E-
!
ip domain-name storagesecurity.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.9.1 255.255.255.0
ip access-group CAL230 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.7.1 255.255.255.0
ip access-group MAC210 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.8.1 255.255.255.0
ip access-group MAC210 out
duplex auto
speed auto
!
interface Serial0/1/0
ip address 10.10.10.1 255.255.255.252
!
interface Serial0/1/1
ip address 10.10.10.10 255.255.255.252
clock rate 64000
!
interface Vlan1
ip address 192.168.100.1 255.255.255.0
shutdown
!
router ospf 10
log-adjacency-changes
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0
network 192.168.9.0 0.0.0.255 area 0
network 192.168.8.0 0.0.0.255 area 0
network 192.168.7.0 0.0.0.255 area 0
!
router rip
version 2
network 10.0.0.0
network 192.168.6.0

```

					КВРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		75

```
network 192.168.7.0
network 192.168.9.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard MAC210
deny 192.168.2.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard AAC220
deny 192.168.1.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard CAL230
deny 192.168.1.0 0.0.0.255
deny 192.168.2.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
!
no cdp run
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
end
```

					КвРКІ. 180242.18.02.15 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		76

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Дола Павло Ігорович

Тема Комп'ютерна мережа організації з віддаленим доступом до ресурсів

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 2; кількість сторінок записки 76

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та налаштовано комп'ютерну мережу для організації з віддаленим доступом до ресурсів із необхідними параметрами безпеки по трафіку.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, У першому розділі проведено огляд та аналіз сучасних комп'ютерних мереж за захисту даних у них, виконана постановка задачі. В другому розділі виконано аналіз відомих засобів для моделювання та дослідження роботи мереж та обґрунтовано вибір пакету для роботи. В третьому розділі розроблено фізичну та логічну топологію мережі, обрано схему адресації та маршрутизації, проведено конфігурування всіх мережних пристроїв, протестовано проходження трафіку через мережу, визначено вартість впровадження проекту.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Практична цінність результатів дослідження полягає в обґрунтуванні вибору засобів та їх налаштуванню для побудови комп'ютерних мереж з віддаленим доступом до ресурсів

5. Негативні сторони роботи В роботі відсутній деталізований опис розробки схеми адресації.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «задовільно».

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

Мероцимо Валерій Володимирович,
зав. кафедрою керування автомобільною та
мобільною територіально-транспортними технологіями

« 13 » 06 2022р.

(підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

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 організації з віддаленим доступом до ресурсів

Автор: Дола Павло Ігорович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: Програмування та захист комп'ютерних систем і мереж

Науковий керівник: Мостовий С.В.

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). 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 (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). 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.	
5	Інше:	

Підтвердження:

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


- 1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
- 2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
- 3) окремі виявлені збіги є загальноживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
- 4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 19.0% і адресується до 240 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

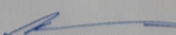
Керівник роботи

Завідувач кафедри КБ, гарант ОП

Дата: 14.06.2022



С.В. Мостовий



Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 10.0%

Словари проверки: en_US, ru_RU, ua_UA. Ошибок в документах: 12%

ID: 105248 Название: Комп'ютерна мережа організації з віддаленим доступом до ресурсів Добавлено в БД: 2022-06-14 Авторы: Дола Павло Ігорович Руководители: Мостовий С.В. Консультанты: Оponentы:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	60511	531	1906 (21%)	237 (19%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
14.06.2022 14:52:06 EEST

Дата звіту:
14.06.2022 14:54:42 EEST

ID перевірки:
1011577073

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: **На плагіат Дола**

Кількість сторінок: 66 Кількість слів: 11715 Кількість символів: 84615 Розмір файлу: 5.02 MB ID файлу: 101144710

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

19% Схожість

Найбільша схожість: 9.56% з джерелом з Бібліотеки (ID файлу: 1011427887)

Не знайдено джерел з Інтернету

19% Джерела з Бібліотеки

2

Сторінка 68

0.07% Цитат

Цитати

1

Сторінка 69

Не знайдено жодних посилань

4.21% Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 2%)

4.1% Вилучення з Інтернету

232

Сторінка 70

0.11% Вилученого тексту з Бібліотеки

102

Сторінка 71

Модифікації

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

Замінені символи

16

Підозріле форматування

14
сторінок