Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Захищена комп'ютерна мережа малого офісу
Назва теми

КвРКІ. 180242.*18.02.15 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 Р.Р.Степанюк Ініціали, прізвище

Керівник _____ 13.06.22 Підпис, дата С.В. Мостовий Ініціали, прізвище

Нормоконтролер _____ 13.06.22 Підпис, дата С.В. Мостовий Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Підпис Ю.П. Кльоц Ініціали, прізвище

«13» червня 2022 р.

Хмельницький 2022

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

Степанюку Ростиславу Романовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Захищена комп'ютерна мережа малого офісу

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 (Е8)

Фізична топологія мережі (Е8)

Результати тестування трафіку в мережі (Е8)

6. Консультанти розділів дипломного проекту (

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., ст. викладач	-	
Антиплагіат	Мостовий С.В., ст. викладач	-	

7. Дата видачі завдання «_01_»_____03_____2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Підготовка вступного розділу	Березень - 1 декада	
2.	Огляд існуючих методів, засобів	Березень - 2 декада	
3.	Обгрунтування обраних рішень	Березень - 3 декада	
4.	Підготовка опису логічної та фізичної топології	Квітень - 1 декада	
5.	Виконання розрахункової частини	Квітень - 1 декада	
6.	Підготовка ескізів креслень	Квітень - 2 декада	
7.	Формулювання висновків	Квітень - 3 декада	
8.	Розробка додатків	Травень - 1 декада	
9.	Погодження розділів з консультантом з нормоконтролю	Травень - 1 декада	
10.	Оформлення графічного матеріалу	Травень - 2 декада	
11.	Оформлення пояснювальної записки	Травень - 2 декада	
12.	Попередній захист кваліфікаційної роботи	Травень - 3 декада	
13.	Доопрацювання кваліфікаційної роботи	Травень - 3 декада	
14.	Подання роботи для перевірки на плагіат	Травень - 3 декада	
15.	Захист кваліфікаційної роботи	Червень - 1 декада	

Студент Підпис Р.Р. Степанюк (Ініціали, прізвище)

Керівник проекту (роботи) Підпис С.В. Мостовий (Ініціали, прізвище)

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ. 180242.18.02.15 ПЗ	Пояснювальна записка	64		
			Графічні матеріали			
2		КвРКІ. 180242.18.02.15 Е8	Логічна топологія	1		
			мережі			
3		КвРКІ. 180242.18.02.15 Е8	Фізична топологія	1		
			мережі			

КвРКІ. 180242.18.02.15 ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Степанюк Р.Р.		13.06.22
Перевір.		Мостовий С.В.		13.06.22
Н. контр.		Мостовий С.В.		13.06.22
Затв.		Кльоц Ю.П		13.06.22

Відомість проекту

Літера	Аркуш	Аркушів
У	1	1

ХНУ, КІ-18-2

АНОТАЦІЯ

Тема кваліфікаційної роботи: «*Захищена комп'ютерна мережа малого офісу*».

Автор роботи: *Степанюк Ростислав Романович*
Керівник роботи: *Мостовий Сергій Володимирович.*
Пояснювальна записка:*64 с., 46 рис., 4 табл., 19 джерел.*
Графічна частина: 2 креслення.

Метою даної роботи є розробка захищеної комп'ютерної мережі для малого офісу

Під час виконання кваліфікаційної роботи, було спроектовано комп'ютерну мережу для невеликого офісу. Для реалізації мережі було обрано та налаштовано відповідне обладнання (реалізовані конфігураційні файли). Мережа була змодельована та протестована у програмному середовищі Packet Tracer.

13.06.22

ЗМІСТ

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

ВСТУП

Прагнення до взаємодії і спілкування один з одним серед всіх найважливіших для існування людей потреб не сильно відстає у потребі підтримки життєдіяльності. Спілкування для людей майже так само необхідне та важливе, як і потреба в їжі, сонячному світлі та житлі. І цю потребу частково вирішили комп'ютерні мережі.

Комп'ютерні мережі або мережі передачі даних є логічним результатом еволюції двох важливих науко-технічних галузей сучасної цивілізації – обчислювальної техніки та телекомунікаційних технологій.

Завдяки комп'ютерним мережам люди у сучасному світі пов'язані між собою як ніколи раніше. Вони отримали змогу миттєво обмінюватись ідеями та думками між собою. Світові новини та події стають відомими усій землі за лічені секунди. Люди, розділені морями та океанами, можуть моментально виходити на зв'язок та взаємодіяти між собою.

Досягнення у сфері мережевих технологій – це, мабуть, найвагоміші зміни за останні часи у світі.

Актуальність теми практики полягає у аналізі та виборі прийнятних засобів для побудови мережі, що забезпечить її захищеність та інформаційну безпеку роботи 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.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальні принципи побудови локальних мереж

Головною ціллю об’єднання комп’ютерів в одну мережу є розділення ресурсів, спільне вирішення інформаційних та обчислювальних задач. Користувачі цих мереж отримують можливість автоматичного доступу до різних ресурсів, які знаходяться разом з ними в локальній мережі, наприклад: принтери, сканери, данні ,які знаходяться в оперативній пам’яті чи на зовнішніх накопичувальних пристроях та отримують додаткову обчислювальну потужність за рахунок запуску своїх програм на «сусідніх» комп’ютерах.

Архітектура корпоративної мережі включає в себе безпровідні і провідні зв’язки. Завдяки чому до неї можна під’єднати різні кінцеві пристрої, такі як принтери, робочі станції, IP телефони, ноутбуки, сканери та інші.

Головні цілі любої архітектури мережі:

– простота застосування – розгортання мережі в швидкі терміни;

– гнучкість та масштабність – модульна архітектура дозволяє впроваджувати тільки ті рішення, які необхідні в даний момент, з можливістю подальшого розвитку та масштабування мережевої архітектури;

– відмовостійкість і безпека – захист користувацького трафіку, виконання, що гарантує стабільну роботу мережі навіть під час атак [4];

– простота в управлінні – централізоване управління всією мережевою інфраструктурою;

– готовність до нових технологій – побудована архітектура дозволяє легко впроваджувати нові сервіси та технології.

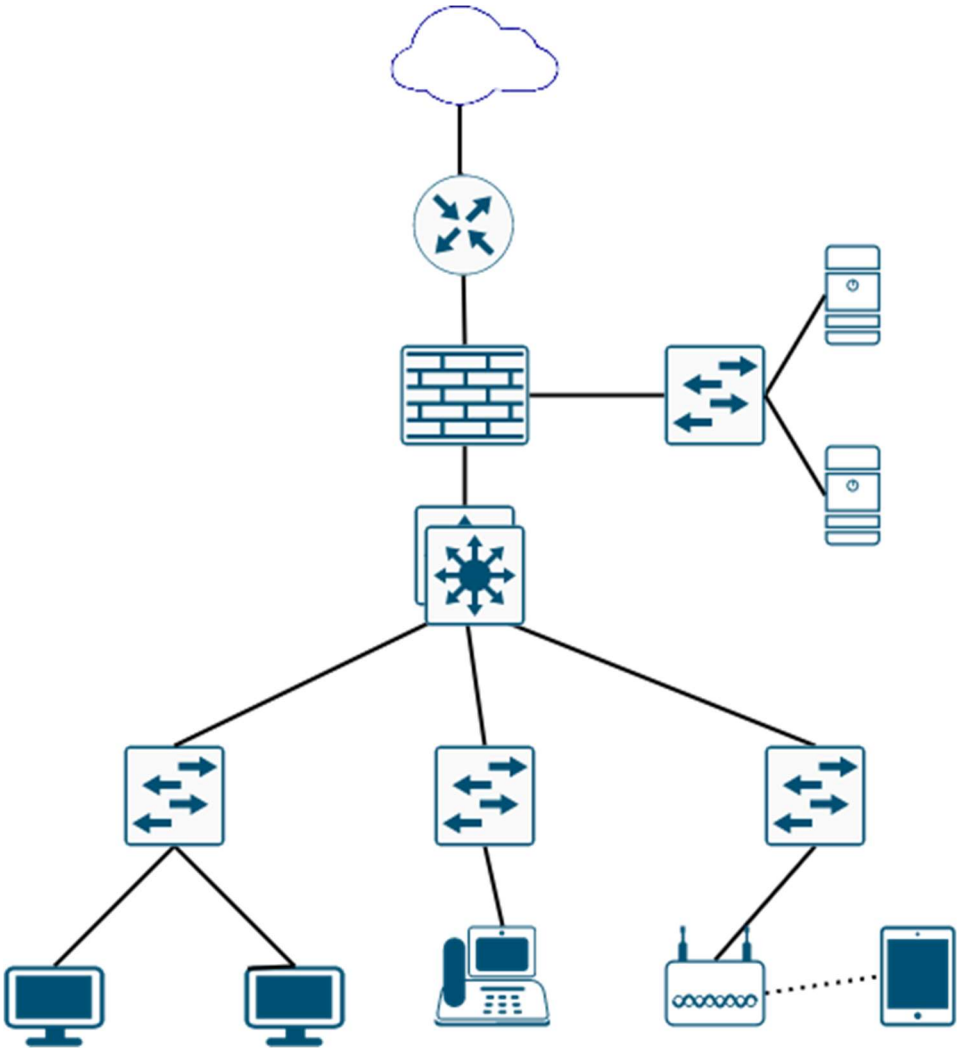


Рисунок 1.1 – приклад архітектура невеликої корпоративної мережі

Розбивши мережеву архітектуру на модулі можна сконцентруватись на функціоналі кожного з них по окремо, що значно спрощує дизайн, впровадження та управління. Потім з таких модулів можна створити мережу, яка відповідає вашим вимогам.

Розбиття великої мережі на невеликі, прості для розуміння, модулі (рівні) сприяє стійкості мережі за рахунок локалізації проблем, що виникають. Таким чином, виникненні будь-якого збою в мережі необхідно визначити на якому рівні виникла помилка, потім приступати до її вирішення, не торкаючись при цьому інших модулів мережі.

1.2 Порівняльний аналіз переваг та недоліків існуючих рішень

Топологія мережі – це розташування мережних пристроїв та зв’язки між ними. Тепер трохи детальніше про класифікацію комп’ютерних мереж:

Локальні мережі (LAN) – це мережна інфраструктура, яка охоплює досить малу географічну прощу. Така мережа обслуговує будинок або кампус.

Глобальні мережі (WAN) – вони з’єднують локальні мережі. Така інфраструктура займає досить значну географічну площу. А згодом і WAN об’єднуються в одну мережу і тоді вони охоплюють цілі континенти.

Існує декілька типів топологій, які використовують для опису LAN і WAN мережі:

– фізична топологія – показує фізичні з’єднання між проміжними та кінцевими пристроями. Також вона може містити в собі конкретне розташування пристрою, наприклад номер кімнати і місце розташування у мережевій шафі.

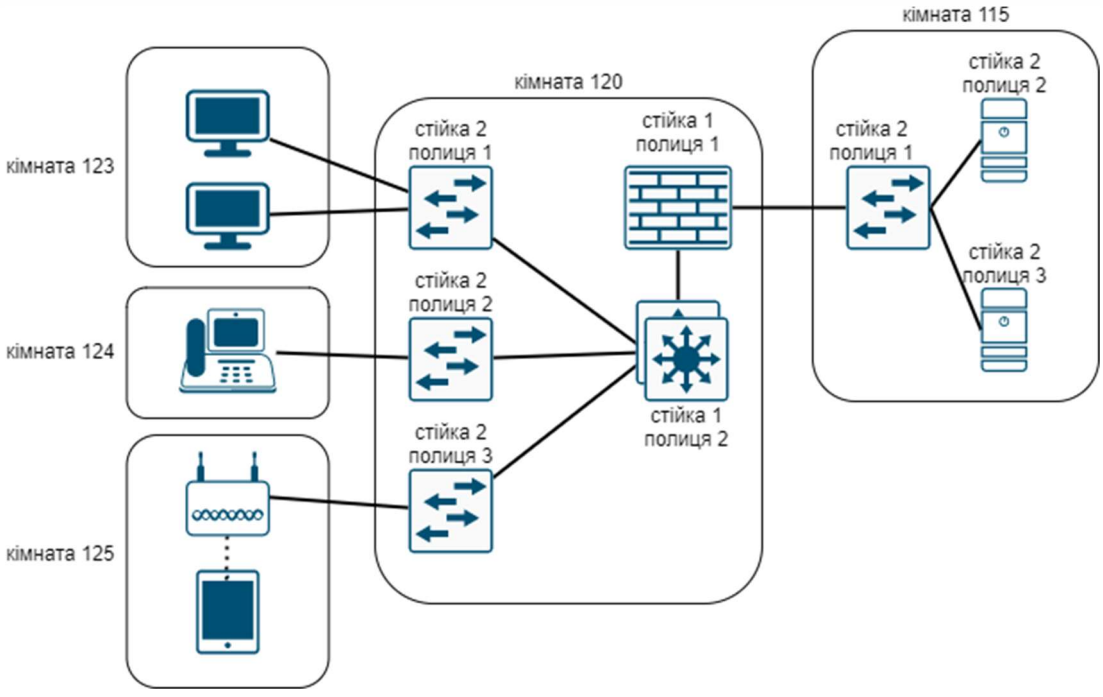


Рисунок 1.2 – Приклад фізичної топологія

– Логічна топологія – показує те, яким шляхом мережа передає кадри від вузла до вузла. На цій топології зазначаються віртуальні інтерфейси та IP-адреси.

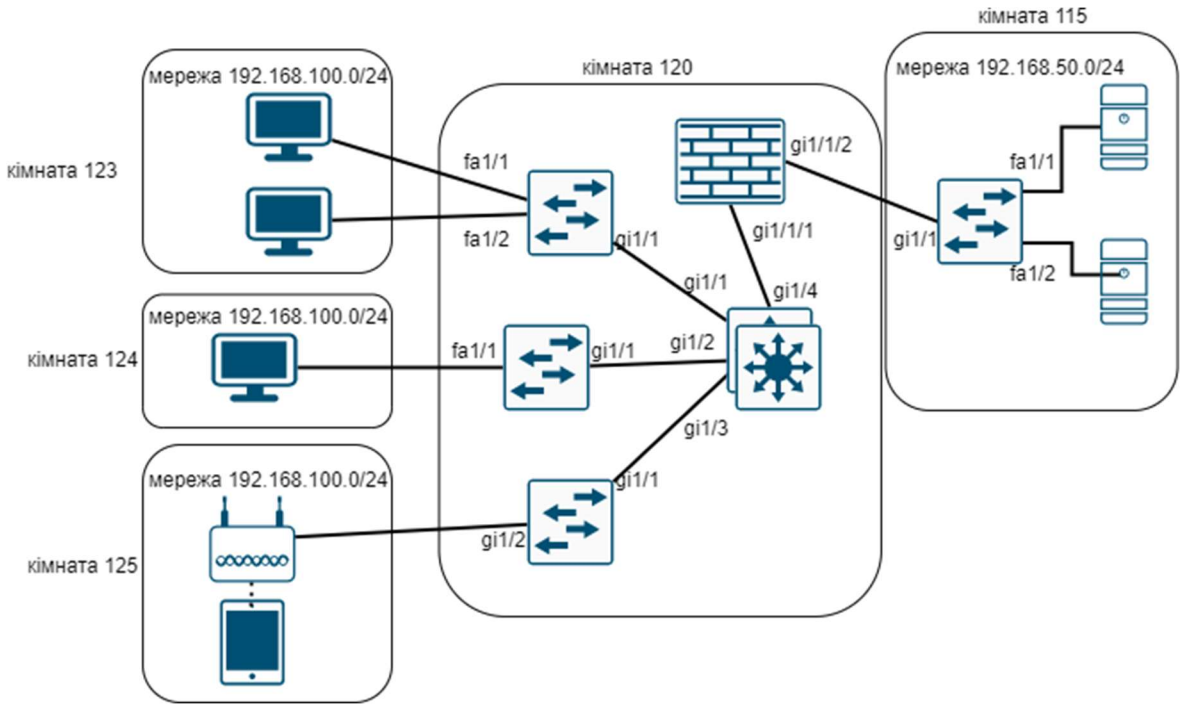


Рисунок 1.3 – Приклад логічної топологія

Типи фізичних топологій:

– шина – у цій топології кожен кінцевий пристрій під'єднаний до загального магістрального кабелю. На кінці кабелю встановлений ковпачок, який має назву – заглушка або термінатор. Заглушка слугує перешкодою для сигналів і перешкоджає виникненню помилок та втрати інформації;

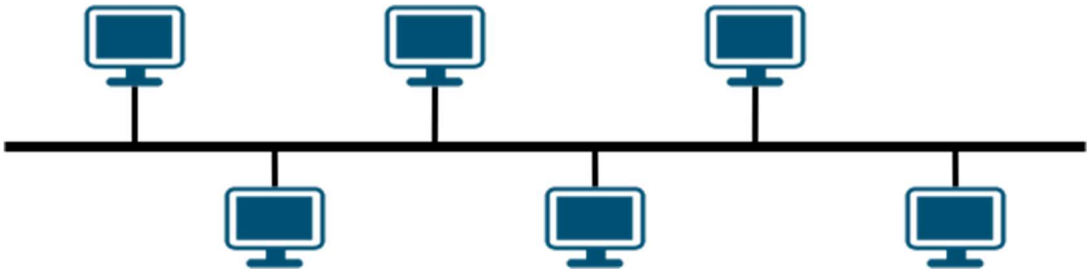


Рисунок 1.4 – Топологія шина (Bus network)

– кільце – кінцеві пристрої підключені один за одним до своїх сусідів, утворюючи кільце, тому тут не потрібен термінатор. А отже кожен сигнал передається по кругу і проходить через кожен кінцевий пристрій;

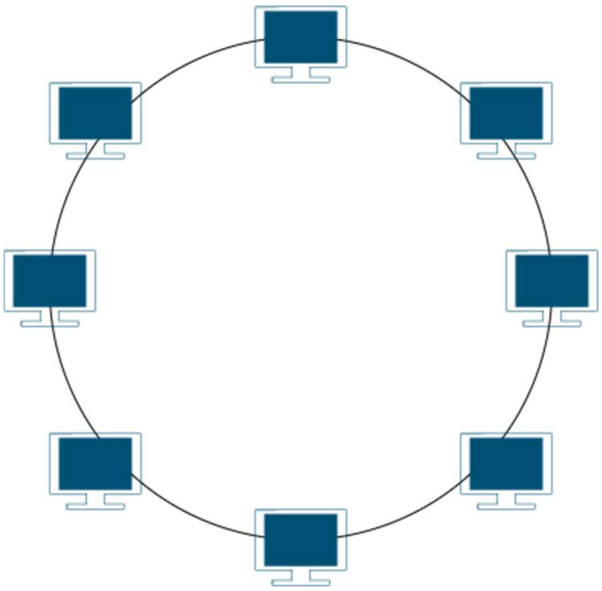


Рисунок 1.5 – Топологія кільце (Ring network)

– зірка – ця топологія відрізняється від інших, тому що для обміну інформацією використовується центральний проміжний пристрій, який у свою чергу з’єднаний з кожним комп’ютером.

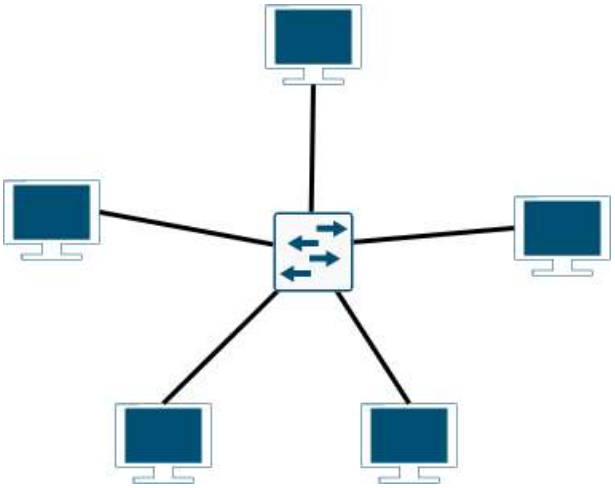


Рисунок 1.6 – Топологія зірка (Star network)

– розширена зірка – це логічне продовження топології звичайної зірки. У цьому випадку тут наявні вже декілька центральних пристроїв, які з’єднані між собою.

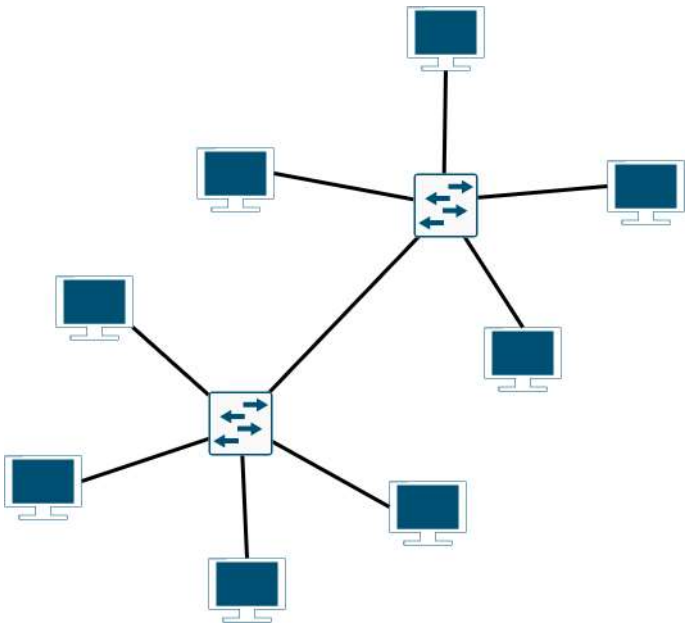


Рисунок 1.7 – Топологія розширена зірка (Extended star)

– Сіткоподібна топоплогія – вона ґрунтується на тому, що кожен хост на пряму під’єднаний до усіх інших хостів і забезпечує досить швидкий процес передавання даних.

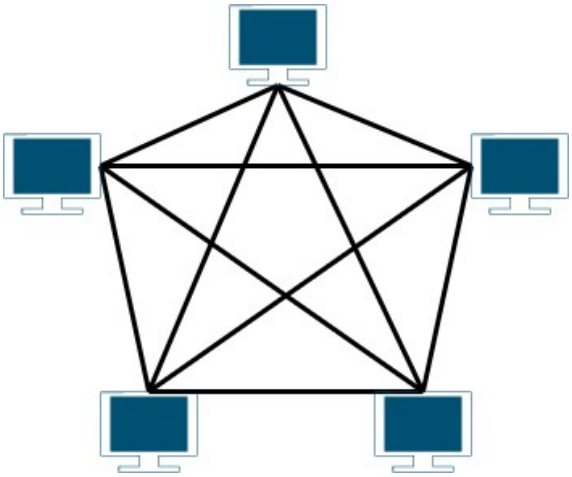


Рисунок 1.8 – Сіткоподібна топологія (Mesh)

Звичайно, кожна топологія має свої переваги і недоліки. Наприклад, топології шина не можна присвоїти властивість відмовостійкої адже критичним недоліком є те, що вразі виведення зі строю або пошкодження магістрального кабелю усі кінцеві пристрої втратять доступ до мережі. Така ж властивість присутня і в топології кільце. Адже при виникненні проблем в одного хоста, рух

інформації у мережі значно обмежиться. А з переваг таких інфраструктур є достатньо дешева вартість і простота реалізації.

Раніше до недоліків топології «зірка» можна було віднести достатньо високу ціну реалізації, адже для створення такої мережі потрібен був концентратор, але з розвитком безпровідних технологій, усім тепер доступні безпровідні точки доступу в яких і використовується саме ця топологія, які у свою чергу мають не високу ціну. Також в ній значно простіше знайти та виправити помилку у мережі.

На сьогоднішній день найпоширенішою є топологія розширеної зірки. Адже вона володіє такими якостями, як достатньо висока відмовостійкість, дешевизна впровадження і простота реалізації.

Комп'ютерні мережі мають ще декілька класифікацій. Наприклад, швидкість передачі та обміну інформації.

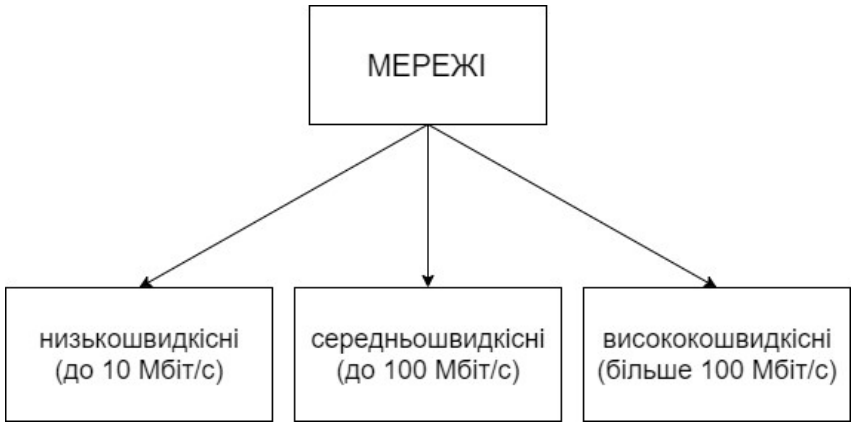


Рисунок 1.8 – Класифікація мереж за швидкістю

Також мережі поділяються за типом підключення кінцевих та проміжних пристроїв, як згадувалось вище. І звичайно в кожного підключення є свої недоліки та переваги.

Мідні кабелі є найпоширенішими в мережах, оскільки вони є недорогими, мають низький електричний опір та легко встановлюються. Проте з іншої сторони вони володіють обмеженою відстанню прокладання та впливом завад на сигнал. Дані передаються по кабелях у вигляді електричних імпульсів і чим більша відстань отримування, тим більше затухання сигналу. Також існують

електромагнітні або радіочастотні завади. Вони можуть спотворити чи погіршити сигнал, що передається по мідних носіях.

Волоконно-оптичний кабель використовується рідше через високу вартість. Це гнучка, але дуже прозора нитка з чистого скла. Для передачі даних біти кодуються у світлові імпульси. І саме через це він має властивості, які його роблять найкращим типом кабелю в певній ситуації. Він передає данні на величезні відстані з шаленою пропускною здатністю. Цей тип кабелю передає данні із значно меншим затуханням, на відміну від мідного кабелю.

Бездротове з'єднання зазвичай для передачі даних використовує електромагнітні або радіочастотні сигнали. Цей тип зв'язку може покрити велику географічну площу, але деякі будівельні матеріали або місцевий ландшафт можуть обмежити ефективне застосування. Також до однієї точки доступу може одночасно під'єднатися значна кількість користувачів, але у той же час велика кількість кінцевих пристроїв може значно знизити пропускну здатність, адже цей тип з'єднання використовує напівдуплексний режим.

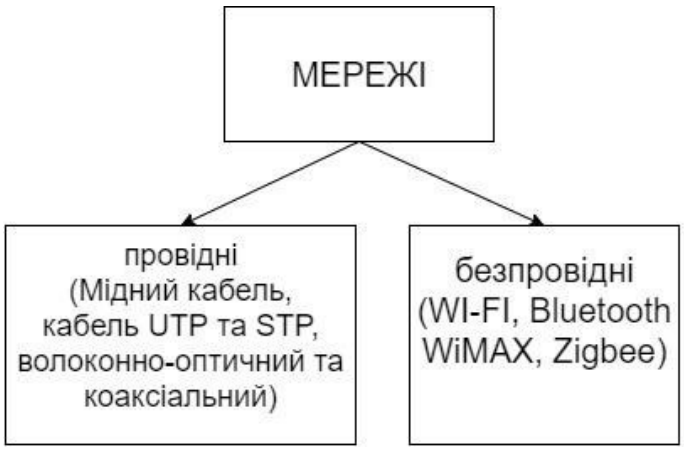


Рисунок 1.8 – Класифікація мереж за типом підключення

1.3 Методологічні підходи до вирішення задачі за темою дослідження

Для того, щоб побудувати мережу потрібні додаткові пристрої, які виконують певну роль в топології. До них відносяться:

Комутатор – мережевий пристрій, який використовується для з’єднання декількох вузлів чи хостів мережі в межах одного сегмента. Він використовує канальний рівень моделі OSI[1,6,7];

Рисунок 1.9 – Зовнішній вигляд комутатора та позначка в топології

Маршрутизатор (router) – використовується для об’єднання декількох мереж. Але основною задачею є маршрутизація трафіку між локальними мережами або в глобальну мережу. Для цього він використовує третій рівень моделі OSI[2,5];

Рисунок 1.10 – Зовнішній вигляд маршрутизатора та позначка в топології

Мережевий екран – інші назви: файрвол, брандмауер. Може мати вигляд окремого пристрою або програмного застосунку. Служить для аналізу, відмови чи доступу трафіку в мережі. У даному проекті основна увага буде належати саме йому. Може виконувати функції маршрутизатора. У залежності від задачі, може перевіряти трафік у двох режимах[3,8,9]:

– stateless – не відслідковує з’єднання між пристроями, а лише фільтрує трафік за чітко вказаними правилами;

– stateful – динамічна фільтрація пакетів. Аналізує трафік з відслідкуваням стану активних з’єднань і використовує цю інформацію для того, щоб вирішити, які пакети пропускати, а які відкидувати. Така перевірка з

відстеженням з’єднань працює в першу чергу на транспортному та мережевому рівні.

Рисунок 1.11 – Зовнішній вигляд мережевого екрана та позначка в топології

Лінії зв’язку та передачі даних – це проміжне та фізичне середовище, по якому передаються дані. Тому для побудови мережі використовуються тільки перевірені на справність кабелі.

Для моделювання та проектування захищеної мережі для підприємства я буду використовувати програмне забезпечення Cisco Packet Tracer. Це цілком безкоштовний та потужний програмний продукт для моделювання мереж.

Це віртуальна лабораторія, яка не потребує фізичного обладнання, була розроблена компанією Cisco для отримання практичних навичок роботи з мережами, Iot пристроями та кібербезпекою. Перевагою є те, що в цій програмі можна створювати проект з необмеженою кількістю абсолютно різних пристроїв. Та заздалегідь виявляти і виправляти помилки ще на стадії проекту.

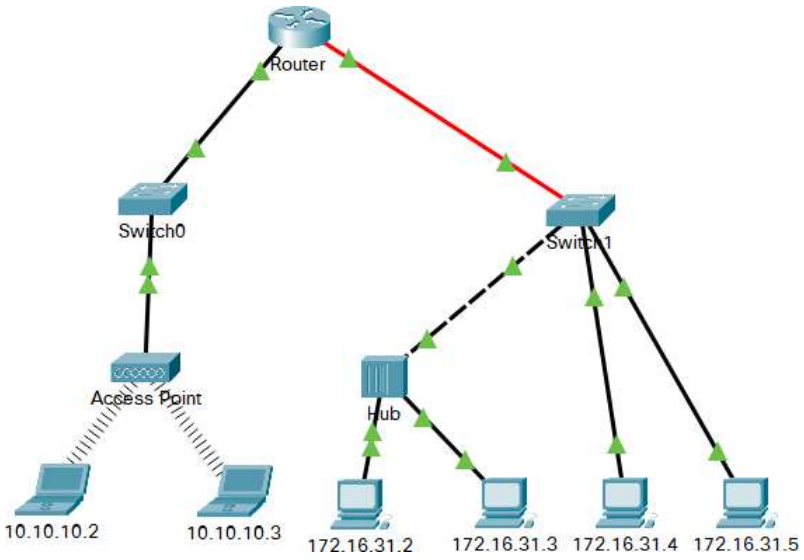


Рисунок 1.12 – Приклад роботи в Packet Tracer

1.4 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.

2 АНАЛІЗ ІСНУЮЧИХ ПРОГРАМ ТА ВИБІР АКТУАЛЬНОГО ВАРІАНТУ

2.1 Огляд і аналіз аналогів програм

Завдання комп'ютерного моделювання телекомунікаційних систем на сьогоднішній Одними з популярних продуктів є OPNET, OMNET ++, NS2, NS3, які є потужним день має досить багато рішень різного роду. засобом моделювання за рахунок об'єктно-орієнтованих мов програмування як вбудованої мови опису. Так само існують вузькоспеціалізовані симулятори, створені лише для моделювання певного моделей телекомунікаційних систем обладнання. забезпечення випускається виробниками телекомунікаційного обладнання Як правило, подібне програмне.

Компанією Cisco Systems, що є виробником мережевого устаткування, моделювання мереж, яке дозволяє експериментувати були запропоновано програмне забезпечення для з різними топологіями мереж і їх поведінкою всередині: симулятори Packet Tracer, Dynamips, GNS3.

2.1.1 Симулятор GNS3

Graphical Network Simulator (рис. 2.1) – це графічний симулятор мережі, з маршрутизаторів і віртуальних машин. Незамінний інструмент для навчання та тестів який дозволяє змоделювати віртуальну мережу. Працює практично на всіх платформах. стендів на десктопних машинах [18]. Дуже добре підходить для створення

Залежно від апаратної платформи, на якій буде використовуватися GNS3, , що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також можлива побудова комплексних проектів серверів під управлінням мережевих

операційних систем.

GNS3 має декілька серйозних недоліків:

– Сильно вимогливий до CPU і пам'яті. Використання процесора можна знизити за допомогою механізму Idle PC. Десяток маршрутизаторів вже всерйоз навантажать ПК.

– Дуже слабо підтримує функції L2. Є тільки подобу комутаторів, на яких і свічові плати для маршрутизаторів можна максимум налаштувати Access/Trunk порти, L2-функціонал яких також дуже обмежений.

– Відсутність можливості повноцінної симуляції комутаторів другого рівня Cisco. Цей недолік як його причиною є кардинальна відмінність в апаратній платформі не буде виправлений в нових версіях, так маршрутизаторів і світчей Cisco.

– До складу GNS3 не належать образи IOS / IPS / PIX / ASA / JunOS, так як відповідних компаній, і ніякого прямого відношення до проекту GNS3 вони є частиною комерційних продуктів не мають.

Однією з найцікавіших особливостей GNS3 є можливість перевірити на практиці будь-який можливість з'єднання проектованої топології з реальною мережею. Це дає просто унікальну проект, без використання реального обладнання. Використання WireShark дозволяє провести моніторинг трафіку всередині проектованої топології, що дає додаткову інформацію для розуміння досліджуваних технологій.

При відсутності можливості практично повноцінною лабораторією отримати доступ до реального обладнання, GNS3 стане.

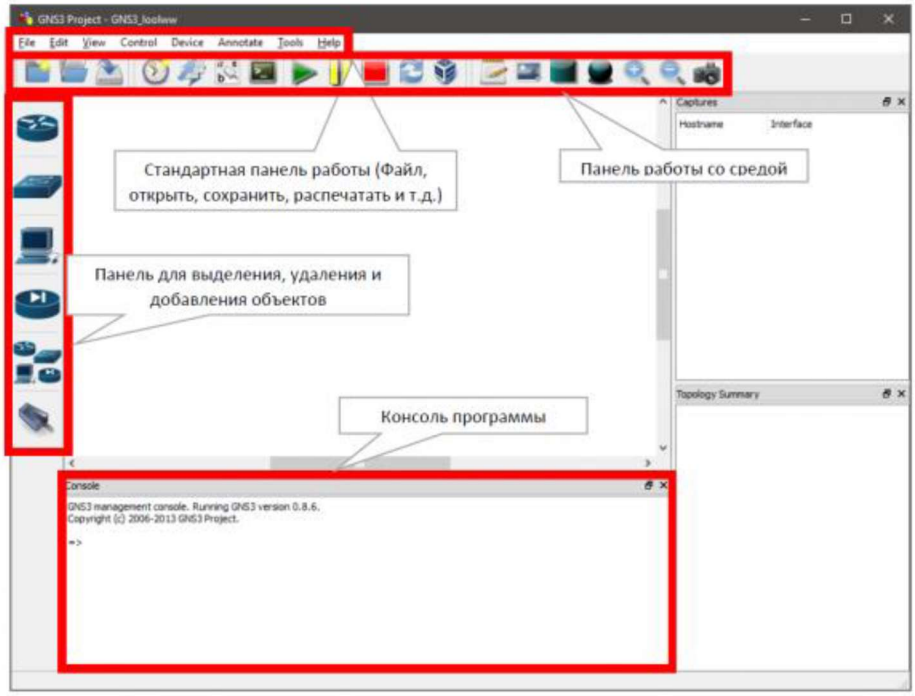


Рисунок 2.1 – Робочий простір GNS3 і його структура

2.1.2 Симулятор Verax SNMP Agent Simulator

Verax SNMP agent simulator дозволяє IT-персоналу створювати віртуальні моделюються мережі пристроїв без придбання будь-якого додаткового обладнання, наприклад, для тестування [19].

Verax кілька агентів SNMPv1 / v2c на одному хості через стандартний порт 161 через мульти-мережу. Окремі відповіді змодельованого агента можуть бути спочатку отримані з існуючих SNMP Simulator (рис. 2.2) – це інструмент, який може імітувати пристроїв і змінені під час виконання за визначеними користувачем правилами.

Продукт може події і шаблони поведінки або пасток. У варіанті віддаленого управління і в розподілених системах може бути кілька симуляторів, кожен має власне комбінувати різні поведінки агентів, налаштовувати движок і графічну консоль управління. У множині варіанті застосування симуляторів – центральне управління має одна проста консоль.

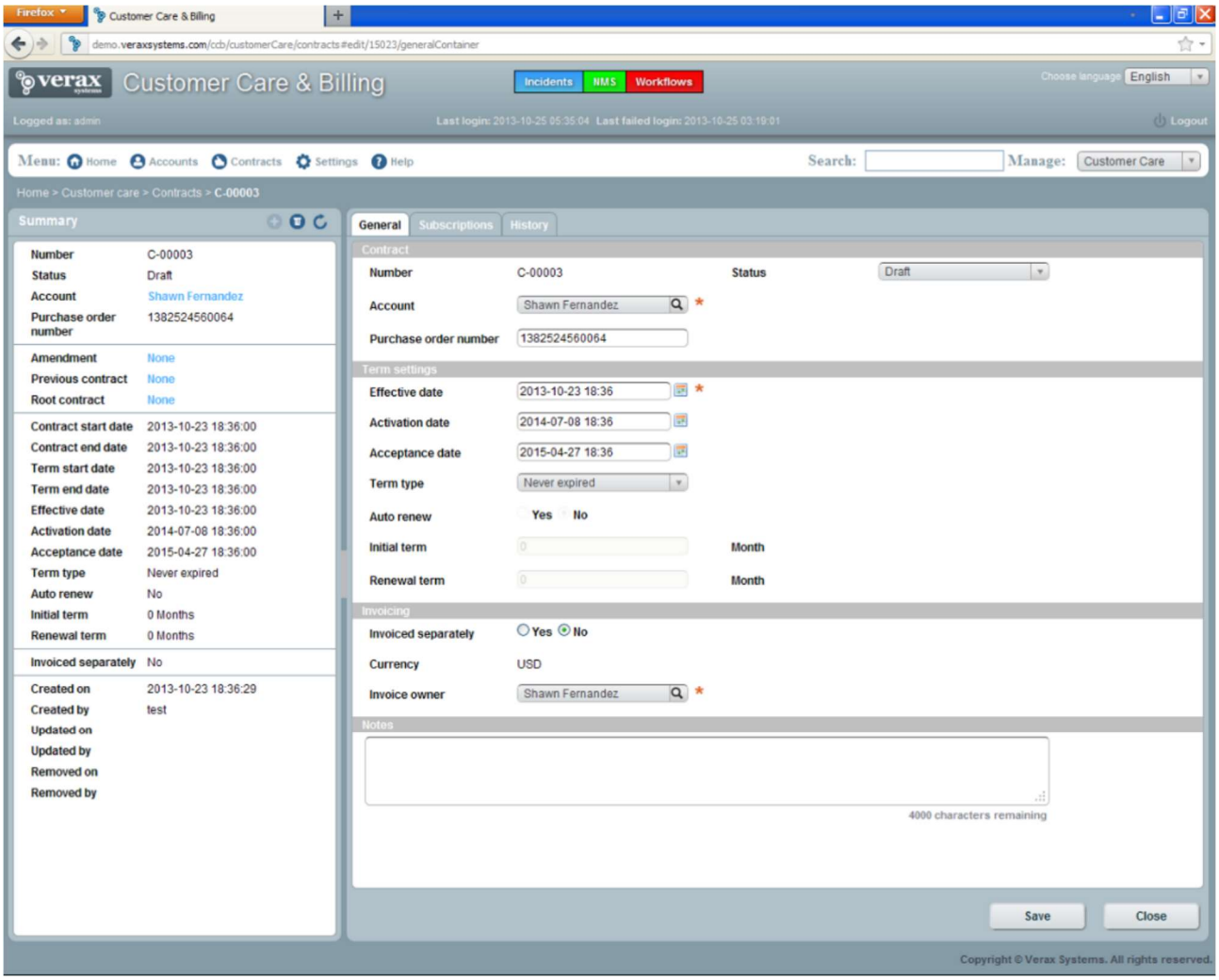


Рисунок 2.2 – Робочий простір Verax SNMP Simulator

Особливості:

– Консоль для управління типами пристроїв, адресами і їх екземплярами;

– Підтримка декількох агентів і декількох мереж на одному хості;

– Файли, сумісні з вихідними даними SNMP, для легкого створення початкових змодельованих конфігурації відповідей SNMP відповідей агента з існуючих пристроїв;

– Багатий набір правил для зміни відповідей агента;

– Генерація, включаючи розширені сценарії, такі як рандомізація тільки частини адреси випадкових MAC-адрес і IP-адрес (наприклад, мережева частина IP-адреси є фіксованою, хостової частина змінюється);

– Генерація випадкового і строкових значень, включаючи сценарії «один раз» або цілого числа, лічильника «кожен раз»;

– Підтримка цілочисельних значення на основі суми арифметичних операцій (наприклад, яке двох інших значень);

– Генерація (напрямок, діапазон кроків, порогове значення скидання), наприклад, для значень на основі тренда збільшення лічильників.

2.1.3 Емулятор Dynamips

Dynamips – це комп'ютерна програма емулятора (рис.2.3), яка була написана. Він був створений Крістофом Філло, який почав свою роботу в серпні 2005 року. для емуляції маршрутизаторів Cisco

Емулятор маршрутизаторів Cisco, який може працювати в Windows, Linix і Mac OS X. (чого не можна сказати про образи, які він використовує). Дозволяє запускати Розповсюджується за ліцензією GNU GPLv2 віртуальну машину з оригінальним чином ОС від старих маршрутизаторів сімейств 1700, 3725, 7200 і деяких інших. і вимираючі ATM і Serial. При цьому Dynamips не може працювати з прошивками Дозволяє імітувати інтерфейси комутаторах і дуже складно Ethernet комутаторів, так як їх ОС орієнтовані на використання ASIC, які у великій кількості зустрічаються в імітуються на x86 системах.

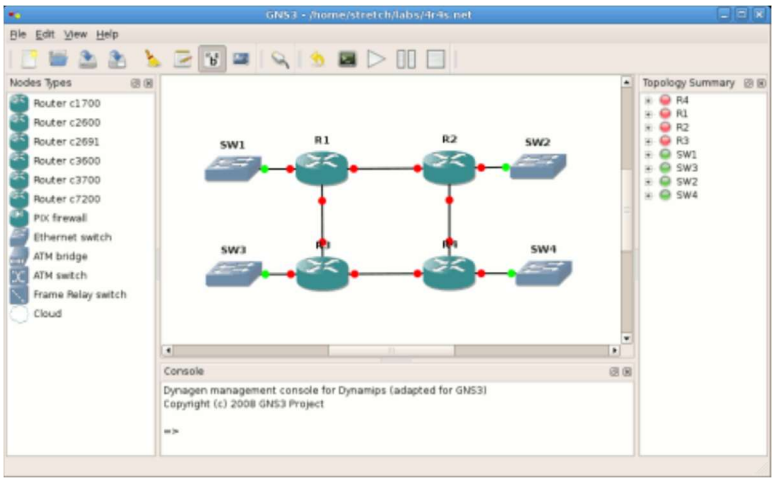


Рисунок 2.3 – Робочий простір Dynamips

2.2 Опис симулятора Cisco Packet Tracer

Даний програмний Cisco і рекомендований використовуватися при вивченні телекомунікаційних продукт розроблений компанією мереж і мережевого устаткування [16]. На основі програмного продукту Packet Tracer є можливість створювати мережеві топології з компанії Cisco, робочих широкого безлічі маршрутизаторів і комутаторів 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 з підтримкою додавання, видалення, переміщення різних компонентів мережевого обладнання.

Даний симулятор дозволяє студентам проектувати відправляючи різні пакети даних свої власні мережі, створюючи і, 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 в ньому режиму симуляції (рис. 2.4). В даному режимі всі пакети, що даного симулятора є наявність пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє студентам наочно продемонструвати, переміщається пакет, який протокол використовується. Працюючи в симуляторі в іншому режимі, режимі реального часу, не можна простежити за переміщенням за яким інтерфейсу в дані момент пакетів, відразу відображається кінцевий результат виконаних дій.

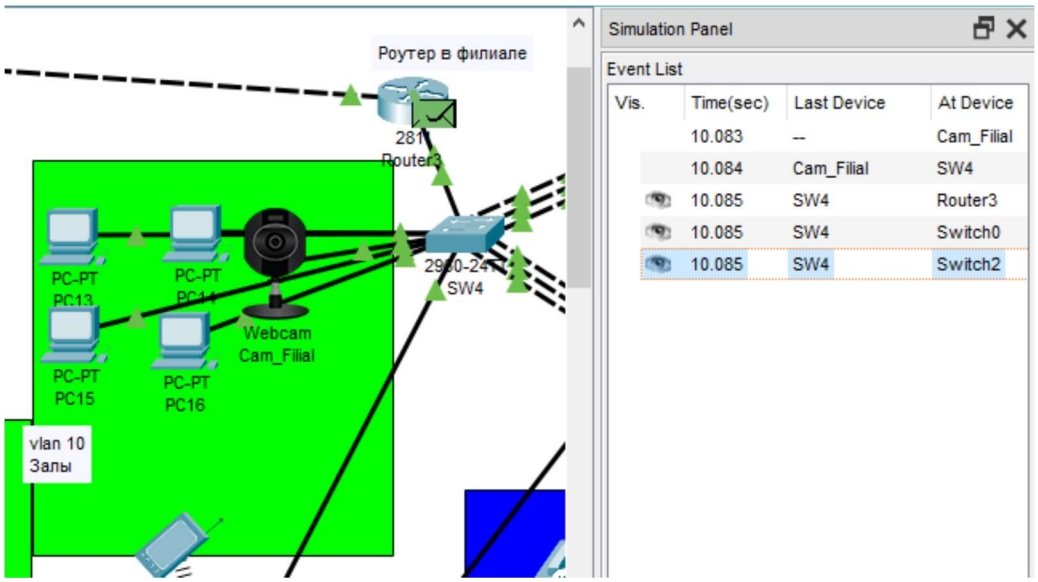


Рисунок 2.4 – Режим симуляції в Packet Tracer

Однак, це не всі симуляції студент може не тільки відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний, переваги Packet Tracer: в режимі а так само вміст пакета, його формат. Tracer здатний моделювати велику кількість пристроїв різного призначення, а зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності так само чимало різних типів [17].

Моделюються пристрої:

– Комутатори другого і третього рівня
– Маршрутизатор
– Мережеві концентратори
– Кінцеві пристрої (робочі станції, ноутбуки, сервери, принтери)
– Бездротові пристрої (точки доступу, бездротові маршрутизатори)
– Глобальна мережа WAN

Підтримувані типи зв'язків між пристроями:

– Консоль
– Мідний кабель з прямим підключенням
– Мідний кабель з перехрещуванням
– Волоконно-оптичний кабель
– Телефонна лінія

– Serial DCE / DTE

Кожен пристрій Packet Tracer може бути налаштоване через вікно властивостей, яке викликається в програмному продукті Cisco по подвійному кліку на пристрої. Перша вкладка Physical (рис. 2.5) відповідає за фізичні параметри пристрою. і комутаторів в них можна додавати нові модулі, в робочі станції і сервери – Під час налаштування маршрутизаторів вставляти мережеві адаптери.

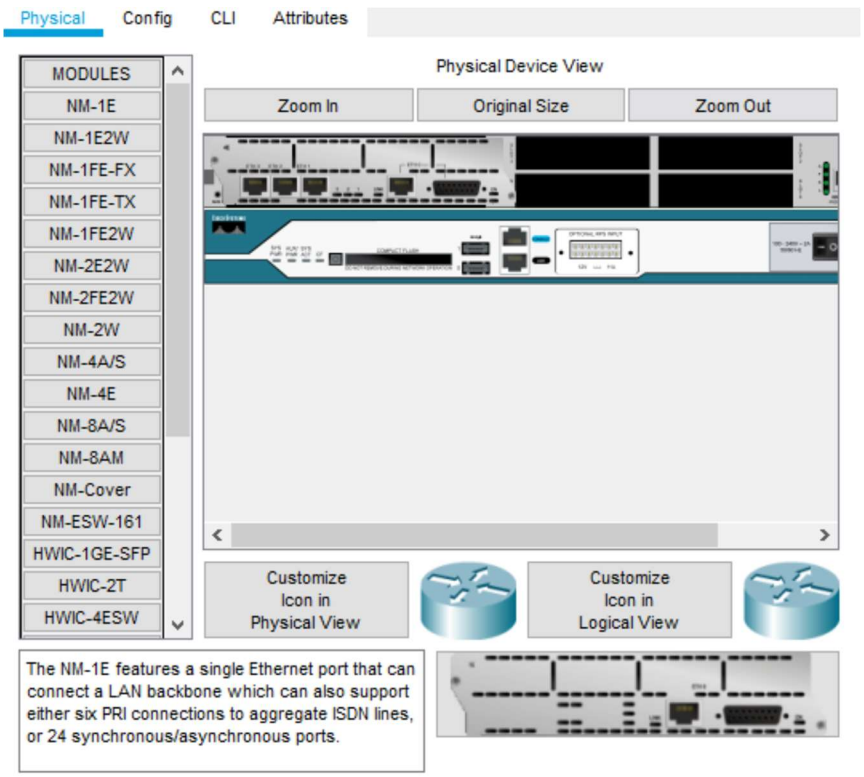


Рисунок 2.5 – Фізичний вигляд пристрою (маршрутизатора)

На вкладці Config (рис. 2.6) можна мережевих інтерфейсів (IP-адреси, маски підмережі, параметри бездротової мережі та ін.) задавати основні параметри У мережевих пристроях маршрутизацію – статичну або динамічну, у серверів – конфігурувати служби також можна конфігурувати.

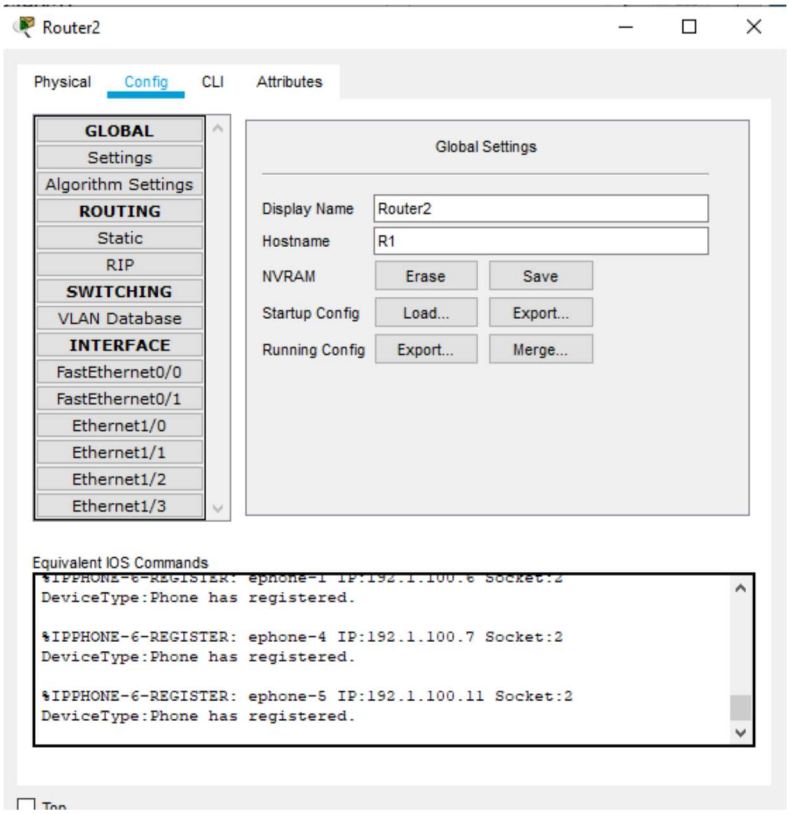


Рисунок 2.6 – Конфігурація сервера

При запуску програми відкривається головне вікно симулятора (рис. 2.7):

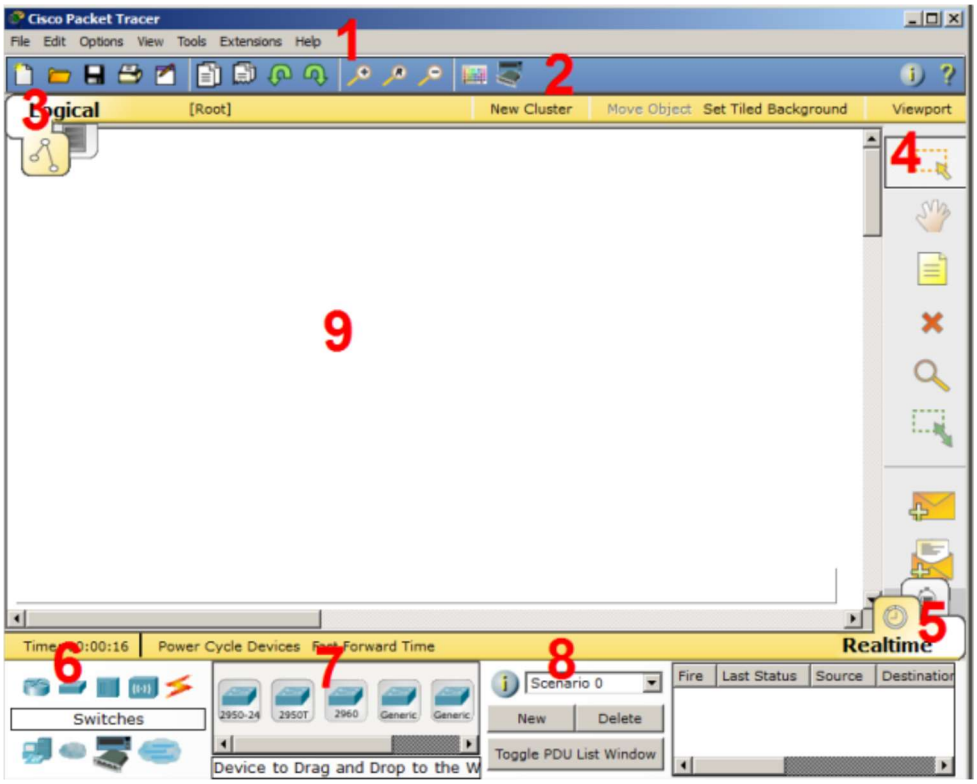


Рисунок 2.7 – Інтерфейс програми Cisco Packet Tracer

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, режим і кілька приблуд, які з CPT (так я іноді буду ласкаво називати Cisco розрахований на багато користувачів Packet Tracer) можуть зробити цілу лабораторію;

– Допомога – містить та містить посилання на додатки допомоги в використані інформацію про програму програми;

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

3) Перемикач між логічного і зниження фізичної організацією;

4) Ще одна інструменти виділення, видалення, переміщення, масштабування панель інструментів, містить 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 комутатори, вузли, точки доступу, провідники.

8) Панель створення пристрої, тут містяться всілякі призначених для користувача сценаріїв;

9) Робочий простір.

Симулятор Packet Tracer підтримує тип кабелю може бути з'єднаний широкий діапазон мережевих з'єднань (таблиця 2.1). Кожен 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 виконані деякі вимоги для роботи між ПК і маршрутизаторами або комутаторами. Повинні бути консольного сеансу з ПК: швидкість з'єднань з обох сторін повинна бути однакова, має бути 7 біт даних (або 8 біт) для обох сторін, повинен бути однаковий, має бути 1 або 2 степових бита (але вони не обов'язково контроль парності повинні бути однаковими), а потік даних може бути чимось завгодно для обох сторін.
2	Мідний прямий 	Цей тип кабелю є пристроїв, який функціонує на різних рівнях OSI. Він повинен бути стандартним середовищем передачі Ethernet для з'єднання 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, рівнях OSI. Він може бути з'єднаний з наступними які функціонують на однакових типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet)
4	Оптика 	Оптоволоконне для з'єднання між оптичними портами середовище використовується (100 Мбіт / с або 1000 Мбіт / с).
5	Телефонний 	З'єднання через телефонну лінію може бути здійснено модемні порти. Стандартне подання модемного з'єднання тільки між пристроями, що мають – це кінцевий пристрій (Наприклад, ПК), додзвонюється в мережеве хмара.
6	Коаксиальний 	Коаксиальне такі як кабельний модем, з'єднаний з хмарою Packet Tracer. середовище використовується для з'єднань між коаксіальними портами,
7	Серійний DCE Серійний DTE 	З'єднання через послідовні порти, часто використовуються на стороні DCE-пристроїв. Синхронізація для зв'язків WAN. Для настройки таких з'єднань необхідно встановити синхронізацію DTE виконується за вибором.

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

2.3 Обладнання, яке були застосовано в проекті Cisco Packet Tracer

2.3.1 Комутатори

Мережевий комутатор (рис. 2.8) – пристрій, декількох вузлів комп'ютерної мережі в межах одного або призначений для з'єднання декількох сегментів мережі. Комутатор працює на канальному (другому) рівні моделі OSI. Комутатори мостових технологій і часто розглядаються як багатопортові мости. Для з'єднання декількох мереж на основі мережевого рівня були розроблені з використанням служать маршрутизатори.

Рисунок 2.8 – Комутатор

Комутатор (що зберігається в асоціативної пам'яті), в якій вказується відповідність MAC-адреси вузла зберігає в пам'яті таблицю комутації порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. В цьому порт дані передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри (фрейми) і, визначивши MAC-адресу хоста-відправника, заносить його в режимі надходять на якийсь таблицю на деякий час. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адресу якого тільки через порт, зазначений у таблиці. Якщо MAC-адресу хоста-одержувача не вже є в таблиці, то цей кадр буде переданий асоційований з яким-небудь портом комутатора, то кадр буде відправлений на всі порти, за винятком того. Згодом комутатор будує таблицю для всіх активних MAC-адрес, в результаті трафік локалізується. Варто відзначити малу латентність (затримку) і високу швидкість пересилки на кожному порту, з якого він був отриманий порту інтерфейсу.

Існує три способи комутації. Кожен таких параметрів, як час очікування і надійність з них – це комбінація передачі [17].

– З проміжним зберіганням (Store and Forward). Комутатор читає всю інформацію помилок, вибирає порт комутації і після цього посилає в нього в кадрі, перевіряє його на відсутність кадр.

– Наскрізний (cut-through). Комутатор зчитує після виконує комутацію в кадрі тільки адреса призначення і. Цей режим зменшує з ньому немає методу атримки при передачі, але в виявлення помилок.

– Безфрагментний (fragment-free) або гібридний. Цей режим є. Передача здійснюється після фільтрації фрагментів колізій модифікацією наскрізного режиму (кадри розміром 64 байта обробляються за технологією store-and-forward, інші – за технологією cut-through).

Комутатори поділяються на керовані і некеровані (найбільш прості). Більш складні комутацією на мережевому (третьому) рівні моделі комутатори дозволяють управляти OSI. Зазвичай їх називають відповідно, наприклад Layer 3 Switch або просто, скорочено L3. здійснюватися за допомогою протоколу Web-

інтерфейсу, SNMP, RMON Управління комутатором може (протокол, розроблений Cisco).

Багато керовані додаткові функції: VLAN, QoS, агрегування, віддзеркалення. комутатори дозволяють виконувати Складні комутатори можна поєднувати в один логічний пристрій – стек, з метою збільшення числа портів (наприклад, можна о або з 96-а портами (якщо б'єднати 4 комутатори з 24 портами і отримати логічний комутатор з (4 * 24-6 = 90) портами, для стекування використовуються спеціальні порти).

2.3.2 Маршрутизатор

Маршрутизатор (рис. 2.9) – спеціалізований мережевий два мережевих інтерфейсу комп'ютер, який має мінімум і пересилає пакети даних між різними сегментами мережі, що приймає рішення про пересилку на і певних правил підставі інформації про топологію мережі, заданих адміністратором.

Рисунок 2.9 – Маршрутизатор

Маршрутизатор. Маршрутизатор працює на більш діляться на програмні і апаратні високому «мережевому» рівні 3 мережевий моделі OSI, ніж комутатор і мережевий міст, які моделі OSI відповідно. 30

Зазвичай маршрутизатор використовує працюють на 2 рівні і 1 рівні адресу

одержувача, вказану в пакетних даних, і визначає по таблиці маршрутизації шлях, по якому слід передати дані. Якщо в таблиці маршрутизації для адреси немає описаного маршруту, пакет відкидається.

Існують і інші пересилки пакетів, коли, наприклад, використовується адреса відправника, способи визначення маршруту використовувані протоколи верхніх рівнів і інша інформація, що міститься в заголовках пакетів мережевого рівня. Нерідко трансляцію адрес відправника і одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування / розшифрування маршрутизатори можуть здійснювати даних, що передаються.

Маршрутизатор допомагають мережі, завдяки її розділенню на домени колізій або зменшити завантаження широкомовні домени, а також завдяки фільтрації пакетів. В основному їх застосовують для об'єднання мереж різних типів, часто несумісних з Нерідко маршрутизатор архітектури і протоколів, наприклад для об'єднання локальних мереж Ethernet і WAN-з'єднань, що використовують протоколи xDSL, PPP, ATM, Frame relay. використовується для забезпечення доступу з локальної мережі в глобальну мережу Інтернет, здійснюючи функції трансляції адрес і міжмережевого екрану.

В як спеціалізований (апаратне) пристрій, так і звичайний комп'ютер, що виконує функції маршрутизатора. Існує кілька пакетів п якості маршрутизатора може виступати рограмного забезпечення (на основі ядра Linux, на основі операційних і багатофункціональний маршрутизатор систем BSD) за допомогою якого можна перетворити ПК в високопродуктивний, наприклад, Quagga, IPFW або простий в застосуванні PF.

Залежно від області застосування, маршрутизатори можна розділити на три класи:

– Верхній. У таких маршрутизаторів дуже високий рівень продуктивності. і забезпечення мережі в крупних компаніях. Верхні маршрутизатори можуть використовувати нестандартні інтерфейси і протоколи. Такі маршрутизатори Вони застосовуються для створення можуть містити

велику кількість портів для різних глобальних і локальних мереж.

– Середній. Застосовується мережу в невеликій організації або в окремій будівлі для того, щоб створити.

– Нижній. для створення локальної мережі в маленькому офісі або для використання в домашніх Такий маршрутизатор застосовується умовах. Нижній маршрутизатор має до 2 портів глобальної мережі і 4 порту локальної.

Існує всього 2 способи, маршрутизатори до мережі якими можна підключити. Він може або бездротовим способом. Теж саме відноситься і до можливості розподілу мережі по різних пристроїв підключатися дротовим.

У маршрутизатора, способом, є невелика перевага. Він може здійснювати передачу інформації ще й за допомогою дротів. На даний момент за допомогою використання який підключається бездротовим технологій бездротового підключення можуть передавати дані без застосування проводів більшість пристроїв. Більш таку роботу і для них необхідно використовувати дроти. За допомогою бездротового роутера можна об'єднати різні пристрої в одну загальну мережу з можливістю доступу в інтернет старі версії обладнання не підтримують.

Дротовий маршрутизатор обов'язково підключається до кожного пристрою, яке. Провідні маршрутизатори використовуються для мережі, в якій є не більше 8 пристроїв. При цьому ці пристрої повинні перебувати постійно на одному і тому ж місці. За допомогою проводового підключення можна легко досягти доступу між всіма знаходиться в мережі учасниками цієї мережі. При такому підключенні з одного пристрою можна отримати дані іншого.

По областях застосування маршрутизатори діляться на кілька класів.

– Магістральні маршрутизатори (backbone routers) призначені для побудови локальних мереж, розкиданих центральної мережі корпорації. Центральна мережа може складатися з великої кількості по різних будівель і використовують найрізноманітніші мережеві технології, типи комп'ютерів і операційних маршрутизатори – це найбільш потужні пристрої, здатні обробляти кілька сотень тисяч або навіть кілька мільйонів пакетів в систем. Магістральні

секунду, які мають велику кількість інтерфейсів локальних і глобальних мереж.

– Маршрутизатор регіональних відділень між собою і з центральною сполучають регіональні відділення мережею. Мережа регіонального відділення, так само як і центральна мережа, може складатися з декількох локальних мереж. Такий маршрутизатор зазвичай є деякою спрощену версію магістрального маршрутизатора.

– Маршрутизатор віддалених офісів з'єднують, як правило, єдину локальну мережу віддаленого можуть підтримувати і два інтерфейси офісу з центральною мережею або мережею регіонального відділення по глобальної зв'язку. У максимальному варіанті такі маршрутизатори локальних мереж. Як правило, інтерфейс локальної мережі – це Ethernet 10 Мбіт / с, а інтерфейс лінія зі швидкістю 64 Кбіт / с, 1,544 або 2 Мбіт / с. Маршрутизатор віддаленого офісу може підтримувати роботу віддаленого глобальної мережі – виділена підключення в якості резервної зв'язку для виділеного каналу.

– Маршрутизатор локальних мереж (комутатори 3-го рівня) призначені для поділу великих. Основна вимога до них – висока швидкість маршрутизації, так як в такій конфігурації відсутні низько-швидкісні порти, такі як модемні порти 33,6 Кбіт / локальних мереж на підмережі с або цифрові порти 64 Кбіт / с.

2.3.3 Сервер

Сервер (рис. 2.10) – це апаратно-програмний, здатний регулювати роботу всіх призначених для комплекс в локальній мережі користувача комп'ютерів.

Рисунок 2.10 – Сервер Cisco UCS S3260

В основі апаратної частини сервера лежить потужний комп'ютер з високою продуктивністю, для швидкої обробки команд від клієнтських ПК. Такий сервер повинен бути не можна сказати про багатоядерним, багатозадачністю і найкращою оптимізацією відмовостійким, з гарячою заміною свого обладнання (hotswap) тобто завжди на «ходу». Чого клієнтські комп'ютери, які частіше потребують ремонту через знос запчастин.

Основні функції сервера локальної мережі можна класифікувати на:

1) Файловий сервер – це одна з ключових сервером забезпечує ролей кожного сервера. Локальна мережа з файловим користувачам необмежений доступ до будь-яких даних, що зберігаються на центральному комп'ютері, а також управління директоріями. Ключова особливість сервера типом доступу до файлів: він полягає в управлінні може призначити загальний доступ до папок або персональний доступ в свою робочу директорію для кожного користувача.

2) Термінальний сервер – це сервер, мережі свої обчислювальні ресурси. На практиці використання такого сервера часто носить бюджетний характер, оскільки на сервері який надає користувачам можна запускати необхідне для роботи ліцензійне ПЗ. Кожен користувач на своєму комп'ютері використовує встановлений клієнт RDP (Remote Desktop Protocol) – протокол віддаленого робочого стола. зв'язку з термінальним сервером користувач бачить вміст робочого столу з необхідними програмами і працює віддалено, використовуючи

обчислювальні ресурси При коректної установки сервера, тобто без навантаження на свій комп'ютер. Переваги т зменшення витрат на програмне ермінального сервера полягають в зниженні витрат електроенергії, забезпечення та підвищення безпеки методом обмеженого робочого місця користувача.

3) Сервер друку необхідний для колективної Даний метод має на увазі віддалену роботи з принтером або факсом. друк на пристрої, не підключеному до вашого робочого місця. Сервер друку може обробляти багатопотокових операції, а також забезпечувати друк інформації від Крім того, розташування декількох комп'ютерів без «простою». всіх друкуючих пристроїв в одній кімнаті значно спрощує офісну роботу. Знаючи IP-адреса сервера можна вибрати загальнодоступне Також управління друком пристрій друку для локальної мережі (або віддаленої групи користувачів). на сервері дозволяє відстежувати обробник завдань друку, який реєструє в журналі кількість роздрукованого паперу.

4) Сервер бази даних – відповідає за цілісність і Робота з даними відбувається збереження sql-даних. у вигляді обробки sql-запитів від користувача безпосередньо до бази даних. Такий набір обробки правил працює з таблицями, секціями, звітами і формулами. Клієнт-користувач, підключаючись до бази даних, може служити комп'ютер використовує обчислювальну потужність сервера. Прикладом такого сервера бази даних з таким поширеним ПО, як: 1С-підприємство, Парус-Бухгалтерія, моніторинг мережі cmysql та багато інших.

5) Веб-сервер – це сервер, робота якого полягає на інформаційному обміні між користувачами, але і в мережі Інтернет. Сервер зберігає всі ресурси веб-сайту, верстки сторінок, шаблонів-стилів, виконуваних скриптів, html-документів. не тільки в локальній мережі Функції сервера л конференцій, мультимедіа, інформаційний окальної мережі полягають в прийомі / відправлення http - пакетів з необхідної користувачеві інформацією. Такий сервер для локальної мережі може реалізувати відеохостинг, трансляцію портал, публікації документів. Веб-сервер багатогранний. Можна задіяти до нього СУБД

(mysql-web), мережі (mrtg, cacti, nagios), проксі-сервер на веб (nginx) і багато інших корисних в роботі програм моніторинг локальної.

6) Поштовий сервер – призначений для зберігання листів і обміну текстовою. Також функції сервера електронної пошти поширюються на зберігання адрес («ящиків») всіх користувачів мережі, між ними, інформацією між користувачами мережі відправки звітів, участі в групах розсилки, а також створення календарних проектів для особистих зустрічей. обміну кореспонденцією

2.3.4 Точка доступу Wi-Fi

Точка доступу – це бездротова базова станція (рис. 2.11), призначена забезпечення бездротового доступу до вже для існуючої мережі (безпроводовий або провідний) або створення абсолютно нової бездротової мережі. Бездротовий зв'язок здійснюється за допомогою технології Wi-Fi.

Рисунок 2.11 – Точка доступу Wi-Fi Cisco Air-CAP3702E

Бездротові мережі з декількох точок у великих офісних приміщеннях, будівлях і на інших великих о доступу встановлюються б'єктах, в основному для того, щоб створити одну бездротову локальну мережу (WLAN). До кожної точки доступу клієнтських комп'ютерів. У більшості випадків недоцільно підключати до однієї точки доступу більше 10 комп'ютерів, можна підключити до 254 тому що швидкість передачі даних на кожного користувача розподіляється в рівних пропорціях «клієнтів», тим менше швидкість у кожного з них і чим більше в однієї точки доступу.

При побудові територіально мереж в будинках, точки доступу об'єднуються в одну розподілених мереж або бездротових загальну мережу через радіоканал або локальну мережу (дротову). При цьому користувач своїм мобільним може вільно переміщатися зі пристроєм в радіусі дії цієї мережі

Точка доступу з бездротовим роутером (бездротового маршрутизатора). Бездротові роутери використовуються для створення окремого сегмента мережі і підтримують підключення до них аналогічна за своїм устроєм всіх комп'ютерів з вбудованими бездротовими мережевими адаптерами. На відміну від точки доступу в інтегрований мережевий перемикач (світч), для того щоб до нього могли додатково підключатися клієнти по протоколу Ethernet або для підключення інших маршрутизаторів бездротової роутер при створенні мережі з декількох бездротових роутерів. Крім того, бездротові роутери мають запобігає небажане вторгнення в мережу зловмисників. В іншому ж, бездротові роутери схожі по влаштуванню з точками доступу вбудований брандмауер, який.

Існує три основні режими роботи точки доступу:

– "Точка доступу". У новому обладнанні режим «точка доступу» встановлено режимі користувач підключається зі свого комп'ютера, оснащеного Wi-Fi адаптером, до бездротової мережі точки доступу. У більшості випадків для роботи в цьому режимі специфічні за умовчанням. В цьому настройки не потрібні.

– «Повторювач». В даному режимі точка Вона приймає слабкий доступу

працює як приймально-передавач або «повторювач». сигнал від іншої точки доступу і, посилюючи його, передає на цій же частоті далі до необхідного адресата.

– «Міст». В цьому режимі точка доступу одне ціле. Використовується об'єднує фізично віддалені сегменти мережі в при побудові «лінків» або, іншими словами, забезпечення зв'язку між віддаленими об'єктами.

2.4 Висновки

В розділі було проаналізовано наявні та доступні засоби для ямоделювання та дослідження мереж. Із запропонованоих варіантів було обрано продукт Packet Tracer від компанії Cisco Systems, оскільки він 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.

3 МОДЕЛЮВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ

3.1 Проектування та сегментація локальних мережі

Для того, щоб спроектувати мережу раніше було описано, що її потрібно будувати з невеликих блоків чи модулів і об'єднувати в одну. Це робиться для того, щоб у подальшому її було простіше адмініструвати, шукати та виправляти помилки. На практиці, щоб це реалізувати потрібно ознайомитись з такою мережевою технологією, як VLAN.

VLAN – це функція на мережевих пристроях, яка об'єднує декілька хостів незалежно від їх фізичного розташування, в одну віртуальну мережу. Такі віртуальні мережі не будуть видимі одна для одної.

VLAN застосовується:

– щоб обмежити потік трафіку і менше навантажувати ниммережу за рахунок розбиття її на сегменти;

– зменшення кількості фізичних приладів для спрощення керування та адміністрування мережею;

– підвищити безпеку за рахунок ізоляції однієї мережі від іншої;

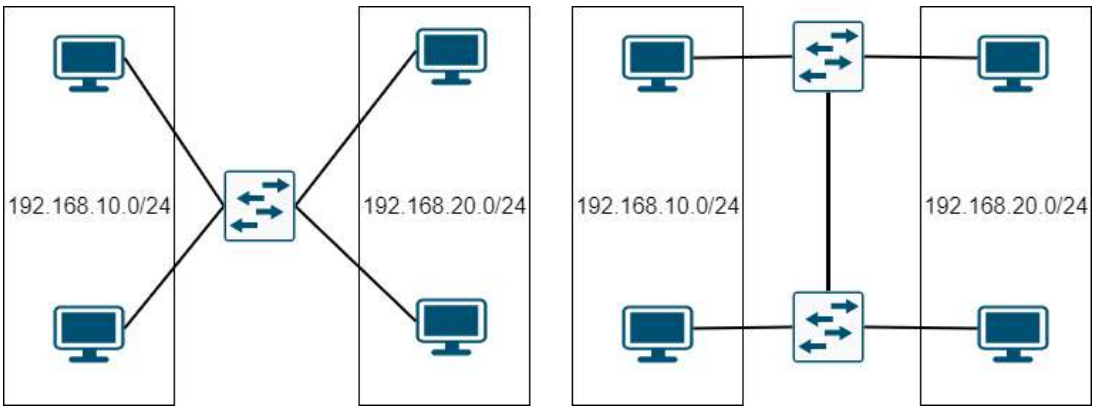


Рисунок 3.1 – Приклади розбиття хостів на різні мережі

У такому випадку мережеве обладнання саме розуміє до якої мережі належить кінцевий пристрій. Тому пакети помічаються спеціальним ідентифікатором (VLAN id).

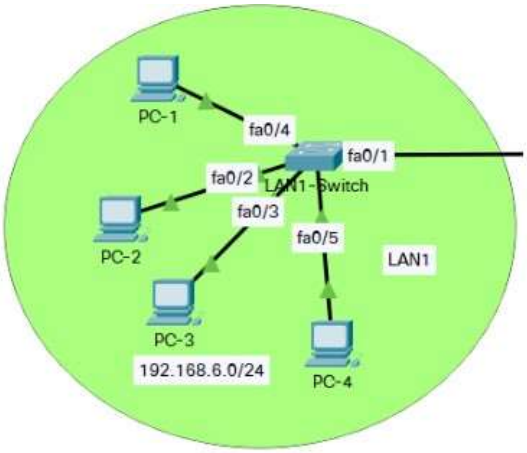
Але так як у подальшому при проектуванні, локальні мережі будуть поділені фізично то на даний момент немає потреби ділити хости на логічні підмережі. Тому я їх усіх віднесу до одного VLAN. І одразу згіднозавдання я зроблю усі необхідні налаштування кінцевих пристрої, тобто призначу IP-адреси та маски мережі.

Таблиця 3.1 – Налаштування адрес на кінцевих пристроях

	Назва пристрою	IP-адреса	Маска мережі	Шлюз
1	PC-1	192.168.6.10	255.255.255.0	192.168.6.1
2	PC-2	192.168.6.11	255.255.255.0	192.168.6.1
3	PC-3	192.168.6.12	255.255.255.0	192.168.6.1
4	PC-4	192.168.6.13	255.255.255.0	192.168.6.1
5	LAN2-PC	10.0.3.10	255.255.255.0	10.0.3.1
6	LAN2-Server	10.0.3.11	255.255.255.0	10.0.3.1
7	DMZ_Server-1	10.0.2.10	255.255.255.0	10.0.2.1
8	DMZ_Server-2	10.0.2.11	255.255.255.0	10.0.2.1

Міжвланова маршрутизація – це звичайна маршрутизація підмереж. Різниця тільки в тому, що кожній підмережі відповідає якийсь VLAN на другому рівні моделі OSI. І для того, щоб маршрутизувати трафік між цими підмережами потрібно вже на третьому рівні присвоїти їм адреса. Ціадреса будуть виступати в ролі шлюзів для виходу в інші підмережі.

Така маршрутизація забороняє клієнту стати членом іншої підмережі, навіть якщо змінити адресу пристрою.



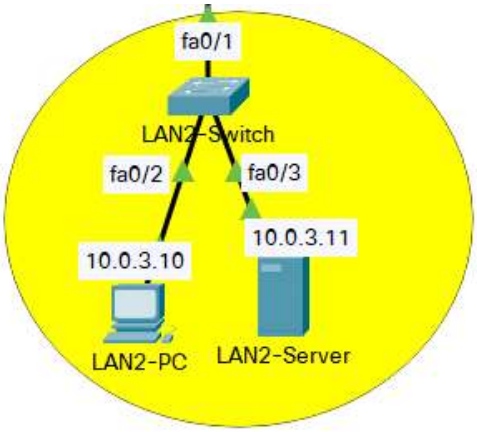

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
2    LAN1                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0
```

Рисунок 3.2 – Результат створення підмережі LAN1

Відповідно до завдання, потрібно створити ще дві підмережі, LAN2 та LAN3, яка в свою чергу буде виконувати роль DMZ.

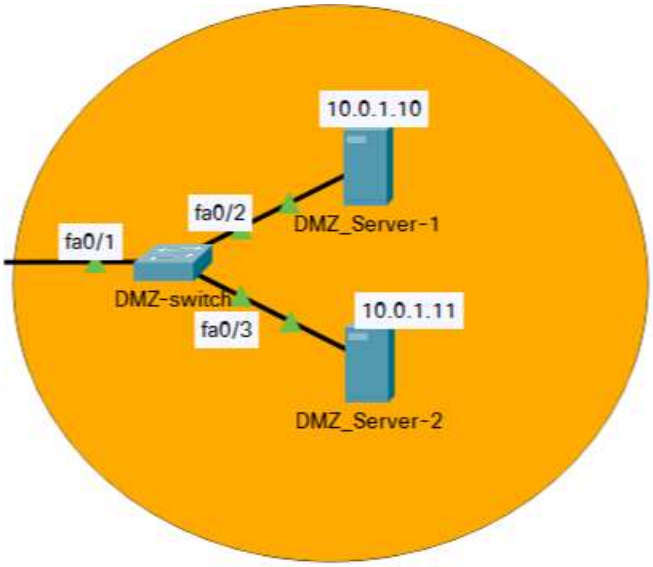
Демілітаризована зона (DMZ) – це сегмент мережі, в якому знаходяться загальнодоступні сервіси, які відділені від інших локальних мереж. Реалізується DMZ за допомогою мережевого екрану фізичного чи програмного. Мета створення такого сегмента мережі – надати додатковийрівень безпеки для інших локальних мереж. DMZ допомагає зменшити ризики в разі атаки. Перед адміністраторами мережі при створені такої зони, виникають певні вимоги[4].

Необхідно ввести контроль при роботі користувачів, захистити та забезпечити конфіденційність інформації. На публічних серверах повинна знаходитись найменш важлива інформація, а будь-яка цінна має знаходитись на локальних серверах. На публічних серверах не має бути ніякої інформації про користувачів чи клієнтів компанії. А інформацію якавсе ж таки буде доступна, потрібно систематично резервно копіювати.




```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    LAN2                             active    Fa0/1, Fa0/2, Fa0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0
```

Рисунок 3.3 – Результат створення підмережі LAN2




```
VLAN Name                             Status    Ports
---- -------------------------------- --------- 
-------------------------------
2    DMZ                              active    Fa0/1, Fa0/2, Fa0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0
```

Рисунок 3.4 – Результат створення підмережі DMZ

Якщо порт повинен приймати та відправляти трафік з різних VLAN,то він повинен знаходитись тегованому або в транковому стані. Такий транковий порт

може передавати або якісь конкретні VLAN, або усі по замовчуванню.

3.2 Трансляція мережевих адрес

Існують декілька видів ipv4 адрес. Публічні – це адреси, які глобально маршрутизуються між інтернет провайдерами та іншими постачальниками послуг інтернету. Також є групи адрес, які використовуються для призначення їх локальним пристроям мереж. Вониназиваються приватними.

Ще у середині дев'яностих попереднього століття разом із впровадженням всесвітньої павутини були введені приватні адреси. Вони не є унікальними і використовуються у всіх локальних мережах підприємств.

Таблиця 3.2 – блоки приватних адрес ipv4

Адреса мережі та префікс	Діапазон приватних адрес RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Однак приватні адреси не можуть маршрутизуватись в інтернет.

Задача маршрутизації, в свою чергу включає в себе дві задачі:

- визначити маршрут для пакетів
- повідомити мережу про обраний маршрут

Задача визначення маршруту полягає у тому, щоб обрати послідовність проміжних пристрої та їх інтерфейсів, через які потрібно передати дані, щоб доправити їх до отримувача. Ця задача не є простою, оскільки майже завжди не існує одного маршрути до одержувача. Тому зазвичай обирається оптимальний маршрут за декількома критеріями. Це можуть бути пропускна здатність, завантаженістю каналу передачі даних, кількість проміжних вузлів, чи затримки викликані кількість вузлів або тією ж завантаженістю каналу.

Маршрут може визначатися вручну адміністратором мережі. Але цей

метод недосконалий та вибагливий для великої мережі.

В такому випадку використовується автоматичний метод вибору маршруту. Для цього потрібне додаткове програмне забезпечення, яке буде давати змогу збирати та обмінюватись інформацією про мережу. І наоснові цих даних визначається маршрут[9].

Для того, щоб маршрутизувати дані в інтернет потрібно налаштувати мережеву технологію NAT.

NAT – здійснює перетворення приватних адрес в публічну. Маршрутизатор зазвичай здійснює зв’язок локальної мережі з мережею інтернет провайдера. Тому для можливості у подальшому мати доступ до інтернету і коректного виконання задачі DMZ потрібно налаштувати NAT на корпоративному маршрутизаторі. Задачу об’єднання локальних мереж та інструментом захисту мережі буде виконувати апаратний мережевий екран - Cisco ASA 5506-X. Також буде створена ще одна локальна мережазадача якої буде полягати в тому, щоб маршрутизувати трафік в інтернет[14].

Для налаштування NAT знадобиться access control list. Це певний фільтр, який створюється для контролювання трафіку. Він використовується у раніше вже згаданому мережевому екрані, для контролювання сеансів. ACL також призначений для створення як і окремих правил так і цілих списків доступу. Тому знадобиться створити список мереж, які будуть транслюватись в глобальну мережу.

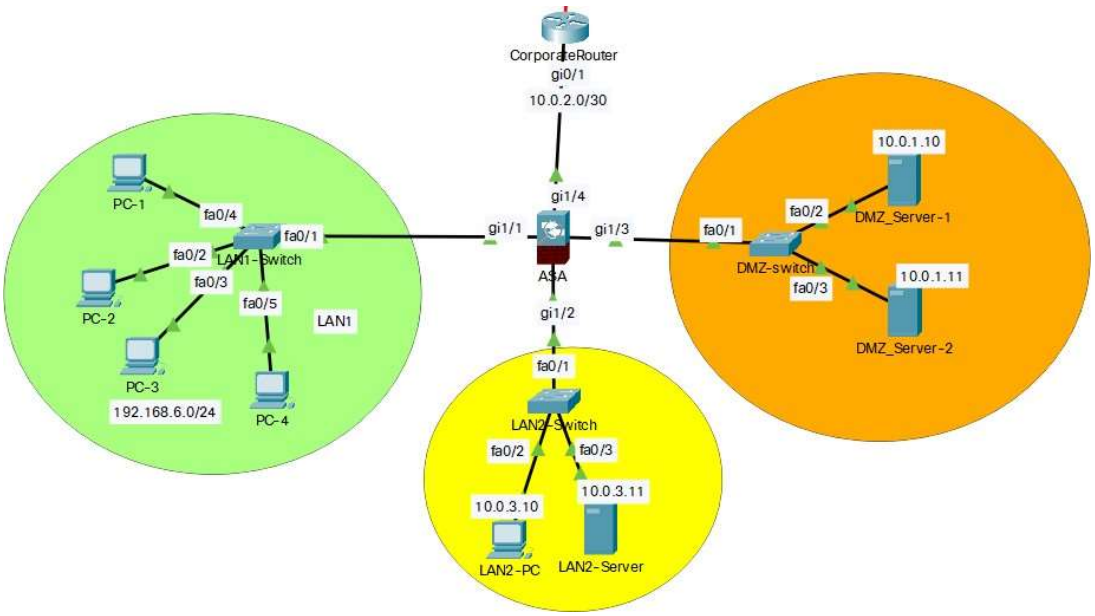


Рисунок 3.5 – Топологія об’єднаних локальних підмереж

```
ip nat inside source list FOR-NAT interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 213.234.10.1
ip route 10.0.1.0 255.255.255.0 10.0.2.2
ip route 10.0.3.0 255.255.255.0 10.0.2.2
ip route 192.168.6.0 255.255.255.0 10.0.2.2
!
ip flow-export version 9
!
!
ip access-list standard FOR-NAT
 permit 10.0.2.0 0.0.0.3
 permit 10.0.3.0 0.0.0.255
 permit 10.0.1.0 0.0.0.255
 permit 192.168.6.0 0.0.0.255
```

```
interface GigabitEthernet0/1
 ip address 10.0.2.1 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 213.234.10.2 255.255.255.252
 ip nat outside
 clock rate 2000000
```

Рисунок 3.6 – налаштування NAT та додаткових статичних маршрутів

Для налаштування я визначив фізичні інтерфейси як внутрішній (inside) та зовнішній (outside). Це потрібно для того, щоб маршрутизатор розумів звідки і куди маршрутизувати локальний трафік. Далі я створив ACL в якому визначив групу адрес, які потрібно транслювати. І для завершення налаштування NAT потрібно ввести команду ip nat із вказаним списком доступу, та зовнішнім інтерфейсом.

Також довелось створити додаткові статичні маршрути, для направлення відповідей до пристроїв, які раніше створювали запит в інтернет.

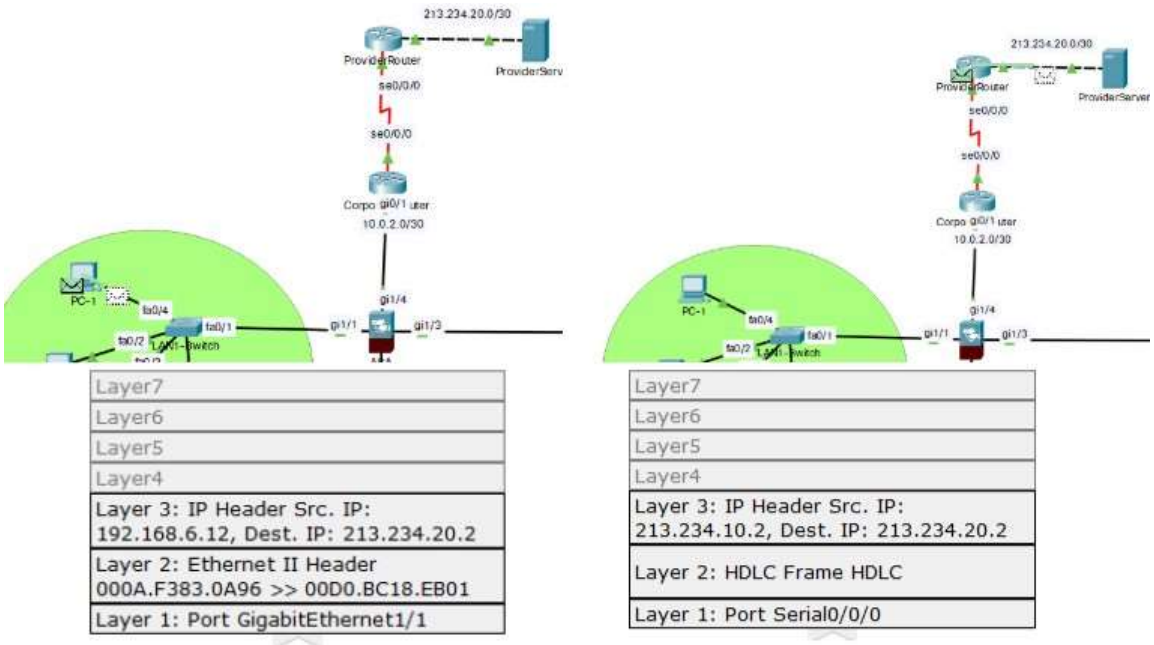


Рисунок 3.7 – відслідковування пакету під час запиту на сервер який імітує інтернет

На рисунку 3.7 чітко видно як на пристрої PC-1, який знаходиться у підмережі LAN1 створюється пакет з IP-адресою джерела 192.168.6.12 та IP-адресою призначення 213.234.20.2. А після того як пакет пройшов через маршрутизатор - IP-адреса джерела змінилася на 213.234.10.2. Отже технологія трансляції мережевих адрес працює коректно.

3.3 Налаштування DMZ

В основному DMZ реалізується з допомогою мережевого екрану, але у даному випадку частина налаштувань буде виконана ще й на корпоративному маршрутизаторі.

Отже, для початку потрібно налаштувати security level на мережевому екрані. Для цього потрібно увійти в налаштування кожного інтерфейсу та ввести там потрібний рівень довіри. Це число від нуля до сотні. Воно показує наскільки є безпечна певна мережа. Чим більше це число тим більша надійність. У такому разі усі локальні мережі повинні мати високий рівень, а зовнішня та DMZ мережа

навпаки, низькийрівень довіри. Тому я використав число дев'яносто п'ять для LAN1 та LAN2 та рівень нуль і п'ятдесят для зовнішньої та DMZ мережі відповідно[10].

```
interface GigabitEthernet1/1
 description LAN1
 nameif LAN1
 security-level 95
 ip address 192.168.6.1 255.255.255.0
!
interface GigabitEthernet1/2
 description LAN2
 nameif LAN2
 security-level 95
 ip address 10.0.3.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif DMZ
 security-level 50
 ip address 10.0.1.1 255.255.255.0
!
interface GigabitEthernet1/4
 description to CorporateRouter
 nameif outside
 security-level 0
 ip address 10.0.2.2 255.255.255.252
```

Рисунок 3.8 – налаштування рівнів довіри на інтерфейсах

У такому разі буде доступ з мережі з високим рівнем довіри до мережі з нижчим рівнем. Але на даний момент будуть блокуватись відповіді на запити, адже вони приходять з мережі з нижчим рівнем довіри. Тому зараз потрібно скористатись технологією, яка була раніше описана.

Stateful inspection або динамічна фільтрація пакетів, адже із її допомогою мережевий екран буде запам'ятовувати пристрої локальної мережі які виконували запит в мережу з нижчим рівнем довіри і пропускати відповіді які призначені саме цим пристроям[15].

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect http
  inspect icmp
!
service-policy global_policy global
```

Рисунок 3.9 – налаштування динамічної фільтрації трафіку

Серверам які знаходяться в DMZ зоні призначено сірі адреса, але основна задача цієї підмережі – це мати доступ до неї із інтернету. І для того , щоб реалізувати дану задачу потрібно скористатись static NAT

Static NAT перетворює сірий адрес в білий таким чином, що з’являється можливість створити зв’язок з обох сторін, отже можна отримати доступ до локального сервера з інтернету.

Статичний NAT також підтримує такі типи трансляції:

– для зіставлення декількох IP-адрес і вказаних діапазонів портів з однією і тією ж IP-адресою і різним діапазоном портів

– щоб зіставити певну IP-адресу та порт з іншою IP-адресою та портом

```
ip nat inside source static tcp 10.0.1.10 80 213.234.10.2 1125
ip nat inside source static tcp 10.0.1.11 80 213.234.10.2 1126
ip nat inside source static tcp 10.0.1.10 443 213.234.10.2 1225
ip nat inside source static tcp 10.0.1.11 443 213.234.10.2 1226
```

Рисунок 3.10 – налаштування static NAT

Отже після усіх налаштувань можна перевірити коректність реалізації DMZ зони. Для цього потрібно створити запит з сервера який імітує інтернет до локального сервера в підмережі LAN3.

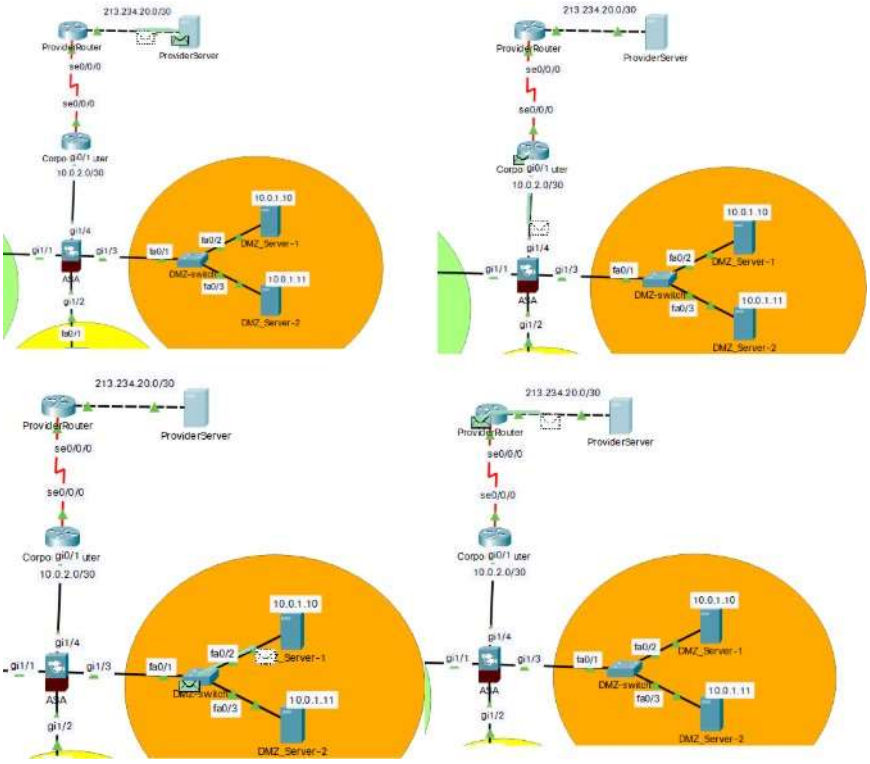


Рисунок 3.11 – процес запиту з інтернету на сервер в DMZ зоні

Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 213.234.20.2, Dest. IP: 213.234.10.2	Layer 3: IP Header Src. IP: 213.234.20.2, Dest. IP: 10.0.1.10
Layer 2: Ethernet II Header 00E0.A36D.A57E >> 0003.E45D.5A01	Layer 2: Ethernet II Header 0030.A3E6.BC02 >> 00D0.BC18.EB04
Layer 1: Port GigabitEthernet0/0	Layer 1: Port GigabitEthernet1/4

Рисунок 3.12 – процес зміни IP-адреси призначення після проходження пакету через маршрутизатор

Під час тестування роботи DMZ (рисунок 3.10) чітко видно, як змінюється IP-адреса призначення з 213.234.10.2 на 10.0.1.0. А отже процес перетворення адрес із допомогою static NAT, виконується коректно.

3.4 Захист мережі

Згідно варіанту мені потрібно заборонити будь-який дозвіл обніму трафіку між локальними мережами і одночасно дозволити усім підмережамати доступ в інтернет. Це задача реалізовується за допомогою раніше описаних списків доступу[12].

Отже, ACL - це певний набір правил для контролювання потоку інформації через певний пристрій. Оскільки у раніше створеній топології увесь мережевий трафік проходить через файрвол то найдоцільніше буде саме на ньому і фільтрувати увесь трафік[8].

Відповідно мого варіанту, LAN1 повинен мати доступ тільки в інтернет. Тоді за допомогою всього трьох правих я зможу заборонити доступ до двох сусідніх підмереж і одночасно дозволити до усіх інших, тобто інтернету.

```
access-list FROM-LAN1 extended deny ip 192.168.6.0 255.255.255.0 10.0.1.0 255.255.255.0
access-list FROM-LAN1 extended deny ip 192.168.6.0 255.255.255.0 10.0.3.0 255.255.255.0
access-list FROM-LAN1 extended permit ip 192.168.6.0 255.255.255.0 any
access-group FROM-LAN1 in interface LAN1
```

Рисунок 3.13 – списки доступу для контролювання вхідного трафіку з LAN1

Як тільки було добавлене хоч одне правило контролю пакетів, попередньо налаштована технологія динамічного фільтрування трафіку вимикається. Отже знову з’явилась проблема блокування пакетів- відповідей з інтернету. Тому потрібно одразу створити правила на інтерфейс, якай веде до зовнішньої мережі. У ньому потрібно дозволити icmp відповіді та http протокол для коректної роботи мережі. Також потрібно створити ще два прали, які згодом знадобляться для правильної роботи DMZ зони[13].

```
access-list FROM-OUTSIDE extended permit icmp any 192.168.6.0 255.255.255.0 echo-reply
access-list FROM-OUTSIDE extended permit icmp any 10.0.3.0 255.255.255.0 echo-reply
access-list FROM-OUTSIDE extended permit icmp any 10.0.1.0 255.255.255.0 echo-reply
access-list FROM-OUTSIDE extended permit tcp any eq www any
access-list FROM-OUTSIDE extended permit tcp any eq 433 any
access-list FROM-OUTSIDE extended permit tcp any 10.0.1.0 255.255.255.0 eq www
access-list FROM-OUTSIDE extended permit tcp any 10.0.1.0 255.255.255.0 eq 443
access-group FROM-OUTSIDE in interface outside
```

Рисунок 3.14 – списки доступу для контролювання вхідного трафіку із зовнішньої мережі

Отже, тепер можна перевірити коректність створених списків доступу просто спробувавши зайти на сайт сервера в інтернеті.

Рисунок 3.15 – списки доступу для контролювання вхідного трафіку із зовнішньої мережі

Після вдалого налаштування списків доступу, можна створити такі ж ід ля інших підмереж, адже їх задача таж сама, заборонити доступ в сусідні підмережі та дозволити доступ в інтернет.

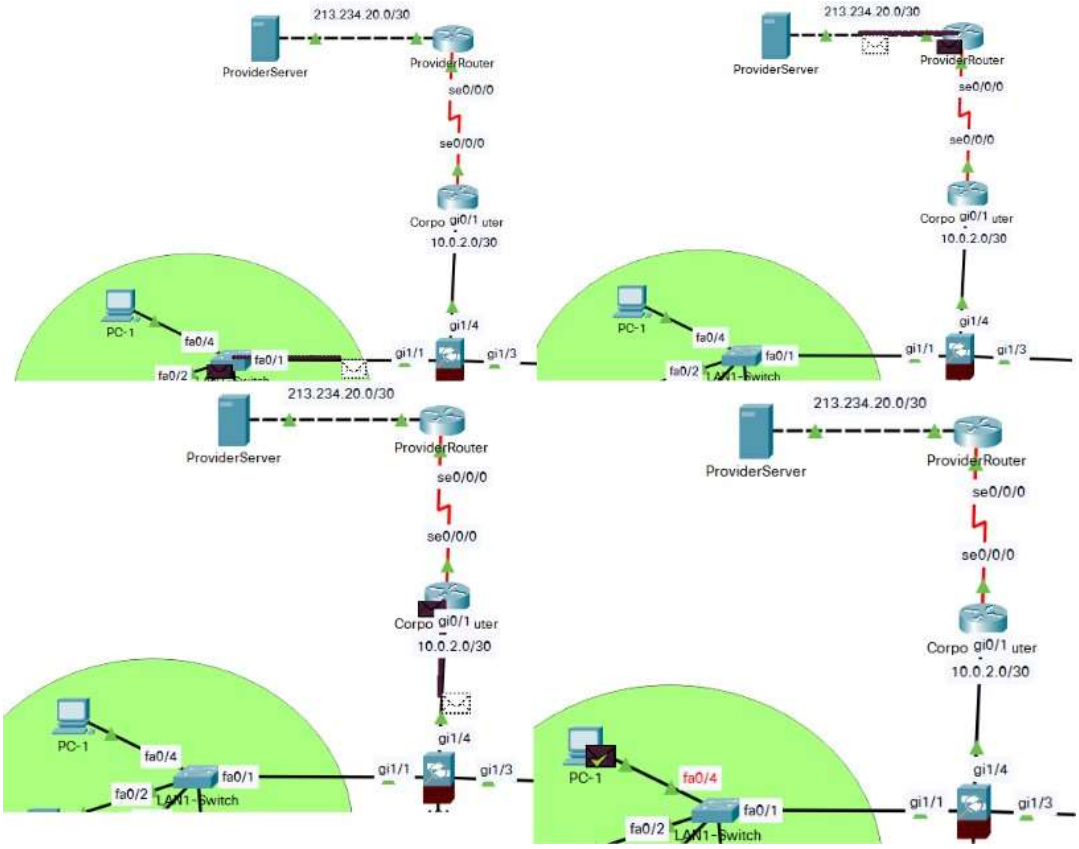


Рисунок 3.16 – перевірка коректності роботи мережі після налаштування списків доступу

Також для віддаленої роботи потрібно налаштувати ssh авторизацію. Для того щоб можна було підключитись до мережевого екрану віддалено. SSH – це захищений мережевий протокол для отримання віддаленого доступу до вузлів чи кінцевого пристрою в мережі. Це логічний розвиток протоколу telnet. Адже telnet створює не зашифрований трафік і його можна запросто прослуховувати, виконавши атаку людина посередині. Тому рекомендується використовувати тільки ssh. Через те, що весь трафік шифрується, але це не означає створювати простіші паролі, тому що навіть зашифрований пароль можна взламати[14].

Для налаштування ssh на мережевому екрані cisco потрібно створити користувача ввівши команду «username» та новий логін і пароль для нього.Далі потрібно активувати технологію ssh і разом з нею вказати яка і звідкимережа зможе авторизуватись. І для завершення потрібно вказати щоавторизація буде виконуватись саме за тими даними, які було створено раніше[15].

```
username admin password pqrZ2iqRGgDD9cbU encrypted
ssh 10.0.3.0 255.255.255.0 LAN2
ssh 192.168.6.0 255.255.255.0 LAN1
ssh timeout 5
```

Рисунок 3.17 – налаштування ssh

```
C:\>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l admin 192.168.6.1

Password:



ASA>
```

Рисунок 3.18 – процес з’єднання з мережевим екраном використовуючи ssh

Отже, після всіх налаштувань та перевірок списків доступу та технології ssh, можна зробити висновок що дана мережа достатньо захищена. Адже у ній значно обмежений рух трафіку та доступу. Усе це було зроблено для підвищення безпеки та надійності корпоративної мережі.

3.5 Розрахунок собівартості мережі

Так як мережа створюється для невеликого підприємства варто стежити за співвідношенням ціни/якості мережної інфраструктури. Адже якщо використовувати занадто дороге обладнання, воно не буде працювати на повну потужність і результативсність цієї мережі не буде відповідати її занадто високої вартості.

Згідно розробленої логічної та фізичної топологій у мережі буде використано 5 робочих станцій, 3 сервера, 1 апаратний брандмауер, 3 комутатора та 1 маршрутизатор.

В якості робочих станцій застосуємо Everest Office 104 на базі процесора Intel Core i5-10400 (2.9 — 4.3 ГГц) із обсягом ОП 16 ГБ та обсгягом SSD 240 ГБ (рис. 3.19)

Рисунок 3.19 – Робоча станція Everest Office 1041

В якості сервера будемо використовувати збірку HPE DL20 Gen9 2LFF / E3-1225v6 на базі процесор ntel Xeon Quad-Core E3-1225 v6 (3.3 - 3.7 ГГц) із обсягом ОП 16 ГБ (рис 3.20):

Рисунок 3.20 – Сервер HPE DL20 Gen9 2LFF / E3-1225v6

Мережне обладнання використаємо від компанії Cisco, а саме брандмауер Cisco ASA 5506-X (рис. 3.21), комутатор Cisco WS-C2960-24-S TP-LINK TL-SG116 (рис 3.22) та маршрутизатор CISCO2911/K9 (рис 3.23).

Рисунок 3.21 – Брандмауер Cisco ASA 5506-X

Рисунок 3.22 – Комутатор Cisco WS-C2960-24-S

Рисунок 3.23 – Роутер CISCO2911/K9

Дані розрахунків зведені у таблицю 3.3.

Таблиця 3.3 – Розрахунок вартості мережі

Пристрій	Модель пристрою	Кількість	Ціна, грн	Загальна вартість, грн
Маршрутизатор	CISCO2911/K9	1	49779	49779
Комутатор	Cisco WS-C2960-24-S TP-LINK TL-SG116	3	12478	37434
Файрвол	Cisco ASA 5506-X	1	15 619	15 619
Сервер	HPE DL20 Gen9 2LFF / E3-1225v6	3	24 082	72082
Робоча станція	Everest Office 1041	5	11 199	55 995
Стійка	CMS 24U	3	5 000	15 000
			Всього	245 909 грн

3.6 Висновки

У розділі було розроблено логічну та фізичну тополгії мережі, розроблено схему адресації та сегментації мережі, виконано конфігурування мережних пристроїв відповідно до обраної схеми адресації. Виконано тестування та перевірку проходження трафіку мережею. Виконано вибір та розраховано вартість впровадження даної мережі.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було проаналізовано і досліджено предметну область, теоретичну інформацію про проєктування комп'ютерних мереж. Автором дослідження була спроєктована, розроблена та реалізована комп'ютерна мережа малого офісу з ціллю налаштування пристроїв захисту інформації компанії від небажаного злому.

Було проведено огляд наявних засобів для моделювання та дослідження мереж та обрано в якості такого пакет Packet Tracer від компанії Cisco. За допомогою нього було 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.

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ

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

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

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

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

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

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

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

8 Виктор Олифер, Наталья Олифер Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – СПБ.: Питер, 2020. – 1008с.

9 Security level [Електронний ресурс] Режим доступу: https://geek-university.com/ccna-security/asa-security-levels-explained. – Назва з екрана. (електронне джерело).

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

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

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

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

14 Aditya Mukherjee. Network_Security_Strategies 2020. - 390c.

15 Sai Huda. Next Level Cybersecurity. Detect the Signals, stop the Hack. 2021. – 220c.

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

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

18 Офіційний сайт емулятора GNS 3 (Електронний ресурс). Режим доступу: www/ URL: https://gns3.com/

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

ДОДАТОК А

(обов'язковий)

Налаштування брандмауера Cisco ASA 5506-х

```
ASA Version 9.6(1)
!
hostname ASA
domain-name ASA.com names
!
interface GigabitEthernet1/1 description LAN1
nameif LAN1 security-level 95
ip address 192.168.6.1 255.255.255.0
!
interface GigabitEthernet1/2 description LAN2
nameif LAN2 security-level 95
ip address 10.0.3.1 255.255.255.0
!
interface GigabitEthernet1/3 nameif DMZ
security-level 50
ip address 10.0.1.1 255.255.255.0
!
interface GigabitEthernet1/4 description to CorporateRouter nameif outside
security-level 0
ip address 10.0.2.2 255.255.255.252
!
interface GigabitEthernet1/5 no nameif
no security-level no ip address shutdown
!
interface GigabitEthernet1/6 no nameif
no security-level no ip address shutdown
!
interface GigabitEthernet1/7 no nameif
```

no security-level no ip address shutdown

!

interface GigabitEthernet1/8 no nameif

no security-level no ip address shutdown

!

interface Management1/1 management-only

no nameif

no security-level no ip address shutdown

!

!

route outside 0.0.0.0 0.0.0.0 10.0.2.1 1

!

access-list FROM-LAN1 extended deny ip 192.168.6.0 255.255.255.0 10.0.1.0

255.255.255.0

access-list FROM-LAN1 extended deny ip 192.168.6.0 255.255.255.0 10.0.3.0

255.255.255.0

access-list FROM-LAN1 extended permit ip 192.168.6.0 255.255.255.0 any

access-list FROM-OUTSIDE extended permit icmp any 192.168.6.0 255.255.255.0 echo- reply

access-list FROM-OUTSIDE extended permit icmp any 10.0.3.0 255.255.255.0 echo-reply access-list FROM-OUTSIDE extended permit icmp any 10.0.1.0 255.255.255.0 echo-reply access-list FROM-OUTSIDE extended permit tcp any eq www any

access-list FROM-OUTSIDE extended permit tcp any eq 433 any

access-list FROM-OUTSIDE extended permit tcp any 10.0.1.0 255.255.255.0 eq www access-list FROM-OUTSIDE extended permit tcp any 10.0.1.0 255.255.255.0 eq 443 access-list FROM-LAN2 extended deny ip 10.0.3.0 255.255.255.0 10.0.1.0 255.255.255.0

access-list FROM-LAN2 extended deny ip 10.0.3.0 255.255.255.0 192.168.6.0

255.255.255.0

access-list FROM-LAN2 extended permit ip 10.0.3.0 255.255.255.0 any

access-list FROM-DMZ extended deny ip 10.0.1.0 255.255.255.0 10.0.3.0 255.255.255.0

access-list FROM-DMZ extended deny ip 10.0.1.0 255.255.255.0 192.168.6.0

255.255.255.0

access-list FROM-DMZ extended permit ip 10.0.1.0 255.255.255.0 any

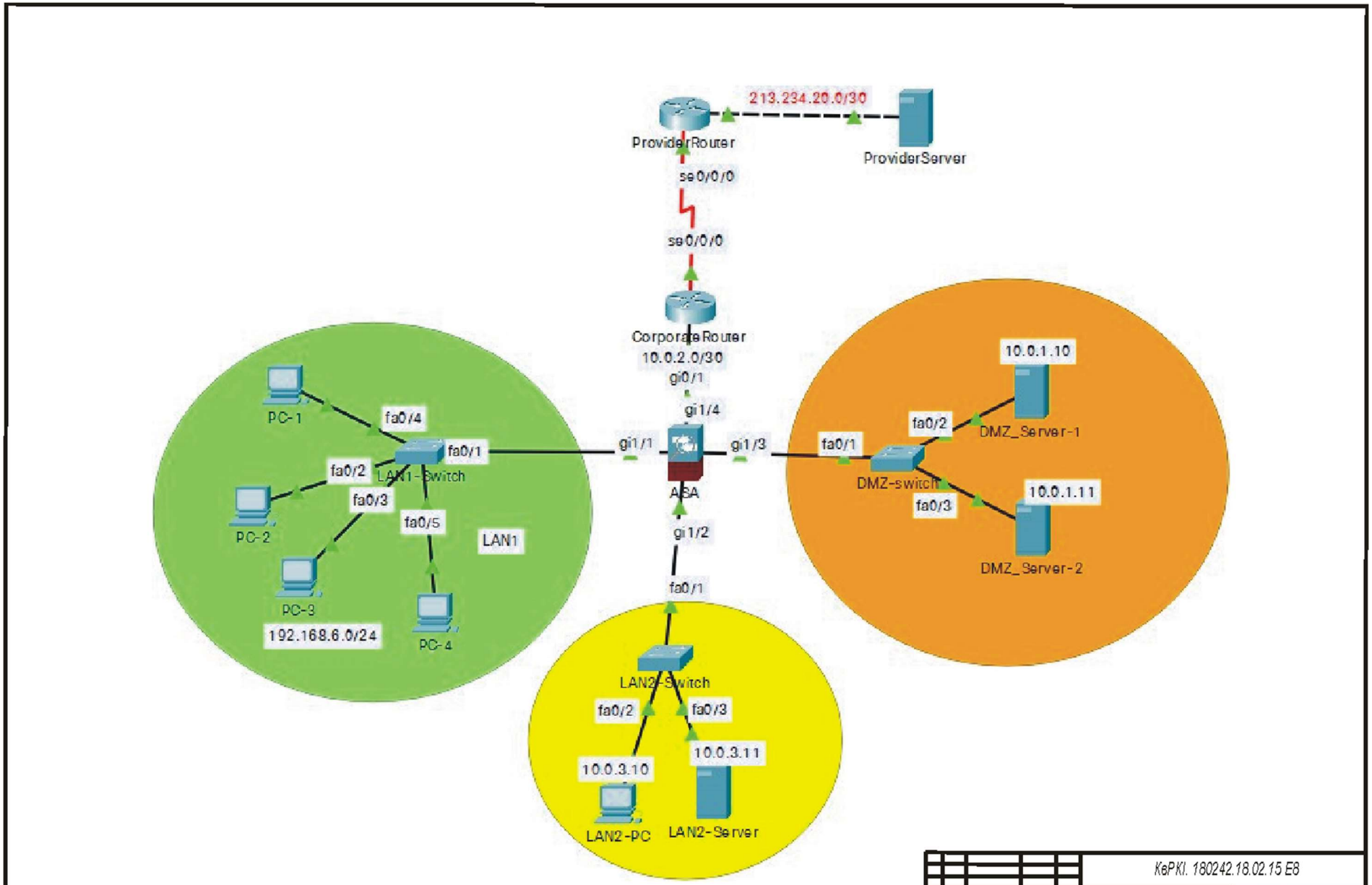
!

```
!
access-group FROM-LAN1 in interface LAN1 access-group FROM-OUTSIDE in interface outside
access-group FROM-LAN2 in interface LAN2 access-group FROM-DMZ in interface DMZ
!
aaa authentication ssh console LOCAL
!
username admin password pqrZ2iqRGgDD9cbU encrypted
!
class-map inspection_default match default-inspection-traffic
!
policy-map global_policy class inspection_default inspect http
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh 10.0.3.0 255.255.255.0 LAN2
ssh 192.168.6.0 255.255.255.0 LAN1
ssh timeout 5
!
```

ДОДАТОК Б

(обов'язковий)

Копія графічної частини



Зм.	Арк.	№докум.	Підпис	Дата

КвРКІ. 180242.18.02.15 ПЗ

Арк. 63

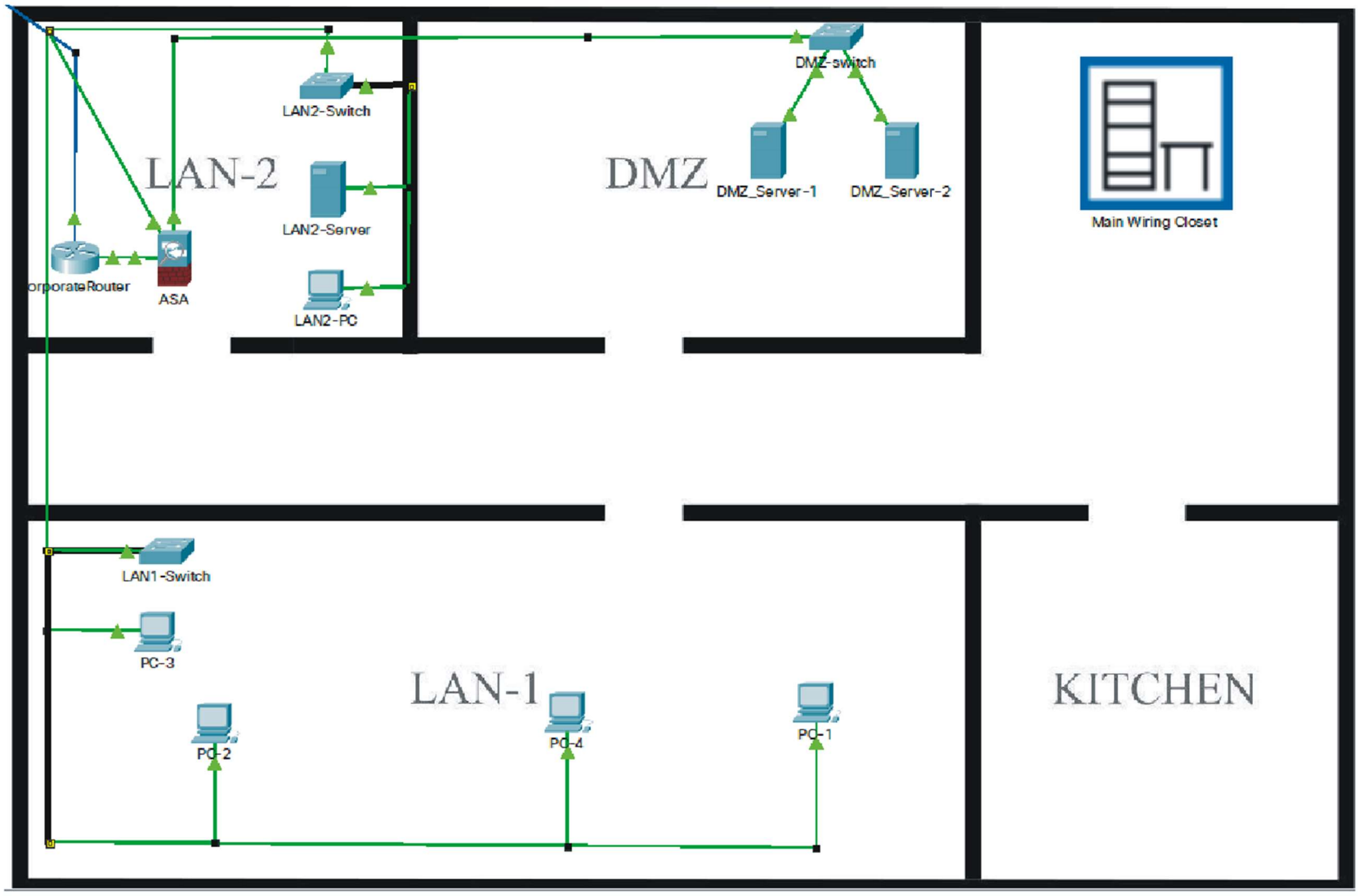
КвРКІ. 180242.18.02.15 Е8

Зм.	Арк.	№ докум.	Підпис	Дата
Розробив	Олексенко Р.Р.			
Перевір.	Мостовий С.В.			
Т. контр.				
Н. контр.	Мостовий С.В.			
Затвердб.	Мороз Ю.П.			

Захищена комп'ютерна мережа малого офісу
Логічна топологія мережі

Літера	Маса	Масшт.
Аркуш 1	Аркушів 2	

ХНУ, гр. КІ-18-2



Зм.	Арк.	№докум.	Підпис	Дата

КвРКІ. 180242.18.02.15 ПЗ

Арк. 64

КвРКІ. 180242.18.02.15 Е8

Вид.	Арк.	№докум.	Підпис	Дата
Розробив		Степанюк Р.Р.		
Перевір.		Мостовий С.В.		
Т. контр.				
Н. контр.		Мостовий С.В.		
Затверд.		Кіяєць Ю.П.		

Захищена комп'ютерна мережа малого офісу
Фізична топологія мережі

Літера	Маса	Масштаб
Аркуш 2	Аркушів 2	

ХНУ, гр. КІ-18-2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Степанюк Ростислав Романович

Тема Захищена комп'ютерна мережа малого офісу

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 2; кількість сторінок записки 64

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та налаштовано комп'ютерну мережу малого офісу 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 корпоративних мереж за захисту даних у них, виконана постановка задачі. В другому розділі виконано аналіз наявніх засобів для проектування та моделювання роботи мереж та обгрунтовано вибір пакету для роботи. В третьому розділі розроблено фізичну та логічну топологію мережі, обрано схему адресації та маршрутизації, проведено конфігування всіх мережних пристроїв, протестовано проходження тарфіку 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 захищених мереж невеликих .

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) Пермінов Валерій Володимирович, завідувач кафедрою автоматизації та комп'ютерно-інтегрованих технологій

«13» 06 2022р. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

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: Захищена комп'ютерна мережа малого офісу

Автор: Степанюк Ростислав Романович

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 загальновживаними 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 13.4% і адресується до 240 першоджерел, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ С.В. Мостовий

Завідувач кафедри КБ, гарант ОП _____ Ю.П. Кльоц

Дата: 13.06.2022

Mon Jun 13 09:22:38 EEST 2022, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 8.0%

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

ID: 105082 Название: Захищена комп'ютерна мережа малого офісу Добавлено в БД: 2022-06-13 Авторы: Степанюк Р.Р. Руководители: Андрощук О.А. Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	51582	748	5756 (11%)	93 (12%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011556322

Дата перевірки:
13.06.2022 10:20:30 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.06.2022 10:21:51 EEST

ID користувача:
100008300

Назва документа: **На плагіат Степанюк**

Кількість сторінок: **59** Кількість слів: **9034** Кількість символів: **69505** Розмір файлу: **2.79 MB** ID файлу: **1011427887**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

13.4%
Схожість

Найбільша схожість: **2.8%** з Інтернет-джерелом (http://samzan.net/188675)

11.4% Джерела з Інтернету	113	Сторінка 61
2.59% Джерела з Бібліотеки	127	Сторінка 62

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	1
Підозріле форматування	14 сторінок