ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук та інформаційних технологій

ВИПУСКНИЙ КВАЛІФІКАЦІЙНИЙ ПРОЕКТ

на тему:

«Розробка імітаційної моделі комп'ютерної мережі підприємства»

Студента 4 курсу, 8 групи, Цимбалюк Антон Дмитровича

спеціальності 122 «Комп'ютерні науки» _____ *підпис студента*

Науковий керівник

Старший викладач кафедри _____ *підпис керівника* Селіванова Анна Віталіївна

Гарант освітньої програми

кандидат технічних наук, професор _____ *підпис керівника* Демідов Павло Георгійович

Київ 2023

Державний торговельно-економічний університет

Факультет інформаційних технологій
Кафедра комп'ютерних наук та інформаційних систем
Спеціальність 122 «Комп'ютерні науки»

Затверджую
Зав. кафедри _____Пурський О.І.
«12» грудня 2022р.

Завдання
на випускну кваліфікаційну роботу (проект) студенту

Цимбалюк Антон Дмитрович
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи (проекту)
«Розробка імітаційної моделі комп'ютерної мережі підприємства»
Затверджена наказом ректора від *«09» грудня 2022 р. № 3332*
2. Строк здачі студентом закінченої роботи *30 травня2023 року*
3. Цільова установка та вихідні дані до роботи
Мета роботи: Створення імітаційної моделі комп'ютерної мережі підприємства
Об'єкт дослідження: процеси функціонування комп'ютерної мережі підприємства
Предмет дослідження: інформаційні технології побудови та моделювання комп'ютерних мереж
4. Перелік графічного матеріалу_____
_____
_____
_____
_____

5. Консультанти по роботі із зазначенням розділів, за якими здійснюється консультування:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Селіванова А.В.		
2	Селіванова А.В.		
3	Селіванова А.В.		

6. Зміст випускної кваліфікаційної роботи (проекту) (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1. Загальна проблематика функціонування комп'ютерних мереж

1.1. Аналіз функціонування комп'ютерних мереж

1.2. Захист комп'ютерних мереж

1.3. Інформаційні технології побудови та моделювання комп'ютерних мереж.

РОЗДІЛ 2. Розробка імітаційної моделі комп'ютерної мережі підприємства

2.1. Специфіка побудови імітаційної моделі комп'ютерної мережі підприємства

2.2.Проектування структури комп'ютерної мережі підприємства

2.3. Модель функціонування комп'ютерної мережі підприємства

РОЗДІЛ 3. Реалізація імітаційної моделі комп'ютерної мережі підприємства

3.1. Налаштування імітаційної моделі комп'ютерної мережі підприємства

3.2. Реалізація захисту комп'ютерної мережі підприємства

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

7. Календарний план виконання роботи

№ Пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	фактично
1	2	3	4
1	*Вибір теми випускної кваліфікаційної роботи*		
2	*Розробка та затвердження завдання на випускну кваліфікаційну роботу*		
3	*Вступ*		
4	*РОЗДІЛ 1. Загальна проблематика функціонування комп'ютерних мереж*		
5	*РОЗДІЛ 2. Розробка імітаційної моделі комп'ютерної мережі підприємства*		
6	*РОЗДІЛ 3. Реалізація імітаційної моделі комп'ютерної мережі підприємства*		
7	*Висновки*		
8	*Здача випускної кваліфікаційної роботи на кафедру науковому керівнику*		
9	*Попередній захист випускної кваліфікаційної роботи*		
11	*Виправлення зауважень, зовнішнє рецензування випускної кваліфікаційної роботи*		
12	*Представлення готової зшитої випускної кваліфікаційної роботи на кафедру*		
13	*Публічний захист випускної кваліфікаційної роботи*	*За розкладом роботи ЕК*	

8. Дата видачі завдання «15» грудня 2022 р.

Керівник випускної кваліфікаційної роботи (проекту)
Селіванова А.В.
_____
(прізвище, ініціали, підпис)

Гарант освітньої програми Демідов П.Г.
_____
(прізвище, ініціали, підпис)

Завдання прийняв студент-дипломник Цимбалюк А.Д.
_____
(прізвище, ініціали, підпис)

9. Відгук керівника випускної кваліфікаційної роботи (проекту)
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Керівник випускної кваліфікаційної роботи (проекту)
_________________ 30.05.2023 р.
(підпис, дата)

10. Висновок про випускну кваліфікаційну роботу

Випускна кваліфікаційна робота студента _________________________
(прізвище, ініціали)
може бути допущена до захисту в екзаменаційній комісії.

Гарант освітньої програми_________________________ Демідов П.Г.
(підпис, прізвище, ініціали)

Завідувач кафедри _________________________________ Пурський О.І.
(підпис, прізвище, ініціали)
«_____»_________________2023 р.

Аннотація

У випускній кваліфікаційній роботи було проведене дослідження функціонування комп'ютерних мереж підприємства, їх структури та методи моделювання. Теоретично обґрунтовано принцип роботи комп'ютерних мереж підприємства та запропоновано власну структуру корпоративної мрежі. Розроблено структуру працюючої та ефективної комп'ютерної мрежі. Створено імітаційну модель у середовищі Cisco Packet Tracer для наглядного прикладу роботи корпоративної мережі.

Ключові слова: корпоративна мережа, протокол, сервер, комутатор, підприємство.

Anotation

The graduation qualification work is devoted to development of functioning of enterprise computer networks, their structures and modeling methods. The principle of operation of the company's computer networks is theoretically substantiated, and the own structure of the corporate network is proposed. The structure of a working and effective computer network has been developed. A simulation model was created in the Cisco Packet Tracer environment for a visual example of the operation of a corporate network.

Keywords: corporate network, protocol, server, switch, enterprise.

ЗМІСТ

ВСТУП

Корпоративні мережі є невід'ємною складовою сучасного бізнес-середовища, що забезпечує ефективне функціонування і сприяє досягненню бізнес-цілей. Вивчення та розуміння принципів, особливостей та технологій, що стоять за побудовою та управлінням корпоративними мережами, має велике значення для фахівців у сфері інформаційних технологій. Комп'ютерні мережі підприємства відіграють критичну роль у забезпеченні безперебійного обміну даними та комунікації всередині організації. Вони дозволяють підприємствам підключати різноманітні пристрої, такі як комп'ютери, сервери, принтери, маршрутизатори та інші мережеві пристрої, створюючи єдину інфраструктуру зв'язку. Це сприяє обміну даними, спільному доступу до ресурсів, спілкуванню та співпраці між співробітниками організації. Побудова та ефективне управління корпоративними мережами вимагає глибокого розуміння їх структури, протоколів зв'язку, безпекових механізмів та передових технологій. Враховуючи зростаючу складність та розмір корпоративних мереж, виникає необхідність у вивченні стратегій масштабування, оптимізації ресурсів та забезпечення безпеки мережевих інфраструктур. Особлива увага приділяється практичному застосуванню технологій та інструментів, які допомагають управляти та оптимізувати корпоративні мережі, що і зумовило **актуальність** обраної темидослідження, його мету і завдання.

Мета і завдання дослідження. Метою даної роботи є створення імітаційної моделі комп'ютерної мережі підприємства. Для досягнення мети було вирішено поставити наступні **завдання:**

- Провести аналіз функціонування комп’ютерних мереж.
- Визначити роль мереж у діяльності підприємства.

- Дослідити різни структури корпоративних мереж.
- Розробити власну функціонуючу структуру і модель мережі.
- Опрацювати отримані результати дослідження

Об'єкт дослідження: процеси фунціонування комп'ютерної мережі підприємства.

Методи дослідження: Теоретичною основою дослідження є загальнонауковий аналітичний метод, а також системний підхід і праці провідних вчених з комп'ютерних мереж, та моделюванню мереж.

Практичне значення. Розроблена мережа має практичне значення на реальному підприємстві. Дослідження незвичайних структур мереж і проблем, які виникають при моделюванні.

РОЗДІЛ 1.
ЗАГАЛЬНА ПРОБЛЕМАТИКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Аналіз функціонування комп'ютерих мереж

Комп'ютерні мережі виконують важливу роль у сучасному інформаційному суспільстві, забезпечуючи зв'язок і обмін даними між комп'ютерами та іншими пристроями. Майже кожне підприємство використовує власну корпоративну мережу для підтримки роботи. Ефективне управління комп'ютерними мережами є ключовим аспектом їх функціонування.

Корпоративна мережа (Corporate Network) - це інформаційна і комунікаційна інфраструктура, створена для підтримки роботи певного підприємства або організації. Вона є основним засобом обміну даними, комунікації та спільної роботи між різними відділами, робочими станціями, серверами та іншими пристроями, що знаходяться в межах організації[1,8-10].

Корпоративні мережі розрізняються від загальнодоступних мереж, таких як Інтернет, тим, що вони призначені виключно для внутрішнього використання працівниками підприємства. Це дозволяє організації контролювати та забезпечувати безпеку своїх даних та ресурсів.

Корпоративні мережі можуть бути побудовані з використанням різних технологій, таких як локальні мережі (LAN), великі об'єднані мережі (WAN), бездротові мережі (Wi-Fi), віртуальні приватні мережі (VPN) та інші. Вони можуть включати сервери, комутатори,

маршрутизатори, файрволи, системи зберігання даних та інші мережеві пристрої.

Основна мета корпоративної мережі - забезпечити ефективний обмін даними, спільну роботу та комунікацію між співробітниками організації, полегшуючи доступ до спільних ресурсів, таких як файли, друк, електронна пошта, бази даних тощо. Крім того, корпоративні мережі можуть включати інші функціональні складові, такі як системи безпеки, резервне копіювання даних, системи моніторингу, системи управління мережею тощо.

Важливим аспектом корпоративних мереж є їх масштабованість і здатність до розширення. Вони повинні бути проектовані та побудовані з урахуванням потреб організації в майбутньому, зокрема щодо збільшення кількості користувачів, обсягу даних та розширення функціональних можливостей.

Дослідженню питань комп'ютерних мереж присвячена велика кількість праць як закордонних дослідників Larry L. Peterson, Bruce S. Davie, James F. Kurose, Keith W. Ross, A. S. Tanenbaum, N. Feamster, D. Wetherall [1,10], так і вітчизняних, зокрема О. С. Городецька, В. А. Гикавий, О. В. Онищук, Б.Ю. Жураковський, І.О. Зенів [2,17].

В залежності від розмірів підприємства та його потреб у мережевих ресурсах виділяють різні типи корпоративних мереж.

Одним з них є **мережа відділу (departmental network)**, яка забезпечуютє ефективну комунікацію та обмін інформацією в межах певного підрозділу або відділу підприємства. Вона відіграє важливу роль у забезпеченні безперебійної роботи та взаємодії працівників, сприяючи оптимізації бізнес-процесів та підвищенню продуктивності.

Основна мета мереж відділу полягає у забезпеченні доступу до спільних ресурсів, таких як файли, друкована документація, програмне забезпечення та інші ресурси, необхідні для роботи працівників даного відділу. Вони створюють сприятливу інформаційну інфраструктуру, що сприяє ефективному обміну даними та спільній роботі між працівниками.

Мережі відділу, як правило, відрізняються від інших типів мереж, таких як корпоративні мережі або мережі кампусу, меньшими розмірами та масштабами. Їхній обсяг зазвичай обмежений до певного відділу або групи працівників, і вони здебільшого не мають окремих підмереж або розділеної інфраструктури. Мережі відділу можуть містити один або два файлових сервери та обслуговувати відносно невелику кількість користувачів, зазвичай до тридцяти працівників.

Важливим аспектом мереж відділу є їхня надійність та безпека. Забезпечення конфіденційності, цілісності та доступності даних стає пріоритетною задачею. Для досягнення цих цілей використовуються різні заходи безпеки, такі як файрволи, антивірусне програмне забезпечення, механізми аутентифікації та авторизації, шифрування даних тощо. Крім того, важливо забезпечити надійне резервне копіювання даних та відновлення системи в разі виникнення непередбачених ситуацій.

У сучасному бізнес-середовищі мережі відділу є невід'ємною складовою успішної роботи організації. Вони забезпечують швидку та надійну комунікацію між працівниками, сприяють обміну інформацією та спільній роботі, а також забезпечують високий рівень безпеки та захисту даних. Приклад мережі відділу подано на рисунку 1.1.

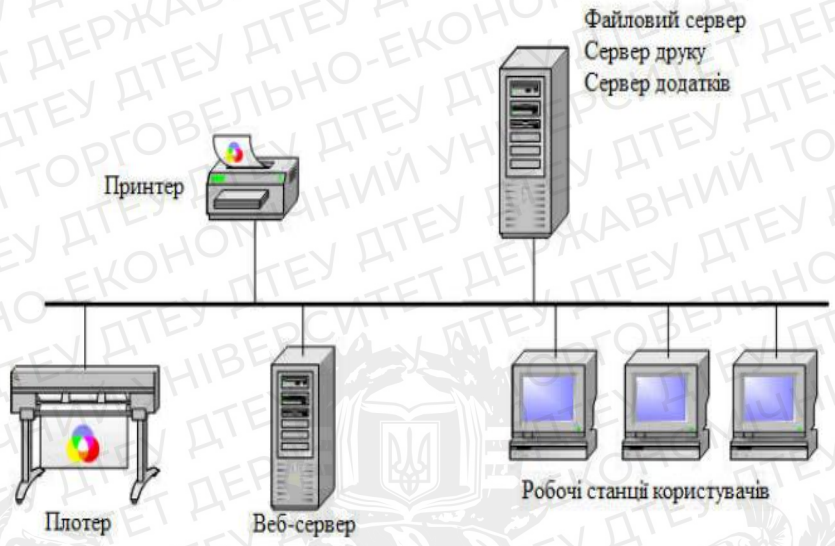

Рисунок 1.1 – Приклад мережі відділу

Ще одним типом є **мережа кампусу (campus network)**, яка об'єднує різні локальні мережі в межах кампусу навчального закладу, або великого підприємства. Основною метою мереж кампусу є забезпечення ефективного обміну даними та ресурсами між різними приміщеннями, відділеннями та підрозділами.

Одна з головних особливостей мереж кампусу полягає в їх розмірі та розмаїтості. Вони можуть охоплювати велику площу території і включати в себе різноманітні будівлі, такі як навчальні корпуси, аудиторії, лабораторії, адміністративні приміщення тощо. Крім того, мережі кампусу можуть об'єднувати різні типи пристроїв, включаючи комп'ютери, сервери, принтери, маршрутизатори, комутатори та інші мережеві пристрої.

Організація мережі кампусу вимагає ретельного планування, проектування та налагодження. Вона повинна забезпечувати надійну та безперебійну передачу даних, а також захист від несанкціонованого доступу та інших загроз безпеці. Для досягнення цих цілей використовуються різні технології, включаючи високошвидкісні

комутаційні пристрої, віртуальні приватні мережі (VPN), мережеві брандмауери та системи ідентифікації та автентифікації користувачів. Приклад мережі кампусу подано на рисунку 1.2.

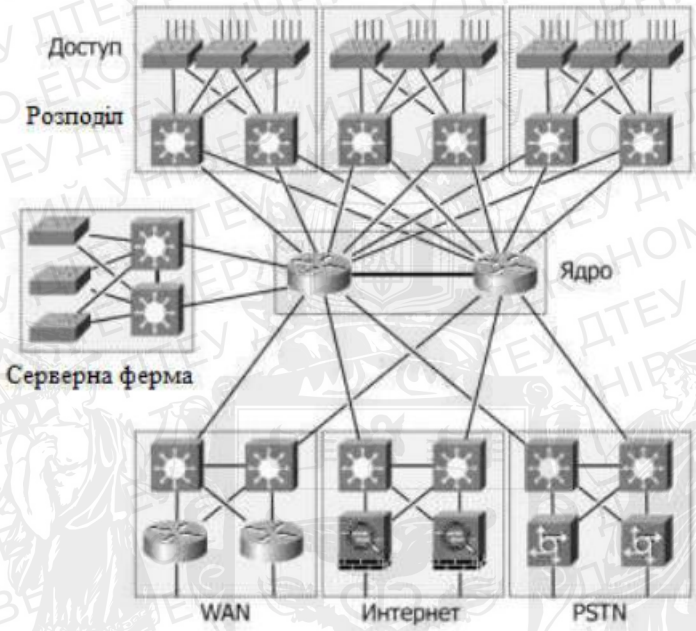

Рисунок 1.2 – Приклад мережі кампусу

Загальною метою мереж кампусу є забезпечення надійності, масштабованості та ефективності мережевих послуг в межах кампусу. Це включає управління пропускною здатністю, керування мережевим трафіком, моніторинг мережевої інфраструктури та забезпечення безпеки даних.

Окремо виділяється **корпоративна мережа (enterprise network)**, яка підтримує роботу підприємства або організації. Вона забезпечує зв'язок та обмін даними між різними вузлами та пристроями в рамках внутрішньої інфраструктури. Користувачами корпоративних мереж є виключно співробітники підприємства, а не зовнішні сторони або користувачі.

Головна мета корпоративних мереж полягає у підтримці роботи організації шляхом надання доступу до спільних ресурсів, таких як файли,

друкована документація, програмне забезпечення тощо. Це дозволяє співробітникам ефективно спілкуватися, співпрацювати та обмінюватися інформацією в рамках організаційних процесів.

Однією з головних особливостей корпоративних мереж є їхній масштаб та складність. Вони можуть включати в себе значну кількість комп'ютерів, серверів, маршрутизаторів, комутаторів та інших мережевих пристроїв. Крім того, корпоративні мережі можуть охоплювати кілька відділень або навіть розташовуватися на різних географічних місцезнаходженнях. Це ставить вимоги до надійності, масштабованості та безпеки мережевої інфраструктури[9-12]. Приклад корпоративної мережі подано на рисунку 1.3.

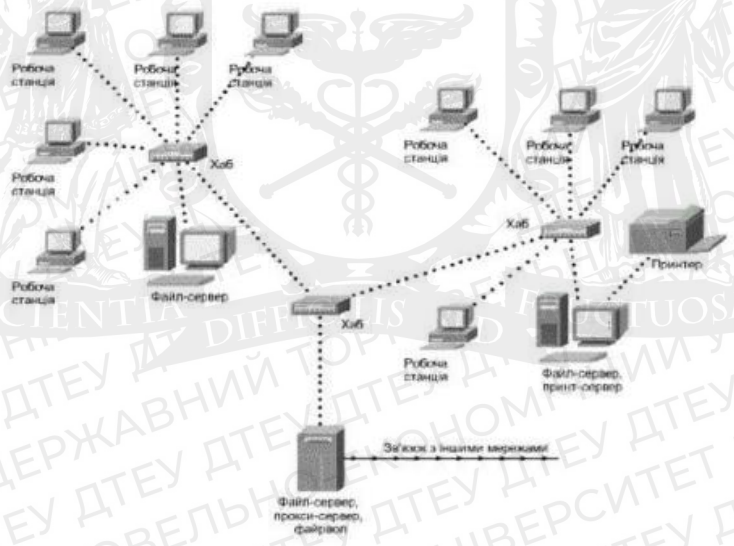

Рисунок 1.3 – Приклад корпоративної мережі

Кожна організація може мати свої власні особливості функціонування корпоративної мережі, враховуючи свої потреби та вимоги.

1.2 Захист комп’ютерних мереж

Комп'ютерна безпека - це захист цінних об'єктів, які називаються активами комп'ютера або комп'ютерної системи. Щоб визначити, що потрібно захищати, спочатку ми повинні визначити, що має цінність і для кого. На комп'ютерні мережі можуть бути спрямовані різноманітні види кібератак з метою незаконного доступу до інформації, порушення функціонування мережі, викрадення даних або завдання іншої шкоди [3,4].

З урахуванням частоти та різноманітності існуючих атак, а також загрози нових і більш руйнівних майбутніх атак, мережева безпека стала центральною темою у галузі комп'ютерних мереж .

Корпоративна мережа вважається критичною інфраструктурою для багатьох організацій, оскільки вона забезпечує передачу та обмін конфіденційною інформацією, функціонування внутрішніх процесів та спільну роботу працівників. Запобігання несанкціонованому доступу, витоку даних, а також забезпечення цілісності, конфіденційності та доступності цієї інформації є основною метою захисту корпоративних мереж.

Для досягнення високого рівня безпеки корпоративних мереж, використовуються різноманітні технічні та організаційні заходи. **Технічні заходи** включають в себе використання мережевих фаєрволів, систем виявлення вторгнень, шифрування даних, механізми аутентифікації та авторизації, а також резервне копіювання даних. Для ефективного застосування цих технічних заходів необхідно проводити аналіз ризиків, розробляти політики безпеки та впроваджувати правильну архітектуру мережі.

Організаційні заходи включають в себе навчання персоналу щодо безпеки мережі, встановлення процедур управління інцидентами, здійснення моніторингу та аудиту безпеки, а також впровадження строгих

політик доступу та використання інформації. Крім того, важливо забезпечити фізичну безпеку серверних приміщень та мережевого обладнання.

Основні аспекти безпеки корпоративної мережі включають:

1. **Аутентифікація і авторизація:** Для забезпечення безпеки важливо мати механізми аутентифікації, які перевіряють ідентичність користувачів і контролюють їх доступ до ресурсів. Авторизація дозволяє встановлювати права доступу для користувачів на основі їхніх ролей та відповідності політикам безпеки.
2. **Захист мережевого трафіку:** Корпоративна мережа повинна мати механізми шифрування та захисту мережевого трафіку. Використання протоколів шифрування, таких як SSL/TLS, IPSec і VPN, дозволяє захистити конфіденційну інформацію під час передачі по мережі.
3. **Виявлення та запобігання вторгненням:** Корпоративна мережа повинна мати системи виявлення та запобігання вторгненням (Intrusion Detection and Prevention Systems, IDS/IPS), які моніторять мережевий трафік і виявляють аномалії та потенційні загрози безпеці. Це допомагає запобігти несанкціонованому доступу і атакам на мережу.
4. **Захист від вірусів і шкідливих програм:** Корпоративна мережа повинна мати антивірусні та антишпіонські рішення, які регулярно оновлюються і сканують системи для виявлення та нейтралізації вірусів, троянських програм і інших шкідливих впливів.
5. **Резервне копіювання та відновлення даних:** Забезпечення резервного копіювання та відновлення даних є важливим аспектом безпеки корпоративної мережі. Регулярне створення резервних копій

даних та розробка планів відновлення допомагають забезпечити доступність даних в разі аварійних ситуацій чи випадку втрати даних.

6. **Строга політика безпеки:** Встановлення і виконання строгої політики безпеки є необхідною умовою для захисту корпоративної мережі. Це включає правила щодо паролів, доступу до ресурсів, обмеження прав користувачів, моніторинг активності та інші безпечні практики.

Постійний моніторинг корпоративної мережі, аналіз подій, виявлення та відповідь на потенційні загрози є необхідними складовими частинами захисту. Застосування системи інтранет-інтернет-периметрів дозволяє ефективно контролювати трафік в межах мережі, а також між мережею і зовнішнім середовищем.

Безпека комп'ютерної мережі - це постійний процес, який вимагає постійного моніторингу, оновлень і удосконалення заходів захисту. Інтеграція кількох різновидів захисту та прийняття комплексного підходу допомагають зменшити ризики і забезпечити безпеку комп'ютерної мережі.

1.3 Інформаційні технології побудови та моделювання комп’ютерних мереж

Для побудови та моделювання комп'ютерних мереж використовуються різні інструменти та технології. Ось кілька з них:

1. **Програмне забезпечення моделювання мережі:** Існують спеціальні програми, які дозволяють моделювати комп'ютерні мережі, їхню архітектуру та поведінку. Такі програми дозволяють створювати віртуальні моделі мережі, задавати параметри пристроїв, з'єднань та трафіку, імітувати різні сценарії та проводити аналіз результатів.
2. **Програмне забезпечення для аналізу трафіку:** Ці програми збирають та аналізують дані про мережевий трафік, включаючи обсяги, швидкість передачі, затримки, втрати пакетів та інші параметри. Вони допомагають ідентифікувати проблеми в мережі, виявляти загружені ділянки, точки перебою та незвичайну активність.
3. **Програмне забезпечення для налаштування мережевих протоколів:** Комп'ютерні мережі використовують різні протоколи для обміну даними та керування мережевими пристроями. Існують спеціальні програми, які дозволяють налаштовувати ці протоколи, встановлювати параметри маршрутизації, керувати каналами зв'язку та забезпечувати правильну роботу мережі.
4. **Програмне забезпечення для віддаленого керування мережею:** Ці програми дозволяють адміністраторам віддалено керувати мережею, налаштовувати пристрої, моніторити їх стан та виконувати різні адміністративні завдання. Вони спрощують управління великими мережами та дозволяють ефективно впроваджувати зміни та налаштування.

5. **Апаратне забезпечення:** Побудова комп'ютерних мереж вимагає використання фізичних компонентів, таких як мережеві комутатори, маршрутизатори, мережеві кабелі, бездротові точки доступу та інше обладнання. Вибір правильного апаратного забезпечення є важливим аспектом побудови мережі.
6. **Протоколи та стандарти:** У світі комп'ютерних мереж існує безліч протоколів та стандартів, які визначають спосіб передачі даних, формат пакетів, керування мережевим трафіком та інші аспекти мережевої комунікації. Дотримання цих протоколів та стандартів є важливим для сумісності та ефективної роботи мережі.

Ці інструменти та технології спільно використовуються для побудови, моделювання, аналізу та оптимізації комп'ютерних мереж, забезпечуючи їхню надійність, ефективність та безпеку.

РОЗДІЛ 2.
РОЗРОБКА ІМІТАЦІЙНОЇ МОДЕЛІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

2.1 Специфіка побудови імітаційної моделі комп'ютерної мережі підприємства

Для визначення структури мережі використористовують аналіз функціональних вимог та особливостей корпоративної мережі. Цей аналіз спрямований на визначення потреб і вимог, що ставляться до мережі, а також виявлення особливостей, які впливають на її функціонування та ефективність. Під час аналізу функціональних вимог здійснюється збір та уточнення вимог, що ставляться до мережі. Це включає ідентифікацію потреб користувачів, бізнес-вимог, а також технічних вимог, пов'язаних зі забезпеченням безпеки, масштабованості, надійності та продуктивності мережі. Завдання аналізу полягає в тому, щоб визначити, які функції мережі повинні бути реалізовані для задоволення вимог користувачів та досягнення бізнес-цілей.

Особливості корпоративної мережі включають в себе різноманітні аспекти, які впливають на її проектування та функціонування. Серед них можуть бути[13]:

1. **Розмір та масштаб:** Корпоративні мережі можуть бути розгорнуті в різних масштабах, від невеликих офісних мереж до глобальних мереж, що об'єднують кілька офісів чи філій. Аналіз масштабу дозволяє визначити потреби у пропускній здатності, маршрутизації, керуванні та інших аспектах мережі.

2. **Топологія:** Вибір топології мережі (наприклад, зірка, шина, кільце, дерево) залежить від потреб організації та вимог до надійності та масштабованості. Аналіз топології допомагає визначити найбільш оптимальну структуру мережі.
3. **Безпека:** Корпоративні мережі потребують високого рівня безпеки для захисту конфіденційної інформації та запобігання несанкціонованому доступу. Аналіз вимог до безпеки допомагає визначити необхідні заходи та технології для забезпечення захисту мережі.
4. **Служби та додатки:** Корпоративна мережа може підтримувати різноманітні служби та додатки, такі як електронна пошта, відеоконференції, спільний доступ до файлів тощо. Аналіз функціональних вимог допомагає визначити необхідність підтримки цих служб та засоби їх реалізації.

Після аналізу функціональних вимог та особливостей корпоративної мережі можна приступати до проектування та реалізації мережевої інфраструктури.

2.2 Проектування структури комп’ютерної мережі підприємства

Масштаби корпоративних мереж є важливими аспектами їх проектування та розгортання. Вони визначають розмір, протяжність та складність мережевої інфраструктури, яка обслуговує організацію:

1. **Малі:** Малі корпоративні мережі характеризуються невеликою кількістю вузлів та простими мережевими структурами. Вони часто зустрічаються у невеликих підприємствах або філіях більших організацій. Основними компонентами таких мереж є комутатори, маршрутизатори та файрволи. У малому масштабі вимоги до масштабованості та безпеки є меншими, але ефективне керування мережею залишається важливим аспектом.
2. **Середні:** Середні корпоративні мережі охоплюють більше кількості вузлів і мають більш складну структуру. Вони зазвичай знаходяться в середніх підприємствах або компаніях з декількома відділеннями. У таких мережах можуть бути застосовані різноманітні технології, такі як віртуалізація, VPN тунелі та багатошарова архітектура мережі. Вимоги до безпеки, масштабованості та продуктивності зазвичай зростають у середньому масштабі.
3. **Великі:** Великі корпоративні мережі є складними та розгалуженими системами, які охоплюють багато відділень, філій або навіть різних країн. Вони можуть об'єднувати тисячі вузлів та мати глобальний охоплення. У таких мережах вимоги до масштабованості, надійності та продуктивності є найвищими. Забезпечення безпеки, ефективного керування та моніторингу стають важливими аспектами.

Топологія корпоративних мереж визначає структуру та зв'язки між їх складовими елементами, такими як вузли, комутатори, роутери та інші мережеві пристрої. Вибір топології залежить від потреб і вимог

корпоративної мережі, а також від розмірів і географічного розташування підприємства. Існує декілька видів топологій мережі:

1. Зірка - одна з основних топологій, використовуваних в корпоративних мережах. У цій схемі всі вузли підключені до центрального комутатора або концентратора, утворюючи структуру, схожу на вигляд зірки. У зірковій топології кожен вузол мережі має окреме з'єднання з центральним комутатором. Цей комутатор виступає в ролі центрального вузла, через який здійснюється комунікація між всіма вузлами мережі. Кожен пакет даних, що надходить до комутатора, розсилається до призначеного вузла, який приймає дані, а решта вузлів не отримують ці дані. На рисунку 2.1 представлена схема топології «зірка».

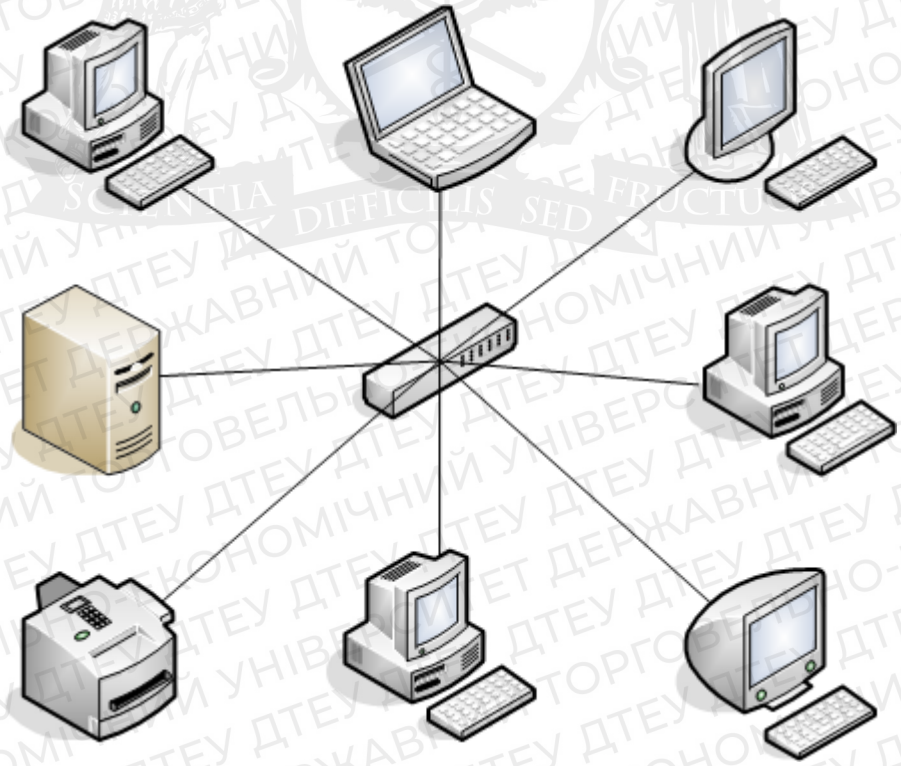

Рисунок 2.1 – Схема топології «зірка»

2. Шина - в цій схемі всі вузли мережі підключені до однієї загальної комунікаційної лінії, яка називається шиною. Кожен вузол може передавати дані на шину, а всі інші вузли можуть сприймати ці дані. ВКузли підключені до шини за допомогою спеціальних з'єднувачів або розгалужувачів. Коли вузол бажає передати дані, він розміщує їх на шині, а всі інші вузли слухають шину, щоб отримати ці дані. Ця топологія передачі даних використовує принцип спільного доступу до мережевого каналу. На рисунку 2.2 надана схема топології «шина»

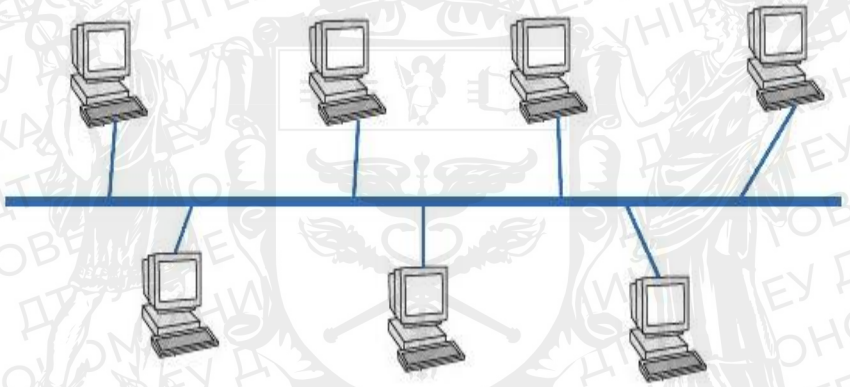

Рисунок 2.2 – Схема топології «шина»

3. Кільце - вузли мережі підключені у вигляді кільця, де кожен вузол має пряме з'єднання з двома сусідніми вузлами. Дані передаються вздовж кільця в одному напрямку, утворюючи замкнений шлях передачі інформації. Кожен вузол пропускає дані через себе, передаючи їх наступному вузлу в кільці. Цей процес називається "передачею маркера". Лише вузол, який володіє маркером, може передавати дані, тоді як всі інші вузли прослуховують канал для отримання інформації. Якщо вузол не є призначеним отримувачем, він просто передає отримані дані далі по кільцю. Рисунок 2.3 надає уявлення про топологію

«кільце».

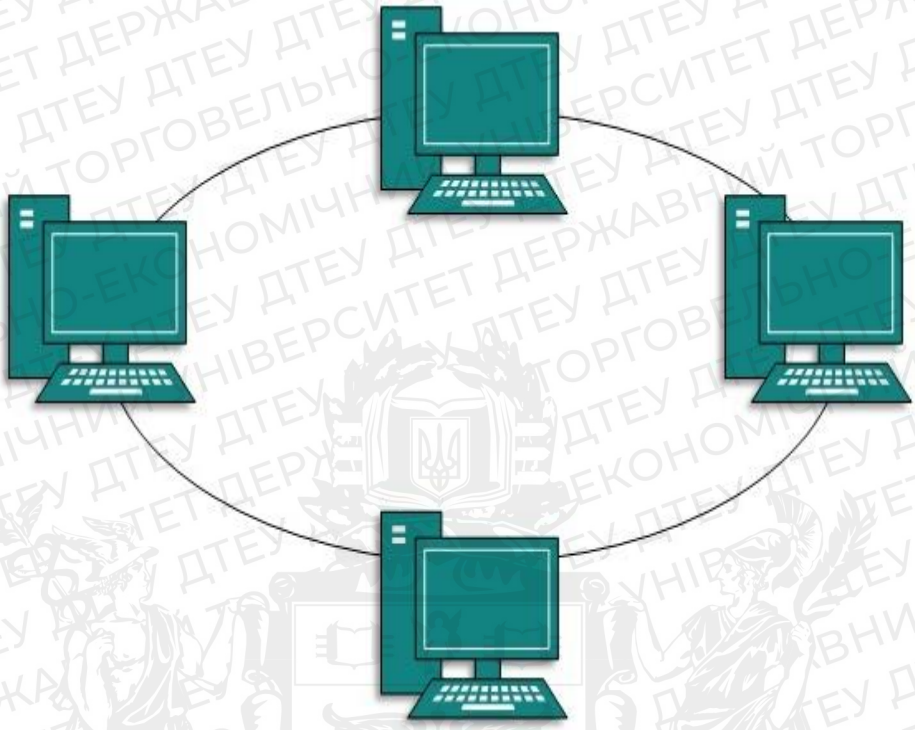

Рисунок 2.3 – Топологія «кільце»

4. Дерево - є ієрархічною структурою, в якій вузли організовані у вигляді дерева з одним головним вузлом (коренем) і декількома підвузлами (гілками). Кожен вузол може мати свої підвузли, і таким чином створюється деревоподібна структура зі шляхами спуску від кореня до листків. Забезпечує ефективну організацію мережі, зокрема, легку розширюваність та гнучкість. Головний вузол (корінь) здатний керувати трафіком і розподіляти ресурси між підвузлами. Підвузли можуть включати інші підвузли або кінцеві вузли, такі як комп'ютери чи пристрої. Ця ієрархічна структура дозволяє зменшити затримки передачі даних та забезпечити більш ефективне керування мережею, що добре видно на схемі (рис.2.4).

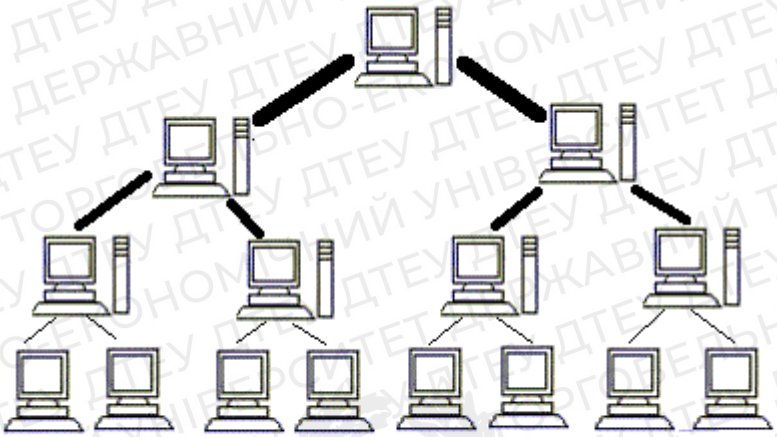

Рисунок 2.4 – Топологія «дерево»

Безпека корпоративних мереж є однією з найважливіших аспектів їх проектування, налаштування та експлуатації. Однією з основних складових безпеки корпоративної мережі є захист від несанкціонованого доступу. Це досягається шляхом розробки і реалізації механізмів аутентифікації та авторизації, використання паролів, мережевих файрволів, віртуальних приватних мереж (VPN), інтрафейсів контролю доступу (ACL) та інших захисних механізмів.

Окрім захисту від несанкціонованого доступу, безпека корпоративних мереж також охоплює захист від шкідливих програм, таких як віруси, черв'яки та троянські програми. Для цього використовуються антивірусні програми, системи виявлення та запобігання вторгнень (IDS/IPS), спам-фільтри.

Однією зі специфічних особливостей безпеки корпоративних мереж є захист конфіденційності та цілісності даних. Застосування шифрування, включаючи шифрування трафіку та шифрування даних в спеціальних зонах, може забезпечити захист від несанкціонованого доступу та змін до даних під час їх передачі через мережу.

Крім того, резервне копіювання та відновлення даних, регулярні аудити безпеки, моніторинг мережі та подій також відіграють важливу роль у забезпеченні безпеки корпоративної мережі.

Найважливішою службою корпоративних мереж є електронна пошта. Вона надає можливість спілкування між співробітниками організації шляхом обміну електронними повідомленнями. Електронна пошта дозволяє надсилати, отримувати та зберігати повідомлення, а також організовувати календарі, списки завдань та контакти. Ця служба є важливим інструментом для спілкування та співпраці в рамках організації.

Спільне використання файлів та документів дозволяє співробітникам ділитися, зберігати, редагувати та синхронізувати документи, сприяючи ефективній командній роботі та спільній розробці проектів.

Для вичення процесів функціонування комп'ютерних мереж буде створена середня корпоративня мережа, яка складається з одного головного офісу та двох філій. Побудована за допомогою топології дерево, яка передбачає ієрархічне розподілення мережевих пристроїв та з'єднань для забезпечення ефективності та масштабованості мережі. Ця топологія базується на використанні комутаторів (switches) та роутерів (routers), які виконують роль вузлів мережі та забезпечують передачу даних між різними підрозділами та компонентами мережі.

У такій структурі корпоративної мережі можна виділити декілька рівнів:

1. Перший рівень – на ньому розташовуються комутатори, які забезпечують з'єднання до робочих станцій, серверів та інших мережевих пристроїв. Кожна група робочих станцій може бути підключена до свого власного комутатора, що забезпечує локальний

доступ та обмін даними всередині групи. Це сприяє зменшенню навантаження на мережу та покращує пропускну здатність.

2. Другий рівень - комутатори більш високого рівня, які забезпечують з'єднання між різними групами робочих станцій та серверами. Ці комутатори дозволяють передавати дані між різними вузлами мережі та забезпечувати маршрутизацію даних у мережі. Вони також можуть мати підключення до вищого рівня мережі, наприклад, до головного комутатора або роутера.
3. Вищий рівень – розташований головний комутатор або роутер. Він забезпечує з'єднання до інших мереж та зовнішніх ресурсів, таких як Інтернет або інші підрозділи компанії. Головний комутатор або роутер також може включати функції безпеки, які забезпечують захист мережі від несанкціонованого доступу та загроз.

Для спільного доступу до файлів буде налаштований файловий сервер або сховище даних, до яких мають доступ співробітники. Ці сервери забезпечують централізоване зберігання файлів та документів, що дозволяє співробітникам легко обмінюватися та спільно працювати над ними.

2.3 Модель функціонування комп'ютерної мережі підприємства

Cisco Packet Tracer надає широкий спектр можливостей та великий вибір технічних компонентів для розробки корпоративної мережі. Для реалізації описаної структури моделі були обрані наступні компоненти:

- Маршрутизатор(router) Cisco 1941/K9 – має вбудовані мережеві сервіси, розроблений для невеликих компаній та віддалених філій. Покращена архітектура ISR G2 надає кращу підтримку медіапотоків та медіаданих, збільшуючи ефективність та продуктивність за рахунок багатоядерності, гігабітних роз'ємів 1Gb LAN/WAN з розширеним POE та контролем енергоспоживання. Підтримує роботу на швидкості до 25 Мбіт/с.

- Міжмережевий екран Cisco ASA5506-K8 – призначений для розширеного захисту від новітніх загроз та шкідливих програм. час атаки і після її завершення - шляхом об'єднання в одному пристрої можливостей міжмережевого екрану Cisco ASA5506-K8 та найкращих у галузі функцій захисту від загроз та шкідливих програм Sourcefire.

- Комутатор(switch) Cisco Catalyst 3560-24PS - Устаткування дозволяє зберегти простоту традиційної комутації локальних мереж та при цьому розгорнути інтелектуальні мережеві сервіси, такі як QoS, Обмеження швидкості передачі даних, списки контролю доступу (ACL), управління мультимовленням та високопродуктивна IP-маршрутизація.

- Комутатор(switch) Cisco Catalyst 2960-24TT - це комутатор рівня доступу фіксованої конфігурації з інтелектуальними сервісами рівня 2-4 забезпечує пропускну здатність до 16 Гбіт/с і продуктивність (64-байта) до 6,5 Мп/с. Комутатор

підходить для організацій середнього розміру та філій. Можливе розгортання та експлуатація без участі користувача за допомогою набору функцій Catalyst Smart Operations: Cisco Smart Install та Cisco Auto SmartPorts.

- Умовний сервер DHCP - клієнт-серверний протокол динамічної конфігурації хоста (Dynamic Host Configuration Protocol), за допомогою якого в IT-інфраструктурі мережні параметри кожного нового пристрою прописуються автоматично. Використання DHCP значно спрощує роботу системних адміністраторів у випадках розширення мережі.

РОЗДІЛ 3.
РЕАЛІЗАЦІЯ МОДЕЛІ КОМП.ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЕМСТВА

3.1 Налаштування імітаційної моделі комп'ютерної мережі підприємства

Для реалізації розробленої структури моделі був використаний додаток Cisco Packet Tracer.

Cisco Packet Tracer є інноваційним інструментом, розробленим компанією Cisco Systems, призначеним для моделювання, симуляції та візуалізації комп'ютерних мереж. Це програмне середовище забезпечує студентам, інженерам та іншим зацікавленим особам можливість дослідження та експериментування з різними аспектами мережевих технологій. Додаток надає широкий набір інструментів та функцій, які дозволяють користувачам створювати віртуальні мережі, підключати різні мережеві пристрої, налаштовувати їх параметри та спостерігати за передачею даних. Інтерфейс користувача простий та інтуїтивно зрозумілий, що дозволяє швидко вивчити основні функціональності і приступити до моделювання мереж [5].

За допомогою Cisco Packet Tracer можна створювати різні типи мереж, включаючи локальні мережі (LAN), глобальні мережі (WAN), бездротові мережі та інші. Користувачі можуть додавати мережеві пристрої, такі як маршрутизатори, комутатори, мережеві сервери, телефони, відеокамери тощо, і налаштовувати їх різними способами, включаючи IP-адресацію, VLAN, маршрутизацію, безпеку. Одним з важливих аспектів Cisco Packet Tracer є можливість симуляції роботи мережі. Користувачі можуть запускати трафік, надсилати пакети даних, спостерігати за їх маршрутизацією та доставкою, а також аналізувати мережеві протоколи та перевіряти ефективність мережі.

Рівнева архітектура мережі Cisco дозволяє раціонально організувати та керувати мережевою інфраструктурою. Вона дозволяє розподілити функції та навантаження між різними рівнями, що сприяє ефективному використанню ресурсів мережі. Крім того, ця архітектура забезпечує гнучкість та масштабованість мережі, дозволяючи легко розширювати та змінювати її конфігурацію залежно від потреб підприємства.

За визначеною структурою будуємо модель середньої корпоративної мережі(рис.3.1). Розміщуємо елементи дотримуючись топології дерева, вгорі маршрутизатор, під ним міжмережевий екран з двома серверами:

- HTTPS (Hypertext Transfer Protocol Secure) - це протокол, який забезпечує безпечний обмін даними між клієнтом та сервером через інтернет. Використовуючи шифрування, цей протокол забезпечує конфіденційність, цілісність та автентичність передаваних даних. Головна особливість цього протоколу це використання шифрування за допомогою іншого протоколу: SSL/TLS (Secure Sockets Layer/Transport Layer Security). Це забезпечує захищений канал зв'язку між клієнтом та сервером.
- DNS (Domain Name System) -розподілена система, що використовується для перетворення доменних імен в IP-адреси та забезпечення надійної ідентифікації комп'ютерів і ресурсів в мережі Інтернет. Вона виконує фундаментальну роль у функціонуванні Інтернету, забезпечуючи зручний спосіб навігації в мережі.

Під ними розташований комутатор Cisco Catalyst 3560-24PS, файлове сховище та DHCP сервер, який спрощує адміністрування мережі та полегшує додавання нових пристроїв. Завдяки DHCP серверу, підприємство легко зможе збільшити кількість робочих місць. Файлове

сховище зберігає будь-яку корпоративну документацію, до якої мають доступ усі працівники.

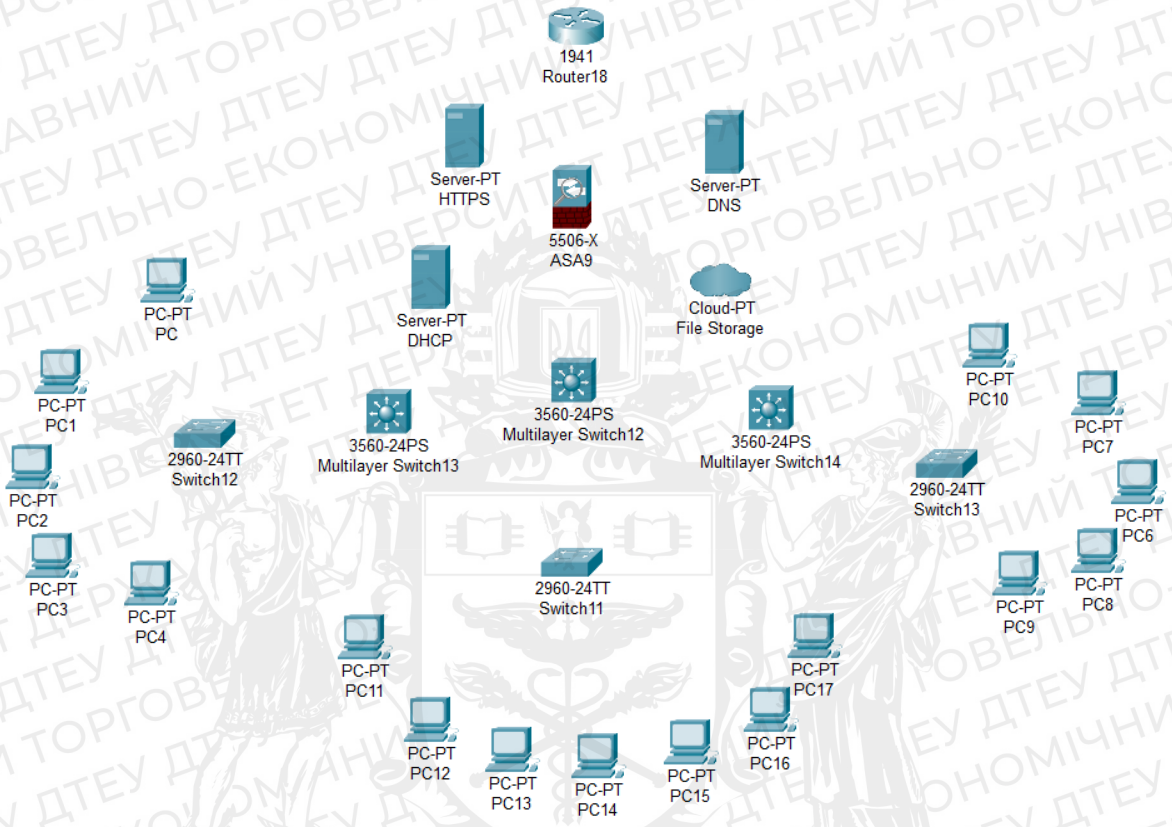

Рисунок 3.1 – Модель корпоративної мережі без підключень

Комутатор Cisco Catalyst 2960-24TT на моделі розташований під Cisco Catalyst 3560-24PS і створює разом із сімома персональними комп’ютерами головний офіс підприємства. Два комутатори Cisco Catalyst 3560-24PS розташовані зліва і справа від такого ж самого комутатора, який по суті є підкорневим. Біля цих двох комутаторів розташовано ще по одній моделі комутатора Cisco Catalyst 2960-24TT, біля яких знаходяться по п’ять персональних комп’ютерів на кожний.

Проводимо послідовне підключення. Від маршрутизатора до міжмережевого екрану, який підключається до серверів HTTPS та DNS. Згідно топології дерево, міжмережевий екран підключається до комутатора Cisco Catalyst 3560-24PS, який також підключається до двох аналогічних і

ще одного Cisco Catalyst 2960-24TT, що розташований у головному офісі. З'єднуємо усі персональні комп'ютери головного офісу з комутатором. У кожній філії знаходиться подібний комутатор, що і в головному офісі. Підключаємо їх до розташованих поряд Cisco Catalyst 3560-24PS. Між комутаторами було підключено по два зв'язки для безперебійної роботи. У разі несправності одного зв'язку, інший бере на себе передачу пакетів данний. Це добре видно на рисунку 3.2.

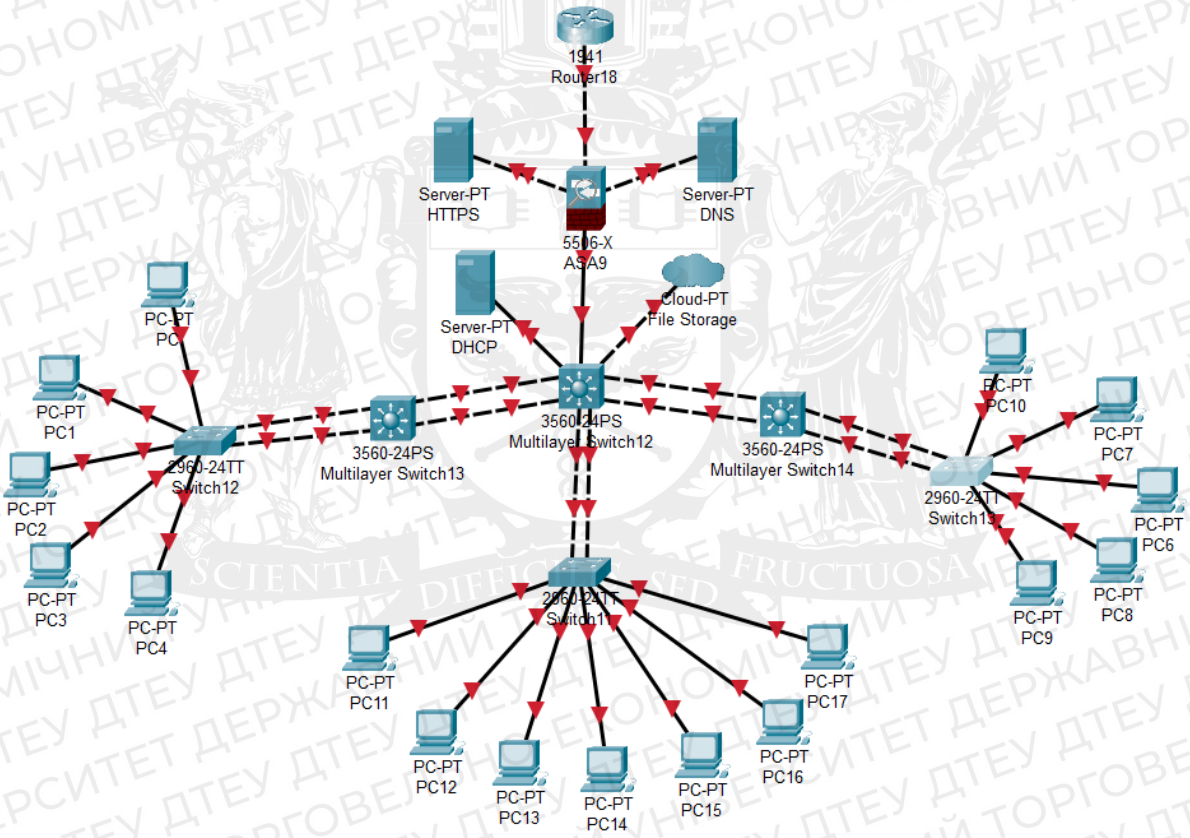

Рисунок 3.2 – Підключена неналаштована середня корпоративна мережа

Прописуємо IP-адресу 192.168.100.1 у маршрутизаторі та запускаємо вхід GigabitEthernet0/0. Дана адреса відноситься до спеціально виділених IP-адрес для приватних мереж.

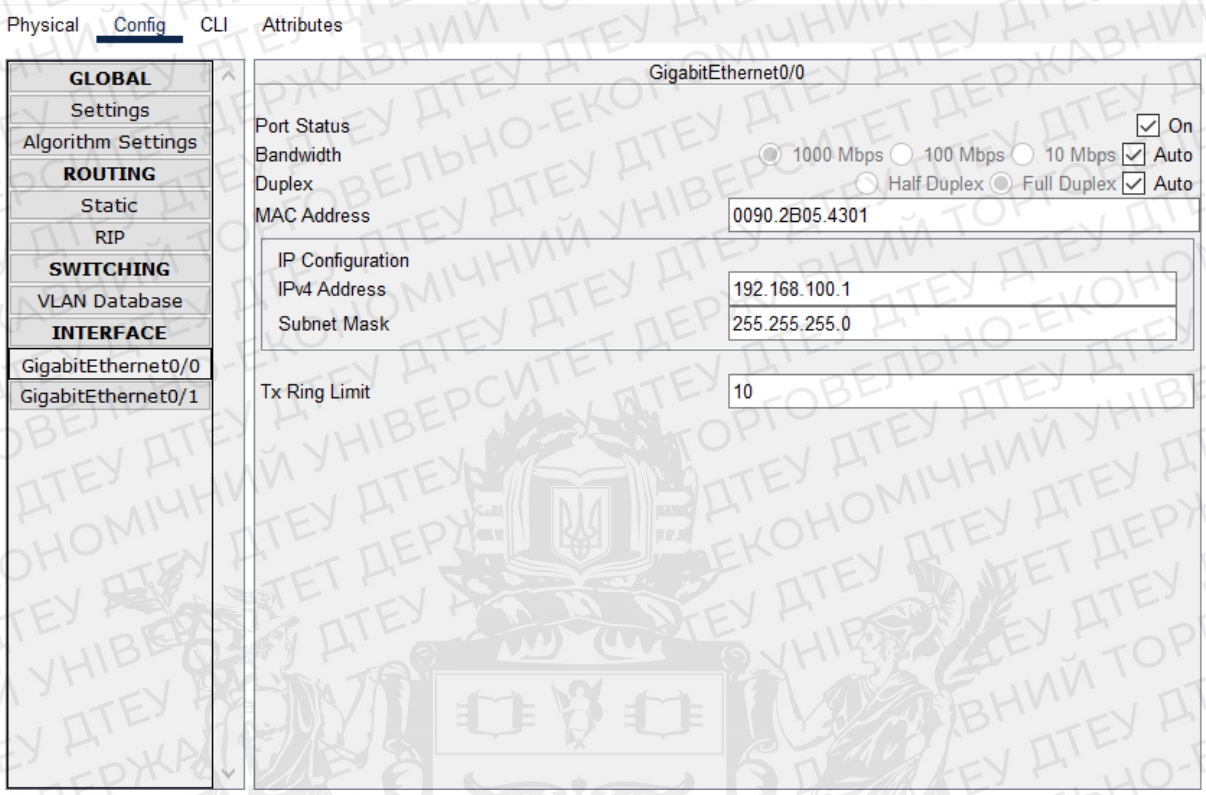

Рисунок 3.3 – Консоль налаштувань маршрутизатора

Запускаємо міжмережевий екран на базових налаштуваннях, прописуємо IP-адресу 192.168.100.2 та відкриваємо входи GigabitEthernet1/1, GigabitEthernet1/2, GigabitEthernet1/3, GigabitEthernet1/4. Зв'язки змінюють індикацію з червоної на зелену це означає, що по ним можуть передаватися пакети даних. Відкриваємо входи в які підключено кабель на кожному комутаторі. Усі з'єднання повинні горіти зеленим як на рисунку 3.4.

Перевіряємо роботу DHCP сервера. Обираємо будь який персональній комп'ютер, переходимо у вкладку Desktop → IP Configuration. При роботі сервера, протокол має автоматично присвоїти IP-адресу комп'ютеру як на рисунку 3.5.

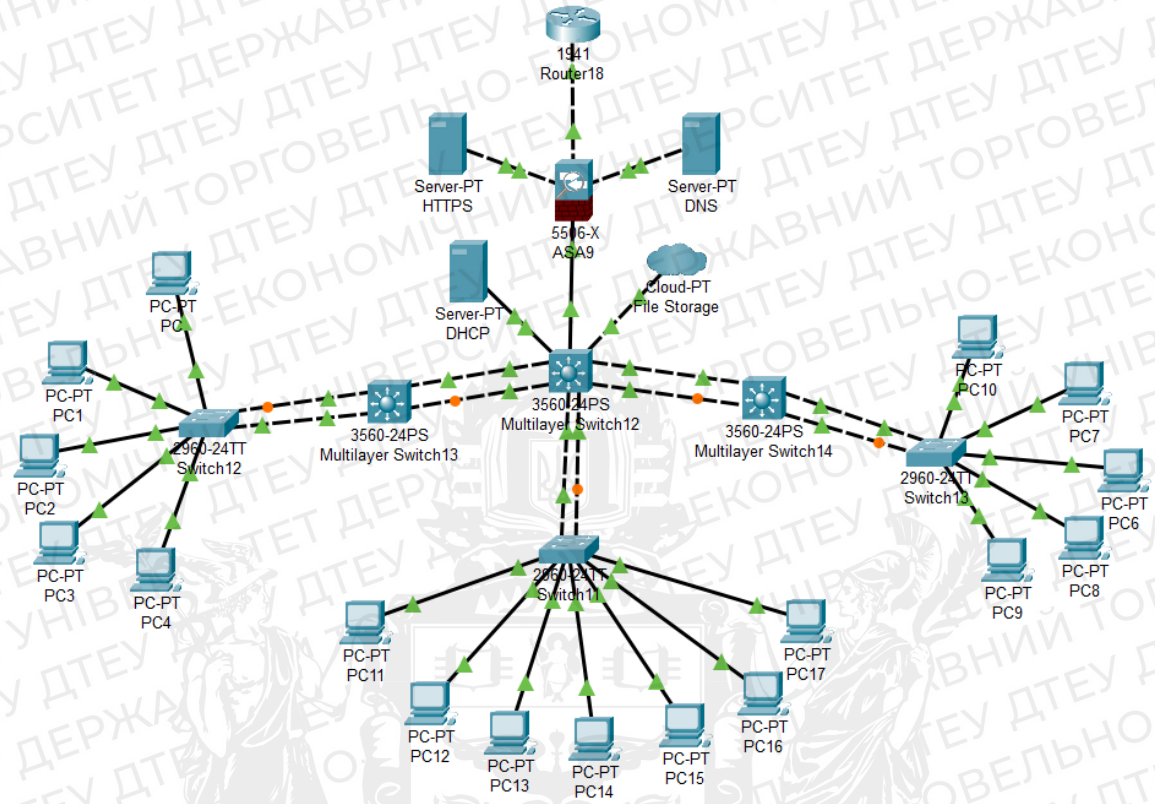

Рисунок 3.4 – Підключена корпоративна система з відкритими входами

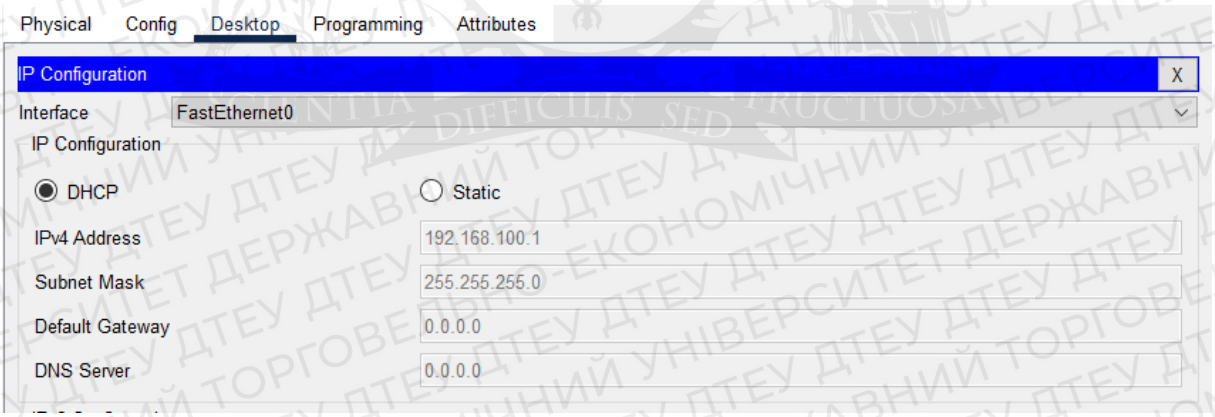

Рисунок 3.5 – Виконання протоколу DHCP

Останній етап створення імітаційної моделі корпоративної мережі є перевірка роботи мережі і усунення можливих помилок.

Коректність налаштування пристроїв було проведено шляхом введення консольної команди «ping». Ця команда з прописаною поряд IP-адресою певного комп'ютера або сервера, відсилає пакет файлів і чекає

коректної відповіді що вони отримані. Результат перевірки представлений на рисунку 3.6.

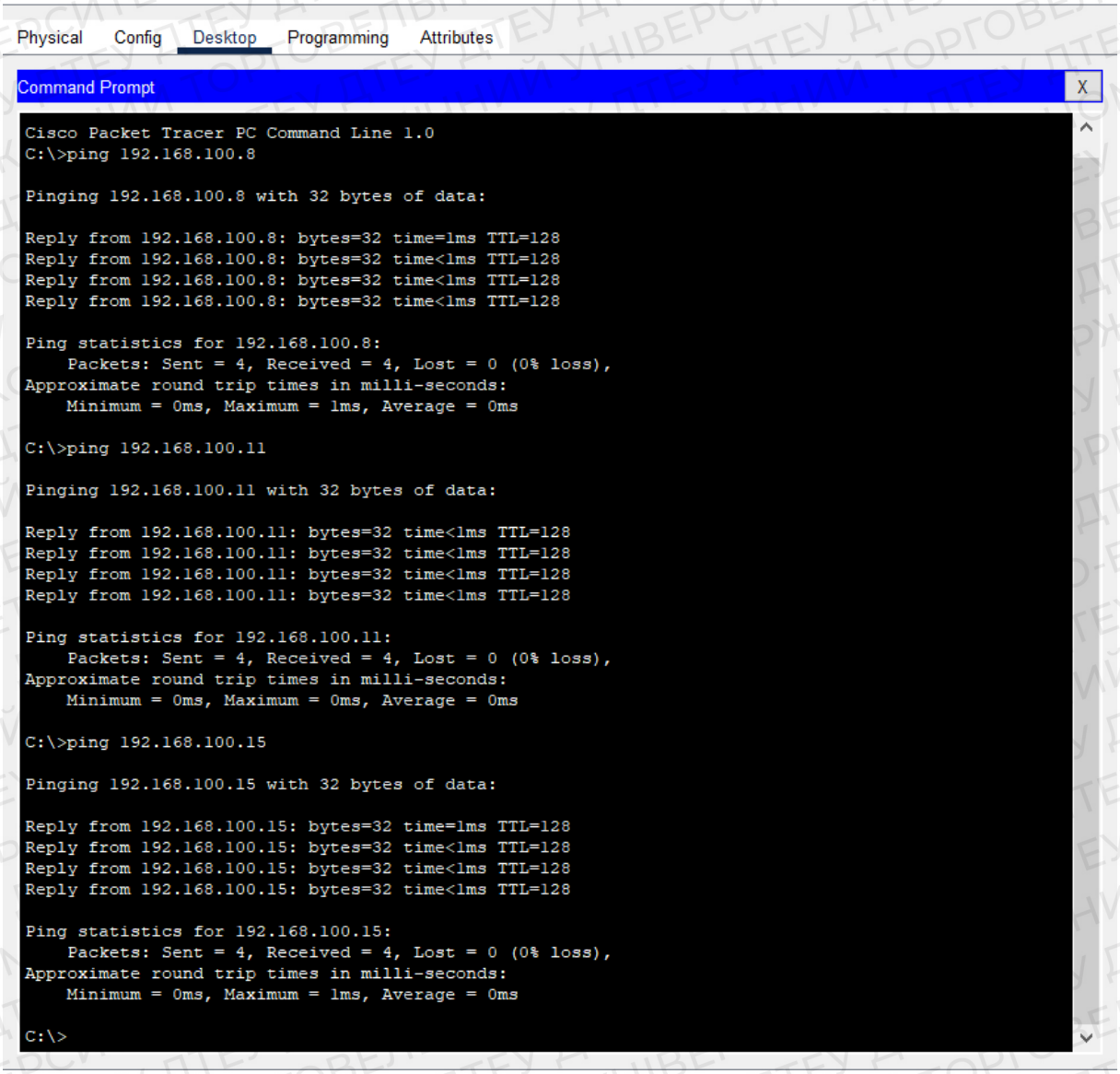

Рисунок 3.6 – Результат перевірки мережі

На рисунку 3.7 подано перевірку потоку трафіку в режимі симуляції від Cisco Packet Tracer. Згідно результатам усі налаштування працюють коректно.

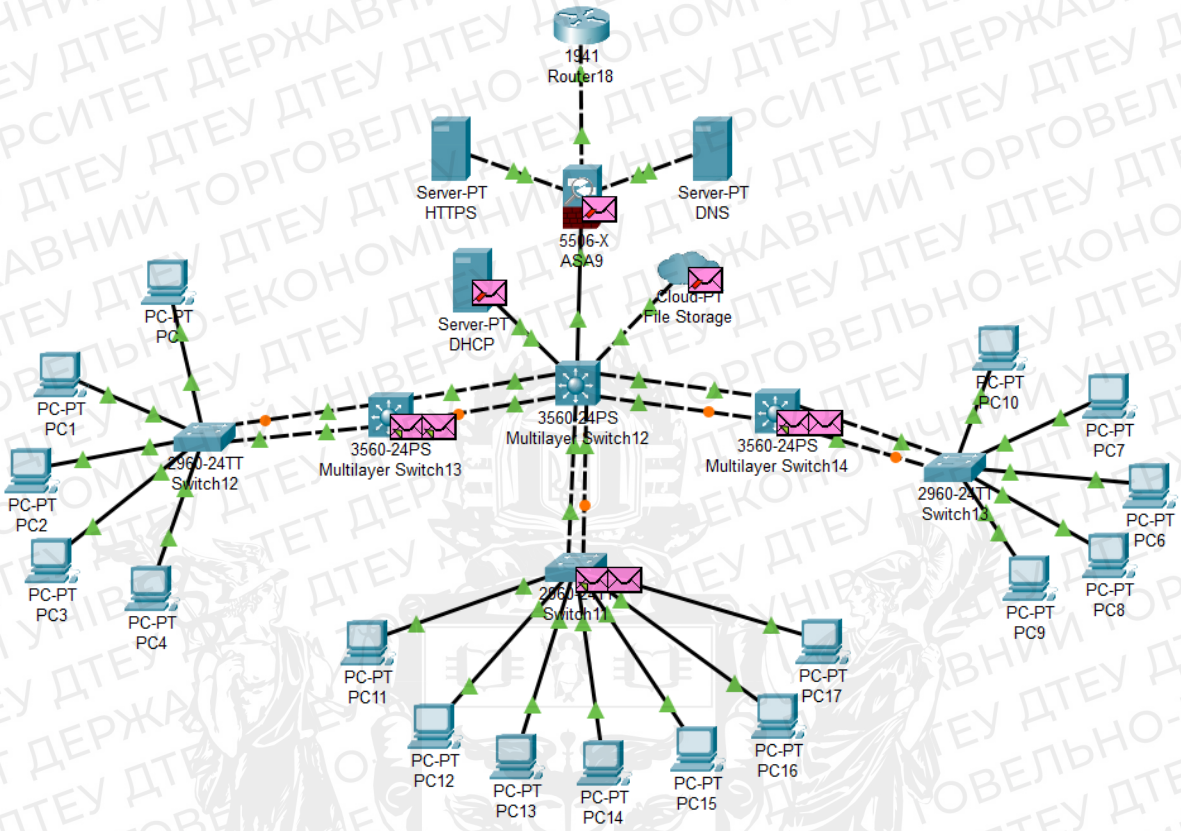

Рисунок 3.7 – Перевірка комутаторів

3.2 Реалізація захисту комп'ютерної мережі підприємства

Захист мережі здійснений завдяки міжмережевого екрану та протоколів HTTPS та DNS.

Міжмережевий екран (firewall) – це пристрій для забезпечення безпеки корпоративної мережі шляхом контролю та фільтрації трафіку, який проходить через мережеві межі. Основна функція полягає в запобіганні несанкціонованого жоступу до мережі і захисту внутрішніх ресурсів від зовнішніх загроз. Екран створює бар'єр між довіреними та недовіреними мережами, контролює трафік що проходить крізь нього. Використовує пакетний фільтринг, інспекцію стану пакетів, проксі-сервери для аналізу трафіку і прийняттю рішень про блокування пакетів на основі заданих правил безпеки.

NAT є технологією, яка перетворює IP-адресу та порти пакетів між локальною і зовнішньою мережами. NAT є важливою технологією, що використовується для забезпечення комунікації між локальними мережами та глобальним Інтернетом. Вона забезпечує безпеку, масштабованість та ефективне використання ресурсів IP-адрес, сприяючи нормальному функціонуванню мережевих інфраструктур.

РЕЗУЛЬТАТИ І ВИСНОВКИ

Корпоративні мережі безумовно є невід'ємною частиною підприємств у сучасному світі. Доступ до документації, конференції, мітинги – це лише маленька частина переваг. Мною було досліджено різні структури комп'ютерних мереж підприємства, переглянуто чималий обсяг інформації з цієї теми, розроблена і змодельована власна мережа. Найефективнішою топологією мережі є гібридна, яка включає в себе різні види. При описі розробки моделі була використана назва топологія «дерева», але це не зовсім коректно. Дерево було дещо модифіковане використанням топології «зірка» і «кільце», що допомогло змоделювати стабільну працюючу мережу з можливістю її подальшого покращення. Використання протоколу DHCP значно спрощує керування та адміністрування як середніми мережами, які налічують до 30 працівників, так і масивними підприємствами с сотнями і тисячами працівників. Для злагодженої роботи без необхідності безпосереднього контакту з колегами і втраті часу на дорогу мною для зручності було створено файлове сховище. Це допоможе оптимізувати роботу і підняти продуктивність. Проблемою залишається лише захист системи. Без належного обладнання будь-який інтузіаст зможе отримати доступ до цінних документів, або навіть «сяде за кермо» мережі. Ціна на гарне обладнання досить вискока, невеликі підприємства просто не зможуть собі їх дозволити. Рішенням цього є найм відповідного спеціаліста, який спроектує мережу і допоможе її налагодити. Корпоративні мережі і надалі продовжать розвиватися, навіть зараз людина може спокійно працювати вдома використовуючи віддалений доступ, хоча декілька років тому це було чимось неможливим.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. S. Tanenbaum, N. Feamster, and D. Wetherall "Computer Networks" (6th Edition)
2. Б.Ю. Жураковський, І.О. Зенів "Комп’ютерні мережі частина 1 навчальний посібник"
3. Charles P. Pfleeger, S. Lawrence Pfleeger and J. Margulies "Security in Computing" (5th Edition)
4. C. Kaufman, R. Perlman and M. Speciner "Network Security: Private Communication in a Public World"
5. Cisco Networking Academy "Cisco Networking Academy's Introduction to Packet Tracer"
6. E. Aboelela "Network Simulation Experiments Manual"
7. E. Maiwald "Network Security: A Beginner's Guide"
8. I. Marsic "Computer Networks: Performance and Quality of Service"
9. James D. McCabe "Network Analysis, Architecture, and Design"
10. James F. Kurose and Keith W. Ross "Computer Networking: A Top-Down Approach" (7th Edition)
11. K. Dooley "Designing Large-Scale LANs"
12. L. Larry Peterson and Bruce S. Davie "Computer Networks: A Systems Approach" (6th Edition)
13. M. Slim "Network Modeling and Simulation: A Practical Perspective"
14. Michael F. Hattersley "Enterprise Networking: Multilayer Switching and Applications"
15. M. Stamp "Information Security: Principles and Practice"
16. Nader F. Mir "Computer and Communication Networks"
17. О. С. Городецька, В. А. Гикавий, О. В. Онищук "Комп’ютерні мережі навчальний посібник"
18. Thomas M. Chen, T. Rahman та Saadat M. Alhashmi "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare"
19. W. Stallings and L. Brown "Computer Security Principles and Practice" (3rd Edition)
20. W. Stallings "Network Security Essentials: Applications and Standards"