Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комп'ютерна мережа магазину з розмежуванням доступу користувачів
Назва теми

КвРКІ 180225.18.02.02 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 _____ М.С. Бойко
Підпис Ініціали, прізвище

Керівник _____ 10.06.22 _____ Ю.П. Кльоц
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ 10.06.22 _____ С.В. Мостовий
Підпис, дата Ініціали, прізвище

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

«10» 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

Зав. кафедри Ю.П. Кльоц

" 11 " 01 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Бойко Микиті Сергійовичу

Прізвище, ім'я, по батькові студента

1 Тема проекту (роботи) Комп'ютерна мережа магазину з розмежуванням доступу користувачів.

Керівник проекту (роботи) Кльоц Юрій Павлович к.т.н., доцент

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

Затверджена наказом ректора університету від 01.03.2022 р. № 18

2. Строк подання студентом проекту (роботи) на кафедру 02.06.2022 р.

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

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

Дослідження кіберфізичної системи «Розумний будинок» та постановка задачі

Проєктування підсистем керування електроживленням та відслідковування енергоспоживання в режимі реального часу

Програмно-апаратна реалізація та тестування підсистем керування електроживленням та відслідковування енергоспоживання в режимі реального часу в кіберфізичній системі «Розумний будинок»

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

Схеми логічної та фізичної топології мережі

6. Консультанти розділів дипломного проекту (роботи)

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

7 Дата видачі завдання «_11_»_____01_____2022 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2022	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2022	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2022	виконано
4	Робота над розділом 2 – формування вимог	01.04.2022	виконано
5	Робота над розділом 3 – програмно-апаратна реалізація комп'ютерної мережі	30.04.2022	виконано
6	Оформлення пояснювальної записки згідно вимог	31.05.2022	виконано
7	Попередній захист ВКР	02.06.2022	виконано
8	Захист ВКР на засіданні ЕК	Червень 2022 року	

Студент _____ М.С. Бойко
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 180225 18.02.02 ПЗ	Пояснювальна записка	59		
			Графічні матеріали			
2		КвРКІ 180225 18.02.02	Логічна топологія	1		
3		КвРКІ 180225.18.02.02	Фізична топологія	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 180225 18.02.02 ВП		
Розробив		Бойко М.С.		10.06.22	Відомість проєкту	Літера	Аркуш	Аркушів
Перевір.		Кльоц Ю.П.		10.06.22		У	1	1
Н. контр.		Мостовий С.В.		10.06.22		ХНУ, КІ-18-2		
Затв.		Кльоц Ю.П.		10.06.22				

АНОТАЦІЯ

Автор: Бойко Микита Сергійович.

Назва роботи: Комп'ютерна мережа магазину з розмежуванням доступу користувачів

Спеціальність: 123 – комп'ютерна інженерія

Освітньо-професійна програма: Комп'ютерна інженерія

Анотація: Метою кваліфікаційної роботи є проєктування та реалізація комп'ютерної мережі магазину з розмежуванням доступу. Поставлена у кваліфікаційній роботі мета досягається розв'язанням наступних задач:

1) виконати аналіз існуючих методів та засобів вирішення поставленої задачі;

2) здійснити обґрунтований вибір мережевого обладнання для створення комп'ютерної мережі магазину та проаналізувати середовища передачі даних в системі.

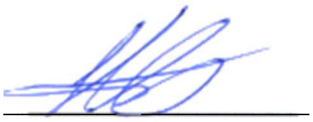
3) визначити список задач, які має виконувати комп'ютерна мережа магазину з демілітаризованою зоною. Згідно розроблених задач скласти імітаційну модель корпоративної мережі. Описати процес створення DMZ-зони та її налаштування в Cisco Packet Tracer, спроектувати комп'ютерну мережа магазину з розмежуванням доступу користувачів.

Отримані результати і їх новизна – бюджетний варіант комп'ютерної мережі магазину з розмежуванням доступу користувачів, що дозволяє підвищити ефективність роботи та функціонування системи.

Область застосування – комп'ютерна інженерія, інженерія комп'ютерних мереж та кібербезпека.

Ключові слова: Система з розмежованим доступом, інформаційна система, волоконна лінія, розмежований доступ, демілітаризована зона, канали передачі.

Кількість сторінок: 86



Підпис студента

26.05.2022

Дата

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ 4
ВСТУП..... 5
1 ДОСЛІДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ З РОЗМЕЖОВАННЯМ ДОСТУПУ КОРИСТУВАЧІВ ТА ПОСТАНОВКА ЗАДАЧІ 6
1 1 Концепція комп'ютерної мережі з розмежуванням доступу 6
1.2 Принцип роботи комп'ютерної мережі з демілітаризованою зоною 6
1.3 Переваги у використанні демілітаризованої зони 7
1.4 Порівняльний аналіз переваг та недоліків існуючих архітектурних рішень по проектуванню систем з розмежованим доступом 9
1.5 Аналіз важливості і необхідності комп'ютерних мереж з розмежуванням доступу 11
1.6 Висновки. Постановка задачі 12
2 ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАГАЗИНУ З РОЗМЕЖОВАННЯМ ДОСТУПУ КОРИСТУВАЧІВ 14
2.1 Вимоги по проектуванню мережі 14
2.2 Вибір топології мережі 16
2.3 Вибір середовищ передачі даних в комп'ютерній мережі магазину 19
2.4 Обґрунтування вибору мережевих пристроїв для реалізації комп'ютерної мережі магазину 21
2.5 Вимоги до програмного забезпечення та його функціонал..... 24
2.6 Вимоги до захисту мережевих пристроїв 25
2.7 План виконання роботи 26
2.8 Висновки 27
3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАГАЗИНУ З РОЗМЕЖУВАННЯМ ДОСТУПУ 28
3 1 Проектування комп'ютерній мережі магазину з розмежованим доступом 28

3.2 Розробка топології та розподіл ролей в комп’ютерній мережі магазину 29
3.3 Налаштування демілітаризованої зони в комп’ютерній мережі магазину 36
3.4 Розгортання та налаштування комп’ютерної мережі магазину за допомогою засобу імітаційного моделювання..... 43
3.4 Налаштування захисту на мережевому обладнанні. 48
3.5 Тестування комп’ютерної мережі магазину в розмежуванням доступу 50
3.6 Створення фізичної топології 53
3.7 Розрахунок вартості обладнання та кабельних мереж для комп’ютерної мережі 57
3.8 Висновки 58
ВИСНОВКИ..... 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 62
Додаток А Копія графачної частини 66
Додаток Б Лістинг налаштувань мережевих пристроїв 68

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AAA – Authentication, authorization and accounting

CLI – Command line interface

DMZ – Demilitarized zone

DNS – Domain name system

DHCP – Dynamic host configuration protocol

FTP – File transfer protocol

LAN – Local area network

MPF - Modular policy framework

NAT – Network address translation

PAT – Port Address Translation

IoT – Internet of things

SSH – Secure shell

VPN – Virtual private network

VLAN – Virtual local area network

WAN – Wide area network

WLAN – Wireless local area network

ВСТУП

В сучасних реаліях тяжко уявити будь-яку організацію без локальної мережі і відсутнім доступом до інтернету - технології, яка поліпшує роботу будь-якої компанії забезпечуючи доступ до інформації, обміну документами та різного виду даними. Але це з одного боку. З іншої сторони при широкому використанні мережі Інтернет виникає потреба у вирішенні проблеми захисту інформації а також локальної мережі в цілому.

Питання безпеки особливо істотно постає, коли компанія має публічні інтернет-сервіси такі як: веб-сервери, файлові-сервери, сервіси для поштової розсилки, які розміщені в локальної комп'ютерній мережі. До таких серверів надається вільний доступ, тобто будь-який користувач може без виконання авторизації або аутентифікації, отримати доступ до розміщених на веб-сервері ресурсів, до розділів файлового-сервера і немає ніякої гарантій в тому, що разом з листом який прийде поштою не потрапить на сервер шкідливе ПЗ і що серед тисячі користувачів не виявиться одного такого, хто захоче з конкурентних або власних мотивів отримати доступ до локальної мережі організації.

Саме тому метою роботи є проектування і реалізація комп'ютерної мережі магазину з розмежованим доступом користувачів.

Об'єктом дослідження є апаратно-технічний засіб – комп'ютерна система (мережа) магазину з розмежованим доступом користувачів в інструментарії візуального моделювання Cisco Packet Tracer.

Предметом дослідження є комп'ютерні мережі з розмежованим доступом користувачів, способи реалізації демілітаризованої зони в комп'ютерних системах.

Практична цінність роботи полягає в спроектованій та змодельованій комп'ютерній мережі магазину з розмежованим доступом користувачів, яка має місце бути в сучасних реаліях.

1 ДОСЛІДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ З РОЗМЕЖОВАННЯМ ДОСТУПУ КОРИСТУВАЧІВ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Концепція комп'ютерної мережі з розмежуванням доступу

Системою з розмежованим доступом, або як її ще називають демілітаризована зона – здебільшого являє собою підмережу, яка знаходиться між публічною мережею і приватною мережею підприємства[1-3].

Кінцевою метою ДЗ є надання доступу організації до недовірених мереж, таких як інтернет, і при цьому забезпечувати безпеку своєї приватної або локальної мережі. Сучасні організації зберігають зовнішні послуги і ресурси, як і сервери для систем доменних імен(DNS), зберігання файлів(FTP), пошти, проксі, телефонні лінії(VoIP) і веб сервери в мережах з розмежованим доступом.

Дані сервери і ресурси ізольовані і мають обмежений доступ до локальної або приватної мережі, щоб до них був доступ ззовні(з інтернету) але щоб internal LAN(внутрішня локальна мережа) до них не мала доступу. І як результат створення мережі з ДЗ ускладнює життя хакера-зловмисника, який намагається отримати прямий доступ до даних організації і внутрішніх серверів через мережу інтернет.

1.2 Принцип роботи комп'ютерної мережі з демілітаризованою зоною

Для більш наглядного прикладу принципу роботи комп'ютерної мережі розглянемо ситуацію, коли в нас є бізнес з веб-сайтом, в якого є власна вибірка користувачів і для якого потрібно надати доступ з мережі інтернет. Якщо надати публічний доступ до такого веб-сайту, без брандмауера, то про надійність внутрішньої мережі можна забути. Щоб запобігти ризикам, організація може: платити хостинговій фірмі за розміщення веб-сайту або встановити брандмауер(firewall), але це вплине продуктивність роботи нашого сервісу. Тому замість того публічні сервера розміщуються в окремій та ізольованій мережі[4].

Мережа з розмежуванням доступу, в даній ситуації, забезпечує буфер між інтернетом і приватною мережею організації. Дана мережа ізольована шлюзом безпеки(security gateway), тобто мережевим екраном, який фільтрує трафік між DMZ і LAN. Стандартний DMZ-сервер захищений іншим брандмауером який фільтрує трафік який надходить із зовнішніх мереж.

В ідеальному середовищі він розташований між двома брандмауерами, а налаштування DMZ брандмауера гарантують, що вхідний пакети перевіряються брандмауером(або іншим засобом безпеки), перед тим, як вони доберуться до серверів розміщених у ДЗ. А це означає, що навіть якщо досвідчений зловмисник спромігся подолати перший брандмауер, то йому доведеться до захищених служб у ДЗ, перш ніж нашкодити бізнесу.

Якщо зловмиснику вдалося пробитись через брандмауер і скомпрометувати роботу системи в ДЗ їм також потрібно пройти через внутрішній брандмауер перед тим як отримати доступ до конференційної інформації підприємства. Тому навіть якщо зловмиснику до снаги пройти безпеку ДЗ, це має відбиватись на ресурсах в ній і видавати попередження про те, що в системі відбувається порушення.

Також є відома практика, коли організаціям потрібно моніторинг на таких системах і вони роблять проксі сервер в ДЗ. Це дає їм можливість з легкістю перевіряти і записувати активність користувачів, встановлювати фільтрацію веб-контенту і надавати робітникам системи доступ до інтернету.

1.3 Переваги у використанні демілітаризованої зони

Основний плюс ДЗ – це надання внутрішній мережі розширеного рівня безпеки, обмежуючи доступ до конфіденційних даних і серверів. ДЗ надає можливість відвідувачам веб-сайту отримувати певні послуги, забезпечуючи буфер між ними і мережею організації. Як результат ДЗ також надає додаткові переваги в безпеці(рис. 1.1), такі як[3,4]:

- контроль доступу (enabling access control);
- запобігання розвідці мережі (preventing network reconnaissance);
- блокування підміни IP-адреси (blocking IP spoofing).

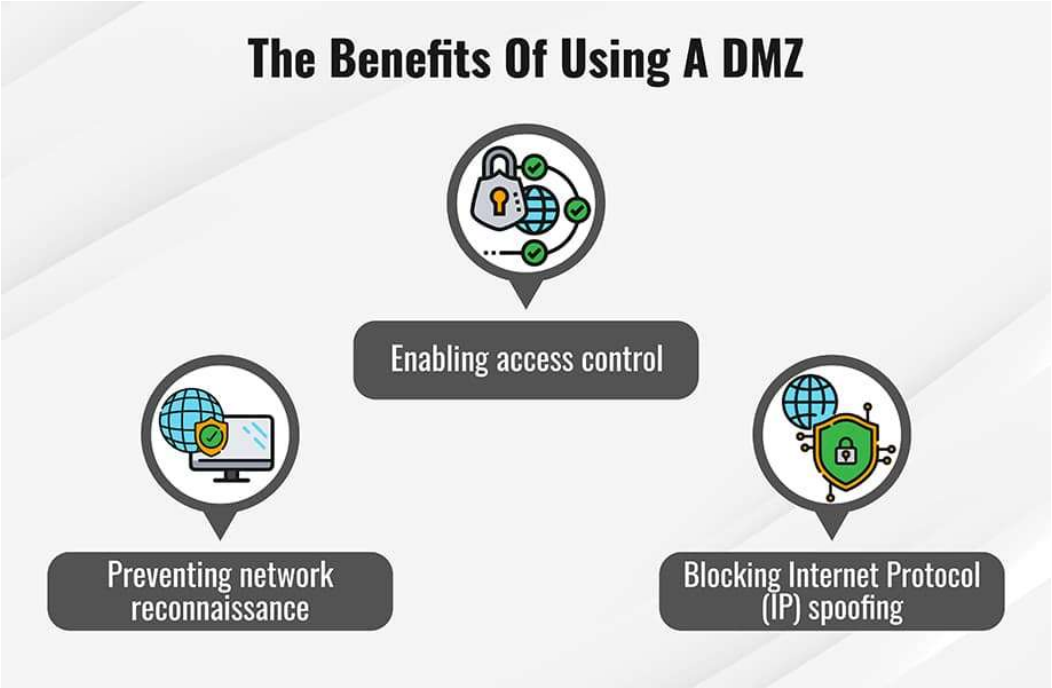


Рисунок 1.1 – Переваги у використанні демілітаризованої зони

Контроль доступу. Коли підприємства можуть надавати різного виду доступ до послуг за межами своєї мережі через Інтернет. ДЗ надає доступ до цих послуг, реалізовуючи сегментацію мережі, щоб ускладнити доступ неавторизованим користувачам до приватної мережі. ДЗ також може включати проксі-сервер, який централізує потік трафіку та спрощує моніторинг цього трафіку.

Запобігання розвідці мережі. Забезпечуючи буфер, ДЗ запобігає зловмисникам виконувати розвідувальну роботу, яку вони здійснюють для пошуку потенційних цілей. Сервери в ДЗ відкриті для всіх, але брандмауер знаходиться на іншому рівні безпеки, який не дозволяє зловмисникові бачити внутрішню мережу. Навіть якщо система ДЗ буде скомпрометована, внутрішній брандмауер відокремлює приватну мережу від ДЗ, щоб забезпечити безпеку та ускладнити зовнішню розвідку мережі.

Блокування підміни IP-адреси. Коли зловмисники намагаються знайти способи отримати доступ до систем і підробляють IP-адресу та видають себе за підтверджений пристрій, увійшов в мережу. ДЗ може виявляти та зупиняти такі спроби спуфінгу(підміни), оскільки інша служба перевіряє легітимність IP-адреси.

ДЗ також забезпечує сегментацію мережі, щоб створити простір для організації трафіку та доступу до державних послуг далеко від внутрішньої приватної мережі.

Мережу з розмежованим доступом можна використовувати з такими технологіями як:

- DNS сервери;
- FTP сервери;
- поштові сервери;
- проксі сервери;
- веб-сервери.

1.4 Порівняльний аналіз переваг та недоліків існуючих архітектурних рішень по проектуванню систем з розмежованим доступом

Демілітаризована зона являє собою відкриту мережу (wide-open network), проте існує декілька архітектурних рішень для її створення.

Систему з розмежуванням доступу можна реалізувати декількома способами, починаючи з одного брандмауер до наявності двох або й більше брандмауерів. Більшість сучасних рішень ДЗ використовують подвійні брандмауери, які в майбутньому можна розширити для розробки більш складних систем.

Підхід через один брандмауер вимагає трьох і більше мережевих інтерфейсів. Перший для зовнішньої мережі, яка під’єднана до інтернету. Другий для внутрішньої мережі, а третій для підключений до ДЗ. Різні правила і налаштування брандмауера контролюють трафік, якому дозволено отримати доступ до ДЗ, і обмежують підключення до внутрішньої мережі. Приклад даного підходу можна побачити на рисунку 1.2

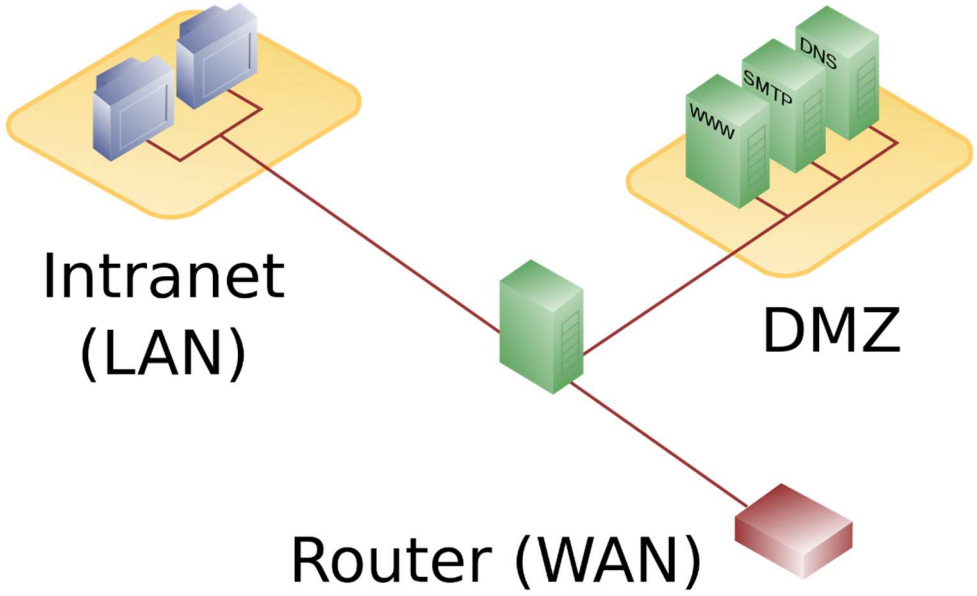


Рисунок 1.2 –Реалізація демілітаризованої зони через 1 брандмауер

Підхід через розгортання двох брандмауерів з ДЗ між ними, як правило, є більш безпечним варіантом. Оскільки перший брандмауер дозволяє лише зовнішній трафік до ДЗ, а другий дозволяє лише трафік, який надходить із ДЗ у внутрішню мережу. В даному випадку зловмиснику скомпрометувати обидва брандмауери, щоб отримати доступ до локальної мережі організації. Приклад даного підходу можна побачити на рисунку 1.3

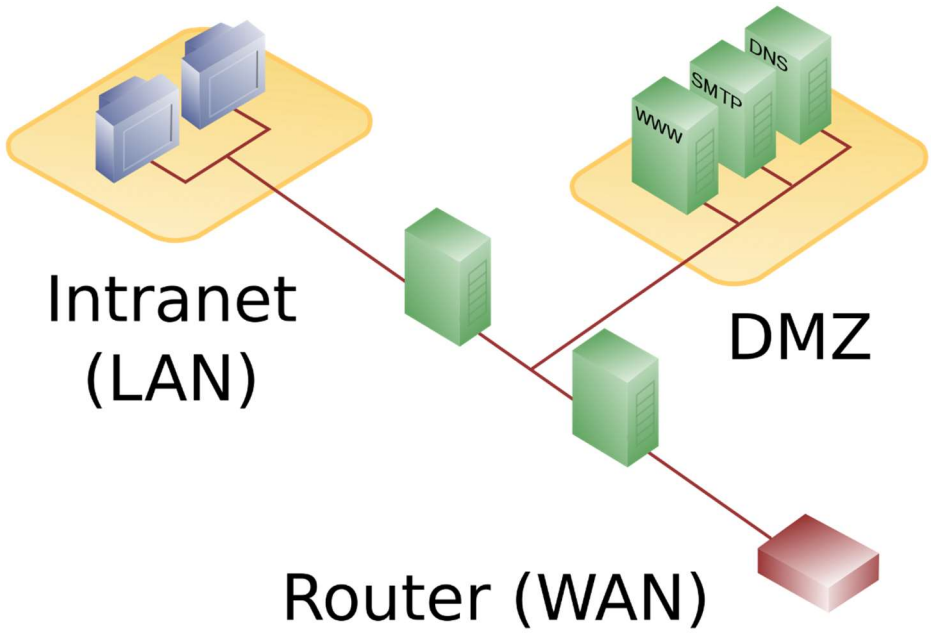


Рисунок 1.3 –Реалізація демілітаризованої зони через 2 брандмауера

Організації також можуть точно налаштувати контроль безпеки для різних сегментів мережі. Це означає, що систему виявлення вторгнень (IDS – intrusion detection system) або систему запобігання вторгненню (IPS – intrusion prevention system) в межах ДЗ можна налаштувати на блокування будь-якого трафіку, крім запитів Hypertext Transfer Protocol Secure (HTTPS) до порту 443 протоколу керування передачею (TCP).

1.5 Аналіз важливості і необхідності комп'ютерних мереж з розмежуванням доступу

Мережі з ДЗ стали основою для захисту глобальних корпоративних мереж з моменту впровадження брандмауерів. Вони захищають конфіденційні дані організацій, а також їхні системи та ресурси, відокремлюючи внутрішні мережі від систем, які можуть бути мішенню зловмисників. Також ДЗ дозволяють організаціям контролювати та зменшувати рівні доступу до чутливих систем.

Підприємства все частіше використовують контейнери та віртуальні машини для ізоляції своїх мереж або окремих програм від решти своїх систем. Зростання хмарних технологій означає, те що багатьом підприємствам більше не потрібні внутрішні веб-сервери. На сьогоднішній день бізнеси інтегрують значну частину своєї зовнішньої інфраструктури до хмар за допомогою додатків Software as-a-Service (SaaS).

Для прикладу, сервіс по наданню послуг для роботи з хмарою, як-от Microsoft Azure, дозволяє організації, яка запускає програми локально та у віртуальних приватних мережах (VPN), використовуючи гібридний підхід із ДЗ, розташованим між ними. Цей метод також можна використовувати, коли вихідний трафік потребує аудиту або для контролю трафіку між локальним центром обробки даних і віртуальними мережами.

Крім того, ДЗ виявляються корисними для протидії ризикам безпеки, створеним новими технологіями, такими як пристрої Інтернету речей (IoT - Internet-of-Things) та системи операційних технологій (OT – operational technology system), які роблять наше життя та виробництво легшим, але створюють величезну

поверхню загроз. Це виникає із-за того, що обладнання ОТ не було розроблено для протидії кібератакам або відновленню після них, як це було з цифровими пристроями IoT, що становить значний ризик для критичних даних і ресурсів організацій. ДЗ забезпечує сегментацію мережі, щоб знизити ризик атаки, яка може завдати шкоди промисловій інфраструктурі.

Ще однією причиною створення мережі з ДЗ є виснаження публічного адресного простору IPv4 стало проблемою, починаючи з середини 1990-х років. З 2011 року IANA і чотири з п'яти RIR вичерпали адресний простір IPv4. Хоча організації здійснюють перехід на IPv6, залишок адресного простору IPv4 залишається вкрай обмеженим. Це означає, що організація повинна максимізувати власну обмежену кількість публічних IPv4-адрес. Це вимагає від адміністратора мережі свого публічного адресного простору для підмережі з різними масками підмережі, щоб звести до мінімуму кількість не використовуваних адрес вузлів у підмережі.

1.6 Висновки. Постановка задачі

На першому етапі роботи було: дано конкретне означення системи з розмежованим доступом; визначено принципи роботи демілітаризованої зони, а також відбулося ознайомлення з методами створення комп’ютерної системи з розмежованим доступом.

На основі проведеного аналізу відомих технічних і комерційних рішень комп’ютерних мереж з розмежованим доступом користувачів, можна дійти висновку, що дані системи є одним з провідних способів створення мережевої безпеки в системах з публічним доступом.

На основі вище описаних методів, визначивши основні принципи роботи комп’ютерних мереж з розмежованим доступом, можна виділити основні під задачі, які необхідно виконати для реалізації комп’ютерної мережі магазину з розмежованим доступом користувачів, а саме:

1) визначитись зі способом реалізації демілітаризованої зони;

2) визначити типи необхідних мережевих пристроїв для реалізації комп’ютерної мережі;

3) розробити логічну схему мережі;

4) розробити фізичну схему мережі;

5) провести аналіз затрат згідно фізичної схеми.

На основі здійсненого аналізу існуючих рішень було визначено два можливих рішення поставленої задачі, реалізація яких буде здійснена в програмному забезпечені візуального моделювання Cisco Packet Tracer.

2 ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАГАЗИНУ З РОЗМЕЖОВАННЯМ ДОСТУПУ КОРИСТУВАЧІВ

2.1 Вимоги по проектуванню мережі

В даному розділі розглянемо основні вимоги по проектуванню комп'ютерної мережі перед тим як її створювати.

1) Вагомим етапом створення комп'ютерної мережі – це складання документації. Грамотно написана документація економить час і гроші. Незалежно від розмірів комп'ютерної мережі, по можливості потрібно задокументувати кожну деталь своєї мережі[5].

Одна з речей, яку необхідно зробити на початку будь-якого проекту – це написати документ з вимогами. Цей документ повинен включати всі вимоги до проекту, їхній опис, а також висловленні припущення.

Після створення документу з вимогами він подається вищому керівництву компанії, для того щоб воно його переглянуло і схвалило; як вимоги задокументовані та затверджені, розпочинається етап проектування.

Першим кроком при проектуванні будь-якої мережі вважається – складання списку всіх пристроїв, які будуть задіяні в мережі. У випадку з локальними мережами(LAN) варто обдумати декілька питань:

- скільки користувачів потрібно обслуговувати ?
- скільки серверів потрібно обслуговувати ?
- скільки принтерів буде в мережі і де вони знаходитимуться ?
- які застосунки оперуватимуть в мережі і яким чином користувачі взаємодіятимуть з ними(HTTP, окреме програмне забезпечення, термінали, Citrix)?
- який вид безпеки необхідно встановити ?
- чи буде збільшуватись мережа ?
- чи всі інтерфейси повинні бути гігабітними ?
- чи потрібно в мережі підтримувати VoIP?

– чи будете підтримуватись одне фізичне місце або кілька (включаючи кілька поверхів в одній будівлі)?

Кінцевою метою є – визначення кінцевого числа типів інтерфейсів для користувачів. Врахувавши ці цифри, вирішується, яке обладнання необхідно замовити та складається список. Потім згідно цього списку складається таблиця пристроїв з розподілом ролей для них.

Сумісно з фізичним плануванням пристроїв і їхніх портів, виникає необхідність в складані мапи IP-адресації і VLAN-шарів. На даному етапі здійснюється планування наперед, навіть, коли ще не визначено точно з відділами в мережі. Створюється таблиця для кожної підмережі, в яку будуть заноситись дані про кожен пристрій в мережі і виділений для нього VLAN.

Наступним кроком є створення макету(плану) для розміщення мережевого обладнання на стійці, підведення живлення та системи охолодження.

Після того як всі попередні етапи пройдені інженер переходить до створення фізичної та логічної топології комп'ютерної мережі. При цьому варто притримуватись декількох правил:

– не ускладнювати(чим більше включити в малюнок, тим важче його буде зрозуміти);

– розділити фізичні і логічні ідеї.

2) Архітектурний підхід в створені комп'ютерних мереж – це вибір виключно інженера комп'ютерної мережі, оскільки тільки він вирішує і відповідає за подальшу її експлуатацію, проте, існують окремі набори правил для таких типів мереж як[5-8, 24]:

– корпоративні мережі;

– веб-сайти електронної комерції;

– сучасні віртуальні серверні середовища;

– малі мережі.

Де для малих мереж відносять малі бізнеси з одним офісом і декількома відділами. Таким мережам немає необхідності створювати триярусної архітектури,

оскільки вони по своїй суті прості, а комплексна архітектура дорога в своїй реалізації.

2.2 Вибір топології мережі

Топологія комп'ютерної мережі – це форма або фізичне розташування комп'ютерів відносно один до одного. Форма топології визначає вимоги до типу кабелю, мережевих пристроїв, можливі методи керування обміном, можливості розширення мережі, надійність роботи[8-11, 23]. Загалом можна виділити такі основні типи топології: шина; зірка; кільце або змішана.

1) «Шина» – в даній моделі всі комп'ютери паралельно підключаються до однієї лінії зв'язку та інформація від кожного комп'ютера одночасно передається всім іншим комп'ютерам.

В Топології «шина» передбачається ідентичність мережевого устаткування і рівноправність всіх абонентів. Оскільки комп'ютери здатні передавати дані тільки по черзі, оскільки лінія зв'язку у них єдина, в інакшому випадку передана інформація буде спотворена в результаті конфлікту. У даної топології відсутня можливість мати сервер, через який передаватиметься вся інформація. Для запобігання відображення сигналу, на кінцях шини(кабелю) знаходяться термінатори.

2) «Зірка» – топологія де до одного центрального комп'ютера приєднуються інші периферійні комп'ютери, де кожен з них використовує свою окрему лінію зв'язку. Приклад даної топології зображено на рисунку 2.1.

В даній топології весь обмін інформацією відбувається через центральний комп'ютер, на який розподіляється значне навантаження. Як правило, за центральним комп'ютером називають, – комутатор, і саме на нього покладаються функції управління обміном даних. Із-за того, що керування повністю централізоване, в даній топології неможливі конфлікти.

Рисунок 2.1 - Топологія мережі «Зірка»

3) «Кільце» – в даній топології комп’ютери передають інформацію завжди наступному в ланцюжку пристрою, а одержується інформація тільки від попереднього в ланцюжку.

В даній топології немає окремо виділеного центрального пристрою, але на відміну від топології «шина», тут комп’ютери не є повністю рівноправними. Однак досить часто в «кільці» виділяють спеціального абонента, який керує або контролює обмін. Як наслідок: наявність керуючого абонента знижує надійність комп’ютерної мережі, тому що його вихід з ладу відразу ж паралізує мережу.

4) «Змішана» – пристрої знаходяться на одному рівні і можуть передавати повідомлення безпосередньо один одному. При такій організації мережі знижується навантаження на канали передачі даних, але керованість мережі різко падає. Також відсутня “третя сторона“, яка може виступати арбітром при виникненні спірних ситуацій між різними організаціями і підрозділами організації. Приклад даної топології зображено на рисунку 2.2.

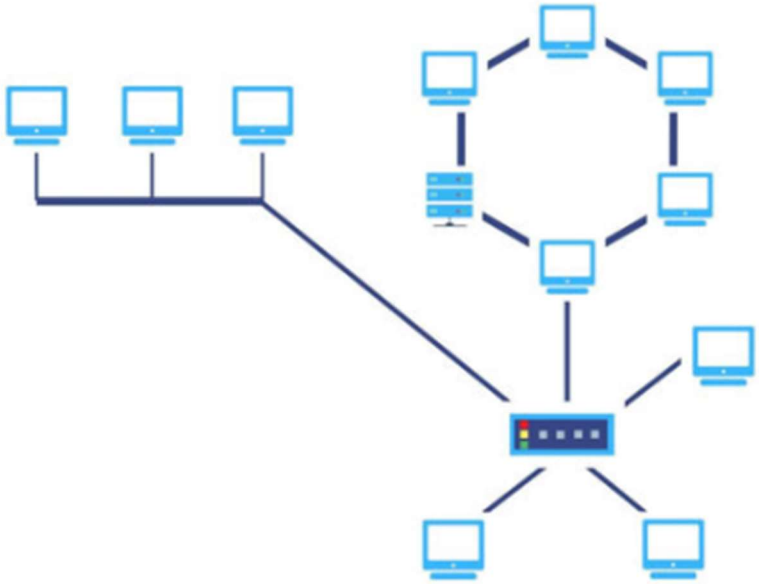


Рисунок 2.2 - Топологія мережі «Змішана»

Для створення комп’ютерної мережі підприємства типу магазину, можна виділити топологію типу, – «зірка». Дана топологія найбільш поширена в сучасних комп’ютерних мережах, оскільки вона включає в себе наступні переваги:

– вихід з ладу периферійного комп’ютера ніяк не впливає на функціонуванні іншої частини мережі;

– на лінії зв’язку перебувають тільки два абоненти: один з периферійних і центральний, що істотно спрощує мережеве обладнання в порівнянні із «шиною» і не потребує застосування додаткових зовнішніх термінаторів;

– пошкодження кабелю в якійсь конкретній точці або коротке замикання впливає тільки на один кінцевий пристрій, а всі інші комп’ютери можуть продовжувати свою роботу;

– легко локалізувати несправності;

– висока продуктивність комп’ютерної мережі.

А до недоліків «зірки» можна віднести:

– залежність від централізованих систем типу – мережевого обладнання;

– велика витрата кабелю, на відмінну від інших топологій, а це істотно впливає на вартість всієї мережі в цілому.

2.3 Вибір середовищ передачі даних в комп’ютерній мережі магазину

Після того як було визначено мережеві пристрої які будуть задіяні в комп’ютерній мережі магазину залишається визначити середовище передачі даних. В комп’ютерних мережах використовують три фізичні середовища передачі даних:

- мідний кабель(вита пара);
- оптоволоконний кабель;
- бездротове підключення.

Мідний кабель характерний в мережах через невисоку вартість, простоту монтажу і низький електричний опір. Найбільш доцільне використання витої пари – це підключення комутаторів з кінцевими пристроями, такими як маршрутизаторами та комп’ютери. Проте даний вид кабелю має обмеження в максимальну довжину сегменту в 100 метрів, що зумовлено стійкості до перешкод. Даний кабель поділяють на два типи:

- неекранована;
- екранована.

Неекранована вита пара використовується в телефонних системах і її не доцільно використовувати в комп’ютерній мережі магазину. Тому для з’єднання мережевих пристроїв використовуватиметься екранована пара. Приклад екранованої витої пари можна побачити на рисунку 2.3

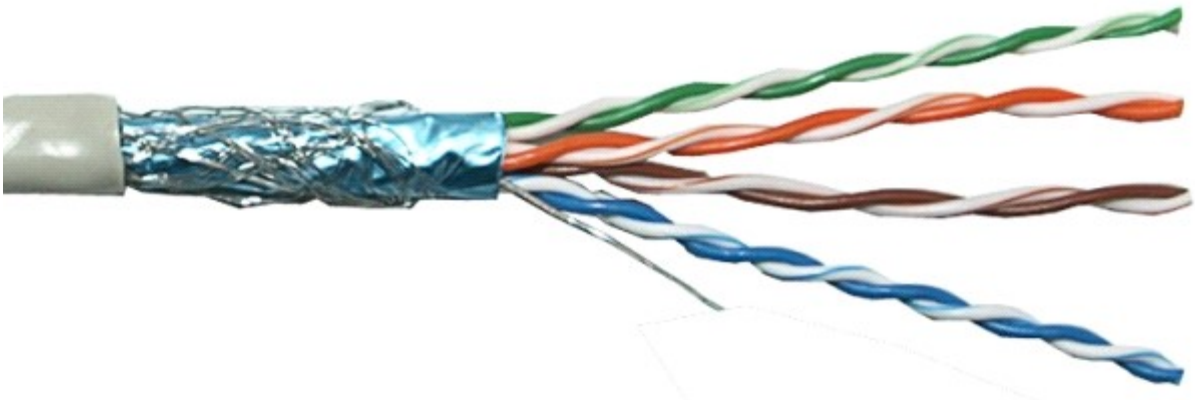


Рисунок 2.3 – Екранована вита пара

Оптоволоконний кабель надає можливість передавати данні на великі відстані і більшою пропускною здатністю, ніж вита пара. Оптоволоконний кабель несприйнятливий до впливу електромагнітних і радіочастотних перешкод. Єдиним недоліком є те, що даний вид кабелю легко пошкодити. Найбільш доцільне використання даного кабелю в підключенні маршрутизаторів з інтернет провайдером. Зображення оптоволоконного кабелю можна побачити на рисунку 2.4.

Рисунок 2.4 – Оптоволоконний кабель

До бездротового з’єднання можна віднести Wi-Fi, який надає можливість передачі даних по радіоканалах. Встановлення бездротової точки доступу є ефективним рішенням, коли способи розгортання кабельної системи не є можливими, економічно доцільними або ергономічними у використані.

В якості бездротової точки доступу для комп’ютерної мережі магазину можна використати бездротовий маршрутизатор WRT300N, зображення якого можна побачити на рисунку 2.5. Даний маршрутизатор слугуватиме точкою доступу для гостей магазину.

Рисунок 2.5 – Бездротовий маршрутизатор WRT300N

2.4 Обґрунтування вибору мережевих пристроїв для реалізації комп’ютерної мережі магазину

Для створення комп’ютерної мережі магазину, як і для будь-якої комп’ютерної мережі необхідне таке мережеве обладнання як:

- маршрутизатор;
- комутатор;
- брандмауер.

Основним компонентом створення комп’ютерної мережі є маршрутизатор, оскільки він надає можливість поєднувати дві і більше мережі, а також керує процесом маршрутизації. Даний пристрій приймає рішення про пересилання пакетів мережевого рівня. В нашому випадку даний пристрій підключається між локальною мережею й інтернетом.

В якості маршрутизатора розглянемо маршрутизатор типу Cisco 2811, що зображений на рисунку 2.6.

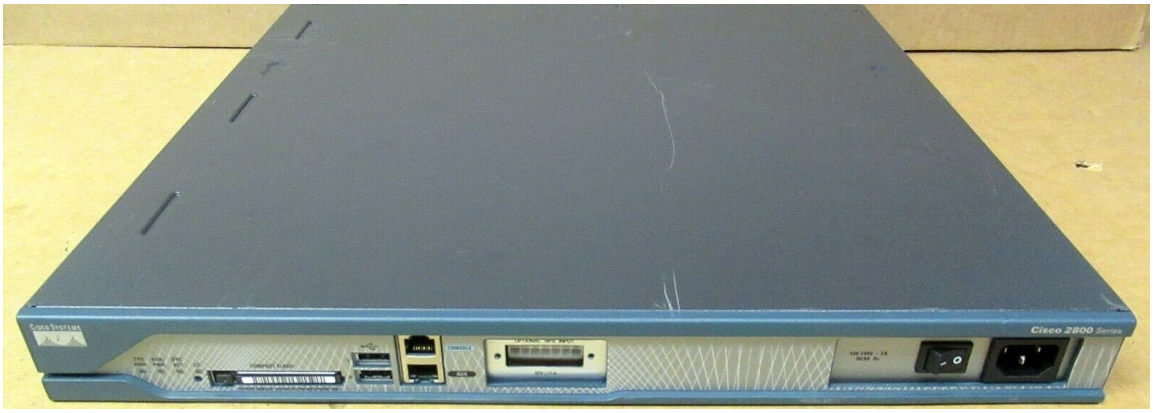


Рисунок 2.6 –Маршрутизатор Cisco 2811

Даний маршрутизатор серії Cisco 2800 – є маршрутизатором з інтеграцією сервісів (Integrated Services Routers, ISR), оптимізовані для безпечної передачі даних, голосу та відео на швидкості каналу зв'язку. Маршрутизатор має вбудовані засоби апаратного прискорення шифрування (DES, 3DES, AES 128, AES 192, AES 256; підтримуються у версіях програмного забезпечення Cisco IOS Software з функціональністю забезпечення мережної безпеки). Також, пристрій має вбудовані порти Fast Ethernet 10/100 і Gigabit Ethernet 10/100/1000. Оснащений слотами для встановлення мережевих модулів (NME), для встановлення інтерфейсних модулів (HWIC), для підтримки додаткових голосових інтерфейсів (EVM), а також спеціальними слотами на системній платі маршрутизатора для встановлення модулів обробки голосу та сервісних модулів (PVDM та AIM). Інтерфейси NME та HWIC мають зворотну сумісність із модулями NM та WIC відповідно.

Основною причиною вибору даного пристрою є його наявність в симуляторі Cisco Packet Tracer і дешевизна порівняно з іншими пристроями подібного типу.

Далі визначимось з брандмауером, оскільки даний пристрій є основним для створення демілітаризованої зони у нашій мережі, оскільки згідно його набору правил, він може: відмовляти, допускати, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі. Розглянемо більш детально маршрутизатор Cisco ASA 5505 (рис. 2.7).

Рисунок 2.7 –Брандмауер Cisco ASA 5505

Сучасний багатофункціональний пристрій для захисту локальних мереж від зовнішніх атак та вторгнень. Побудований на базі апаратної платформи мережевий екрани Cisco ASA 5505 забезпечують високу надійність та безпеку локальної мережі від зовнішніх атак. Даний брандмауер забезпечує високий рівень безпеки з достатнім рівнем гнучкості, на випадок розростання компанії.

Після того як ми визначились з маршрутизатором і брандмауером залишається ще один мережевий пристрій типу комутатора. Даний пристрій, призначення якого з'єднання декількох вузлів комп'ютерної мережі в межах локальної мережі. Також даний пристрій збільшує продуктивність і безпеку мережі, звільняючи інші сегменти мережі від необхідності обробляти дані, які їм не призначалися, оскільки комутатор передає дані лише безпосередньо отримувачу. На відміну від маршрутизатора, комутатор працює виключно на канальному рівні.

В якості комутатора можна обрати Cisco WS-C2960-24TT-L. Цей комутатор є лінійкою комутаторів з фіксованою конфігурацією та портами Fast Ethernet та Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня та мереж віддаленого офісу, тобто є гарним бюджетним рішенням, коли потрібно розробити мережу магазину. Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних та відео, а також безпечний доступ. Крім того, вони

надають масштабоване управління зі зміною потреб бізнесу. Зображення даного пристрою можна побачити на рисунку 2.8.

Рисунок 2.8 – Комутатор Cisco WS-C2960-24TT-L

Підсумовуючи усе вище описане можна отримати наступні вимоги до мережевого обладнання для створення комп'ютерної мережі магазину з розмежованим доступом користувачів:

1) маршрутизатор Cisco 2811;
2) комутатор Cisco WS-C2960-24TT-L;
3) брандмауер Cisco ASA 5505;
4) бездротовий маршрутизатор WRT300N;
5) екранована вита пара;
6) оптоволоконний кабель.

2.5 Вимоги до програмного забезпечення та його функціонал

Якщо говорити про програмне забезпечення, то для реалізації обміну даними у мережі, необхідно встановити відповідне комунікаційне програмне забезпечення[2, 15].

Мережевим програмним забезпеченням вважається набір програм, що забезпечує роботу мережевого обладнання та обмін інформацією між комп'ютерами в мережі. На всіх мережевих пристроях фірми Cisco, які були обрані для створення мережі в попередньому розділі, дане ПЗ вже встановлено компанією, тому потреба в його встановленні на пристрої – відсутня.

Для взаємодії з мережевим обладнанням використовуються різні режими конфігурації, типу:

- режим користувача;
- привілейований режим;
- режим глобальної конфігурації;
- режими специфічної конфігурації.

В режим користувача входить тільки обмежений перелік команд, виконання яких не зашкодить функціонуванню пристрою.

В привілейований режим можна перейти виконавши команду enable і в разі необхідності ввести пароль. Після переходу, нам стає доступний повний перелік команд і можливість переходу в режим конфігурації. Таким чином, знаючи пароль на вхід на пристрій і пароль на привілейований режим, людина має повний доступ до комутатора.

Режим глобальної конфігурації використовується для створення віртуальних підмереж на пристрої та загального налаштування пристрою. З нього можна перейти в режими специфічної конфігурації, який вже використовується для налаштування специфічного інтерфейсу на пристрої.

2.6 Вимоги до захисту мережевих пристроїв

Захист кабельної системи теж є важливим оскільки саме кабельна система в половині випадків є джерелом всіх відмов комп'ютерної мережі. Тому при проектуванні кабельної системи їй варто приділити особливу увагу. Сучасним рішенням вважаються структуровані кабельні системи, що використовують однакові кабелі для передачі даних у локальній обчислювальній мережі, локальної телефонної мережі, передачі відеоінформації чи сигналів від датчиків пожежної безпеки або охоронних систем. До структурованим кабельних систем відносять[2]:

- SYSTIMAX SCS фірми AT & T;
- OPEN DEC connect компанії Digital;
- кабельна система корпорації IBM.

Для фізичного захисту мережевого обладнання комп'ютерної мережі магазину варто виділити окрему технічну кімнату в якій встановлена протипожежна система, фальшпідлога і система кондиціонування, оскільки техніка може сильно нагрівати приміщення.

В сучасному світі проблема з несанкціонованим доступом – особливо загострилася при поширенні локальних і глобальних комп'ютерних мереж, а також потрібно відзначити, що найбільше бізнес страждає не від зловмисників, а від помилок користувачів. Із-за цього, крім контролю доступу важливим елементом захисту інформації є розмежування повноваження користувачів.

Для захисту мережевого пристрою від стороннього доступу, на ньому встановлюється пароль на:

- консоль;
- SSH і Telnet;
- привілейований режим.

Оскільки дані паролі зберігаються в конфігураційному файлі мережевого пристрою, то для щоб приховати і ці паролі треба включити службу шифрування паролів.

2.7 План виконання роботи

1. Розміщується мережеве обладнання на логічній схемі.
2. Виконується з'єднання усіх мережевих пристроїв. Всі необхідні комутатори з'єднуються з брандмауером, а брандмауер підключається до маршрутизатора. Пристрої з'єднуються мідним кабелем типу – вита пара.
3. Виділяємо три основні зони взаємодії і налаштовуємо їх на брандмауері:

- зовнішній сегмент (outside);
- ДЗ сегмент (DMZ);
- внутрішній сегмент (inside).

Далі налаштовуємо три основні політики взаємодії між зонами:

– з inside до outside;

– з inside до DMZ;

– з outside до DMZ.

4. Створюється необхідні віртуальні підмережі для внутрішнього сегменту та виділяється адресний простір для них.

5. Встановлюється захист мережевих пристроїв від несанкціонованого доступу користувачів за допомогою встановленого на них програмного забезпечення

6. Складається опис та план підключення мережевого обладнання до віртуальних підмереж.

7. Виконується тестування комп'ютерної мережі магазину. Тестується розмежування доступу користувачів.

8. Згідно розробленої логічної схеми створюється фізична топологія, яка проєктується на існуючий план будівлі на якій зображується з'єднання кінцевих пристроїв з технічною кімнатою.

9. Згідно фізичної топології здійснюється аналіз та розраховуються затрати мідного кабелю на приміщення.

2.8 Висновки

В даному розділі був здійснений аналіз існуючого апаратного забезпечення, та було обране мережевого обладнання, яке найбільше підходить для створення комп'ютерної мережі магазину з розмежованим доступом користувачів.

Згідно проведеного аналізу

Програмного забезпечення для налаштування мережевих пристроїв Cisco завчасно встановлене принцип роботи якого було розглянуто в даному розділі. Також був складений перелік необхідного обладнання дня виконання даного проекту, та був покроково описаний план виконання роботи згідно якого буде виконуватись робота в подальшому розділі.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАГАЗИНУ З РОЗМЕЖУВАННЯМ ДОСТУПУ

3.1 Проектування комп'ютерній мережі магазину з розмежованим доступом

Перши кроком при проектуванні комп'ютерної системи з демілітаризованою зоною, є організація локальних комп'ютерних мереж, що вирішує такі задачі[11-14]:

- визначення з кількістю та розташуванням робочих станцій;
- формування додаткових завдань, на кшталт демілітаризованої зони або системи безпеки магазину;
- вибір типу мережі: однорангові з'єднання, чи мережа з централізованим управлінням;
- обґрунтований вибір мережевої операційної системи
- визначення топології мережі і методу доступу;
- вибір апаратного забезпечення типу: серверів, робочих станцій тощо.
- з'єднання та налаштування мережевих пристроїв.

При правильному вирішенні цих питань буде вирішуватись працездатність комп'ютерної системи магазину та мережі в цілому, і як наслідок – витрати на її створення та експлуатацію.

Для подальшої розробки визначимось з правилами призначення адрес пристроям.

Клієнтські пристрої кінцевих користувачів – більшість мереж динамічно виділяють IPv4-адреси клієнтським пристроям за допомогою протоколу динамічної конфігурації вузла (DHCP). Це знижує навантаження на співробітників служби підтримки мережі та практично виключає помилки введення. За допомогою DHCP адреси надаються для використання лише на певний проміжок часу, і їх можна повторно використовувати, коли термін використання закінчиться. Це

важлива функція для мереж, яка підтримує непостійних користувачів та бездротові пристрої. Зміна схеми розподілу на підмережі означає, що DHCP-сервер потрібно повторно переналаштувати, а клієнти повинні поновити адреси IPv4. Клієнти IPv6 можуть отримати відомості про адресу за допомогою DHCPv6 або SLAAC

Сервери і периферійні пристрої – повинні мати передбачувану статичну IP-адресу.

Сервери, які доступні з Інтернету – сервери, які повинні бути загальнодоступними в Інтернеті, повинні мати публічну IPv4-адресу, доступ до якої здійснюється за допомогою NAT. У деяких організаціях внутрішні сервери (не загальнодоступні) повинні бути доступними для віддалених користувачів. В більшості випадків цим серверам призначаються приватні внутрішні адреси, і користувачеві потрібно створити під’єднання віртуальної приватної мережі (VPN, Virtual Private Network) для доступу до сервера. Це має такий ефект, ніби користувач отримує доступ до сервера від вузла в межах інтрамережі.

Проміжні пристрої – цим пристроям призначаються адреси для керування мережею, моніторингу та безпеки. Оскільки ми повинні знати, як зв'язуватися з проміжними пристроями, вони повинні мати передбачувані, статично призначені адреси.

Шлюз – маршрутизатори та пристрої брандмауера мають IP-адресу, призначену кожному інтерфейсу, який служить шлюзом для вузлів у цій мережі. Як правило, для інтерфейсу маршрутизатора використовується найнижча або найвища адреса в мережі.

3.2 Розробка топології та розподіл ролей в комп’ютерній мережі магазину

Вид комп’ютерної мережі та її топологія залежить від поставлених задач. Розробка швидкої та надійної мережі вимагає великих витрат, що не завжди є оптимальним. При виборі топології мережі обирається компроміс між вартістю мережевого обладнання та його доцільністю, враховується можливе розширення мережі, необхідність підключення робочих станцій.

Оскільки під створення комп’ютерної мережі магазину не виставлено ніяких конкретних вимог окрім демілітаризованої зони, то вихідні дані для магазину:

– компанія якій належить магазин складається з трьох будівель: офісу, магазину та склад;

– виділяється сім груп користувачів: офіс, магазин, безпека магазину, склад, відвідувачі, персонал обслуговування, серверна, керування.

– доступ між деякими відділами розмежований, для прикладу користувачі персонал обслуговування не можуть мати доступ до офісного;

– користувачі груп офісу та серверної будуть розміщуватись в офісній будівлі, складу – будівлі складу, а магазину, безпеки магазину та відвідувачів – в будівлі магазину.

Тепер коли було визначено кількість користувачів, видами комунікаційних інтерфейсів та каналами зв'язку, можна переходити до складання схеми мережі та IP-адресації.

В якості архітектури мережі була обрана – ієрархічна архітектура мережі, оскільки дана модель передбачає спрощується розуміння організації мережі, можливість розширення мережі, простоту знаходження проблеми, підвищення відмовостійкості за рахунок дублювання пристроїв.

В ієрархічній архітектурі мережі, також виділяють такі переваги як:

– дозволяє створити найбільш стабільну структуру мережі і більш раціонально розподілити ресурси;

– високий рівень захисту.

Згідно описаних вимог розробимо схеми комп’ютерної мережі магазину у відповідності до трьох рівнів OSI. Схеми мережевого, канального та фізичного рівнів зображено на рисунках 3.1-3.3.

На схемі мережевого рівня (рисунок 3.1) зображено логіку маршрутизації локальних підмереж системи з відповідними до них маршрутизаторами. Мережевий рівень визначає шлях переміщення даних по мережі, дозволяючи їм знайти отримувача. Мережевий рівень можна розглядати як службу доставки.

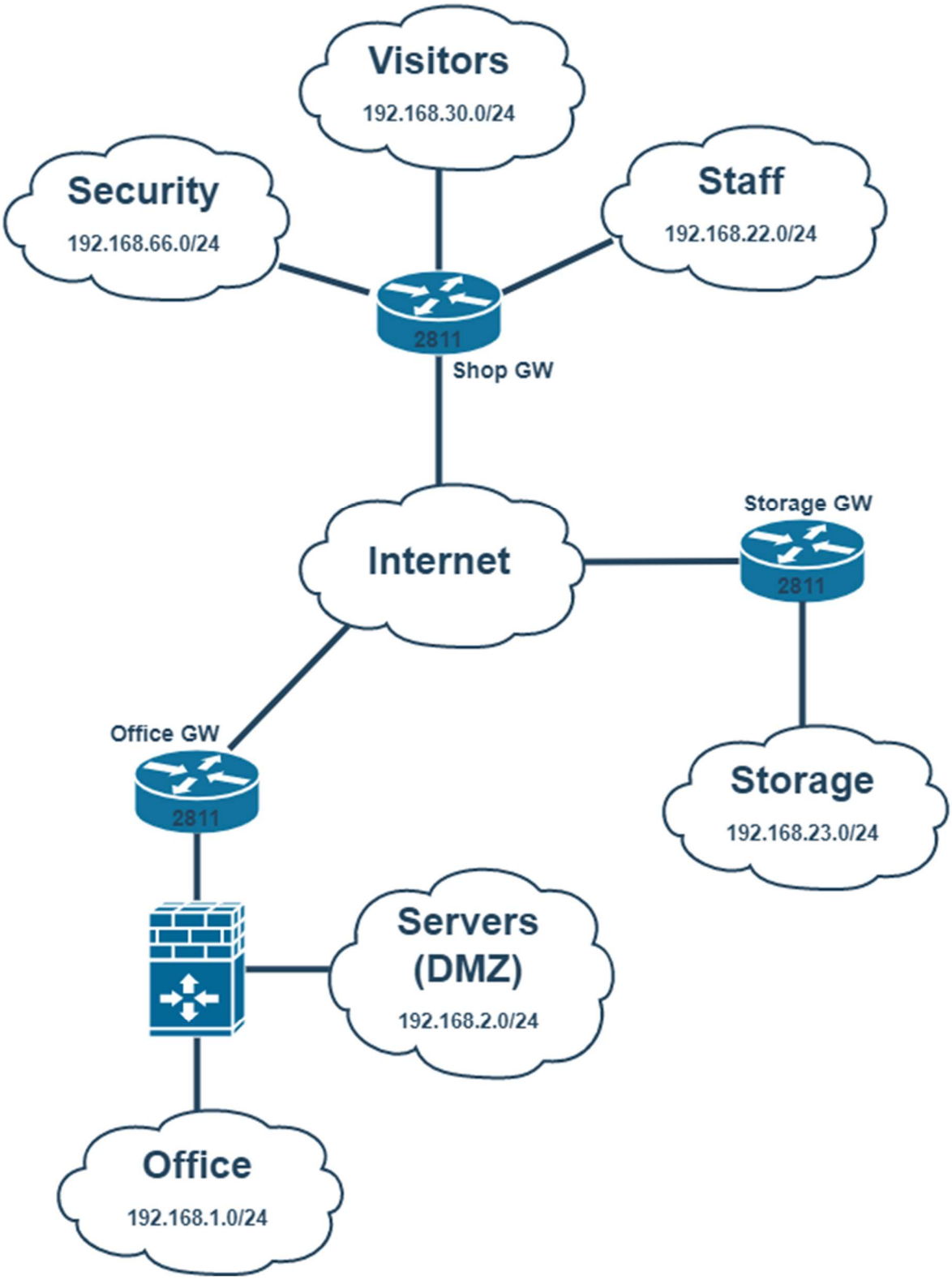


Рисунок 3.1 –Загальна схема комп’ютерної мережі магазину мережевого рівня

На схемі канального рівня (рисунок 3.2) зображено кінцеві робочі станції, сервери та мережеве обладнання, також на схемі позначені VLAN-підмережі. Рівень з’єднування призначений для передачі даних від фізичного рівня до

мережевого та навпаки. Мережева плата в комп'ютері – приклад реалізації рівня з'єднування. Вона залежить від мережевої технології.

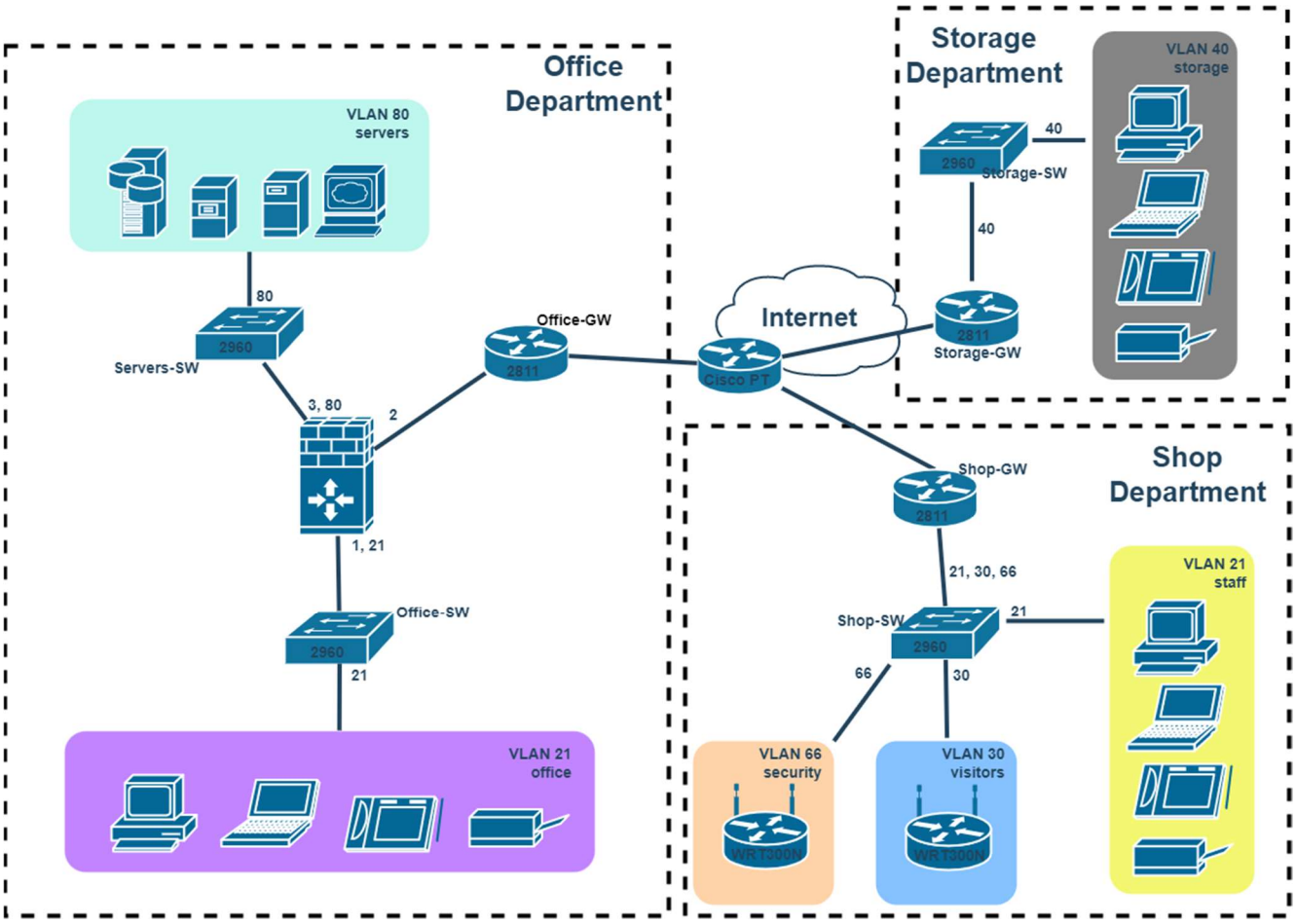


Рисунок 3.2 – Схема комп'ютерної мережі магазину канального рівня

На схемі фізичного рівня (рисунок 3.3) наносяться значення портів для підключення мережевих та кінцевих пристроїв. Фізичний рівень складається з фізичних елементів, які використовуються безпосередньо для передачі інформації по мережевим каналам зв'язку. До фізичного рівня відносяться також методи електричного перетворення сигналів, що залежать від мережевої технології, яка застосовується (Ethernet, Fddi тощо).

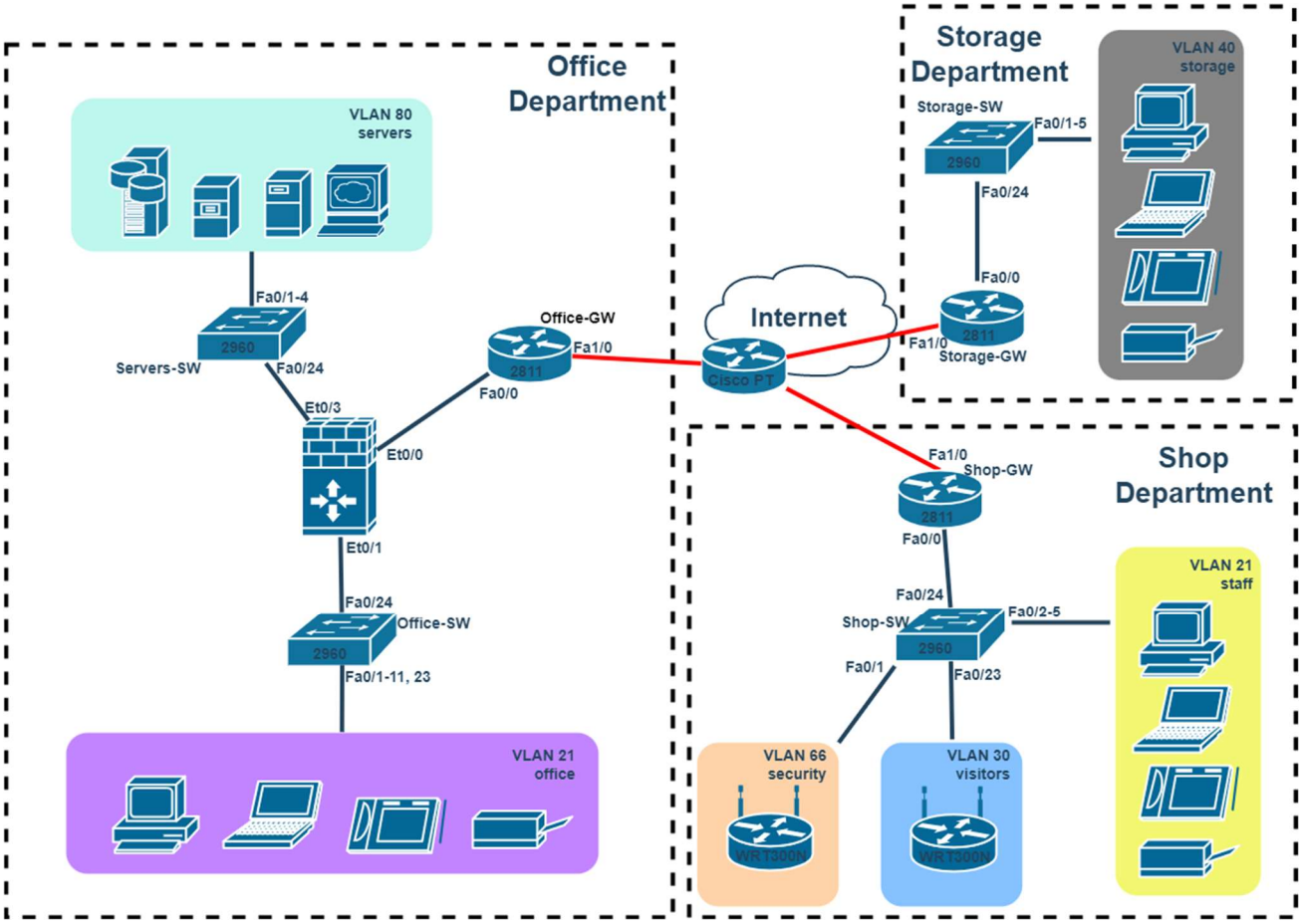


Рисунок 3.3 – Схема комп'ютерної мережі магазину фізичного рівня

На рисунку 3.2 можна побачити групи пристроїв, які виділені в окремий VLAN. Завдяки цьому створюється розмежування мережі. Список з VLAN-підмережами можна побачити в таблиці 3.1.

Таблиця 3.1 – Розподіл віртуальних локальних мереж

ID	Назва	Опис
1	default	Стандартна мережа, яка не використовується
21	office	Для офісного персоналу
22	staff	Для персоналу магазину
30	visitors	Для гостей магазину
40	storage	Для користувачів складу
66	security	Для пристроїв які відповідають за безпеку
80	servers	Для серверів мережі
100	management	Для адміністраторів

Згідно рисунку 3.1 створимо IP-план для локальних мереж з групами IP-адрес, які виділені під робочі станції користувачів та мережевого обладнання. Складений IP-план можна переглянути в таблиці 3.2.

Таблиця 3.2 – IP-план внутрішніх підмереж комп'ютерною мережі магазину

IP-адрес	Примітка	VLAN
1	2	3
192.168.1.0/24	Офіс	21
192.168.1.1	Шлюз на Office-ASA	
192.168.1.20-50	Робочі станції офісу, адреси видаються автоматично системою DHCP на брандмауері	
192.168.2.0/24	Серверна	88
192.168.2.1	Шлюз на Office-ASA	
192.168.2.3	Веб-сервер	
192.168.2.4	DNS-сервер	
192.168.2.5	DHCP-сервер	
192.168.2.6	FTP-сервер	
192.168.40.0/24	Склад	40
192.168.40.1	Шлюз на Storage-GW	
192.168.40.20-50	Робочі станції складу	
192.168.22.0/24	Обслуговуючий персонал магазину	22
192.168.22.1	Шлюз на Shop-GW	
192.168.22.60-254	Робочі станції магазину	
192.168.30.0/24	Відвідувачі	30
192.168.30.1	Шлюз на Shop-GW	
192.168.30.30	Бездротовий маршрутизатор	
192.168.66.0/24	Безпека магазину	66
192.168.66.1	Шлюз на Shop-GW	
192.168.66.2	Бездротовий маршрутизатор	

Продовження таблиці 3.2

1	2	3
192.168.100.0/24	Керування	100
192.168.100.1	Шлюз на маршрутизаторах: Shop-GW, Storage-GW	
192.168.100.2	Shop-SW, Storage-SW	

Згідно рисунку 3.3 створимо план підключення мережевого обладнання, опис винесено в таблицю 3.3.

Таблиця 3.3 – План підключення мережевого обладнання

Пристрій	Порт	Назва	VLAN	
			Access	Trunk
1	2	3	4	5
Office-GW	Fa1/0	ISP		
	Fa0/0	Shop-ASA	2	
Shop-ASA	Et0/0	Office-GW	2	
	Et0/1	Office-SW	1	
	Et0/2	Servers-SW	3	
Office-SW	Fa0/24	Shop-ASA	21	
	Fa0/23	Wireless-GW	21	
	Fa0/1-11	Office devices	21	
Servers-SW	Fa0/24	Shop-ASA	80	
	Fa0/1	DNS server	80	
	Fa0/2	Web server	80	
	Fa0/3	DHCP server	80	
	Fa0/4	File server	80	
Shop-GW	Fa1/0	ISP		
	Fa0/0	Shop-SW		22, 30, 66, 100

Продовження таблиці 3.3

1	2	3	4	5
Shop-SW	Fa0/1	Security Gateway	66	
	Fa0/2-5	Staff devices	22	
	Fa0/23	Guests Router	30	
	Fa0/24	Show-GW		22, 30, 66, 100
Storage-GW	Fa1/0	ISP		
	Fa0/0	Storage-SW		40, 100
Storage-SW	Fa0/24	Storage-GW		40, 100
	Fa0/1-5	Storage devices	40	

3.3 Налаштування демілітаризованої зони в комп'ютерній мережі магазину

З використанням програмного засобу імітаційного моделювання комп'ютерних мереж – Cisco Packet Tracer, створимо демілітаризовану зону та розмістимо такі компоненти на логічній схемі:

- один брандмауер типу Cisco ASA 5505;
- два комутатора типу Cisco 2960–24TT;
- три маршрутизатора типу Cisco 2811.

З'єднаємо маршрутизатори між собою оптоволоконним кабелем. Інші мережеві пристрої з'єднаємо мідним кабелем типу – вита пара. Результат описаних дій можна побачити на рисунку 3.4.

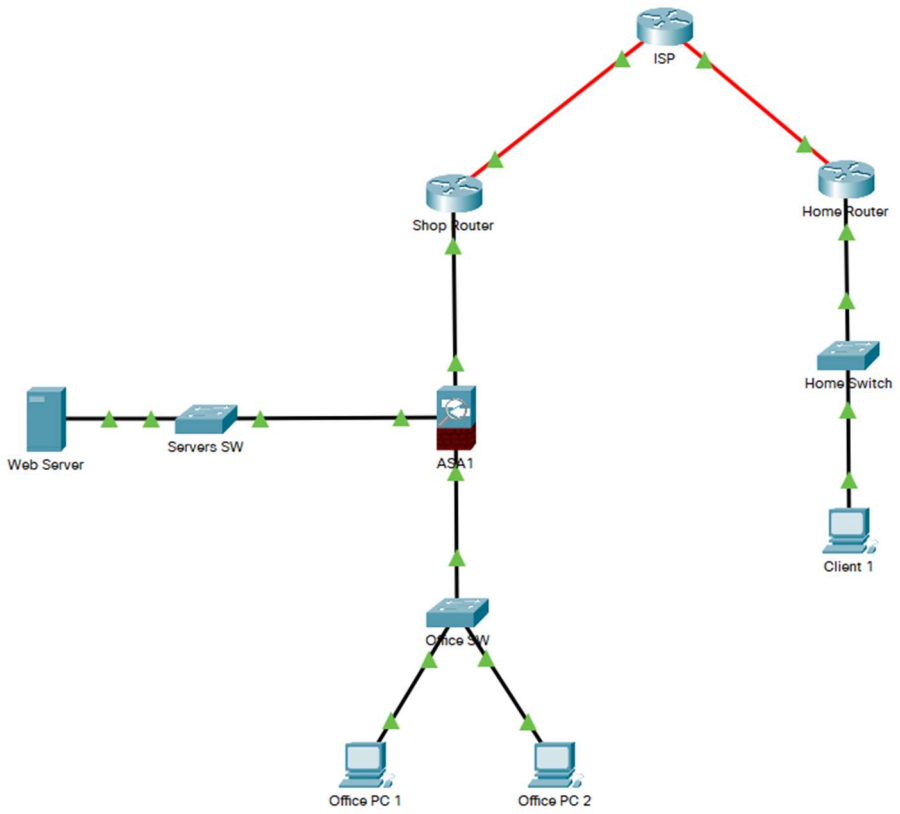


Рисунок 3.4 – Логічна топологія для комп'ютерної мережі з демілітаризованою зоною

Далі починається налаштування брандмауера. Модель даного брандмауера по стандарту має два типи VLAN: inside та outside. Використовуючи CLI (командну строку пристрою) призначимо даним віртуальним мережам IP-адреси. В командному рядку вводимо наступні вказівки:

Office-ASA > enable

Office-ASA # configure terminal

Office-ASA (config)# domain-name shopsecurity.com

Office-ASA (config)# interface vlan 1

Office-ASA (config-if)# nameif inside

Office-ASA (config-if)# ip address 192.168.1.1 255.255.255.0

Office-ASA (config-if)# security-level 100

Office-ASA (config)# interface vlan 2

Office-ASA (config-if)# nameif outside

Office-ASA (config-if)# ip address 209.165.200.226 255.255.255.248

Office-ASA (config-if)# security-level 0

Після того як задали адресні простори для віртуальних мереж брандмауера створимо шлюз, через який наша внутрішня мережа матиме доступ до інтернету. Ввівши наступну команду в режимі глобальних конфігурацій.

Office-ASA (config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225

В даному випадку брандмауер налаштований так, що трафік з внутрішньої мережі може пройти на зовні але відповіді не буде, оскільки ISP маршрутизатор не знає де знаходиться відправник. Тому наступним кроком є налаштування маршрутизації а точніше NAT(перетворення мережевих адрес) – механізм в комп'ютерних мережах, який дозволяє змінювати IP-адресу в заголовку пакунку, який проходить через пристрій маршрутизації[28]. Для цього вводимо наступні вказівки в CLI брандмауера:

Office-ASA (config)# object network inside-net

Office-ASA (config-network-object)# subnet 192.168.1.0 255.255.255.0

Office-ASA (config-network-object)# nat (inside, outside) dynamic interface

Office-ASA (config-network-object)# end

Тепер всі пакети які проходять через брандмауер змінюють свою адресу на 209.165.200.226, що є адресую зовнішнього інтерфейсу брандмауера. Проте виконавши команду ping можна спостерігати, що exo відповідь не повертається. Скориставшись режимом симуляції в Cisco Packet Tracer можна спостерігати, що зовнішній трафік блокується брандмауером і причиною цього є не налаштований MPF. Cisco MPF – це налаштування, які визначають набір правил для застосування функцій брандмауера, таких як: перевірка трафіку, QoS тощо; до трафіку що проходить через брандмауер[25]. Вводимо наступні команди в CLI.

Office-ASA # configure terminal

Office-ASA (config)# class-map inspection_default

Office-ASA (config-cmap)# match default-inspection-traffic

Office-ASA (config-cmap)# exit

Office-ASA (config)# policy-map global_policy

Office-ASA (config-pmap)# class inspection_default

Office-ASA (config-pmap-c)# inspect icmp

Office-ASA (config-pmap-c)# exit

Office-ASA (config)# service-policy global_policy global

Зберігаємо зміни і перевіряємо командою ping зміни. Результати виконання команди можна побачити на рисунку 3.5.

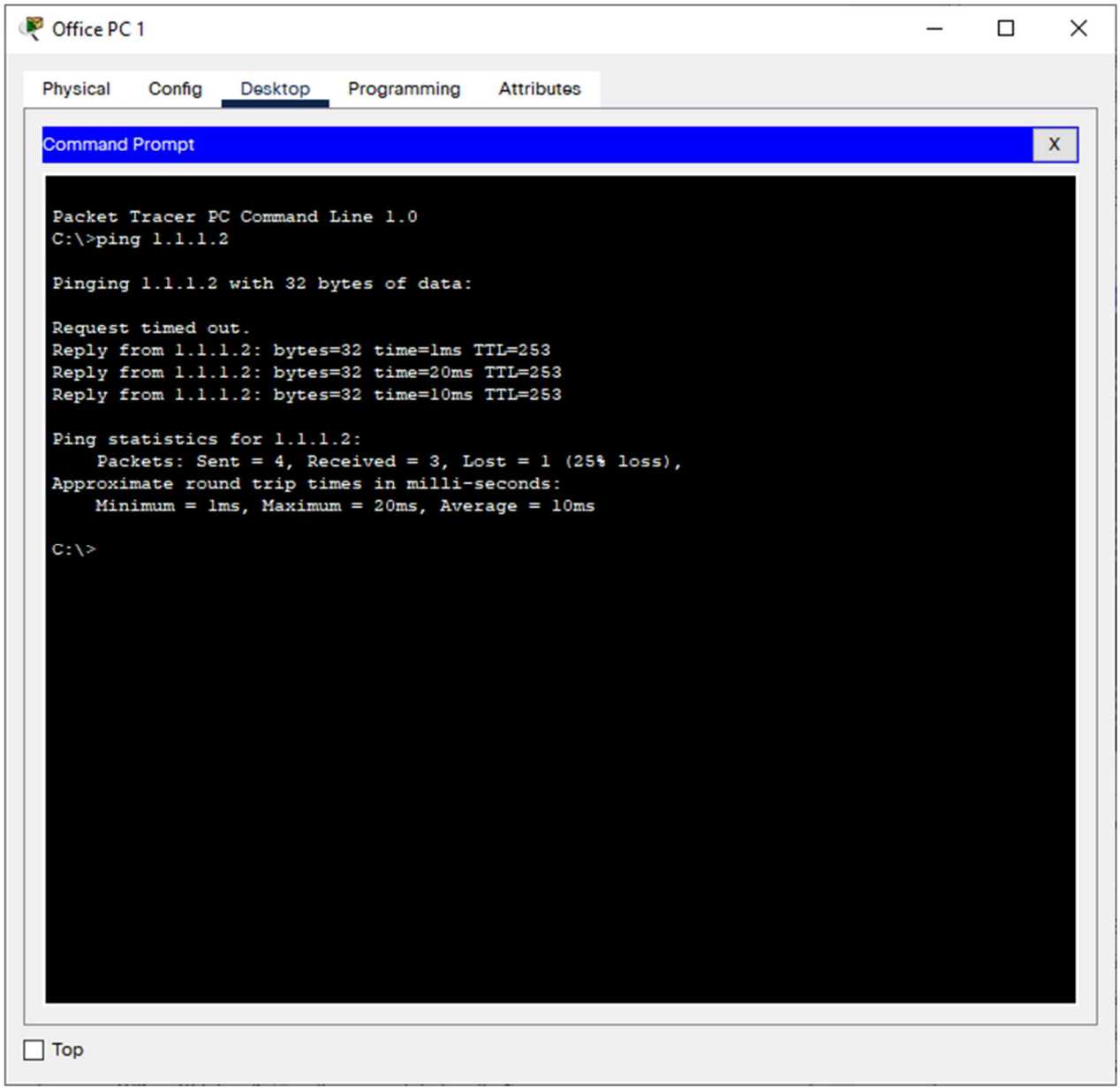


Рисунок 3.5 – Результат виконання команди ping 1.1.1.2 з комп’ютера Office PC 1

Брандмауер вміщує комплексне програмне забезпечення і надає можливість налаштовувати DHCP діапазон адрес, створимо його для inside-мережі.

Office-ASA (config)# dhcpd add 192.168.1.20-192.168.1.50 inside

Office-ASA (config)# dhcpd dns 8.8.8.8 interface inside

Office-ASA (config)# dhcpd enable inside

Оскільки брандмауер основний елемент який відповідає за безпеку комп'ютерної мережі на ньому варто встановити авторизацію. По стандарту Cisco ASA включає в собі структуру AAA – служба яка відповідає за аутентифікацію, авторизація та облік, контролює доступ до ресурсів пристрою, забезпечує виконання політик та перевіряє використання. AAA та його комбіновані процеси відіграють важливу роль в управлінні мережею та кібербезпеці, перевіряючи користувачів і відстежуючи їхню діяльність, коли вони підключені.

Служба AAA працює в поєднанні з SSH, де SSH – це мережевий протокол рівня користувачів, за допомогою якого можна отримати віддалене управління комп'ютером.

Щоб налаштувати SSH на брандмауері створимо користувача зашифруємо його пароль, а потім налаштуємо аутентифікацію на пристрої[30].

Office-ASA (config)# username admin password admin

Office-ASA (config)# aaa authentificaton ssh console LOCAL

Office-ASA (config)# crypto key generate rsa modulus 1024

Office-ASA (config)# ssh 192.168.1.0 255.255.255.0 inside

Тепер адміністратор з LAN може підключатись до брандмауера по SSH. Якщо вникне потреба, то можна і надати доступ для якогось пристрою з WAN.

Після того як всі базові налаштування були здійсненні можна приступати до виділення адресного простору під демілітаризовану зону та створити новий VLAN на брандмауері, який матиме назву DMZ.

Office-ASA (config)# interface vlan 3

Office-ASA (config-if)# ip address 192.168.2.1 255.255.255.0

Office-ASA (config-if)# no forward interface vlan 1

Office-ASA (config-if)# nameif dmz

Office-ASA (config-if)# security-level 70

Office-ASA (config-if)# interface e0/2

Office-ASA (config-if)# switchport access vlan 3

Зі створеною мережею під демілітаризовану зону логічна топологія мережі матиме вигляд зображений на рисунку 3.6.

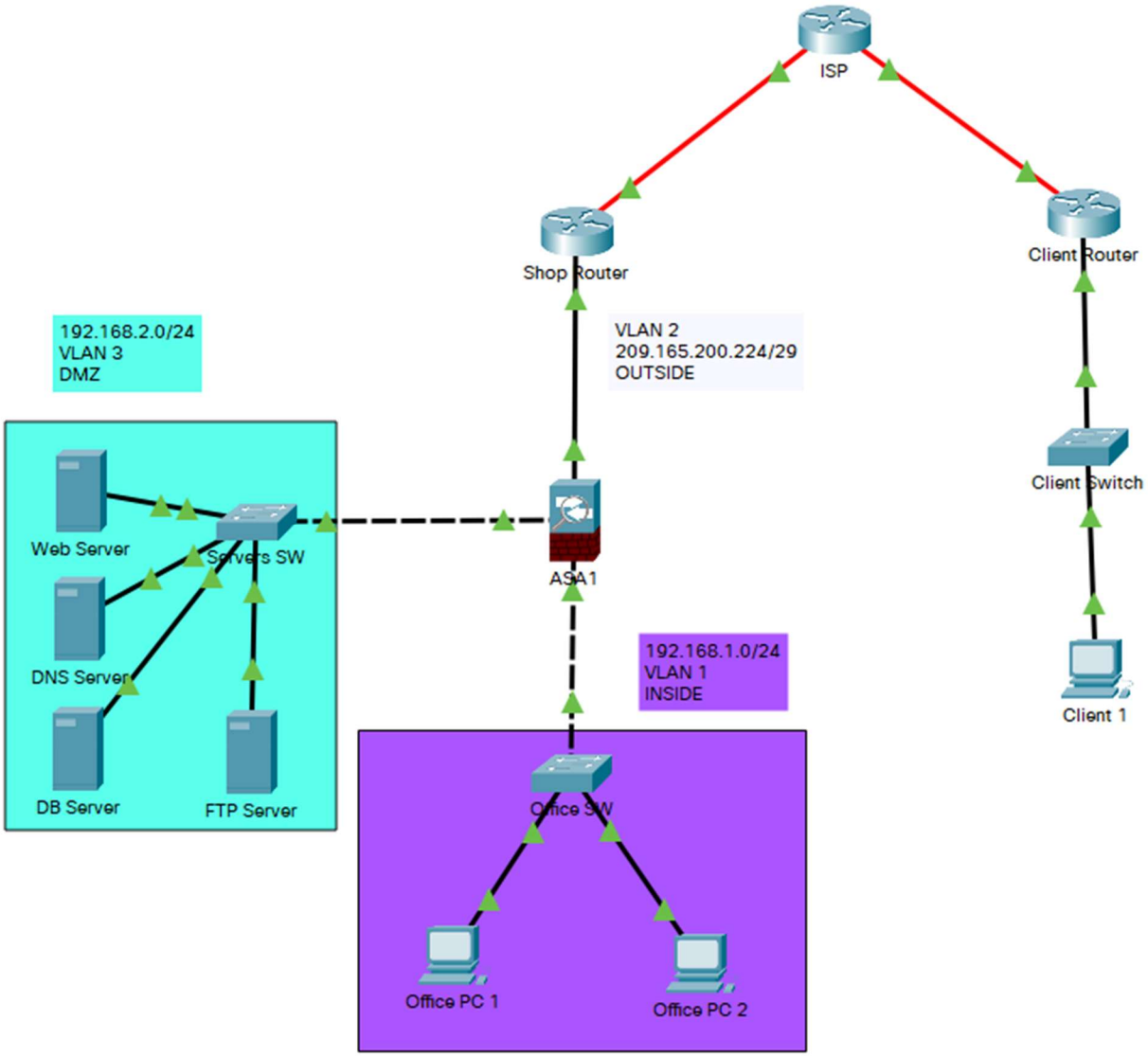


Рисунок 3.6 – Логічна топологія комп'ютерної мережі з демілітаризованою зоною

Створимо нову мережу в налаштуваннях Cisco ASA з назвою dmz-server. В ній буде знаходитись тільки один сервер, який включатиме в себе веб налаштування. Також створимо список контроля[29] на брандмауері.

Office-ASA (config)# object network dmz-server

Office-ASA (config-network-object)# host 192.168.2.3

Office-ASA (config-network-object)# nat (dmz, outside) static 209.165.200.227

Office-ASA (config-network-object)# exit

Office-ASA # configure terminal

Office-ASA (config)# access-list OUSIDE-DMZ permit icmp any host 192.168.2.3

Office-ASA (config)# access-list OUSIDE-DMZ permit icmp any host 192.168.2.3

Подібним чином(описаному вище) налаштуємо об’єкти тиру серверів видавши їм публічні IP-адреси. Результуючу IP-адресацію можна побачити в таблиці 3.4.

Таблиця 3.4 – Таблиця IP-адресації

Пристрій	Інтерфейс	IP-адреса	Шлюз за замовченням	Публічна IP-адреса
Office Router	Fa0/0	209.165.200.224/29	N/A	–
	Fa1/0	1.1.1.1/30	N/A	–
Home router	Fa0/0	13.23.23.1/24	N/A	–
	Fa1/0	2.2.2.1/30	N/A	–
ISP	Fa4/0	1.1.1.2/30	N/A	–
	Fa5/0	2.2.2.2/30	N/A	–
Office-ASA	VLAN 1(E0/1)	192.168.1.1/24	N/A	–
Office-ASA	VLAN 2(E0/0)	209.165.200.226/29	N/A	–
Office-ASA	VLAN 3(E0/2)	192.168.2.1/24	N/A	–
Web Server	NIC	192.168.2.3/24	N/A	209.165.200.227/29
DNS Server	NIC	192.168.2.4/24	N/A	209.165.200.228/29
DHCP Server	NIC	192.168.2.5/24	N/A	209.165.200.229/29
FTP Server	NIC	192.168.2.6/24	N/A	209.165.200.230/29

3.4 Розгортання та налаштування комп'ютерної мережі магазину за допомогою засобу імітаційного моделювання

Подальше розгортання мережі відбуватиметься з урахуванням створеної і налаштованої демілітаризованої зони, тому пройдені кроки не будуть описуватись повторно.

Для початку для вже створеної мережі призначимо окремі віртуальні мережі. Згідно рисунку 3.6 створимо віртуальні мережі:

- servers, для виділеної демілітаризованої зони;
- office, для локальної мережі в якій оперує штатний персонал f,j техперсонал.

Для того щоб створити VLAN на комутаторі, в CLI комутатора вводяться наступні команди:

Switch> enable

Switch# configure terminal

Switch(config)# vlan 80

Switch(config-vlan)# name servers

Подібним чином створимо віртуальні мережі на комутаторах: Servers SW, Market SW. Як тільки нові віртуальні мережі були внесені в базу даних комутатора, змінимо тип доступу на інтерфейсах комутатора; Оскільки по стандарту на них висталений VLAN 1 default. Тип доступу на комутаторі міняється наступним чином:

Switch# configure terminal

Switch(config)# interface FastEthernet0/24

Switch(config-if)# switchport access vlan 80

Налаштувавши віртуальні мережі для локальної та демілітаризованої зони перша частина логічної схеми комп'ютерної мережі магазину з розмежованим доступом буде виглядати так як на рисунку 3.7.

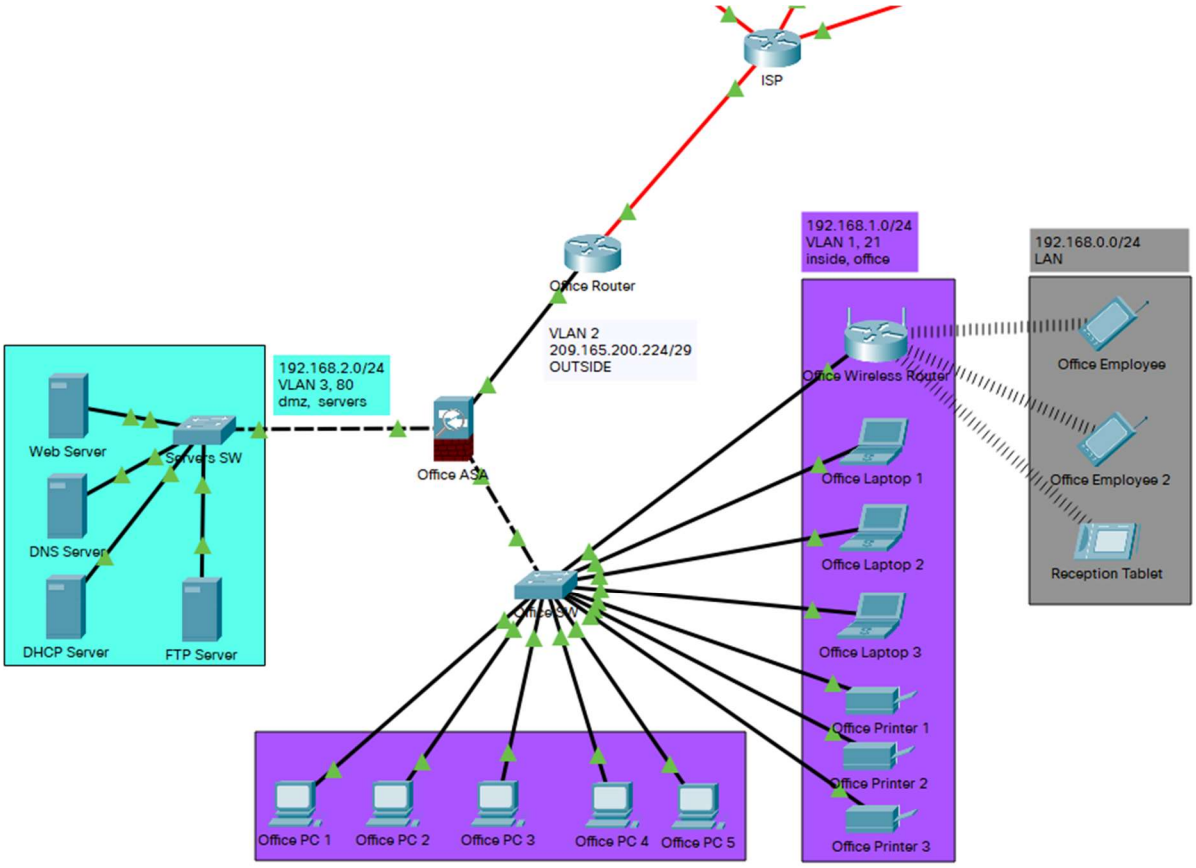


Рисунок 3.7 – Логічна топологія комп’ютерної мережі магазину з демілітаризованою зоною для офісного та серверного відділу

Наступною кроком в створенні комп’ютерної мережі магазину є розгортання логічної топології для відділів які відносяться безпосередньо до магазину. Мережа магазину включатиме в себе віртуальні підмережі для:

- персоналу магазину;
- відвідувачів;
- керування мережевими пристроями
- пристроїв безпеки.

Згідно вже описаних методів з’єднаємо та налаштуємо мережеві пристрої магазину. Результат виконаної роботи можна побачити на рисунку 3.8.

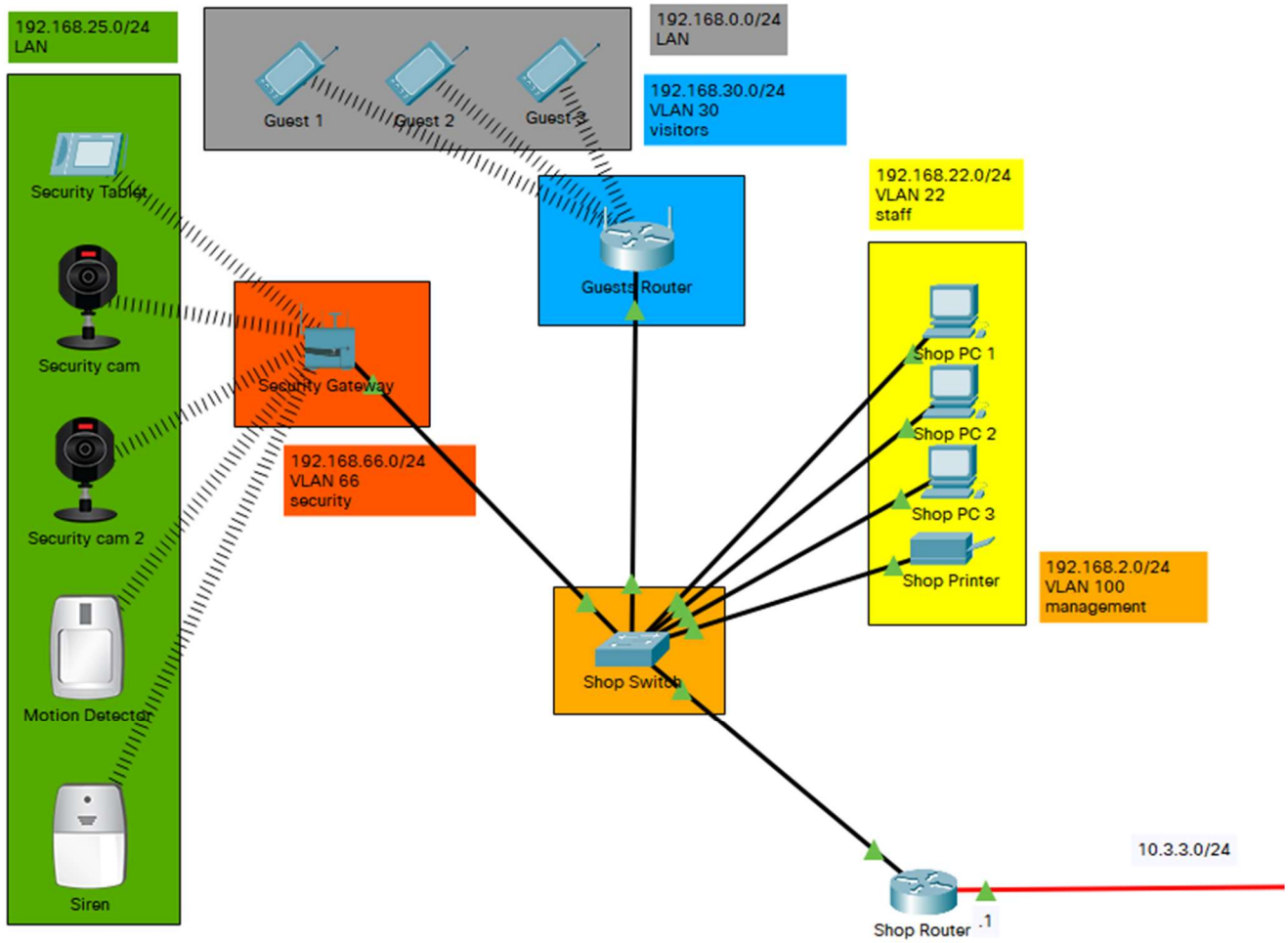


Рисунок 3.8 – Логічна топологія комп'ютерної мережі магазину для техперсоналу, відвідувачів і пристроїв безпеки

Як видно на рисунку 3.8 присутні пристрої типу IoT, які відповідають за безпеку приміщення. Пристрої безпеки налаштовуються з використанням відповідного планшету(на рисунку Security Tablet), який підключений до шлюзу безпеки. Приклад інтерфейсу для налаштування зображено на рисунку 3.9.

Маршрутизатор комп'ютерної мережі магазину налаштований таким чином, що користувачі гостьової мережі не можуть звертатися до пристроїв які відносяться до пристроїв магазину. Також маршрутизатор здійснює перетворення внутрішніх мереж в публічні, які знаходяться в діапазоні від 3.3.3.5 до 3.3.3.10.

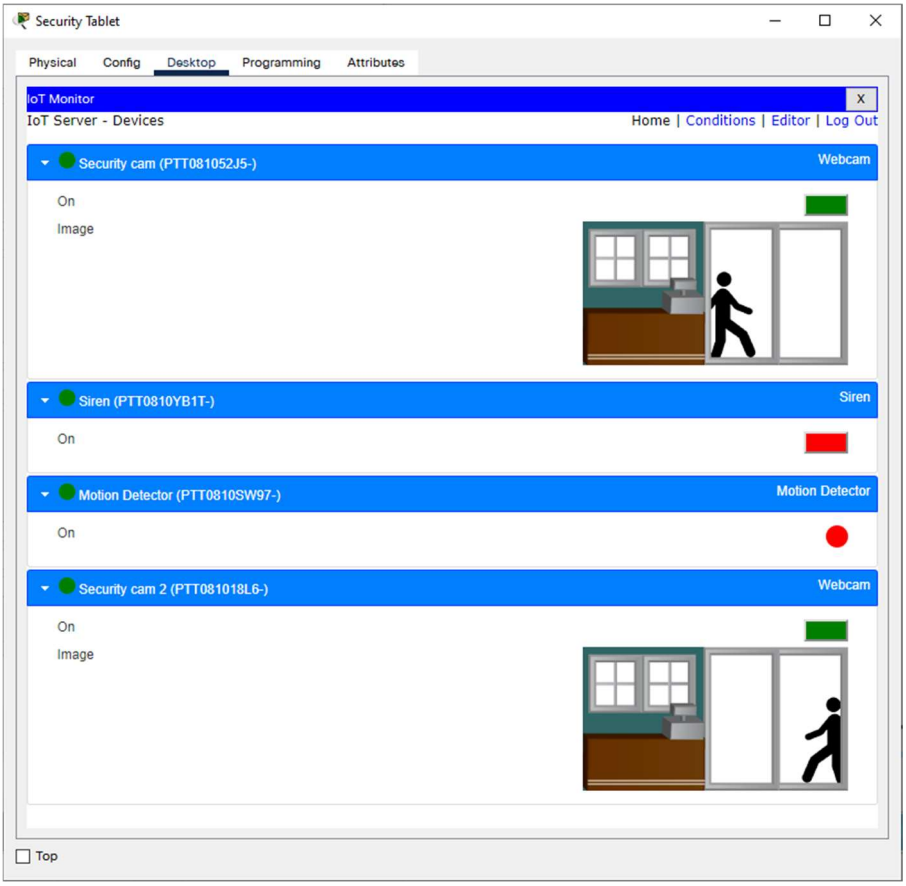


Рисунок 3.9 – Інтерфейсу для налаштування безпеки магазину

Після того як була створена комп'ютерна мережа магазину, залишається створити мережу для складу, щоб логічна топологія комп'ютерної мережі мала остаточний вигляд. Для цього розмістимо мережеве обладнання згідно рисунку 3.10.

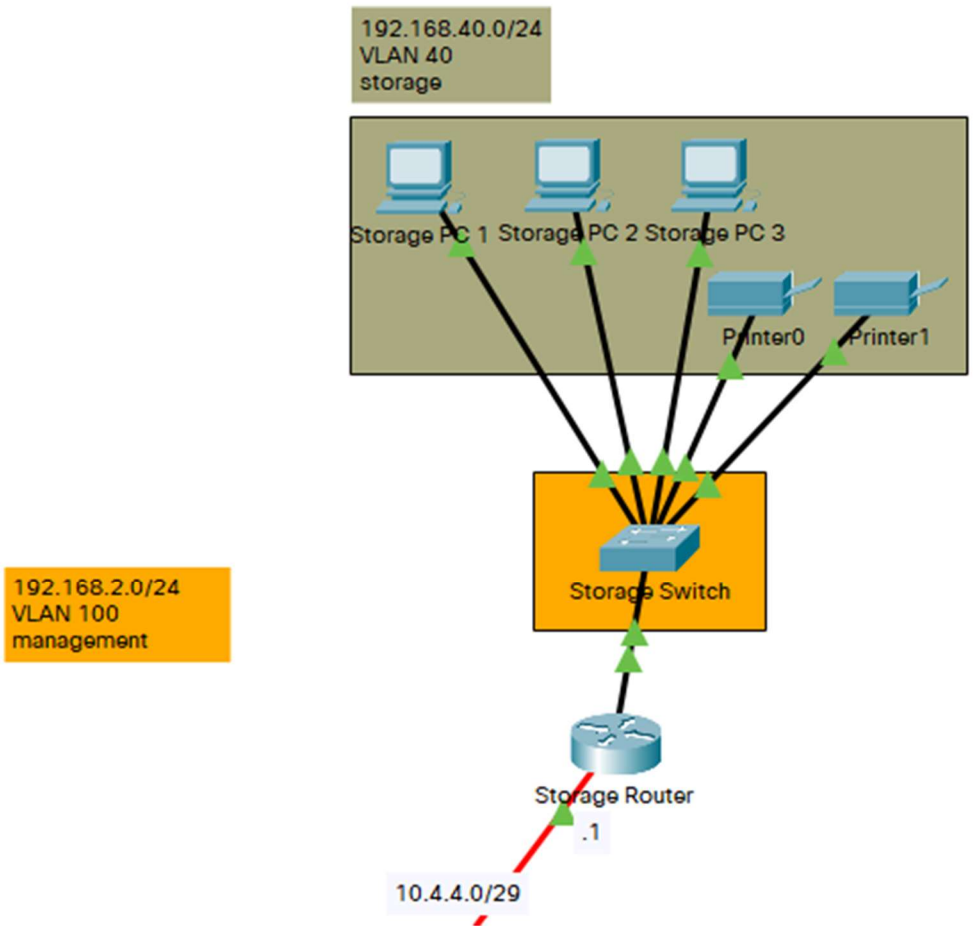


Рисунок 3.10 – Логічна топологія комп'ютерної мережі магазину для відділу складу

Після того як всі мережеві компоненти були розміщені на логічній схемі складемо таблицю 3.5 – таблицю IP-адресації.

Таблиця 3.5 – Таблиця IP-адресації

Пристрій	Інтерфейс	IP-адреса	Шлюз за замовченням	Публічна IP-адреса
Shop-GW	Fa0/0.22	192.168.22.1/24	N/A	–
	Fa0/0.30	192.168.30.1/24	N/A	–
	Fa0/0.66	192.168.66.1/24	N/A	–
	Fa0/0.100	192.168.100.1/24	N/A	–
	Fa1/0	3.3.3.1/24	N/A	–

Продовження таблиці 3.6

Shop-SW	VLAN 100	192.168.100.2/24	N/A	–
Guests Router	0/0	192.168.30.30/24	N/A	–
Security Gateway	0/0	192.168.66.2/24	N/A	–
Staff End Devices	Fa0	192.168.22.60-100/24	N/A	3.3.3.5-10/24
Storage-GW	Fa0/0.40	192.168.40.1/24	N/A	–
	Fa0/0.100	192.168.100.1/24		
	Fa1/0	4.4.4.1/24	N/A	–
Shop-GW	Fa0/0.40	192.168.40.1/24	N/A	–
	Fa0/0.100	192.168.100.1/24	N/A	–
	Fa1/0	3.3.3.1/24	N/A	–
Storage-SW	VLAN 100	192.168.100.2/24	N/A	–
Storage End Devices	Fa0	192.168.40.60-100/24	N/A	4.4.4.5-10/24

3.4 Налаштування захисту на мережевому обладнанні.

Налаштування паролів на мережевому обладнанні є ключовим елементом в створенні надійної комп'ютерної мережі магазину з розмежуванням доступу. До мережевих пристроїв можна підключитись трьома способами за допомогою:

- Telnet;
- SSH;
- консольного кабелю.

З наведених методів найбільш надійним та безпечним є SSH, характеристика йому була дана в розділі 3.3, тому в даному розділі буде розглядатись спосіб створення середовища та налаштування SSH авторизації на мережевих пристроях типу маршрутизатора або комутатора.

Налаштування SSH можна розділити на декілька підпунктів[30]:

1) Виділення IP-адресації для керування мережевими пристроями.

Для цього в розділі 3.2 в таблиці 3.1 було виділено VLAN – management з ідентифікатором 100 і виділено під нього мережу 192.168.100.0/24. Призначимо кожному мережевому пристрою адресу з даного діапазону.

Switch> enable

Switch # configure terminal

Switch (config) # interface vlan 100

Switch (config-if) # ip address 192.168.100.2 255.255.255.0

2) Встановлення ім’я для хосту та доменну.

Switch # configure terminal

Switch (config) # hostname Shop-SW

Switch (config-if) # ip domain-name shop.com

3) Створення RSA ключі.

Shop-SW (config) # crypto key generate rsa

How many bits in the modulus [512]: 1024

4) Налаштування конфігурації лінії VTY.

Shop-SW (config) # line vty 0 4

Shop-SW (config-line) # login local

Shop-SW (config-line) # password admin

Shop-SW (config-line) # exit

5) Створення користувача і пароль для нього. Також здійснюється шифрування паролів.

Shop-SW (config) # username admin password admin

Shop-SW (config) # enable secret admin_password

Shop-SW (config) # service password-encryption

6) Перевіряємо доступі налаштування SSH.

Shop-SW (config) # show ip ssh

Результатом виконання даної команди буде відображення версії SSH, тайм-аут аутентифікації та кількість доступних спроб для авторизації.

3.5 Тестування комп'ютерної мережі магазину в розмежуванням доступу

Перевіримо на працездатність та відмовостійкість комп'ютерну мережу магазину з демілітаризованою зоною. Для цього виділимо наступні можливі сценарії роботи в мережі:

1. Відділ staff: має доступ до інтернету, жоден користувач з зовні не має доступу до цього відділу;
2. Відділ servers: має доступ до інтернету і всі користувачі ззовні мають доступ до нього;
3. Відділ security: внутрішня локальна мережа магазину і доступ ззовні до неї неможливий;
4. Відділ visitors: має доступ до інтернету, не має доступу до інших VLAN-підмереж;
5. Відділ office: має доступ до демілітаризованої зони і інтернету, жоден користувач з зовні не має доступу до цього відділу.

Перевірка роботи комп'ютерної мережі здійснюється за допомогою команди ping в системі симуляції комп'ютерної мережі Cisco Packet Tracer. Перевіривши мережу на працездатність, наступним кроком буде створення фізичної моделі комп'ютерної мережі магазину з розмежуванням доступу.

Нижче будуть наведені результати виконання тестування в комп'ютерній мережі магазину з розмежованим доступом, у відповідності до описаних вище сценаріїв. Результати тестування зображено на рисунках 3.11-3.15.

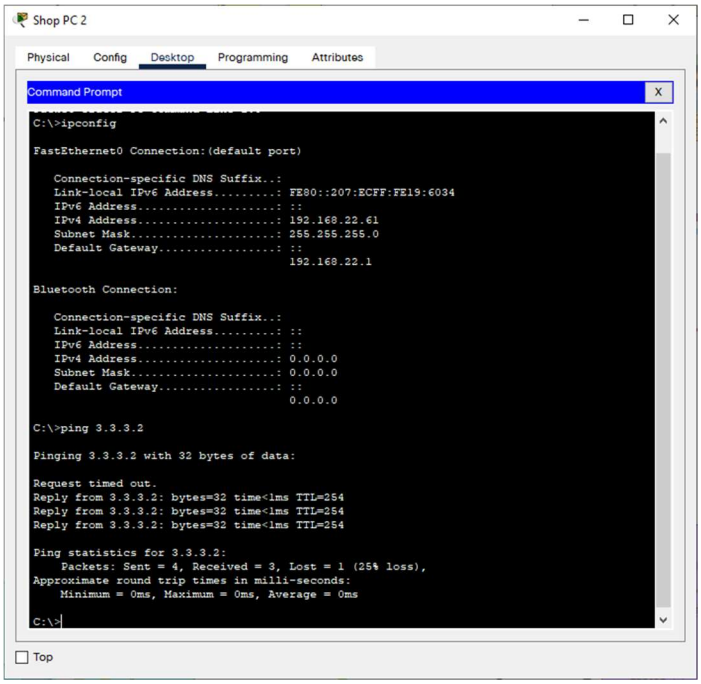


Рисунок 3.11 – Результати тестування 1-го сценарію роботи мережі

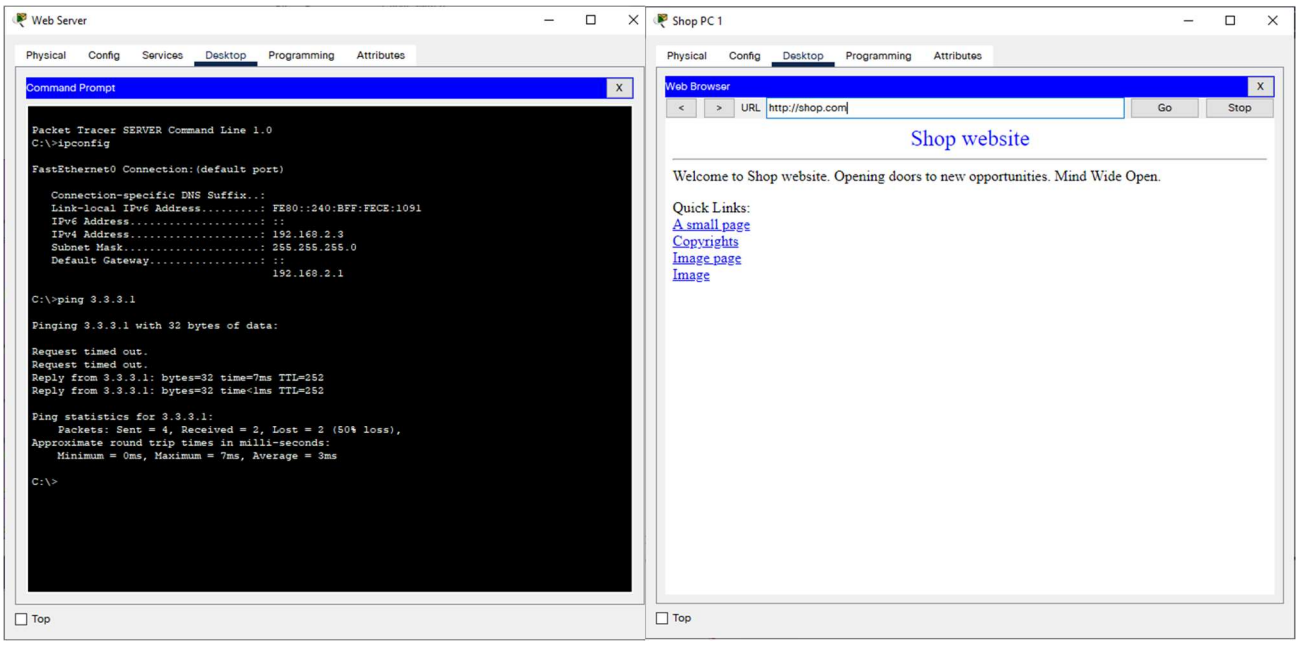


Рисунок 3.12 – Результати тестування 2-го сценарію роботи мережі

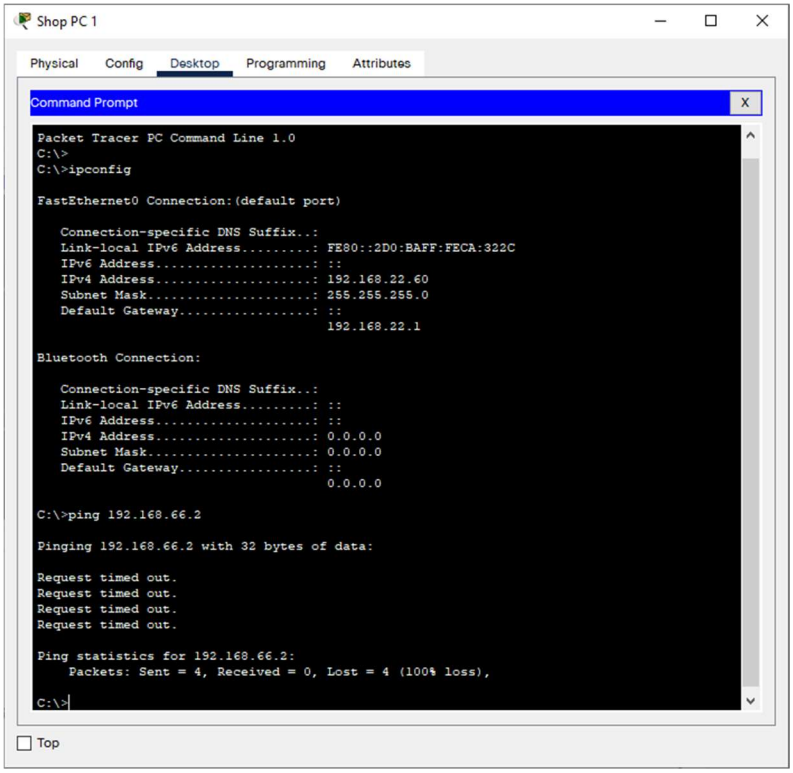


Рисунок 3.13 – Результати тестування 3-го сценарію роботи мережі

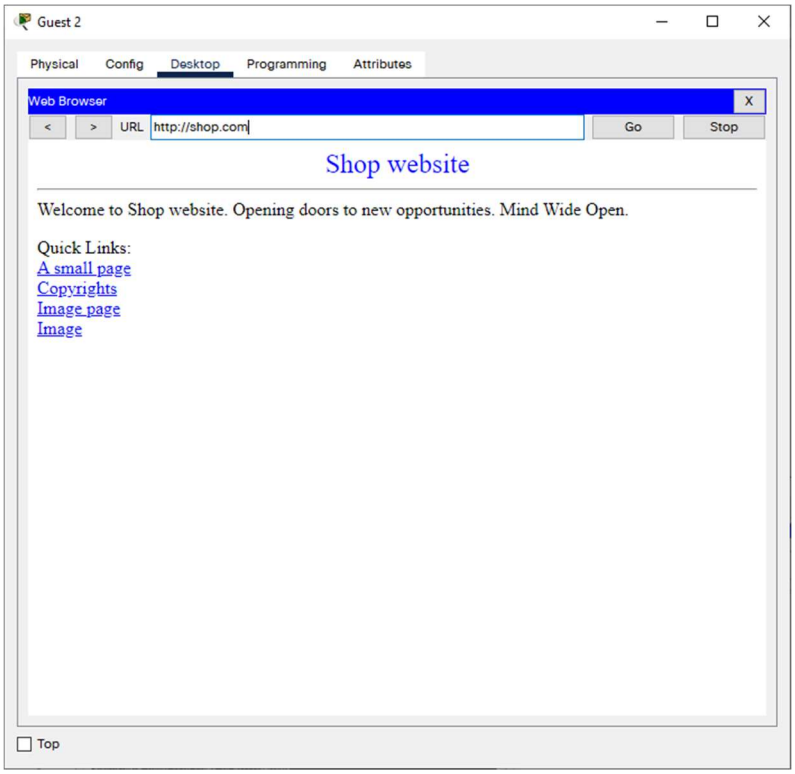


Рисунок 3.14 – Результати тестування 4-го сценарію роботи мережі

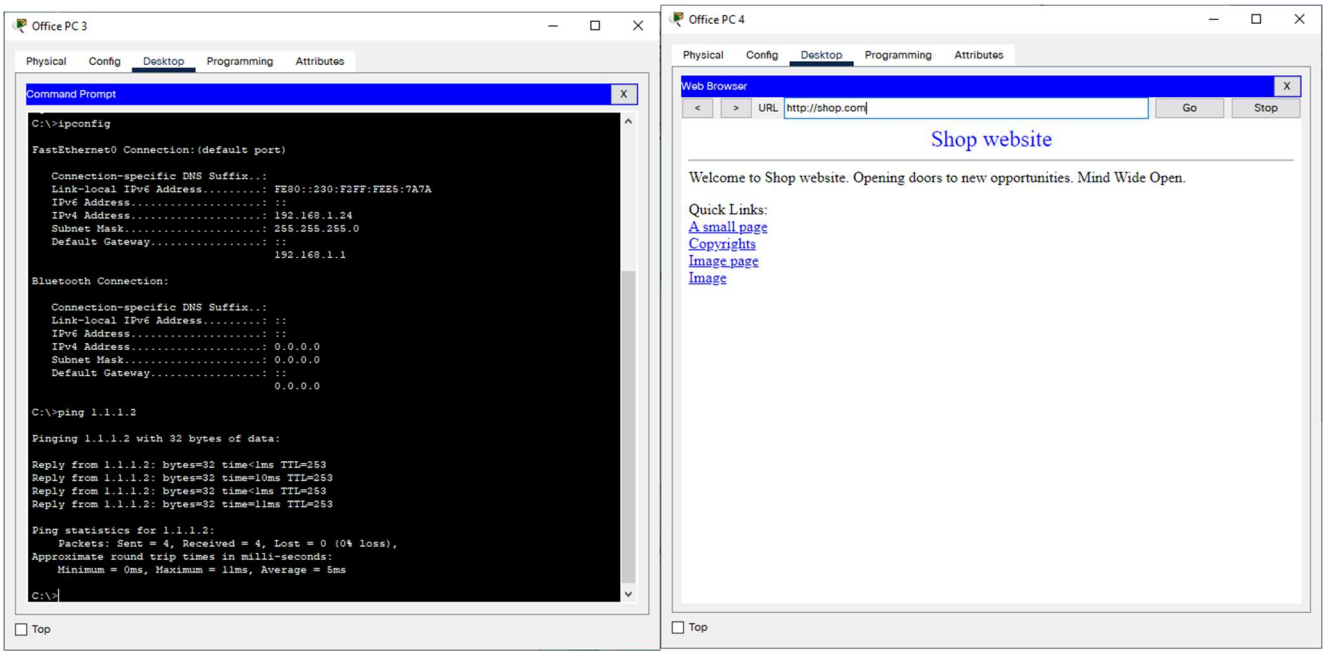


Рисунок 3.15 – Результати тестування 5-го сценарію роботи мережі

Згідно результатів тестування можна дійти висновку, що комп'ютерна мережа магазину виконує всі заплановані сценарії її роботи.

3.6 Створення фізичної топології

В основі системи покладена деревовидна топологія з центром в технічній кімнаті. Функцію вузлів виконують комутатори, які розташовані в спеціальній шафі виділеній під мережеві пристрої, в ній також знаходяться маршрутизатори та брандмауери. Також в технічній кімнаті розташована шафа виділена під сервера мережі які оперують в локальні мережі підприємства. Зображення шаф для приміщень типу: офіс, магазин, склад; можна побачити на рисунках 3.16-3.17.

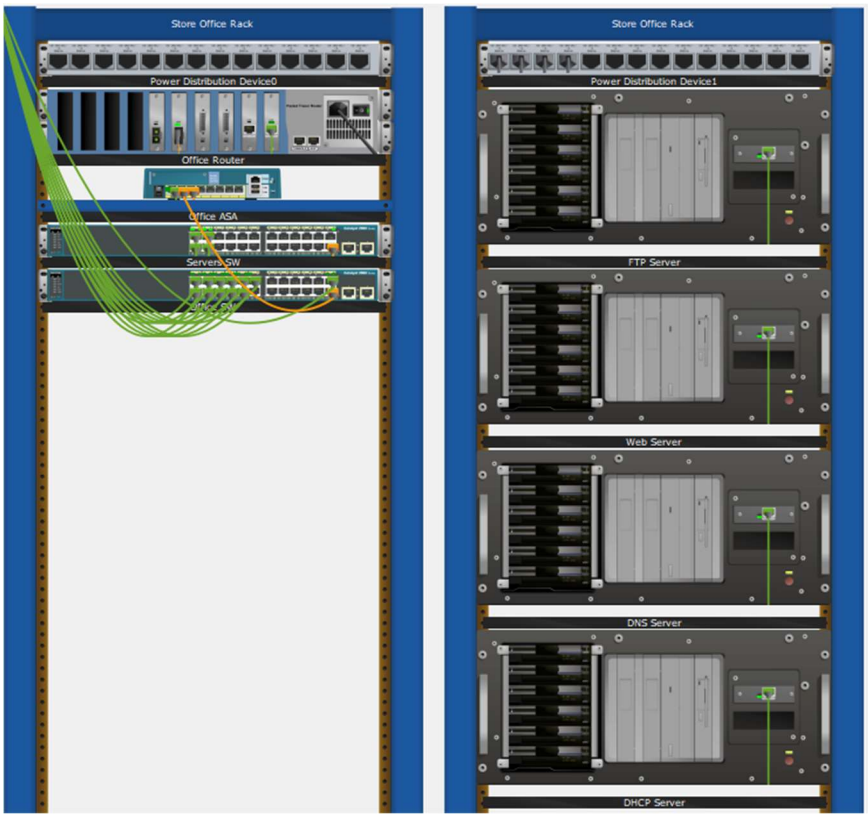


Рисунок 3.16 – Зображення шафи виділеної під мережеві пристрої для офісу і серверної

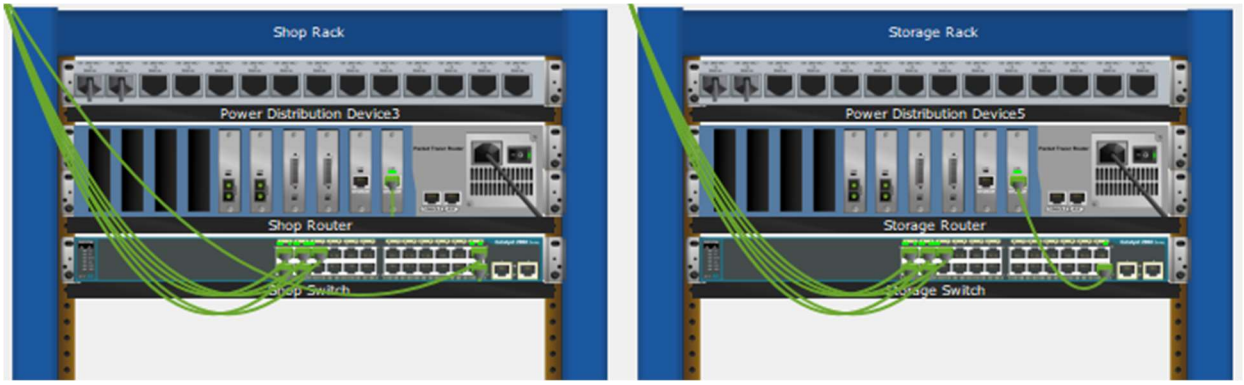


Рисунок 3.17 – Зображення шафи виділеної під відділення магазину та складу

Всі пристрої з’єднані між собою мідними кабелями типу: вита пара або перехресний кабель. Витою парою з’єднанні кінцеві пристрої з мережевим обладнанням, а крос-кабель з’єднує мережеві пристрої, типу комутатор і маршрутизатор.

В технічній кімнаті зазвичай встановлюється протипожежна система, фальшпідлога і система кондиціонування, оскільки техніка може сильно нагрівати

приміщення. Також доступ в дане приміщення здебільшого обмежений, в основному його мають системні адміністратори або інженери.

Найбільш надійним засобом запобігання втрат інформації при короткочасному відключенні електроенергії в даний час є установка джерел безперебійного живлення. Різні за своїми технічними і споживчими характеристиками, подібні пристрої можуть забезпечити споживання всієї локальної мережі або окремого комп'ютера протягом проміжку часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітні носії. Більшість джерел безперебійного живлення одночасно виконує функції і стабілізатора напруги, що є додатковим захистом від стрибків напруги в мережі. Багато сучасних мережеві пристрої – сервери, концентратори, мости і т. д. - оснащені власними дубльованими системами електроживлення.

Найкращим способом захисту кабелю від фізичних (а іноді і температурних і хімічних впливів, наприклад, у виробничих цехах) є прокладання кабелів з використанням у різного ступеня захищених коробів. При прокладці мережевого кабелю поблизу джерел електромагнітного випромінювання необхідно виконувати наступні вимоги:

а) неекранована вита пара повинна відстояти мінімум на 15-30 см від електричного кабелю, розеток, трансформаторів і т. д.

б) вимоги до коаксіального кабелю менш жорсткі - відстань до електричної лінії або електроприладів повинно бути не менше 10-15 см.

Фізичні схеми для комп’ютерної мережі магазину з розмежованим доступом користувачів в масштабі 1:100, можна побачити на рисунках 3.18-3.20. Повна фізична топологія з прокладанням мідного кабелю винесена в додаток Б.

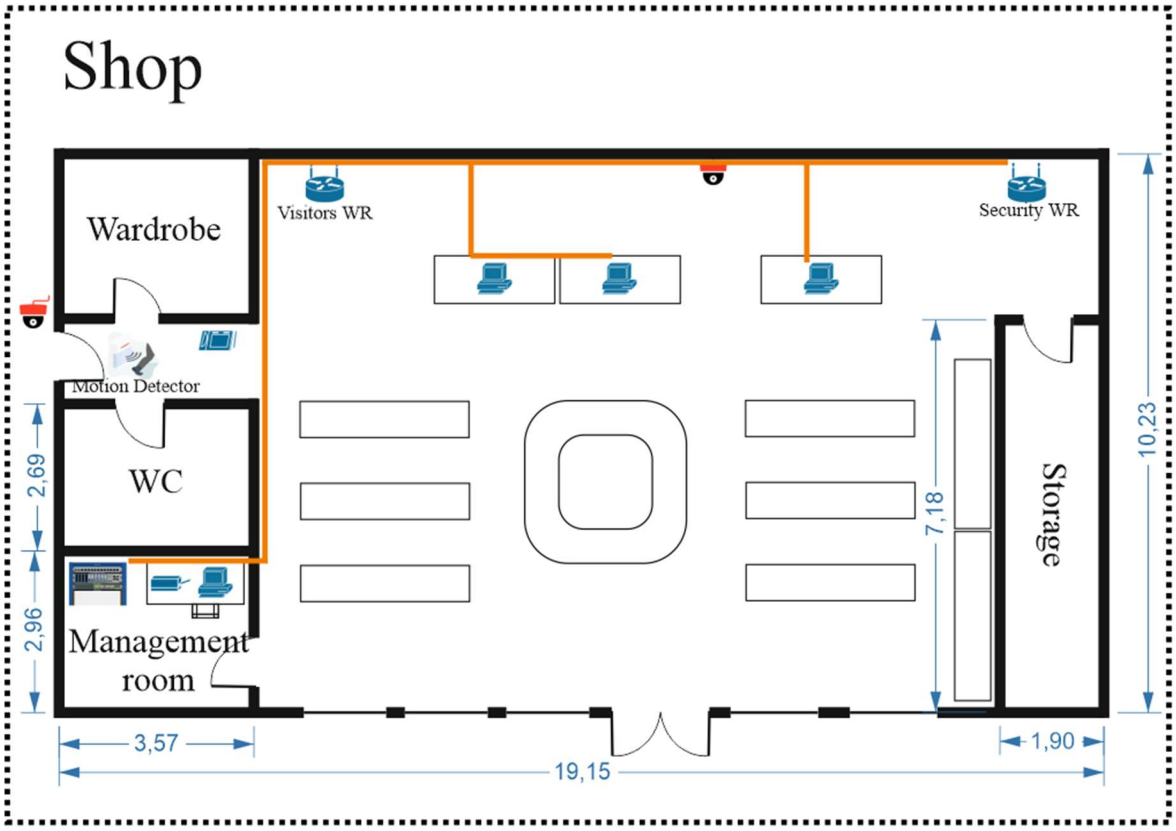


Рисунок 3.18– Фізична топологія комп'ютерної мережі магазину для відділу магазину

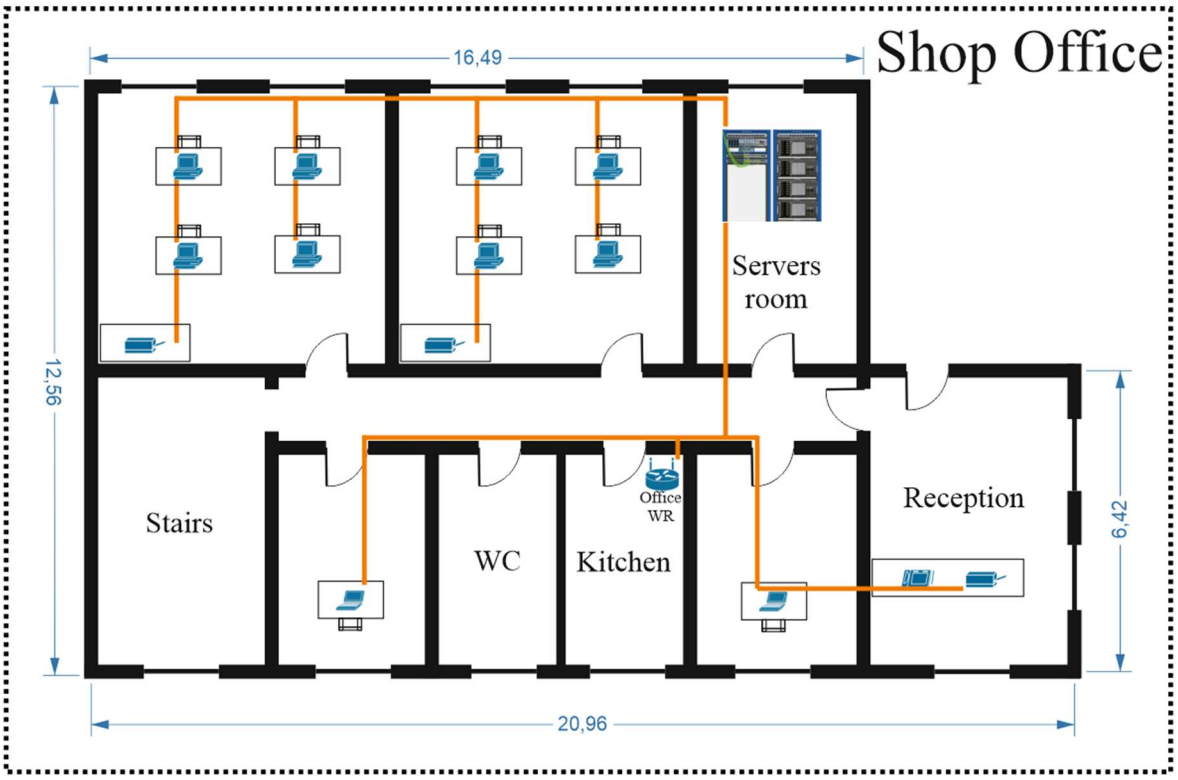


Рисунок 3.19 – Фізична топологія комп'ютерної мережі магазину для відділу офісу

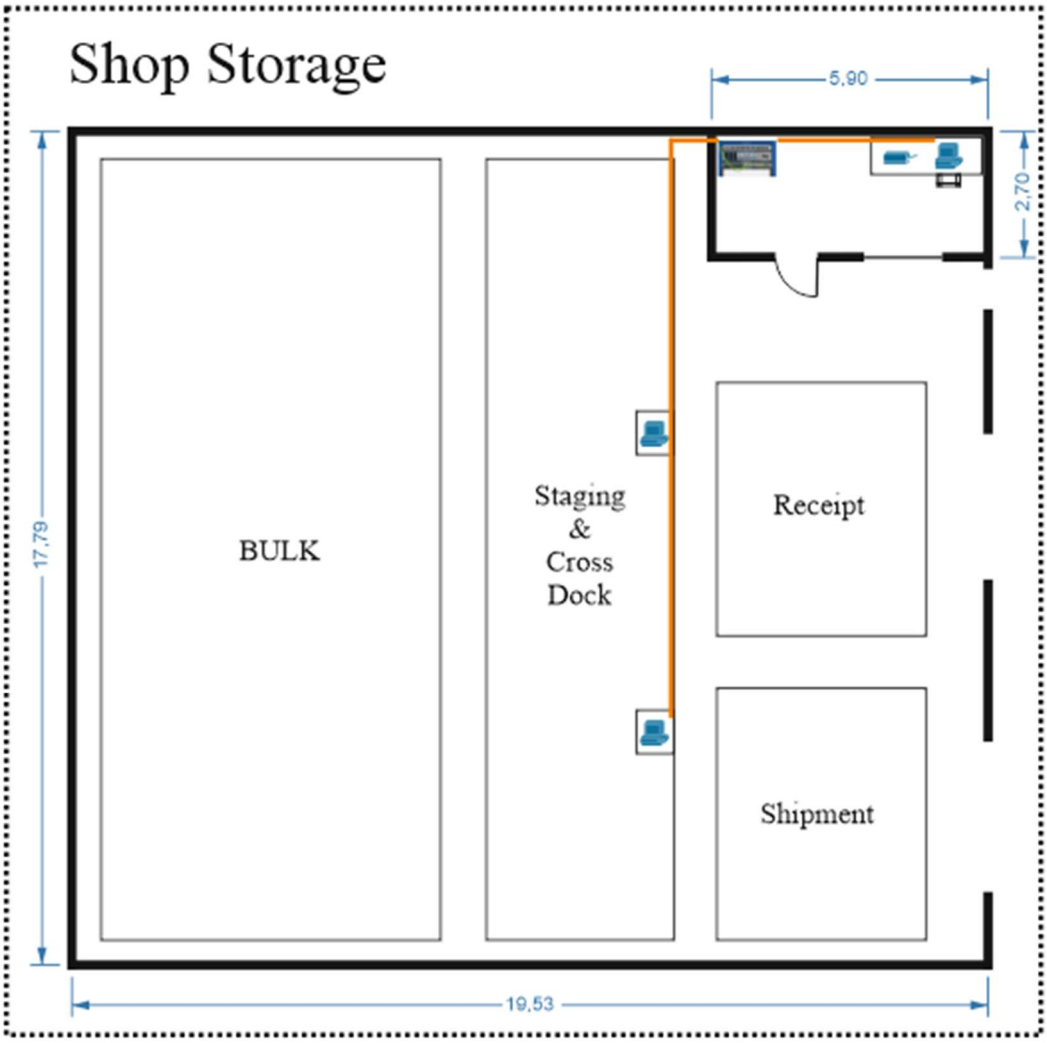


Рисунок 3.20 – Фізична топологія комп'ютерної мережі магазину для відділу складу

3.7 Розрахунок вартості обладнання та кабельних мереж для комп'ютерної мережі

Відповідно логічної топології розробленої в інструменті для симуляції комп'ютерної мережі – Cisco Packet Tracer, винесемо всі мережеві пристрої в таблицю 3.6 та розрахуємо вартість всього мережевого обладнання, задіяного в мережі.

Таблиця 3.6 – Таблиця розрахунку вартості мережевих пристроїв

Прилад, модель	Ціна за 1 за шт. в $	Кількість	Загальна ціна в $
Коммутатор, Cisco WS-C2960-24TT-L	941,02	4	3764,08
Маршрутизатор, CISCO2811	1259,65	3	3778,95
Брандмауер, Cisco ASA 5505	418,89	1	418,89
Бездротові маршрутизатори, Cisco-Linksys WRT300N	39.97	2	79,94

Згідно таблиці 3.6 вартість всього обладнання буде становити 8041.86$. І це без врахування комп'ютерів і принтерів в офісі. Проаналізувавши логічну схему, можна дійти до висновку, що її можна спростити як мінімум на 1 комутатор (забрати Servers-SW), тоді загальна вартість становитиме: 7100.84$.

Стандартний кабель витої-пари зараз коштує 0,63$ за метр, зробивши виміри на фізичній схемі, отримаємо довжину необхідного покриття для: офісу 156.29 м, магазину 93.35 м, складу 26,51. Врахуємо можливі ризики(+10% на ризики) і отримаємо загальну кількість необхідного мідного кабелю: 303.8 м. Загальна ціна мідного кабелю становитиме 191.4$.

В результаті вартість всієї системи становитиме 8233.26$, або більш бюджетна версія мережі 7292.24$.

3.8 Висновки

В даному розділі роботи було реалізовано:

1) логічну топологію комп’ютерної мережі магазину;
2) фізичну топологію комп’ютерної мережі магазину;
3) налаштовано мережеве обладнання;
4) здійснено тестування мережі;
5) здійснено розрахунок вартості комп’ютерної мережі.

Розроблені топології і здійснений аналіз комп’ютерної мережі магазину, можуть бути застосовані для реалізації комп’ютерної мережі магазину з розмежуванням доступу користувачів.

ВИСНОВКИ

З розвитком сучасних технологій виникає все більше потреб в створенні корпоративних мереж, типу мереж магазину з розмежованим доступом користувачів. Для реалізації такої мережі задіються такі елементи як: мережеве обладнання, різноманітні середовища передачі даних, мережеве програмне забезпечення, а також моделювання та проекція мережі в середовищі симулювання і головне протоколи зв'язку моделі OSI або TCP/IP.

Метою роботи було створення комп'ютерної мережі магазину з розмежуванням доступу користувачів, де розмежування доступу налаштовувалося би за допомогою брандмауера або маршрутизатора.

Під час виконання кваліфікаційної роботи автором здійснені основні науково-практичні результати:

1. Здійснений аналіз комп'ютерної мережі з демілітаризованою зоною, розглянуті основні компоненти для створення демілітаризованої зони. Показані умови створення DMZ, наведені конкретні приклади з використанням її в сучасних хмарних технологіях. Також були визначені переваги у використанні демілітаризованої зони в якості елементу для розмежування доступу користувачів в комп'ютерній системі.

2. Здійснений: обґрунтований вибір мережевого обладнання для створення комп'ютерної мережі магазину та проаналізовано середовища передачі даних в системі. Був складений опис вимог до: програмного забезпечення на мережевих пристроях та способів захисту мережевих пристроїв. Складено план розробки комп'ютерної мережі з розмежуванням доступом користувачів.

3. Було визначено список роботи задач, які має виконувати комп'ютерна мережа магазину з демілітаризованою зоною. Згідно розроблених задач була складена імітаційна модель корпоративної віртуальної мережі VLAN. Описано процес створення DMZ-зони та її налаштування в Cisco Packet Tracer, що дало можливість створити робочу модель комп'ютерної мережі магазину з розмежуванням доступом користувачів.

4. Спроектована комп’ютерна мережа магазину з розмежуванням доступу користувачів з централізованим управлінням, за топологією «зірка». В процесі розробки проектування було: розроблено три логічні схеми мережі(мережевого, канального та фізичного рівня), розроблено фізичну топологію мережі для трьох будівель(офісу, магазину та складу) та здійснено розрахунок вартості комп’ютерної мережі магазину з розмежуванням доступу.

Отже, плани в реалізації комп’ютерної мережі магазину з розмежуванням доступу – було досягнуто. Реалізація і симуляція мережі відбувалася в середовищі Cisco Packet Tracer. Тестування мережі відбувалося в тому самому середовищі.

Можна зробити висновок, що цінність даного дослідження полягає в удосконаленні кваліфікаційного рівня розвитку студента, як інженера комп’ютерних мереж, а також зробити доступнішим спосіб створення бюджетної комп’ютерної мережі магазину, тому що у багатьох компоненти або готові системи мають високу вартість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Корпоративна мережа [Електронний ресурс] // Вікіпедія : вільна енциклопедія. – Режим доступу: http://wikipedia.ua.nina.az/wiki/%D0%9A%D0 (дата звернення 01.06.2021) . – Назва з екрану.

2. Електронний посібник «Комп'ютерні мережі» [Електронний ресурс]. – Режим доступу: https://km.ptngu.com/ (дата звернення 25.05.2022). – Назва з екрану.

3. Організація комп'ютерних мереж «демілітаризована зона» [Електронний ресурс]. – Режим доступу: https://kremenetskyy.blogspot.com/2017/11/blog-post.html (дата звернення 25.05.2022). – Назва з екрану.

4. DMZ [Electronic resource]. – Access mode: https://www.fortinet.com/resources/cyberglossary/what-is-dmz (last access: 25.05.2022). – Title from the screen.

5. Gary A. Donahue Network Warrior / Gary A. Donahue. – Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2011. – 627 p.

6. Wireless Sensor Networks: A Survey / I. F. Akyildiz, W. Su, Y. Sankarasubramaniam E. Cayirci, // Computer Networks. – 2012. - Vol. 38. – No. 4, p. 393-422.

7. A Taxonomy of Wireless Microsensor Network Models / S. Tilak, N. B. Abu-Ghazaleh, W. Heinzelman // ACM Mobile Computing and Communications Review. - Vol. 6, - No. 2, p. 28-36.

8. The Coverage Problem in a Wireless Sensor Network / C. F. Huang, Y. C. Tseng // Proceedings of ACM WSNA, San Diego. – 2013, p. 519-528.

9. Трояновська Т. І. Корпоративна мережа, як засіб організації роботи підприємства [Електронний ресурс] / Т. І. Трояновська, Д. О. Віниченко. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/viewFile/1844/1562 (дата звернення 01.06.2021). – Назва з екрану.

10. Структура корпоративної мережі [Електронний ресурс]. – Режим доступу: https://fossdocmail.com/uk/network/ (дата звернення 01.06.2021). – Назва з екрану.

11. Hari Subedi How to Build A Computer Network for Your Small Business - Part 1 [Electronic resource]. – Mode of access: https://www.itjones.com/blogs/2020/3/15/how-to-build-a-computer-network-for-your-small-business-part-1-the-basics (Viewed on May 25, 2022). – Title from the screen.

12. How Do I Set Up a Small Business Network? [Electronic resource]. – Mode of access: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/how-to-set-up-a-network.html (Viewed on May 25, 2022). – Title from the screen.

13. How To: Small Business Network Setup? [Electronic resource]. – Mode of access: https://securenetworksitc.com/small-business-network-setup/ (Viewed on April 29, 2021). – Title from the screen.

14. Small Business Network Setup Checklist [Electronic resource]: [Web-site]. – Mode of access: https://www.neweggbusiness.com/smartbuyer/over-easy/small-office-network-setup/ (Viewed on May 19, 2022). – Title from the screen.

15. Network operating system [Electronic resource] // Wikipedia: The free Encyclopedia. – Mode of access: https://en.wikipedia.org/wiki/Network_operating_system (Viewed on April 31, 2021). – Title from the screen.

16. Vulnerabilities of network OS and mitigation withstate-based permission system [Electronic resource] / J. Noh, S. Lee, J. Park, S. Shin, B. B. Kang // Graduate School of Information Security, School of Computing, Korea Advanced Institute of Science and Technology, Daejeon, Korea. – Mode of access: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1369 (Viewed on April 31, 2021). – Title from the screen.

17. What's The Difference: Host vs. Guest OS [Electronic resource]: [Web-site]. – Mode of access: https://www.datto.com/blog/whats-the-difference-host-vs-guest-os (Viewed on May 22, 2022). – Title from the screen.

18. Patrick Molck-Ude A corporate network is part of a company's IT strategy [Electronic resource]. – Mode of access: https://www.t-systems.com/en/perspectives/networks/network-techniques/data-networks-375244 (Viewed on May 22, 2022). – Title from the screen.

19. David Scott The IT Professional's Guide To Corporate Networks [Electronic resource]. – Mode of access: https://www.techopedia.com/the-it-professionals-guide-to-corporate-networks/2/25665 (Viewed on May 25, 2022). – Title from the screen.

20. Змерзлий І. Клієнт-серверна архітектура та ролі серверів [Електронний ресурс] / Змерзлий І. // Режим доступу: https://medium.com/@IvanZmerzlyi (дата звернення 01.06.2021). – Назва з екрану.

21. Що таке корпоративний сервер? [Електронний ресурс]. – Режим доступу: https://uk.icyscience.com/enterprise-server (дата звернення 25.05.2022). – Назва з екрану.

22. Тарнавський Ю. А. Організація комп'ютерних мереж / Ю. А. Тарнавський, І. М. Кузьменко // Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». – 2018 https://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_merej.pdf.

23. Hari Subedi. A guide to network topology: 2020 [Electronic resource]. – Access mode: https://www.itjones.com/blogs/2020/11/22/a-guide-to-network-topology (last access: 25.05.2022).

24. Hari Subedi. Types Of Computer Network Designs For Business: 2020 [Electronic resource]. – Access mode: https://www.itjones.com/blogs/2020/12/1/types-of-computer-network-designs-for-business (last access: 25.05.2021). – Title from the screen.

25. Cisco Modular Policy Framework (MPF): A brief Introduction [Electronic resource]. – Access mode: https://www.jaacostan.com/2018/06/cisco-modular-policy-framework-mpf.html (Viewed on May 25, 2022). – Title from the screen.

26. Глоба Л.С. Розробка інформаційних ресурсів / Л.С. Глоба // Національний технічний університет України «Київський політехнічний інститут». – Київ 2013. – Том 1. – с. 72 – 82. – Режим доступу:

http://www.dut.edu.ua/uploads/l_1690_29298415.pdf (дата звернення 01.05.2022). – Назва з екрану.

27. Port forwarding [Electronic resource] // Wikipedia: The free Encyclopedia. – Mode of access: https://en.wikipedia.org/wiki/Port_forwarding (Viewed on May 25, 2021). – Title from the screen.

28. Configuring dynamic NAT in Cisco devices [Electronic resource]. – Access mode: https://www.manageengine.com/network-configuration-manager/configlets/configure-dynamic-nat-cisco.html (last access: 25.05.2022). – Title from the screen

29. Configuring IP Access Lists [Electronic resource]. – Access mode: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html (last access: 25.05.2022). – Title from the screen.

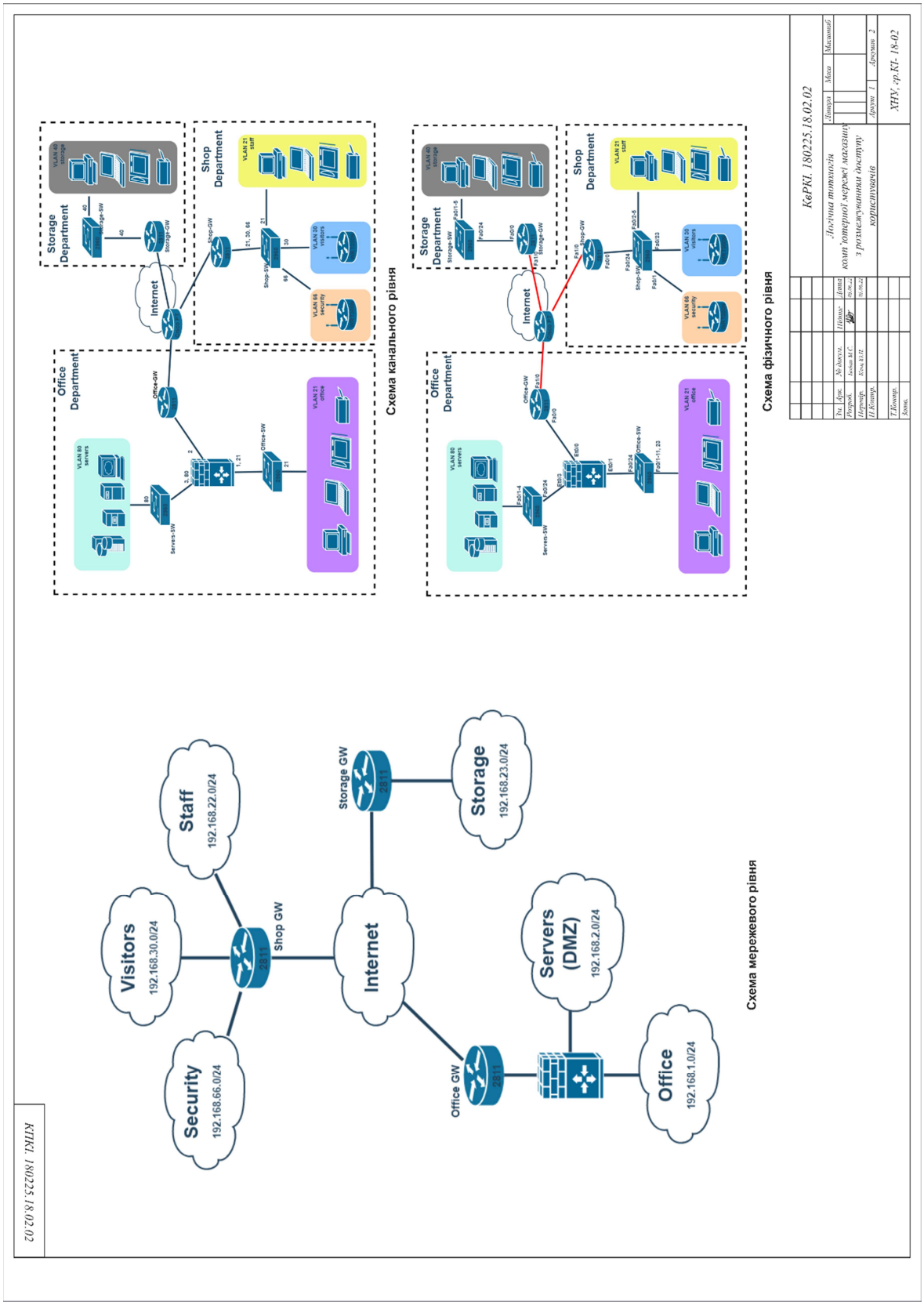
30. How to Enable SSH on Cisco Switch, Router and ASA [Electronic resource]. – Access mode: https://www.thegeekstuff.com/2013/08/enable-ssh-cisco/ (last access: 25.05.2022). – Title from the screen.

Додаток А

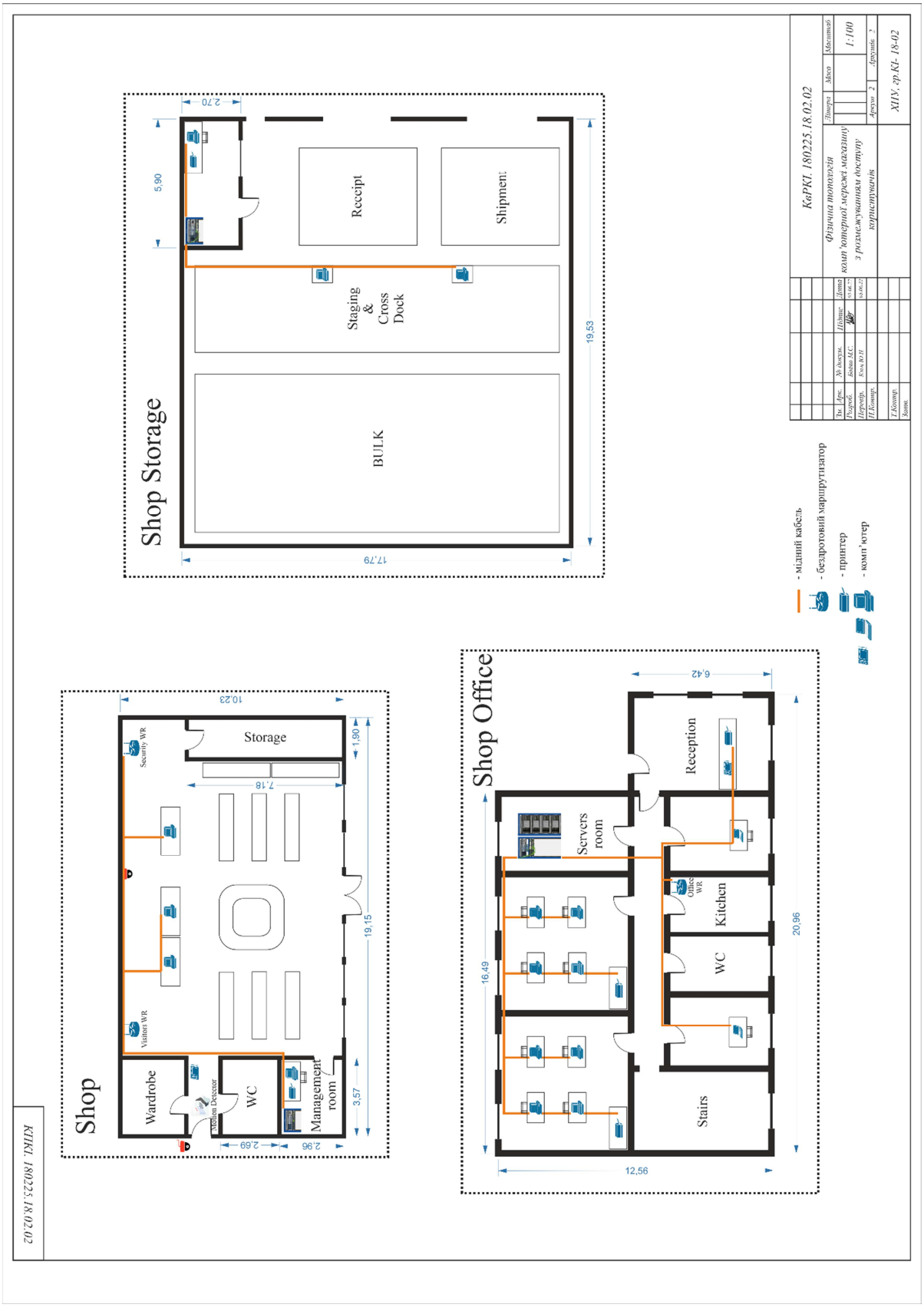
(обов’язковий)

Копія графічної частини

Схеми логічної топології комп’ютерної мережі з розмежуванням доступу користувачів



Схеми фізичної топології комп’ютерної мережі магазину з розмежуванням доступу користувачів



Додаток Б

Лістинг налаштувань мережевих пристроїв

Office ASA_startup-config.txt

```
: Saved
: Written by enable_15 at 00:29:41 UTC Бер 1 1993
: Call-home enabled from prompt by enable_15 at 00:29:41 UTC Бер 1 1993
:
ASA Version 8.4(2)
!
hostname Office-ASA
domain-name shopsecurity.com
enable password lBj1hocrznP5YTi6 encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
 switchport access vlan 1
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Ethernet0/3
 switchport access vlan 1
 switchport trunk allowed vlan 1
!
interface Ethernet0/4
 switchport access vlan 1
!
interface Ethernet0/5
 switchport access vlan 1
!
interface Ethernet0/6
 switchport access vlan 1
!
interface Ethernet0/7
 switchport access vlan 1
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
```

```
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
object network dmz-db-server
 host 192.168.2.5
object network dmz-dns-server
 host 192.168.2.4
object network dmz-ftp-server
 host 192.168.2.6
object network dmz-net
 subnet 192.168.2.0 255.255.255.0
object network dmz-server
 host 192.168.2.3
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.255 1
!
access-list OUTSIDE-DMZ extended permit icmp any host 192.168.2.3
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq www
access-list OUTSIDE-DMZ extended permit udp any host 192.168.2.4
access-list OUTSIDE-DMZ extended permit udp any host 192.168.2.5
!
!
access-group OUTSIDE-DMZ in interface outside
object network dmz-db-server
 nat (dmz,outside) static 209.165.200.229
object network dmz-dns-server
 nat (dmz,outside) static 209.165.200.228
object network dmz-ftp-server
 nat (dmz,outside) static 209.165.200.230
object network dmz-net
 nat (dmz,outside) dynamic interface
object network dmz-server
 nat (dmz,outside) static 209.165.200.227
object network inside-net
 nat (inside,outside) dynamic interface
!
```

```
aaa authentication ssh console LOCAL
!
username admin password pqrZ2iqRGgDD9cbU encrypted
!
class-map inspection_default
 match default-inspection-traffic
class-map inside_dmz
 match any
!
policy-map global_policy
 class inspection_default
  inspect icmp
policy-map inside_dmz_policy
 class inside_dmz
  inspect icmp
!
service-policy global_policy global
service-policy inside_dmz_policy interface inside
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.20-192.168.1.50 inside
dhcpd dns 192.168.2.4 interface inside
dhcpd enable inside
!
!
!
!
```

Office Router_startup-config.txt

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Office-GW
!
!
!
!
```

```
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 209.165.200.225 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
```

```
 ip address 1.1.1.1 255.255.255.252
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 209.165.200.225 0.0.0.0 area 0
 network 1.1.1.1 0.0.0.0 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Office SW_startup-config.txt

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Office-SW
!
!
!
!
```

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 21
!
interface FastEthernet0/2
 switchport access vlan 21
!
interface FastEthernet0/3
 switchport access vlan 21
!
interface FastEthernet0/4
 switchport access vlan 21
!
interface FastEthernet0/5
 switchport access vlan 21
!
interface FastEthernet0/6
 switchport access vlan 21
!
interface FastEthernet0/7
 switchport access vlan 21
!
interface FastEthernet0/8
 switchport access vlan 21
!
interface FastEthernet0/9
 switchport access vlan 21
!
interface FastEthernet0/10
 switchport access vlan 21
!
interface FastEthernet0/11
 switchport access vlan 21
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
```

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport access vlan 21
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 21
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch-SW
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 80
!
interface FastEthernet0/2
 switchport access vlan 80
!
interface FastEthernet0/3
 switchport access vlan 80
!
interface FastEthernet0/4
 switchport access vlan 80
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
```

```
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport access vlan 80
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Shop-GW
!
!
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin password 7 082048430017
!
!
!
!
!
!
!
!
!
ip domain-name shop.com
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 ip helper-address 209.165.200.229
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/0.22
 encapsulation dot1Q 22
 ip address 192.168.22.1 255.255.255.0
 ip helper-address 209.165.200.229
 ip access-group 2 out
 ip nat inside
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 209.165.200.229
 ip nat inside
!
interface FastEthernet0/0.66
 encapsulation dot1Q 66
 ip address 192.168.66.1 255.255.255.0
 ip helper-address 209.165.200.229
 ip access-group 2 out
 ip nat inside
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 ip address 3.3.3.1 255.255.255.0
 ip nat outside
!
```

```
interface FastEthernet5/0
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 3.3.3.1 0.0.0.0 area 0
!
router rip
!
ip nat pool STAFF_POOL 3.3.3.5 3.3.3.10 netmask 255.255.255.0
ip nat inside source list 1 pool STAFF_POOL
ip classless
ip route 0.0.0.0 0.0.0.0 3.3.3.2
!
ip flow-export version 9
!
!
access-list 2 deny 192.168.30.0 0.0.0.255
access-list 2 permit any
access-list 1 permit 192.168.22.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.66.0 0.0.0.255
!
!
!
!
!
!
line con 0
 password 7 0832444119
 login
!
line aux 0
!
line vty 0 4
 password 7 0832444119
 login local
 transport input ssh
!
!
!
end
```

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Shop-SW
!
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
!
!
!
ip domain-name shop.com
!
username admin privilege 1 password 7 082048430017
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 66
!
interface FastEthernet0/2
 switchport access vlan 22
!
interface FastEthernet0/3
 switchport access vlan 22
!
interface FastEthernet0/4
 switchport access vlan 22
!
interface FastEthernet0/5
 switchport access vlan 22
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
```

```
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport access vlan 30
!
interface FastEthernet0/24
 switchport trunk allowed vlan 2-1005
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
!
!
!
!
```

```
line con 0
!
line vty 0 4
 password 7 0832444119
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
!
end
```

Storage Router_startup-config.txt

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Storage-GW
!
!
!
!
ip dhcp excluded-address 192.168.40.1 192.168.40.59
!
ip dhcp pool StoreDHCP
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 209.165.200.228
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 ip helper-address 209.165.200.229
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 ip address 4.4.4.1 255.255.255.248
 ip nat outside
!
interface FastEthernet5/0
```

```
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.1 0.0.0.0 area 0
 network 192.168.40.1 0.0.0.0 area 0
!
router rip
!
ip nat pool STORAGE_POOL 4.4.4.4 4.4.4.6 netmask 255.255.255.248
ip nat inside source list 1 pool STORAGE_POOL
ip classless
ip route 0.0.0.0 0.0.0.0 4.4.4.2
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.40.0 0.0.0.255
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Storage Switch_startup-config.txt

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Storage-SW
!
enable secret 5 $1$mERr$wuhxbrVVh6mHlxzsCADtB0
!
```

```
!
!
ip domain-name shop.com
!
username admin privilege 1 password 7 082048430017
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 40
!
interface FastEthernet0/2
 switchport access vlan 40
!
interface FastEthernet0/3
 switchport access vlan 40
!
interface FastEthernet0/4
 switchport access vlan 40
!
interface FastEthernet0/5
 switchport access vlan 40
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
```

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport trunk allowed vlan 2-1005
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
 password 7 0832444119
 login local
 transport input ssh
line vty 5 15
 login
!
!
end
```

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 16%**

ID: 104749 Название: Комп'ютерна мережа магазину з розмежуванням доступу користувачів Добавлено в БД: 2022-06-08 Авторы: Бойко Микита Сергійович Руководители: Кльоц Ю.П. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	53351	500	1718 (3%)	29 (6%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011504777

Дата перевірки:
08.06.2022 12:57:43 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.06.2022 13:27:31 EEST

ID користувача:
100008300

Назва документа: **Бакалаврська_робота_Бойко М.С_на_антиплагіат**

Кількість сторінок: **62** Кількість слів: **10193** Кількість символів: **82874** Розмір файлу: **2.47 MB** ID файлу: **1011379802**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

7.37%
Схожість

Найбільша схожість: **1.57%** з джерелом з Бібліотеки (ID файлу: **1008383715**)

5.38% Джерела з Інтернету	220	Сторінка 64
2.79% Джерела з Бібліотеки	103	Сторінка 66

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	15 сторінок

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНИЙ ПРОЕКТ

Дипломник Бойко Микита Сергійович
Тема Комп'ютерна мережа магазину з розмежуванням доступу користувачів
Спеціальність 123 Комп'ютерна інженерія

Обсяг дипломного проекту:

кількість листів креслень 2; кількість сторінок записки 80

1. Короткий зміст ДП та прийнятих рішень В рамках дипломного проекту розроблено проєкт комп'ютерної мережі магазину з розмежуванням доступом користувачів.

2. Висновок про відповідність ДП дипломному завданню Дипломний проект у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині даного проекту.

3. Характеристика виконання кожного розділу проекту, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому, теоретичному, розділі дипломного проекту якісно та в повній мірі розглянуті методи вирішення поставленої задачі, був проаналізований кожен аспект, який стосується теми дипломного проекту. У наступному розділі було здійснено обґрунтування обраної структури мережі на основі порівняння різних можливих варіантів побудови цієї мережі, а також сформовані вимоги. У основній проектній частині диплому була реалізована сучасними методами та рішеннями логічна топологія мережі і фізична топологія мережі. Проектування виконано в середовищі Cisco Packet Tracer. Спроектована мережа дозволить забезпечити потреби користувачів мережі магазину та враховує особливості розмежування доступу.

4. Позитивні сторони проекту Дипломний проект відповідає сучасним вимогам до проектування локальних комп'ютерних мереж та містить ряд рішень, що відповідають умовам сучасного магазину. Побудована мережа передбачає використання наявних оптоволоконних ліній та створення демілітаризованої зони.

5. Негативні сторони проекту _____

6. Оцінка графічного оформлення та пояснювальної записки проекту Графічне оформлення виконане відповідно до суті дипломного проекту. На першому кресленні відображено три логічні топології мережі, на другому кресленні відображено фізичну топологію мережі, використання технології логічної структуризації мережі. В загальному графічне оформлення виконане на належному рівні. Пояснювальна записка відповідає задекларованим нормам для її оформлення.

7. Відгук про проект в цілому Дипломний проект вирішує поставлену задачу і детально описує її вирішення.

8. Інші зауваження _____

9. Оцінка дипломного проекту Розглянувши позитивні та негативні сторони представленого дипломного проекту, можна зробити висновок, що він заслуговує оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, завідувач кафедри «Автоматизації та комп'ютерно-інтегрованих технологій»

«13» 06 2022 р. _____ (підпис)

ХНУ. Зам. 54; тир. 6000, 2007.

Завідувачу кафедри КБ
к.т.н., доценту Кльоцу Ю. П.

Бойко М.С.

ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ-18-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність плагіату ознайомлений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету

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

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

26 05 22

дата

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 магазину з розмежуванням доступу користувачів

Автор: Бойко Микита Сергійович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Кльоц Ю.П., к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-30 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано набори команд налаштування обладнання, що є типовими для налаштування мережевого обладнання і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) 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 7.37% і адресується до 323 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи Ю.П. Кльоц

Гарант ОП С.М. Лисенко

Завідувач кафедри КБ Ю.П. Кльоц

2022/6/15 11:07