

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту гетерогенної мережі
компанії, побудованої на базі обладнання Cisco та
Mikrotik»

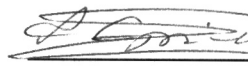
Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Антон Григорусь

Керівник професор кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

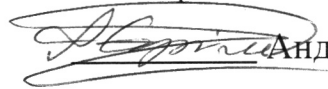
Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій Єфіменко

Державний університет «житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студент: Григорусь Антон Миколайович

Тема роботи: Проект підсистеми захисту гетерогенної мережі компанії, побудованої на базі обладнання Cisco та Mikrotik

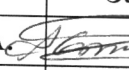
затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 29 червня 2023 р.

Вихідні дані для роботи:

1. Топологія мережі
2. Маршрутизатори і комутатори Cisco та MikroTik
3. Операційні системи.
4. Графічний емулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 01.03.2023	 01.03.2023
2	Єфіменко А.А.	 01.03.2023	 01.03.2023
3	Єфіменко А.А.	 01.03.2023	 01.03.2023

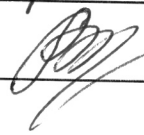
Студент  Антон Григорусь

Керівник  Володимир Воротніков

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	16.03.2023	Виконано
2	Аналіз літературних джерел	17.03.2023	Виконано
3	Аналіз технологій захисту мережі за допомогою налаштувань на маршрутизаторах	23.03.2023	Виконано
4	Аналіз можливостей мережного обладнання	24.03.2023	Виконано
5	Розробка загального проекту мережі організації	25.03.2023	Виконано
6	Вибір обладнання та проектування мережі	29.03.2023	Виконано
7	Створення таблиці маршрутизації	17.04.2023	Виконано
8	Перевірка мережі	18.04.2023	Виконано
9	Налаштування пристроїв у мережі	18.04.2023	Виконано
10	Налаштування мережі	21.05.2023	Виконано
11	Тестування роботи мережі	25.05.2023	Виконано
12	Аналіз результатів виконаної роботи	30.05.2023	Виконано
13	Оформлення пояснювальної записки	21.06.2023	Виконано
14	Створення презентації	23.06.2023	Виконано
15	Відгук та рецензія до кваліфікаційної роботи	26.06.2023	Виконано
16	Захист	28.06.2023	Виконано

Студент  Антон Григорусь

Керівник  Володимир Воротніков

АНОТАЦІЯ

Кваліфікаційна робота складається з «Проект підсистеми захисту гетерогенної мережі компанії, побудованої на базі обладнання Cisco та Mikrotik» та пояснювальної записки до нього. Пояснювальна записка містить 78 сторінки, 67 ілюстрацій та 6 таблиць.

Кваліфікаційна робота присвячений розробці підсистеми захисту гетерогенної мережі компанії, побудованої на базі обладнання Cisco та Mikrotik. Метою проекту є створення комп'ютерної мережі для компанії. Мережа має завжди обмінювати інформацію між користувачами, тому має бути добре захищена. Оскільки у компанії є різні користувачі у проекті буде організовано різні рівні привілеїв у користувачів.

Кваліфікаційна робота складається з трьох розділів і містить у собі: розробку та налаштування захищеної мережі, вибір мережевого обладнання та програмного забезпечення, детальне налаштування мережі та її тестування. В додатках буде вказано конфігурації маршрутизаторів та комутаторів мережі.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМП'ЮТЕРНА МЕРЕЖА, ГЕТЕРОГЕННА МЕРЕЖІ, CISCO, MIKROTIK, BRUTEFORCE, DNS, DOMAINE.

					КІК.КР.Б – 125 – 04 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Григорусь А.М.		23.06.23	Проект підсистеми захисту гетерогенної мережі компанії, побудованої на базі обладнання Cisco та Mikrotik		
Керівник		Воротніков В.В.		23.06.23			
Рецензент.		Єфіменко А.А.		20.06.23			
Н. контр.		Єфіменко А.А.		20.06.23			
Зав. каф.		Єфіменко А.А.		20.06.23			
					Літ.	Арк.	Аркушів
						4	77
					ФІКТ, Гр. КБ-19-1		

ANNOTATION

The qualification work consists of "Design of a security subsystem for a company's heterogeneous network based on Cisco and Mikrotik equipment" and an explanatory note to it. The explanatory note contains 78 pages, 67 illustrations and 6 tables.

The qualification work is devoted to the development of a security subsystem for a company's heterogeneous network built on the basis of Cisco and Mikrotik equipment. The aim of the project is to create a computer network for the company. The network must always exchange information between users, so it must be well protected. Since the company has different users, the project will organise different levels of privileges for users.

The qualification work consists of three sections and includes: design and configuration of a secure network, selection of network hardware and software, detailed network configuration and testing. The appendices will include configurations of routers and switches in the network.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ГЕТЕРОГЕННУ МЕРЕЖУ ТА ЇЇ БУДОВА.....	10
1.1.Особливості будови гетерогенної мережі	10
1.2 Протокол маршрутизації OSPF	12
1.3 Можливі атаки на гетерогенну мережу та захист мережі від них	15
РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ	26
2.1 Принципи роботи мережі	26
2.2 Розробка логічної структури мережі.....	29
2.3 Проект підсистеми, вибір обладнання та програмного забезпечення...	34
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА, ПОБУДОВАНОЇ НА БАЗІ ОБЛАДНАННЯ CISCO ТА МІКРОТІК.	44
3.1 Налаштування мережі.....	44
3.2 Тестування проекту підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik	61
3.3 Аналіз результатів тестування.....	68
ВИСНОВКИ.....	70
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	72
ДОДАТКИ.....	74

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

GNS3 – Graphical Network Simulator-3

VB – Virtual Box

OSPF – Open Shortest Path First

LSA – Link State Advertisement

SPF – Shortest Path First

DNS – Domain Name System

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі майже всі організації та компанії тісно пов'язані з інтернетом, тому майже всі вони мають власні комп'ютерні мережі. Комп'ютерні мережі дуже сильно залежать від їх організації та налаштувань, адже вони повинні швидко реагувати на зміни у мережі, перевстановлювати маршрути, передавати інформацію, але більше всього нас стосується саме захист мережі від зовнішнього впливу. .

Для створення гетерогенної комп'ютерної мережі може піти велика частина часу, адже вся система повинна працювати як один механізм, незважаючи які саме фірми чи типи обладнання будуть залученні у даній системі. У більш розвинутих фірмах можуть бути присутні по декілька маршрутизаторів, серверів та комутаторів різних фірм, можуть використовуватися різні операційні системи на робочих станціях, це також забирає велику долю часу для їх налаштування.

Через те, що наша мережа має доступ до інтернету, є ризик кібератаки на мережу, тому ми повинні обов'язково подбати про захист мережі від зловмисників. Атаки можуть бути націлені на різні складові: виведення обладнання зі строю, крадіжка особистих даних працівників чи клієнтів.

Крім того, рекомендовано використовувати різні рівні привілеї доступу для працівників на основі їхніх обов'язків і відповідальності. Необхідно обмежити доступ до окремих налаштувань до всіх пристроїв та робочих станцій, оскільки не кожному працівникові потрібен повний доступ до всіх можливостей комп'ютерної мережі.

Лише обмеженому колу осіб, які будуть відповідати за формування звітів та загальний стан пристроїв, буде надано доступ до налаштувань всіх пристроїв у системі та робочих станцій.

Оскільки будь-яка система може викликати інтерес у зловмисників або конкурентів, виникає необхідність забезпечення захисту даних організації. Відповідно, нашу систему також необхідно захистити або мінімізувати можливі збитки від зловмисного впливу шляхом використання різних засобів

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

захисту, наданих компаніями CISCO та MIKROTIK. Оскільки при налаштуванні схеми мережі будуть використовуватись комутатори та маршрутизатори цих виробників, ми можемо скористатися їхніми можливостями забезпечення безпеки.

Для практичної реалізації підсистеми мережі буде використаний графічний симулятор GNS3. Цей інструмент дозволить нам емулювати різні компоненти мережі та проводити необхідні тестування.

Для забезпечення гетерогенності мережі будуть використовуватися різні версії операційних систем, зокрема Windows^{[9][10]} та Linux^{[11][12]}. Це дозволить нам виконувати тестування та взаємодію компонентів мережі в різних середовищах та переконатися в сумісності та стабільності системи під час реальної експлуатації.

Метою кваліфікаційної роботи є розробка проекту гетерогенної мережі з можливостями віддалених робочих столів з використанням протоколу OSPF.

Встановлена мета створює наступні завдання:

- аналіз сучасних приладів;
- вибір структури мережі;
- вибір ПЗ для реалізації мережі;
- реалізація підсистеми захисту від різних типів атак;

Об'єктом дослідження є процес налаштування підсистеми захисту гетерогенної мережі, побудованої на базі обладнання Cisco та Mikrotik.

Предметом дослідження є методи і засоби використання для забезпечення безпеки гетерогенної мережі.

У процесі виконання кваліфікаційної роботи був розроблений проект підсистеми захисту мережевої інфраструктури підприємства, яка побудована на обладнанні від компаній Cisco та Mikrotik. Цей проект включає в себе розробку та впровадження набору заходів забезпечення безпеки, використовуючи можливості та функціонал цих виробників обладнання.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ГЕТЕРОГЕННУ МЕРЕЖУ ТА ЇЇ БУДОВА

1.1.Особливості будови гетерогенної мережі

Гетерогенна мережа^[1] - це комп'ютерна мережа, що складається з різних типів пристроїв, платформ, операційних систем та протоколів. Вона використовується для забезпечення зв'язку та обміну даними між різними компонентами системи, які можуть бути розташовані на різних рівнях ієрархії організації.

Однією з особливостей будови гетерогенної мережі є наявність різних типів пристроїв. Це можуть бути сервери, комутатори, маршрутизатори, робочі станції та інші мережеві пристрої різних виробників та моделей. Кожен пристрій може мати свої особливості, функції та можливості, які потрібно враховувати під час налаштування та управління мережею.

Крім того, гетерогенна мережа може використовувати різні операційні системи, такі як Windows, Linux, macOS тощо. Це створює необхідність у взаємодії між різними платформами та забезпеченні сумісності мережевих протоколів та сервісів. У таких випадках важливо враховувати особливості кожної операційної системи та забезпечити взаємодію між ними безперебійно та ефективно.

Керування та підтримка гетерогенної мережі також потребує уваги до різних протоколів та стандартів зв'язку. Необхідно враховувати сумісність протоколів на різних рівнях OSI-моделі та забезпечити правильну настройку та конфігурацію пристроїв.

Одним із викликів, який виникає при будові гетерогенної мережі, є забезпечення безпеки та захисту інформації. З різноманітністю пристроїв та операційних систем можуть виникати потенційні вразливості, які потребують уваги та використання заходів безпеки, таких як фаєрволи, шифрування даних, аутентифікація, контроль доступу та інші заходи.

Враховуючи особливості будови гетерогенної мережі, необхідно докладати зусиль для належного планування, проектування та управління

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

мережею. Це включає в себе вибір відповідного обладнання, настройку інфраструктури, забезпечення безпеки та ефективного функціонування мережі в цілому. Крім основних викликів, пов'язаних з різноманітністю пристроїв, операційних систем та протоколів, гетерогенна мережа може стикатися з додатковими викликами. Деякі з них включають:

Управління та підтримка гетерогенної мережі вимагає глибоких знань про різні типи пристроїв, операційних систем та їх конфігурацію. Адміністратор мережі повинен бути здатним ефективно керувати різноманітними компонентами мережі та вирішувати проблеми, що виникають на різних платформах.

Сумісність та інтеграція: При об'єднанні різних систем у гетерогенну мережу, необхідно вирішувати питання сумісності та інтеграції між різними компонентами. Це може включати налагодження з'єднань, настройку протоколів, розробку механізмів обміну даними між різними системами тощо.

Управління пропускнуою здатністю: Гетерогенна мережа може включати пристрої з різною пропускнуою здатністю та швидкістю передачі даних. Управління пропускнуою здатністю та розподілом трафіку стають важливими аспектами для забезпечення ефективної роботи мережі та запобігання перевантаження окремих компонентів.

Складність управління: Гетерогенна мережа може бути складною для управління через розподілені компоненти, різні протоколи та налаштування. Адміністрування та моніторинг гетерогенної мережі вимагають детального розуміння різних систем та ефективного використання управлінських інструментів.

Однак, гетерогенна мережа також може мати свої переваги, наприклад, більша гнучкість у виборі обладнання та програмного забезпечення, здатність до інтеграції з різними сервісами та можливість використання найкращих рішень для конкретних завдань.

Отже, створення та управління гетерогенною мережею вимагає компетентності та практичних навичок у різних областях. Ефективне

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

вирішення викликів та оптимальне використання потенціалу гетерогенної мережі можуть принести значні переваги для підприємств та організацій, забезпечуючи швидку та надійну комунікацію, захист інформації та забезпечуючи гнучкість в розвитку мережевої інфраструктури.

1.2 Протокол маршрутизації OSPF

Протокол OSPF^[2] (Open Shortest Path First) є одним з найпоширеніших протоколів маршрутизації, який забезпечує швидку та надійну передачу даних у мережі. У цьому розділі розглянуто теоретичні основи побудови мереж з використанням протоколу OSPF.

Принципи роботи OSPF

Протокол OSPF використовує алгоритм Дейкстри для визначення найкоротших шляхів у мережі. Він базується на способі розподілення маршрутної інформації між всіма маршрутизаторами в мережі, що дозволяє забезпечити оптимальний шлях для кожного пакета даних. OSPF використовується у великих мережах зі складною топологією, де вимагається висока швидкість маршрутизації та надійність передачі даних.

Однією з ключових особливостей OSPF є його здатність до динамічної адаптації до змін у мережі. Коли відбуваються зміни у топології мережі, OSPF автоматично оновлює маршрути і забезпечує безперервність передачі даних. Це досягається за допомогою обміну інформацією про маршрутизацію між маршрутизаторами за допомогою Hello-пакетів, LSA-повідомлень (Link State Advertisement) та SPF-алгоритму (Shortest Path First).

OSPF включає наступні основні компоненти:

Маршрутизатор OSPF є пристроєм або програмним забезпеченням, яке виконує протокол OSPF. Він отримує, обробляє та передає OSPF-повідомлення для обміну маршрутною інформацією з іншими маршрутизаторами. Кожен маршрутизатор OSPF має свою власну базу даних про мережу, яка містить інформацію про топологію мережі та маршрути до різних підмереж.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Area (Область). Мережа OSPF може бути розділена на декілька областей для полегшення адміністрування та зменшення обсягу обміну маршрутною інформацією. Кожна область має свій власний OSPF-дерево маршрутів, що включає всі маршрутизатори та підмережі в цій області. Області дозволяють зменшити навантаження на маршрутизатори та забезпечити більшу масштабованість мережі.

OSPF Hello-пакети використовуються для встановлення та підтримки OSPF-сесій між маршрутизаторами. Вони містять інформацію про статус маршрутизатора, його інтерфейси та області, до яких він належить. Hello-пакети регулярно висилаються маршрутизаторами для виявлення змін у стані мережі та підтримки OSPF-сесій.

LSA (Link State Advertisement) є повідомленнями, що містять інформацію про стан мережі та маршрути. Кожен маршрутизатор OSPF відправляє LSA-повідомлення, які містять інформацію про його з'єднання з іншими маршрутизаторами та підмережами. LSA-повідомлення обмінюються між маршрутизаторами для побудови та оновлення OSPF-дерева маршрутів.

SPF-алгоритм (Shortest Path First) використовується для обчислення найкоротших шляхів у OSPF-дереві маршрутів. Він аналізує топологію мережі, враховуючи метрики маршрутів, та визначає найоптимальніший шлях для передачі даних між джерелом та призначенням.

Налаштування OSPF

Для налаштування OSPF необхідно виконати наступні кроки:

Встановлення OSPF-процесу

У кожному маршрутизаторі, який планується використовувати протокол OSPF, потрібно встановити OSPF-процес та призначити йому унікальний ідентифікатор процесу.

```
router ospf <process_id>
```

<process_id> - ідентифікатор процесу OSPF, який має бути унікальним на маршрутизаторі. Ця команда активує протокол OSPF на маршрутизаторі.

Визначення областей

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Мережу необхідно розділити на області. Кожен маршрутизатор має бути призначений до однієї або декількох областей. Для цього використовують команди налаштування областей OSPF.

```
network <network_address> <wildcard_mask> area <area_id>
```

<network_address> - IP-адреса мережі, до якої ви хочете застосувати OSPF.

<wildcard_mask> - маска wildcard для вказаної мережі.

<area_id> - ідентифікатор області, до якої належить вказана мережа.

Ця команда визначає мережеві сегменти, що пов'язані з OSPF та належать до вказаної області.

Налаштування інтерфейсів

Кожен інтерфейс маршрутизатора, який приймає участь у мережі OSPF, потрібно налаштувати для OSPF. Це включає визначення типу мережі, метрики маршрутів та інших параметрів OSPF.

```
interface <interface>
```

```
ip ospf <cost>
```

<interface> - ім'я або номер інтерфейсу, на якому потрібно встановити OSPF.

<cost> - вартість (cost) шляху через вказаний інтерфейс.

Ці команди встановлюють OSPF для вказаного інтерфейсу та задають вартість шляху через нього.

Обмін маршрутною інформацією

Після налаштування OSPF на кожному маршрутизаторі відбувається автоматичний обмін маршрутною інформацією з іншими маршрутизаторами в мережі. Це включає передачу Hello-пакетів, LSA-повідомлень та оновлення OSPF-дерева маршрутів.

Переваги та недоліки OSPF

OSPF має ряд переваг, які роблять його привабливим для використання в комп'ютерних мережах:

- Висока швидкість маршрутизації та надійність передачі даних.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- Здатність до адаптації до змін у мережі та забезпечення безперервності передачі даних.
- Масштабованість та можливість розділення мережі на області для полегшення адміністрування.
- Підтримка декількох метрик маршрутів для вибору оптимальних шляхів.

Однак, OSPF також має свої недоліки, зокрема:

- Висока складність налаштування та адміністрування.
- Вимоги до обчислювальних ресурсів та пропускної спроможності мережі.
- Можливість виникнення петель маршрутизації у великих мережах

1.3 Можливі атаки на гетерогенну мережу та захист мережі від них

У сучасному цифровому світі, де мережі стають все більш гетерогенними та складними, захист мережевої інфраструктури від різних видів атак^[3] стає дедалі важливішим завданням. Гетерогенна мережа, що складається з різноманітних пристроїв, операційних систем та протоколів, може бути піддається різноманітним загрозам. Деякі з найпоширеніших атак та заходи, які можна вжити для захисту мережі, включають таке:

Атаки злому паролів: Ці атаки спрямовані на отримання доступу до системи шляхом перебору або використання слабких паролів. Для захисту від таких атак важливо встановлювати складні та унікальні паролі для кожного пристрою і обов'язково вимагати використання сильних паролів в політиці безпеки мережі.

Атаки на рівень мережі: Ці атаки спрямовані на підриг мережевої інфраструктури шляхом перекривання, зміни або блокування маршрутів. Для захисту від таких атак можна використовувати протоколи маршрутизації з механізмами перевірки цілісності маршрутної інформації, наприклад, протокол OSPF з підтримкою автентифікації.

Атаки на рівень додатків: Ці атаки спрямовані на вразливості програмного забезпечення, що використовується у гетерогенній мережі. Для

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

захисту від таких атак необхідно регулярно оновлювати програмне забезпечення, встановлювати антивірусне програмне забезпечення та фаєрволи, а також контролювати та обмежувати доступ до додатків.

Атаки з використанням соціальної інженерії: Ці атаки спираються на маніпулювання людьми з метою отримання невідповідної інформації або доступу до системи. Для захисту від таких атак важливо навчати співробітників про основні принципи безпеки, використовувати механізми аутентифікації та авторизації, а також встановлювати політику безпеки організації.

Атаки на безпеку бездротових мереж: Гетерогенна мережа може включати бездротові точки доступу, що створюють потенційну вразливість для атак. Атаки, такі як перехоплення даних, злам паролів або вторгнення в мережу, можуть бути спрямовані на безпеку бездротових мереж. Для захисту від цих атак важливо використовувати захищені протоколи безпроводового зв'язку, такі як WPA2 або WPA3, встановлювати сильні паролі для точок доступу, використовувати фільтрацію MAC-адресів та встановлювати ідентифікацію користувачів.

Атаки на фізичний рівень: Ці атаки спрямовані на фізичну інфраструктуру мережі, такі як кабелі, комутатори або сервери. Вони можуть включати фізичну крадіжку даних, злам або використання незахищених портів. Для захисту від таких атак необхідно контролювати фізичний доступ до мережевих пристроїв, встановлювати фізичні заходи безпеки, такі як замки на серверних кімнатах, та застосовувати механізми захисту фізичного рівня, такі як 802.1X або порт-сек'юріті.

Атаки на вузли мережі: Ці атаки спрямовані на комп'ютери або сервери, що входять до гетерогенної мережі. Вони можуть включати видалене виконання коду, викрадення аутентифікаційних даних або використання вразливостей програмного забезпечення. Для захисту від таких атак необхідно регулярно оновлювати програмне забезпечення, встановлювати антивірусне

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

програмне забезпечення, використовувати механізми автентифікації та авторизації, а також навчати користувачів про основні принципи безпеки.

Захист гетерогенної мережі від можливих атак є критично важливим завданням для забезпечення безпеки та надійності мережевої інфраструктури. Нижче наведено кілька можливих атак на гетерогенну мережу та заходи захисту, які можна прийняти для їх запобігання:

Перехоплення даних: Ці атаки спрямовані на отримання конфіденційної інформації, яка передається по мережі. Ця атака передбачає перехоплення та прослуховування передачі даних в мережі. Для захисту від неї необхідно використовувати шифрування даних за допомогою протоколів, таких як SSL (Secure Sockets Layer) або TLS (Transport Layer Security), а також використовувати віртуальні приватні мережі (VPN) для забезпечення конфіденційності та цілісності передачі даних.

Вторгнення в мережу: Ця атака передбачає незаконне проникнення в мережу з метою здійснення несанкціонованого доступу до ресурсів або отримання привілеїв. Для захисту від неї необхідно встановлювати міцні паролі та аутентифікацію для всіх мережевих пристроїв, використовувати фаєрволи для контролю доступу та перевірки пакетів, а також використовувати системи виявлення вторгнень (IDS) та системи попередження про вторгнення (IPS) для виявлення та блокування незвичайної активності.

Фішинг та соціальний інжиніринг: Ці атаки включають маніпулювання користувачами для отримання конфіденційної інформації, такої як паролі або кредитні картки. Для захисту від них важливо проводити навчання користувачів щодо розпізнавання підозрілих електронних листів, посилань або веб-сторінок, а також використовувати механізми двофакторної аутентифікації та антивірусне програмне забезпечення.

Атаки на додаткові сервіси: Ці атаки спрямовані на вразливості веб-додатків, електронної пошти або інших сервісів, що працюють в гетерогенній мережі. Для захисту від них необхідно регулярно оновлювати програмне

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечення, використовувати механізми аутентифікації та авторизації, а також застосовувати відповідні механізми контролю цілісності та моніторингу активності.

Загалом, захист гетерогенної мережі від атак вимагає комплексного підходу та розгляду всіх складових мережевої інфраструктури. Ефективна комбінація технологічних заходів безпеки, політик безпеки, навчання користувачів та постійного моніторингу допоможуть забезпечити безпеку та надійність гетерогенної мережі.

Захист гетерогенної мережі від можливих атак є неперервним процесом, оскільки зловмисники постійно розвивають нові методи і стратегії. Однак, існує кілька загальних заходів безпеки, які можна прийняти для забезпечення захисту гетерогенної мережі:

Фірмове програмне забезпечення: Регулярне оновлення фірмового програмного забезпечення на мережевих пристроях є важливим кроком для запобігання використанню вразливостей. Виробники надають патчі та оновлення для своїх пристроїв, які виправляють виявлені уразливості. Важливо встановлювати ці оновлення якомога швидше.

Фаєрволи: Використання фаєрволів дозволяє контролювати трафік, який входить і виходить з мережі. Фаєрволи дозволяють встановлювати правила доступу, фільтрувати пакети за визначеними критеріями, блокувати небажаний трафік та забезпечувати виявлення інтрузій.

Контроль доступу: Важливо встановити правильні політики контролю доступу в мережі. Це включає налаштування правил аутентифікації та авторизації, використання сильних паролів, обмеження прав доступу користувачів, використання механізмів двофакторної аутентифікації та шифрування комунікації.

Резервне копіювання: Важливо регулярно створювати резервні копії мережевих конфігурацій, даних та інших важливих елементів. Це дозволяє відновити мережу в разі втрати даних або випадкових помилок.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальний підхід до захисту гетерогенної мережі полягає в поєднанні технологічних, організаційних та навчальних заходів. Постійне вдосконалення заходів безпеки, моніторинг мережі та своєчасна реакція на виявлені загрози допоможуть забезпечити безпеку та надійність гетерогенної мережі.

Моніторинг та журналювання: Встановлення системи моніторингу та журналювання дозволяє відстежувати активність в мережі та виявляти підозрілі події або аномалії. Аналіз журналів допомагає виявляти потенційні загрози та вчасно реагувати на них.

Використання віртуальних приватних мереж (VPN): Використання VPN дозволяє створити безпечне з'єднання між віддаленими мережами або користувачами. За допомогою шифрування трафіку та аутентифікації забезпечується безпека передачі даних.

Регулярні аудити безпеки: Виконання регулярних аудитів безпеки дозволяє оцінити стан мережі, виявити слабкі місця і вразливості. Аудити безпеки допомагають виявляти неправильні конфігурації, незахищені сервіси та інші проблеми, які можуть бути використані зловмисниками.

Системи реагування на інциденти: Важливо мати встановлені процедури реагування на інциденти безпеки. Це включає створення екіпажу реагування на інциденти, документацію процедур, регулярне тестування інцидентів та відновлення після інцидентів.

Загальна концепція безпеки гетерогенної мережі полягає в комплексному підході, що включає в себе технологічні, організаційні та людські аспекти. Застосування цих заходів безпеки сприятиме захисту мережі від потенційних атак та забезпечить безпеку та надійність у роботі гетерогенної мережі.

Фізична безпека: Забезпечення фізичної безпеки інфраструктури мережі є важливим аспектом захисту. Це включає обмеження доступу до серверних приміщень, комутаційних кімнат і інших важливих ресурсів. Використання систем відеоспостереження, контролю доступу та інших фізичних заходів допомагає запобігти несанкціонованому доступу до обладнання.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Постійне оновлення та патчі: Важливо встановлювати оновлення та патчі для операційних систем, програмного забезпечення та обладнання. Це дозволяє виправляти виявлені уразливості і запобігати можливим атакам.

Використання брандмауерів: Брандмауери є важливим елементом захисту мережі. Вони дозволяють контролювати трафік, блокувати небажаний доступ та виявляти підозрілу активність. Встановлення брандмауерів на границі мережі та між сегментами допомагає забезпечити безпеку.

Постійне навчання та освіта: Користувачі мережі повинні мати постійне навчання та освіти щодо безпеки мережі. Це включає ознайомлення з базовими принципами безпеки, правилами використання паролів, усвідомленням ризиків і правилами поведінки в мережі.

Управління правами доступу: Користувачам мережі слід надавати права доступу лише до необхідних ресурсів і функцій. Використання механізмів автентифікації, авторизації та обліку допомагає контролювати доступ і запобігати несанкціонованій активності.

Загальна концепція захисту гетерогенної мережі передбачає комплексний підхід, який поєднує технічні, організаційні та людські заходи. Застосування цих заходів допомагає забезпечити високий рівень безпеки в гетерогенній мережі та запобігти можливим атакам і порушенням безпеки. Spoofing є одним зі зловживань в області комп'ютерної безпеки, де зловмисники намагаються приховати свою ідентичність або підробити ідентичність іншої особи або системи. Це включає використання підроблених або підроблених даних, які призводять до обману або недостовірності.

Існує кілька видів спуфінгу, кожен з яких спрямований на певні аспекти мережевої комунікації. Основні типи спуфінгу включають наступні:

IP-спуфінг (IP spoofing): Зловмисники підроблюють джерелову IP-адресу в пакетах мережевого протоколу (наприклад, IP-пакети), щоб виглядати, як будь-який інший комп'ютер або система. Це дозволяє їм обійти механізми автентифікації та перевірки безпеки, використовуючи довірчість, яку має підроблений IP-адреса.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

MAC-спуфінг (MAC spoofing): Зловмисники підроблюють фізичну адресу мережевої карти (MAC-адресу) в мережі. Це дозволяє їм здійснювати атаки, які вимагають аутентифікації за MAC-адресою або обміну даними на основі MAC-адреси.

DNS-спуфінг (DNS spoofing): Зловмисники зловживають протоколом DNS, впроваджуючи неправильні або підроблені DNS-записи. Це може призвести до перенаправлення користувачів на фальшиві веб-сторінки, збирання їх конфіденційної інформації або проведення фармацевтичних атак.

ARP-спуфінг (ARP spoofing): Зловмисники змінюють таблиці ARP (Address Resolution Protocol) в мережі, надсилаючи підроблені ARP-відповіді. Це дозволяє їм отримати неправильні відображення між IP-адресами та MAC-адресами, використовуваними в мережевому обміні, і перехоплювати або модифікувати мережевий трафік.

Для захисту від спуфінгу існують різні заходи безпеки, такі як:

Використання механізмів аутентифікації та авторизації: Впровадження сильних методів аутентифікації, таких як двофакторна аутентифікація, допомагає запобігти підробці ідентичності.

Встановлення мережевих механізмів захисту: Використання брандмауерів, IDS/IPS систем, систем виявлення спуфінгу (anti-spoofing) допомагає виявляти та блокувати підроблені пакети.

Шифрування мережевого трафіку: Використання шифрування, такого як SSL/TLS, при обміні мережевими даними допомагає унеможливити підслуховування та зловживання.

Оновлення програмного забезпечення: Регулярне оновлення програмного забезпечення, включаючи операційні системи, драйвери та застосунки, допомагає заповнювати вразливості, які можуть бути використані для спуфінгу.

Навчання користувачів: Проведення навчання та підвищення обізнаності користувачів щодо спуфінгу та соціальної інженерії допомагає попереджати атаки та запобігати небезпеці.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальна концепція захисту мережі від спуфінгу полягає в поєднанні технічних заходів безпеки, які міцно налаштовують мережеві пристрої та забезпечують виявлення та блокування підроблених пакетів, разом з належними процедурами і навичками користувачів для виявлення та уникнення спуфінгу.

Brute Force (груба сила) - це метод атаки на систему або криптографічний алгоритм, який полягає у випробуванні всіх можливих комбінацій паролів або ключів з метою зламати захист та отримати несанкціонований доступ до системи або розшифрувати зашифровані дані.

Процес Brute Force зазвичай вимагає значних обчислювальних ресурсів та тривалого часу, оскільки він базується на переборі всіх можливих комбінацій. Атакувачі використовують автоматизовані скрипти або програми, що автоматично генерують та перевіряють паролі або ключі.

Цілью атаки Brute Force є зламати пароль або ключ, щоб отримати несанкціонований доступ до системи, облікового запису або зашифрованих даних. Це може бути особливо небезпечно в разі використання слабких або простих паролів.

Для захисту від атак Brute Force використовуються наступні методи:

Складність паролів: Використовуйте складні та унікальні паролі, які важко вгадати або підібрати. Рекомендується використовувати комбінації великих і малих літер, цифр та спеціальних символів. Додатковою захистом може бути вимога до користувачів використовувати двофакторну аутентифікацію.

Блокування після невдалих спроб: Встановіть обмеження на кількість невдалих спроб введення пароля або ключа перед тим, як обліковий запис буде тимчасово заблоковано або буде застосовано затримку перед наступною спробою.

Затримка між спробами: Встановлення затримки між спробами вводу пароля або ключа може ускладнити атаку Brute Force, зменшуючи швидкість перебору.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

Моніторинг і виявлення: Використання систем моніторингу, які аналізують активність в системі та виявляють підозрілі спроби Brute Force.

Блокування IP-адрес: У разі виявлення підозрілої активності з певного IP-адреси можна встановити блокування цього адреса або обмежити доступ з нього.

Використання систем обмеження швидкості: Використовуйте системи обмеження швидкості, які встановлюють обмеження на кількість запитів, що можуть бути виконані за одиницю часу.

Оновлення програмного забезпечення: Регулярне оновлення системи та програмного забезпечення забезпечує закриття вразливостей, які можуть бути використані атакуючими.

Використання систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS): Ці системи можуть виявляти та блокувати підозрілу активність, включаючи спроби Brute Force.

Обмеження доступу: Встановлення правильних прав доступу до ресурсів системи допомагає уникнути несанкціонованого доступу.

Ці заходи допомагають ускладнити атаки Brute Force і забезпечити більшу безпеку для систем та даних.

Компрометація облікових записів електронної пошти є серйозною загрозою для приватності та безпеки користувачів. Цей вид атаки відомий як "Compromise Accounts" або "компрометація облікових записів". Вона полягає у несанкціонованому доступі до облікового запису електронної пошти користувача з метою отримання конфіденційної інформації або зловживання ним.

Основним способом компрометації облікових записів електронної пошти є злам пароля. Зловмисники використовують різні методи для відтворення або вгадування пароля, такі як атаки перебором, словники паролів, соціальна інженерія, фішингові атаки та використання вразливостей в системі.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Після отримання доступу до облікового запису електронної пошти зломисники можуть здійснювати наступні дії:

Перегляд і перехоплення електронних листів: Зломисники можуть прочитати конфіденційні листи, які надсилаються та отримуються від інших користувачів. Це може призвести до витоку особистої інформації або конфіденційних даних.

Відправлення спаму та шахрайських повідомлень: Зломисники можуть використовувати скомпрометований обліковий запис для розсилки небажаних повідомлень, фішингових листів або шахрайських схем. Це може негативно вплинути на репутацію користувача або спричинити шкоду іншим користувачам.

Зміна налаштувань облікового запису: Зломисники можуть змінювати паролі, адреси електронної пошти, фільтри спаму та інші налаштування облікового запису. Це призводить до втрати контролю над обліковим записом та ускладнює його відновлення.

Використання облікового запису для доступу до інших сервісів: Якщо користувач використовує один і той же пароль для різних сервісів, то зломисники можуть використовувати скомпрометований обліковий запис для незаконного доступу до інших онлайн-платформ, соціальних мереж або банківських рахунків.

Захист облікових записів електронної пошти від компрометації включає наступні заходи:

Використання сильних паролів: Рекомендується використовувати унікальні та складні паролі для кожного облікового запису. Паролі повинні містити комбінацію великих і малих літер, цифр та спецсимволів.

Багатофакторна аутентифікація: Використовуйте можливість багатофакторної аутентифікації, яка додає додатковий шар безпеки до процесу входу. Наприклад, введення пароля разом з одноразовим кодом, який надсилається на мобільний пристрій.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

Оновлення програмного забезпечення та застосунків: Регулярно оновлюйте програмне забезпечення електронної пошти та застосунки, щоб закрити вразливості, які можуть бути використані зловмисниками.

Уважне ставлення до підозрілих повідомлень: Не відкривайте вкладені файли або посилання з неперевірених або підозрілих електронних листів, оскільки вони можуть містити шкідливі програми або фішингові спроби.

Використання антивірусного програмного забезпечення: Встановлення та оновлення надійного антивірусного програмного забезпечення допоможе виявити та блокувати шкідливі програми, які можуть бути використані для компрометації облікових записів.

Нагадування про ці прості, але важливі заходи допоможе зменшити ризик компрометації облікових записів електронної пошти і зберегти ваші дані в безпеці. Запам'ятайте, що безпека електронної пошти залежить від вас, як користувача, і важливо бути пильним і обережним під час взаємодії зі своїми обліковими записами.

Висновки до розділу 1

В результаті аналізу особливостей гетерогенних мережі було визначено основні принципи побудови схеми та методи її захисту. Потрібно розробити підсистему гетерогенної мережі на базі пристроїв CISCO^[6] та MIKROTİK^[5].

Було розглянуто можливість встановлення різних типів захисту. Крім того, обрано протокол маршрутизації OSPF та протокол DHCP^[7] для автоматизації підключення нових пристроїв.

З обладнання будемо використовувати провідного виробника – CISCO та MIKROTİK так як на пристроях даних фірми можна налаштувати всі обрані протоколи та технології. Для створення саме гетерогенної мережі буде задіяний симулятор GNS3, який дозволить забезпечити взаємодію комунікаційних пристроїв та віртуальних машин з обраними операційними системами.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ

2.1 Принципи роботи мережі

При розробці мережі важливо структурувати її логічно та враховувати певні вимоги. У даному випадку, мережа складатиметься з декількох локальних мереж (LAN). Під час створення такої мережі необхідно врахувати наступні вимоги:

- 1) Створення підмереж з різними типами пристроїв від компаній CISCO та MIKROTIK. Це дозволить забезпечити різноманітність та гетерогенність мережі, використовуючи різні моделі та типи пристроїв від різних виробників.
- 2) Використання різних операційних систем для досягнення гетерогенності мережі. Запровадження різних операційних систем, таких як Windows та Linux, дозволить робочим станціям працювати в різних середовищах та надасть можливість використання різноманітних програм та сервісів.
- 3) Забезпечення можливості працювати на віддалених робочих станціях. Мережа повинна бути налаштована таким чином, щоб дозволяти віддалений доступ до робочих станцій з-за меж локальної мережі, що дозволить працювати з ними з будь-якого місця.
- 4) Автоматичне отримання IP-адресації (DHCP) для кожної підмережі. Використання протоколу DHCP дозволить автоматизувати процес надання IP-адрес для пристроїв в мережі, забезпечуючи зручну та ефективну адресацію.
- 5) Захищеність підсистеми від дій зловмисників, конкурентів чи недбалості власних працівників. У процесі розробки мережі необхідно приділити увагу заходам забезпечення безпеки, таким як використання захищених протоколів, налаштування брандмауерів, використання сильних паролів та авторизації, а також моніторинг та виявлення вразливостей.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

б) Налаштування DNS записів на домені для захисту від фішингу через пошту. Налаштування правильних DNS записів на домені дозволить ефективно боротися зі спробами фішингу через електронну пошту, забезпечуючи перевірку легітимності поштових повідомлень та запобігаючи небажаним атакам.

Під час проектування схеми мережі необхідно враховувати середню кількість пристроїв, але також забезпечити масштабованість мережі для майбутнього розширення. Важливим аспектом є налаштування протоколу DHCP для автоматизації процесу IP-адресації та забезпечення гнучкості при додаванні або виключенні робочих станцій. Для цього розробляться декілька підмереж з різними DHCP-серверами та різними операційними системами.

Також потрібно розробити IP-топологію мережі, враховуючи наявність багатьох підмереж. Внутрішня адресація буде забезпечуватись протоколом динамічного налаштування вузлів. Детальні параметри адресації будуть визначені у відповідній таблиці.

Ці заходи допоможуть створити логічну та функціональну мережу з врахуванням гетерогенності та безпеки, що задовольнятиме потреби організації.

Таблиця 2.1 – Розподілення на підмережі пристроїв мережі

Назва мережі	Кількість робочих станцій	DHCP-сервер
LAN 1	3 робочі станції: 2 VPCS, Debian	Маршрутизатор
LAN 2	3 робочі станції: 2 VPCS, Win 10	Маршрутизатор
LAN 4	3 робочі станції: 2 VPCS, Ubuntu	Маршрутизатор
LAN 4	3 робочі станції: V2 PCS, Win 7	Маршрутизатор

Таблиця 2.2 – Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Підмережа 1				
Комутатор SW-LAN-1	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC-1	E0	DHCP	255.255.255.0	/24
Робоча станція PC-2	E0	DHCP	255.255.255.0	/24
Робоча станція Debian	E0	DHCP	255.255.255.0	/24

Підмережа 2				
Комутатор SW-LAN-2	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC-3	E0	DHCP	255.255.255.0	/24
Робоча станція PC-4	E0	DHCP	255.255.255.0	/24
Робоча станція Win-10	E0	DHCP	255.255.255.0	/24

Підмережа 3				
Комутатор SW-LAN-3	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC-5	E0	DHCP	255.255.255.0	/24
Робоча станція PC-6	E0	DHCP	255.255.255.0	/24
Робоча станція Ubuntu	E0	DHCP	255.255.255.0	/24

Підмережа 4				
Комутатор SW-LAN-4	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC-7	E0	DHCP	255.255.255.0	/24
Робоча станція PC-8	E0	DHCP	255.255.255.0	/24
Робоча станція Win-7	E0	DHCP	255.255.255.0	/24

Ядро мережі				
Маршрутизатор Cisco-1	E1/1	192.1.1.1	255.255.255.252	/30
	E1/2	192.1.2.1	255.255.255.252	/30
	E1/3	192.1.5.1	255.255.255.252	/30
	E2/1	192.1.6.1	255.255.255.252	/30
	E2/2	DHCP	255.255.255.0	/24
	E2/3	DHCP	255.255.255.0	/24
Маршрутизатор Cisco-2	E0/1	192.1.3.2	255.255.255.252	/30
	E0/2	192.1.4.2	255.255.255.252	/30
	E1/1	192.1.7.1	255.255.255.252	/30
	E1/2	192.1.8.1	255.255.255.252	/30
	E2/1	DHCP	255.255.255.0	/24
	E2/0	DHCP	255.255.255.0	/24
Маршрутизатор Mikrotik-1	E1	192.1.3.1	255.255.255.252	/30
	E2	192.1.4.1	255.255.255.252	/30

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор Mikrotik-2	E3	192.1.5.2	255.255.255.252	/30
	E4	192.1.6.2	255.255.255.252	/30
	E0	DHCP	255.255.255.0	/24
	E1	192.1.2.2	255.255.255.252	/30
	E2	192.1.1.2	255.255.255.252	/30
	E3	192.1.7.2	255.255.255.252	/30
	E4	192.1.8.2	255.255.255.252	/30
	E0	DHCP	255.255.255.0	/24

2.2 Розробка логічної структури мережі

В даній схемі використовується трирівнева ієрархічна модель мережі^[8], що забезпечує надійність та високу продуктивність. Мережа складається з трьох рівнів: ядра, розподілу та доступу.

Переваги такої структури включають:

- 1) Масштабованість: Мережу можна легко розширювати і вдосконалювати у майбутньому, додавати нові пристрої та розширювати її функціональність.
- 2) Швидке усунення неполадок та управління: Ієрархічна модель дозволяє швидко виявляти та усувати неполадки і просто керувати мережею.
- 3) Надійність: Якщо один з основних пристроїв вийде з ладу, на рівні доступу є запасний пристрій, який може виконувати його функції. Також, якщо виникне проблема з підключенням між маршрутизаторами на рівні ядра, існує альтернативний шлях для забезпечення неперервності мережі.
- 4) Швидка працездатність: Ієрархічна структура сприяє високій пропускній здатності мережі, що дозволяє швидко передавати дані між різними пристроями.

Розглянемо кожен рівень окремо:

Рівень ядра: Відповідає за швидке транспортування даних між пристроями рівня розподілу, тобто між комутаторами мережі. Зазвичай на цьому рівні використовуються висококласні та продуктивні комутатори.

Рівень розподілу: Знаходиться між рівнем ядра та рівнем доступу.

Завдання цього рівня полягає в забезпеченні маршрутизації мережі та

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

з'єднання рівня ядра з рівнем доступу. Також на цьому рівні виконується фільтрація ACLs (Access Control Lists) та PBR (Policy-Based Routing). Головна мета рівня розподілу - зменшення навантаження на мережу та оптимізація трафіку.

Рівень доступу: Зазвичай складається з комутаторів та точок доступу, що дозволяють підключатися до робочих станцій, принтерів, IP-телефонів, серверів тощо. На рівні доступу частіше використовуються комутатори другого рівня через їх нижчу вартість.

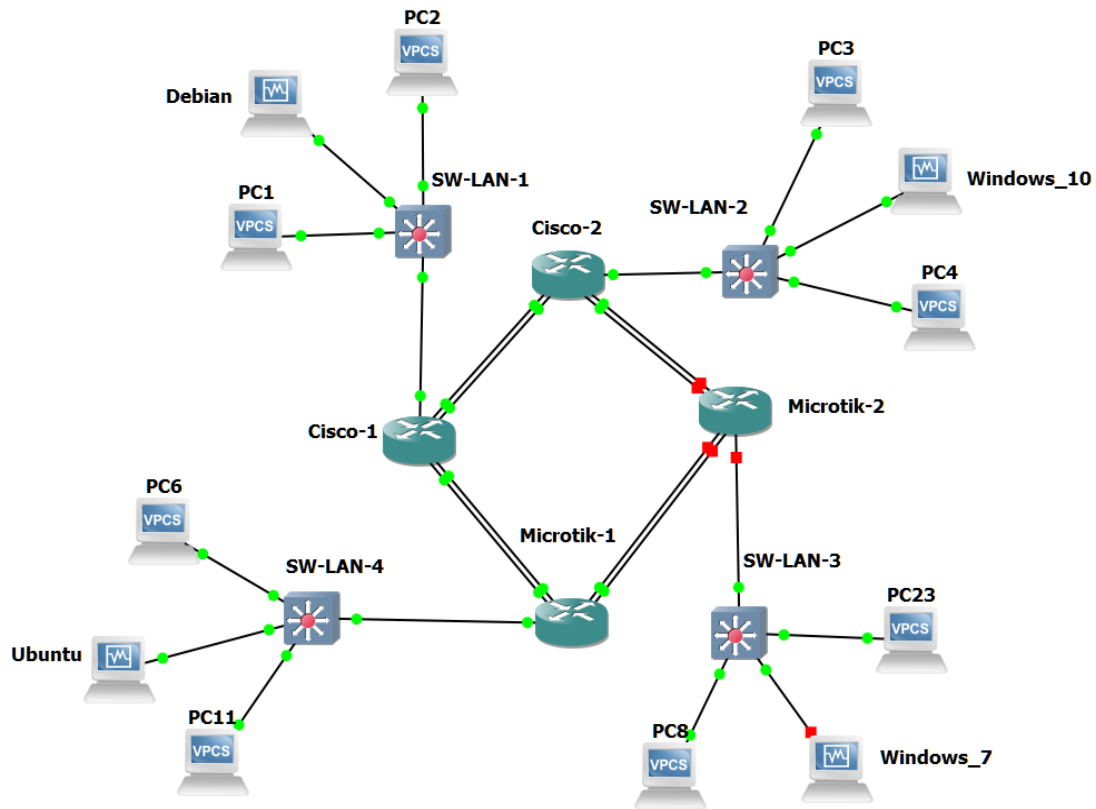


Рисунок 2.1 – Трирівнева ієрархічна модель мережі

Детально розглянемо кожну з підмереж окремо. Зовнішній вигляд всіх LAN наведено на рис.2.2-2.6, пристрої, що входять до складу підмереж, зазначені в табл.2.3-2.6.

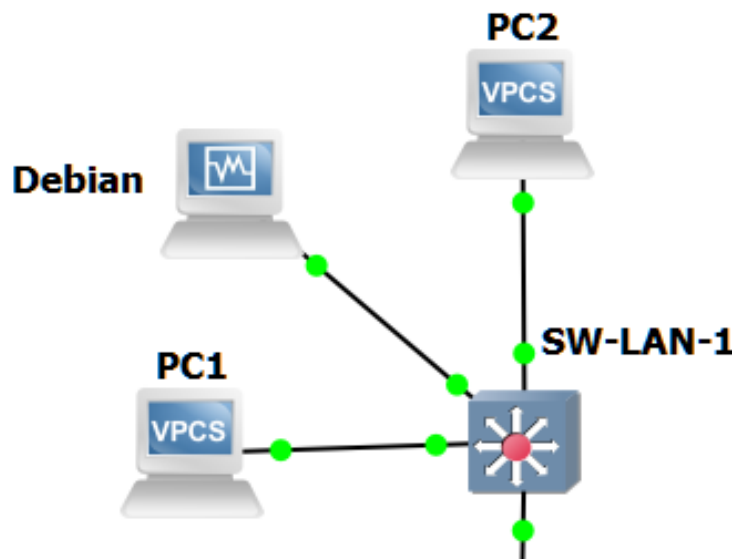


Рисунок 2.2 – Локальна мережа LAN 1

Таблиця 2.3 – Пристрої, що входять до складу LAN 1

Робочі станції	1)Перша станція VPCS 2)Друга станція VPCS 3)Третя станція с операційною системою Debian
Комутатори	Комутатор другого рівня (i86bi-linux-l2-adventerprise-15.1b.bin)

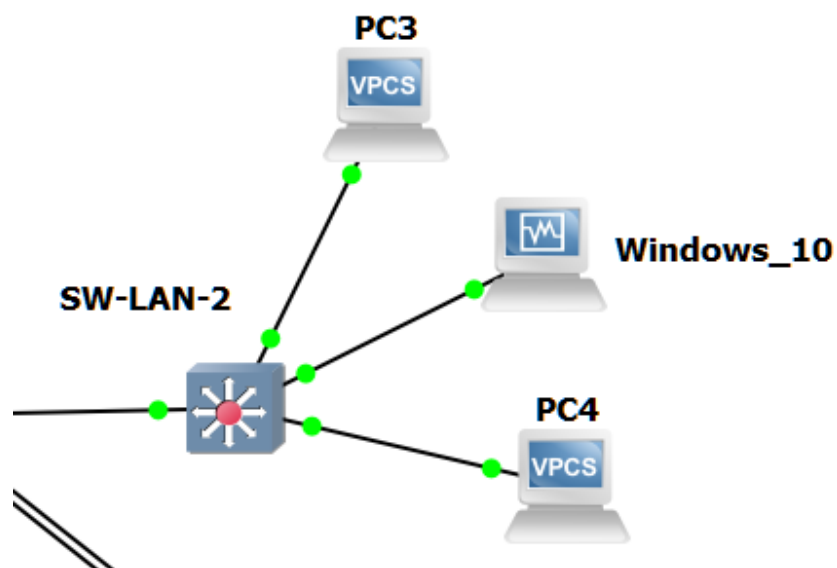


Рисунок 2.3 – Локальна мережа LAN 2

Таблиця 2.4 – Пристрої, що входять до складу LAN 2

Робочі станції	1)Перша станція VPCS
	2)Друга станція VPCS
	3)Третя станція с операційною системою Windows 10
Комутатор	Комутатор другого рівня (i86bi-linux-l2-adventerprise-15.1b.bin)

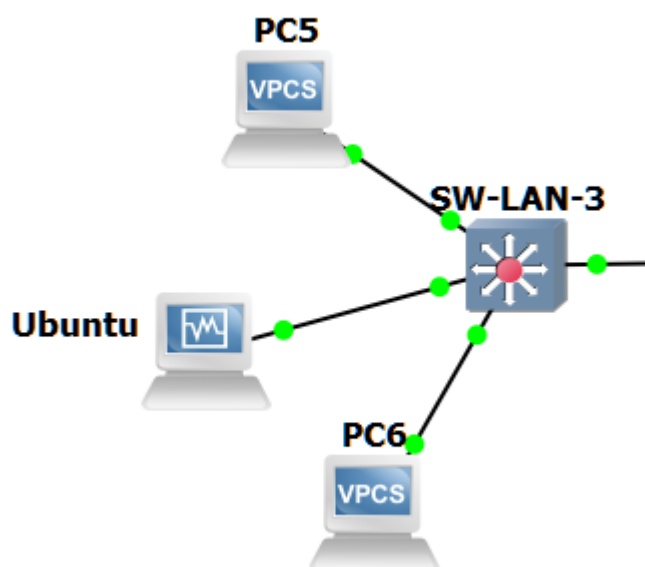


Рисунок 2.4 –Локальна мережа LAN 3

Таблиця 2.5 – Пристрої, що входять до складу LAN 3

Робочі станції	1)Перша станція VPCS
	2)Друга станція VPCS
	3)Третя станція с операційною системою Ubuntu
Комутатор	Комутатор другого рівня (i86bi-linux-l2-adventerprise-15.1b.bin)

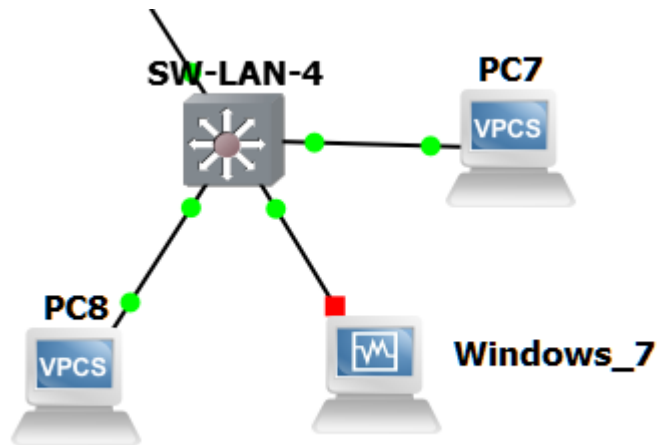


Рисунок 2.5 – Локальна мережа LAN 4

Таблиця 2.6 – Пристрої, що входять до складу LAN 4

Робочі станції	1)Перша станція VPCS 2)Друга станція VPCS 3)Третя станція с операційною системою Windows 7
Комутатор	Комутатор другого рівня (i86bi-linux-l2-adventerprise-15.1b.bin)

Рівень ядра, складається з двох маршрутизаторів CISCO (i86bi-linux-l2-adventerprise-15.1b.bin) та двох маршрутизаторів Mikrotik (chr-6.49.8.vdi). Будова ядра зображена на рис.2.8.

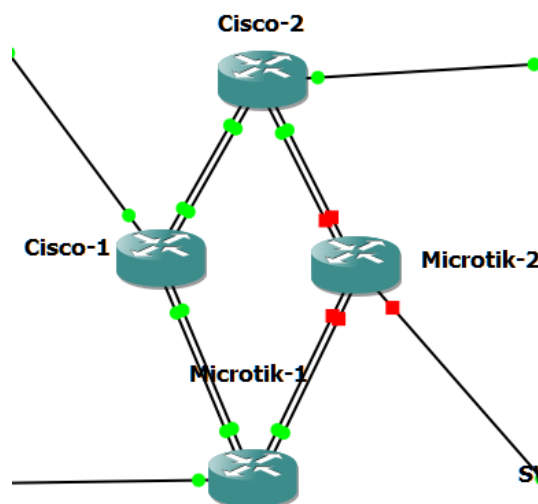


Рисунок 2.6 – Рівень ядра

Проектована гетерогенна мережі створюється для організації чи компанії, тому потрібно забезпечити її максимальну працездатність. Для того, щоб пришвидшити процес відновлення доступу до мережі з робочих станцій при їхньому виході з ладу чи додавання нових робочих станцій, маршрутизатори будуть виступати саме як DHCP-сервера для кожної з підмереж.

Проектована гетерогенна мережа створюється з метою організації інфраструктури для компанії або організації, тому надійність та максимальна працездатність є важливими факторами. Для забезпечення швидкого відновлення доступу до мережі з робочих станцій під час їхнього виходу з ладу або додавання нових робочих станцій, маршрутизатори виконуватимуть функцію DHCP-сервера для кожної підмережі.

Для оптимізації роботи всієї мережі буде використано протокол зв'язку OSPF (Enhanced Interior Gateway Routing Protocol), оскільки він є надійним та швидким у виявленні проблем зі зв'язком. У разі виникнення проблем OSPF швидко повідомляє інші пристрої в мережі та шукає альтернативні шляхи до несправних пристроїв. Крім того, на рівні ядра будуть створені додаткові з'єднання, що забезпечать стабільну роботу мережі у разі відмови одного з основних з'єднань.

Ці заходи спрямовані на забезпечення надійності, швидкості та нормалізації роботи гетерогенної мережі, забезпечуючи ефективний обмін даними та стабільну комунікацію між пристроями в мережі.

2.3 Проект підсистеми, вибір обладнання та програмного забезпечення

У кваліфікаційній роботі будуть використовуватись наступні операційні системи: Windows 7, Windows 10, Debian, Ubuntu.

Наявність захисту на обладнанні та у мережі від атак різних типів.

Для реалізації схеми будемо використовувати обладнання фірми CISCO та Mikrotik.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

Основними перевагами CISCO перед іншими компаніями є:

1. Cisco є однією з провідних компаній у сфері мережевих технологій, і вона має кілька ключових переваг порівняно з іншими компаніями:
2. Широкий спектр продуктів: Cisco пропонує широкий асортимент мережевого обладнання, включаючи маршрутизатори, комутатори, маршрутизатори-перемикачі, мережеві адаптери та інші. Вони мають рішення для різних масштабів та типів мереж, що дозволяє задовольнити потреби як малих підприємств, так і великих корпорацій.
3. Інноваційні технології: Cisco постійно впроваджує нові технології та інновації в області мережевих рішень. Вони активно розвиваються в напрямку мережі нового покоління, включаючи концепції, такі як Software-Defined Networking (SDN), Internet of Things (IoT) та Cloud Computing. Це дозволяє користувачам Cisco бути на передовій технологій та використовувати передові можливості в своїх мережах.
4. Надійність і стабільність: Продукти Cisco відомі своєю високою надійністю та стабільністю. Вони пройшли широкі випробування та сертифікацію, що дозволяє їм працювати в найвимогливіших умовах. Надійність мережі є критично важливою для багатьох компаній, і Cisco забезпечує цю надійність за допомогою своїх технологій та рішень.
5. Широка підтримка та екосистема: Cisco має велику базу клієнтів та широку мережу партнерів, що забезпечує високий рівень підтримки та послуг для своїх клієнтів. Компанія також активно співпрацює з іншими провідними вендорами мережевих технологій, що сприяє сумісності та інтеграції з іншими системами.
6. Багаторічний досвід: Cisco має багаторічний досвід у галузі мережевих технологій та розуміє потреби різних секторів індустрії. Вони мають велику базу знань та експертизу, що дозволяє їм розробляти рішення, відповідні вимогам клієнтів.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

7. Ці переваги роблять Cisco привабливим вибором для компаній, які шукають надійні та ефективні мережеві рішення.
8. Гнучкість і масштабованість: Cisco надає рішення, які можуть легко розширюватись та адаптуватись до змінних потреб бізнесу. Вони пропонують модульні архітектури та конфігураційні опції, що дозволяють користувачам побудувати мережу, яка відповідає їхнім унікальним вимогам. Це забезпечує гнучкість при розширенні мережі та дозволяє легко інтегрувати нові пристрої та технології.
9. Захист та безпека: Cisco відома своїми рішеннями у сфері мережевої безпеки. Вони надають широкий набір інструментів та технологій для захисту мережі від загроз, включаючи мережеві файрволи, системи виявлення вторгнень (IDS) та інші. Компанія також активно відстежує нові загрози та швидко впроваджує оновлення та патчі для забезпечення безпеки мережі.
10. Лідерство на ринку: Cisco є одним з найбільших гравців на ринку мережевих технологій. Вони мають сильну позицію у світі, що дозволяє їм мати доступ до передових досліджень та розробок. Це також означає, що компанія здатна надати стабільну підтримку та оновлення своїм клієнтам.

Загалом, Cisco має довгий список переваг порівняно з іншими компаніями у галузі мережевих технологій. Їхні продукти, інновації, надійність та підтримка роблять їх привабливим вибором для організацій, що шукають найкращі рішення для своїх мереж.

Основними перевагами фірми Mikrotik є

1. Вартість: Однією з основних переваг Mikrotik є їхня вартість. Продукти MikroTik зазвичай доступні за більш доступними цінами порівняно з іншими виробниками мережевих пристроїв. Це робить їх привабливими для малих і середніх підприємств та індивідуальних користувачів з обмеженими бюджетами.
2. Функціональність: MikroTik пропонує широкий спектр функціональних можливостей у своїх пристроях. Вони підтримують різні протоколи

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

маршрутизації, комутації, бездротового зв'язку та мережевої безпеки. Це дозволяє користувачам налаштовувати й управляти мережею згідно зі своїми потребами.

3. Простота у використанні: MikroTik зосереджується на простоті використання своїх пристроїв та програмного забезпечення. Вони пропонують графічні інтерфейси користувача (GUI) та командний рядок (CLI), які дозволяють адміністраторам з легкістю налаштовувати та управляти мережею. Крім того, MikroTik надає детальну документацію та підтримку спільноти, що сприяє швидкому засвоєнню та вирішенню проблем.
4. Надійність: Продукти MikroTik відомі своєю надійністю та стабільністю роботи. Вони розроблені з використанням високоякісних компонентів та пройшли випробування в різних умовах експлуатації. Це дозволяє зменшити витрати на обслуговування та забезпечити безперебійну роботу мережі.
5. Масштабованість: MikroTik пропонує рішення, які можуть легко масштабуватись під ріст потреб мережі. Їхні пристрої підтримують можливість розширення функціональності та додавання додаткових модулів, що дозволяє збільшувати потужність мережі без заміни всього обладнання.
6. Підтримка: MikroTik надає широкий спектр підтримки своїм клієнтам. Вони мають активну спільноту користувачів та форуми, де можна отримати відповіді на питання та підказки. Крім того, компанія пропонує оновлення програмного забезпечення, патчі безпеки та технічну підтримку для своїх продуктів.

Загалом, MikroTik є популярним вибором для малих і середніх підприємств, інтернет-провайдерів та індивідуальних користувачів завдяки їхнім вартісним рішенням, функціональності та надійності. Отже, можна зробити висновок, що прилади фірми CISCO та MIKROTIK є досить гнучкими з точки зору налаштувань і надійності як для великих корпорацій, так і для

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

невеликих бізнесів. Тому ми будемо використовувати образи маршрутизатора серії 7200(CISCO), рис2.9, комутатора 9300(CISCO), рис2.10 та маршрутизатор МІКРОТІК під управлінням RouterOS(6.49.8), рис2.11.

Для створення моделі комп'ютерної гетерогенної мережі з можливістю віддалених робочих столів будемо використовувати програму GNS3. Додатково використовується програма VirtualBox^[14].



Рисунок 2.7 – Маршрутизатор останньої серії (Cisco 7200 Series Integrated Services Routers)



Рисунок 2.8 – Комутатор (Cisco Catalyst серії 9300)



Рисунок 2.9 – Маршрутизатор Mikrotik (MikroTik rb2011uias)

GNS3^[15] (Graphical Network Simulator 3) - це програмне забезпечення, яке дозволяє моделювати, віртуалізувати та емулювати мережеві середовища для тестування, навчання та дослідження мережевих пристроїв. Ось деякі переваги та недоліки GNS3:

Переваги GNS3:

1. Реалістичне моделювання: GNS3 дозволяє створювати віртуальні мережі, які точно відтворюють реальні конфігурації мережних пристроїв. Це дозволяє виконувати реальні тести та експерименти з мережними пристроями без необхідності наявності фізичного обладнання.
2. Підтримка різних платформ: GNS3 підтримує різні платформи, такі як Cisco IOS, Juniper JunOS, MikroTik RouterOS та інші, що дозволяє моделювати мережі, використовуючи різні виробники та їхні операційні системи.
3. Інтеграція з реальним обладнанням: GNS3 може бути інтегрований з реальним мережевим обладнанням, дозволяючи комбінувати віртуальне та фізичне обладнання в одну мережу. Це дозволяє створювати складні тестові середовища з комбінацією віртуальних та фізичних пристроїв.
4. Гнучкість та налаштування: GNS3 надає гнучкі можливості налаштування мережевих пристроїв та параметрів мережі. Ви можете контролювати трафік, розділяти мережу на підмережі, налаштовувати маршрутизацію та інші аспекти мережевої конфігурації.

Недоліки GNS3:

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Високі вимоги до ресурсів: GNS3 вимагає значних ресурсів комп'ютера для емуляції великих мереж. Моделювання складних мереж з великою кількістю пристроїв може призвести до значного навантаження на процесор та оперативну пам'ять.
2. Потребує обладнання для емуляції: Для емуляції деяких мережних пристроїв у GNS3 може бути потрібне власне обладнання або образи програмного забезпечення, які можуть бути обмеженими або вимагати додаткових ліцензій.
3. Відсутність реального трафіку: GNS3 емулює мережеве середовище, але не здатний передавати реальний трафік між віртуальними пристроями та зовнішніми мережами. Це може бути обмеженням для деяких випадків тестування та налагодження мережі.
4. Вимагає технічних знань: Використання GNS3 вимагає розуміння мережевих протоколів, налаштування мережевих пристроїв та загальної технічної компетенції. Для новачків може знадобитися додатковий час та зусилля для вивчення програмного забезпечення та його можливостей.

Усе узагальнюючи, GNS3 є потужним інструментом для моделювання та емуляції мережних середовищ, проте він вимагає відповідних ресурсів та технічної експертизи. Його переваги полягають у реалістичному моделюванні, підтримці різних платформ, інтеграції з реальним обладнанням та гнучкості налаштування. Недоліки GNS3 включають високі вимоги до ресурсів, потребу у спеціалізованому обладнанні, обмеження з передачею реального трафіку та необхідність технічних знань для використання.

VirtualBox є одним з найпопулярніших програмних засобів для віртуалізації, який дозволяє створювати та управляти віртуальними машинами на різних операційних системах. Ось деякі з його переваг та недоліків:

Переваги VirtualBox:

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Безкоштовний та відкритий: VirtualBox є вільно розповсюджуваним програмним забезпеченням, що дозволяє безкоштовно використовувати його без обмежень.
2. Підтримка різних операційних систем: VirtualBox доступний для використання на різних операційних системах, включаючи Windows, macOS, Linux та інші.
3. Простота використання: VirtualBox має зручний інтерфейс, що дозволяє легко створювати, налаштовувати та керувати віртуальними машинами.
4. Гнучкість налаштування: VirtualBox надає широкі можливості для налаштування віртуальних машин, включаючи виділення ресурсів, мережеві налаштування, збільшення або зменшення розміру віртуального диска та інші параметри.
5. Підтримка гостьових розширень: VirtualBox надає набір розширень, які можна встановити в гостьову операційну систему для поліпшення функціональності та зручності використання.

Недоліки VirtualBox:

1. Обмежена продуктивність: Порівняно з деякими іншими програмами віртуалізації, VirtualBox може мати обмежену продуктивність, особливо при роботі з високонавантаженими додатками або великими мережами віртуальних машин.
2. Низька швидкодія віртуалізації апаратного забезпечення: VirtualBox використовує повний апаратний емулятор, що може призвести до певного зниження продуктивності порівняно з гіпервізорами, які використовують віртуалізацію апаратного забезпечення на рівні процесора.
3. Відсутність деяких функцій для підприємницького застосування: У порівнянні з деякими комерційними віртуалізаційними рішеннями, VirtualBox може мати обмежену набір функцій для підприємницького застосування, таких як резервування ресурсів, масштабованість та централізоване керування.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Відсутність офіційної підтримки: VirtualBox, як вільно розповсюджуване програмне забезпечення, не надає офіційної технічної підтримки, і користувачам доводиться спиратися на спільноту користувачів та ресурси Інтернету для отримання допомоги та вирішення проблем.
5. Обмежена інтеграція з хост-системою: У порівнянні з деякими іншими програмами віртуалізації, VirtualBox може мати обмежену інтеграцію з хост-системою, що може впливати на зручність використання та обмін даними між гостьовою та хост-системами.
6. Враховуючи ці переваги та недоліки, VirtualBox залишається популярним вибором для багатьох користувачів, особливо для домашнього використання та невеликих проектів, де безкоштовність та простота використання мають значення. Однак, для підприємств і великих проектів, можуть бути більш підходящі комерційні рішення віртуалізації з більш широким набором функцій та підтримкою.

Висновки до розділу 2

Була розроблена підсистема гетерогенної мережі, яка включає 6 локальних підмереж та маршрутизатори рівня ядра. Використання трирівневої ієрархічної моделі було обґрунтовано з метою досягнення оптимальної працездатності та ефективності мережі.

Для кожного пристрою мережі була створена таблиця параметрів інтерфейсів та адресації. Ця таблиця включає необхідні налаштування, такі як IP-адреси, підмережі та маски підмереж. Це забезпечує коректну комунікацію між пристроями та оптимальне використання ресурсів мережі.

Для рівня ядра були обрані найпотужніші пристрої, які здатні виконувати високонавантажені завдання. Вони мають широкі можливості, які відповідають поставленим вимогам. Наприклад, це можуть бути маршрутизатори з підтримкою різних протоколів маршрутизації, віртуалізації мережі та іншими функціями, які покращують продуктивність та безпеку мережі.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Для створення та моделювання мережі було обрано певне програмне забезпечення, зокрема симулятор. Вибір симулятора залежить від вимог та цілей проекту. Наприклад, можна використовувати GNS3, який надає розширені можливості для моделювання різних пристроїв та їхньої взаємодії в мережі.

Операційні системи, які будуть використовуватися, обрані з метою забезпечення гетерогенності мережі та відповідності вимогам проекту. Різні операційні системи дозволяють використовувати різні протоколи, сервіси та функціональні можливості, що робить мережу більш гнучкою та сумісною з різними пристроями та сервісами.

В цілому, розроблена підсистема гетерогенної мережі враховує особливості та потреби проекту, забезпечуючи оптимальну працездатність, гнучкість та ефективність мережевої інфраструктури.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА, ПОБУДОВАНОЇ НА БАЗІ ОБЛАДНАННЯ CISCO ТА MIKROTIK.

3.1 Налаштування мережі

Зображення повної мережі створеної у минулому розділі за допомогою GNS3, рис.3.1.

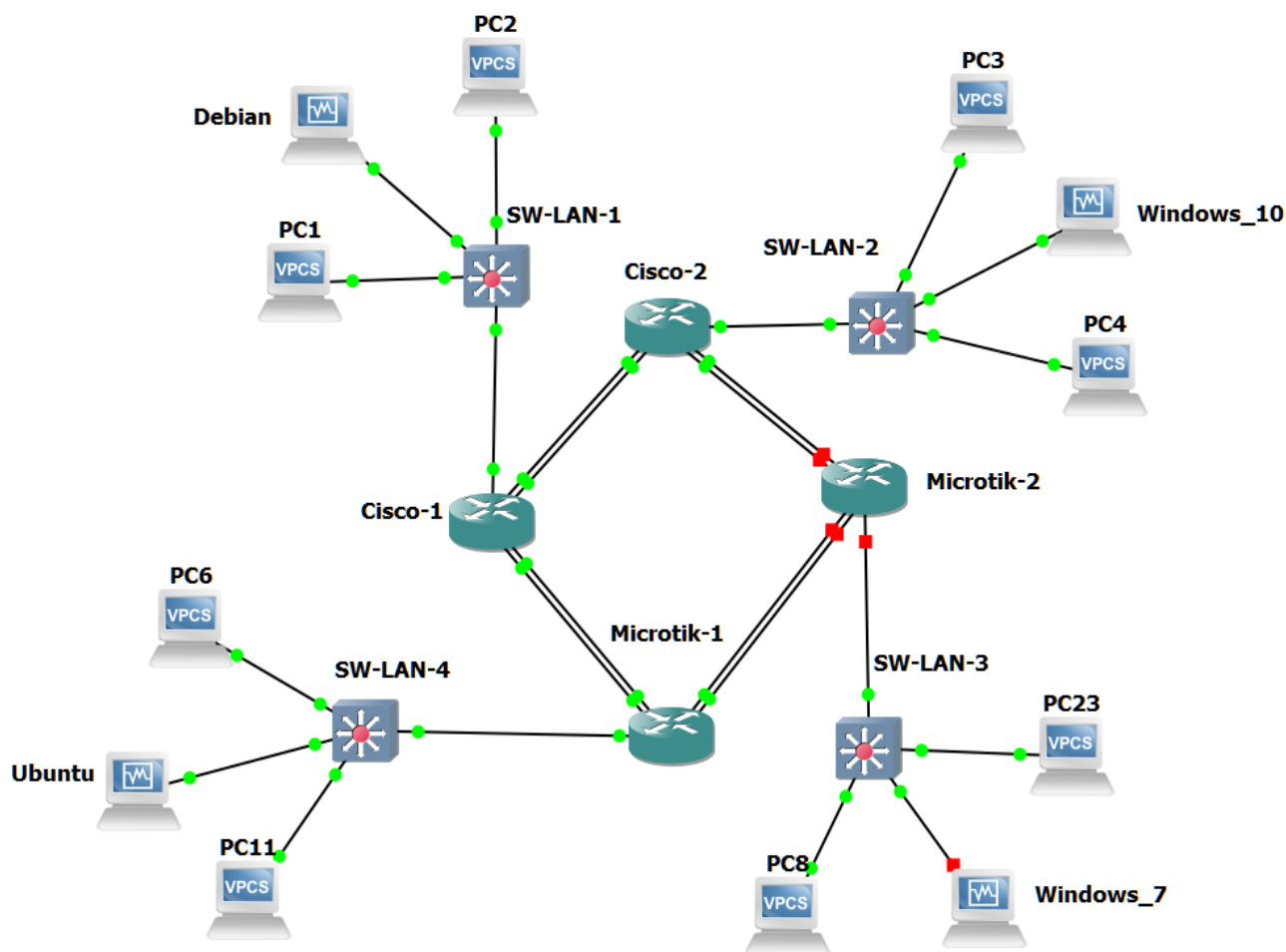


Рисунок 3.1 – Повна схема мережі

Налаштуємо IP-адресацію та інші необхідні налаштування на всіх маршрутизаторах та комутаторах CISCO. Нижче рис.3.2 наведено приклад лістингу налаштування адресації на пристрої CISCO-1.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

```

*Jun 27 01:32:40.803: %SYS-5-CONFIG_I: Configured from console by console
Cisco-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco-1(config)#int e1/1
Cisco-1(config-if)#ip add 192.1.1.1 255.255.255.255
Bad mask /32 for address 192.1.1.1
Cisco-1(config-if)#ip add 192.1.1.1 255.255.255.252
Cisco-1(config-if)#no shut
Cisco-1(config-if)#ex
*Jun 27 01:34:02.803: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
*Jun 27 01:34:03.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
1, changed state to up
Cisco-1(config-if)#ex
Cisco-1(config)#x
% Ambiguous command: "x"
Cisco-1(config)#int e1/2
Cisco-1(config-if)#ip add 192.1.2.1 255.255.255.252
Cisco-1(config-if)#no shut
Cisco-1(config-if)#ex
Cisco-1(config)#
*Jun 27 01:35:21.507: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state to up
*Jun 27 01:35:22.507: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
2, changed state to up
Cisco-1(config)#int e1/3
Cisco-1(config-if)#ip add 192.1.5.1 255.255.255.252
Cisco-1(config-if)#no shut
Cisco-1(config-if)#ex
Cisco-1(config)#
*Jun 27 01:35:46.199: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state to up
*Jun 27 01:35:47.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
3, changed state to up
Cisco-1(config)#int e2/1
Cisco-1(config-if)#ip add 192.1.6.1 255.255.255.252
Cisco-1(config-if)#no shut
Cisco-1(config-if)#ex
Cisco-1(config)#
*Jun 27 01:36:34.803: %LINK-3-UPDOWN: Interface Ethernet2/1, changed state to up
*Jun 27 01:36:35.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/
1, changed state to up
Cisco-1(config)#int e2/2
Cisco-1(config-if)#ip add 192.20.20.1 255.255.255.0
Cisco-1(config-if)#no shut
Cisco-1(config-if)#ex
Cisco-1(config)#
*Jun 27 01:37:37.003: %LINK-3-UPDOWN: Interface Ethernet2/2, changed state to up
*Jun 27 01:37:38.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/
2, changed state to up
Cisco-1(config)#

```

Рисунок 3.2 – Налаштування IP-адресації на CISCO-1

Тепер, для забезпечення зв'язку між маршрутизаторами, комутаторами та іншими пристроями, налаштуємо протокол маршрутизації OSPF, рис.3.3.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Cisco-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco-1(config)#router ospf 1
Cisco-1(config-router)# network 192.1.1.0 0.0.0.3 area 0
Cisco-1(config-router)# network 192.1.2.0 0.0.0.3 area 0
Cisco-1(config-router)# network 192.1.5.0 0.0.0.3 area 0
Cisco-1(config-router)# network 192.1.6.0 0.0.0.3 area 0
Cisco-1(config-router)# network 192.20.20.0 0.0.0.255 area 0
Cisco-1(config-router)#exit

```

Рисунок 3.3. Налаштування протоколу OSPF на CISCO-1

Оскільки в нашій мережі використовується досить багато робочих станцій, то налаштуємо протокол DHCP на маршрутизаторах, рис.3.4.

```

Cisco-1#QQ
Cisco-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco-1(config)#ip dhcp pool Lan-1
Cisco-1(dhcp-config)#network 192.20.20.0 255.255.255.0
% A pool already exists for network 192.20.20.0 / 255.255.255.0.
Cisco-1(dhcp-config)#default-router 192.20.20.1
^
% Invalid input detected at '^' marker.

Cisco-1(dhcp-config)#default-router 192.20.20.1
Cisco-1(dhcp-config)#dns-server 8.8.8.8
Cisco-1(dhcp-config)#

```

Рисунок 3.4 Налаштування протоколу DHCP на CISCO-1

Після налаштування маршрутизації та віддалених робочих станцій, також необхідно врахувати безпеку пристроїв. Для цього, перш за все, забезпечимо захист наших маршрутизаторів шляхом створення користувачів з різними рівнями доступу, рис.3.5-3.7.

```

Cisco-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco-1(config)#privilege exec level 1 show run
Cisco-1(config)#privilege exec level 1 show running-config
Cisco-1(config)#privilege exec level 1 show interface
Cisco-1(config)#privilege exec level 1 show ip interface
Cisco-1(config)#privilege exec level 1 show ip route
Cisco-1(config)#username Anton privilege 1 secret ciscs
Cisco-1(config)#line console 0
Cisco-1(config-line)#exec-timeout 15
Cisco-1(config-line)#end
Cisco-1#
*Jun 27 01:51:13.443: %SYS-5-CONFIG_I: Configured from console by console
Cisco-1#

```

Рисунок 3.5. Налаштування користувачів на CISCO-1

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Cisco-1
% Invalid input detected at '^' marker.

Cisco-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco-1(config)#privilege exec level 4 show interface
Cisco-1(config)#privilege exec level 4 show description
Cisco-1(config)#privilege exec level 4 show shutdown
Cisco-1(config)#username Anton privilege 4 secret cisco
Cisco-1(config)#line console 0
Cisco-1(config-line)#exec-timeout 15
Cisco-1(config-line)#end
Cisco-1#
*Jun 27 01:53:07.111: %SYS-5-CONFIG_I: Configured from console by console
Cisco-1#

```

Рисунок 3.6. Налаштування користувачів на CISCO-1

```

Cisco-1
*Jun 27 01:53:07.111: %SYS-5-CONFIG_I: Configured from console by console
Cisco-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cisco-1(config)#username Administrator privilege 15 secret cisco
Cisco-1(config)#line console 0
Cisco-1(config-line)#login local
Cisco-1(config-line)#exec-timeout 15
Cisco-1(config-line)#end
Cisco-1#
*Jun 27 01:54:39.335: %SYS-5-CONFIG_I: Configured from console by console
Cisco-1#

```

Рисунок 3.7. Налаштування користувачів на CISCO-1

І додатково, проведемо налаштування параметрів безпеки на комутаторах, оскільки у нашій мережі присутні різні DHCP-сервери. Враховуючи можливість зловмисницького підключення зовнішнього DHCP-сервера, необхідно запобігти втраті даних, які знаходяться на робочих станціях. Тому ми налаштуємо функцію "довіреного порту" на комутаторах, рис.3.8.

```

SW-LAN-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-LAN-1(config)#int vlan 1
SW-LAN-1(config-if)#ip add 192.20.20.210 255.255.255.0
SW-LAN-1(config-if)#no shut
SW-LAN-1(config-if)#ex
SW-LAN-1(config)#
*Jun 26 22:59:40.015: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun 26 22:59:41.015: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW-LAN-1(config)#ip dhcp snooping vlan 1
SW-LAN-1(config)#int e2/1
SW-LAN-1(config-if)#ip dhcp snooping trust
SW-LAN-1(config-if)#ip dhcp snooping limit rate 50
SW-LAN-1(config-if)#ex
SW-LAN-1(config)#no ip dhcp snooping information option
^
% Invalid input detected at '^' marker.

SW-LAN-1(config)#no ip dhcp snooping information option
SW-LAN-1(config)#ex
% Ambiguous command: "ex"
SW-LAN-1(config)#

```

Рисунок 3.8. Налаштування довіреного порту на комутаторі SW-LAN-1

Також налаштуємо функцію Port Security на комутаторах, рис..3.9.

```

SW-LAN-1 (config-if-range) #^Z
SW-LAN-1 #^Z
SW-LAN-1 #^Z
SW-LAN-1 #^Z
SW-LAN-1 #Q
*Jun 26 23:05:10.266: %SYS-5-CONFIG_I: Configured from console by console
SW-LAN-1 #QQ
SW-LAN-1 #conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-LAN-1 (config) #int e0/0
SW-LAN-1 (config-if) #switchport mode access
SW-LAN-1 (config-if) #switchport port-security
SW-LAN-1 (config-if) #switchport port-security maximum 5
SW-LAN-1 (config-if) #switchport port-security mac-address sticky
SW-LAN-1 (config-if) #switchport port-security aging time 10
SW-LAN-1 (config-if) #switchport port-security aging type inactivity
SW-LAN-1 (config-if) #

```

Рисунок 3.9. Налаштування Port Security на комутаторі SW-LAN-1

```

Cisco-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco-1(config)#login block-for 60 attempts 3 within 20
      ^
% Invalid input detected at '^' marker.

Cisco-1(config)#login block-for 60 attempts 3 within 20
Cisco-1(config)#login delay 5
Cisco-1(config)#login on-failure log
Cisco-1(config)#login on-success log
Cisco-1(config)#

```

Рисунок 3.10. Налаштування захисту від Bruteforce на CISCO-1

Тепер налаштуємо IP-адресацію та інші налаштування на всіх маршрутизаторах MikroTik^[14] за допомогою WinBox^[16]. На рис.3.11-3.13 наведено налаштування адресації на CISCO_1. На інших пристроях мережі воно проводиться аналогічно.

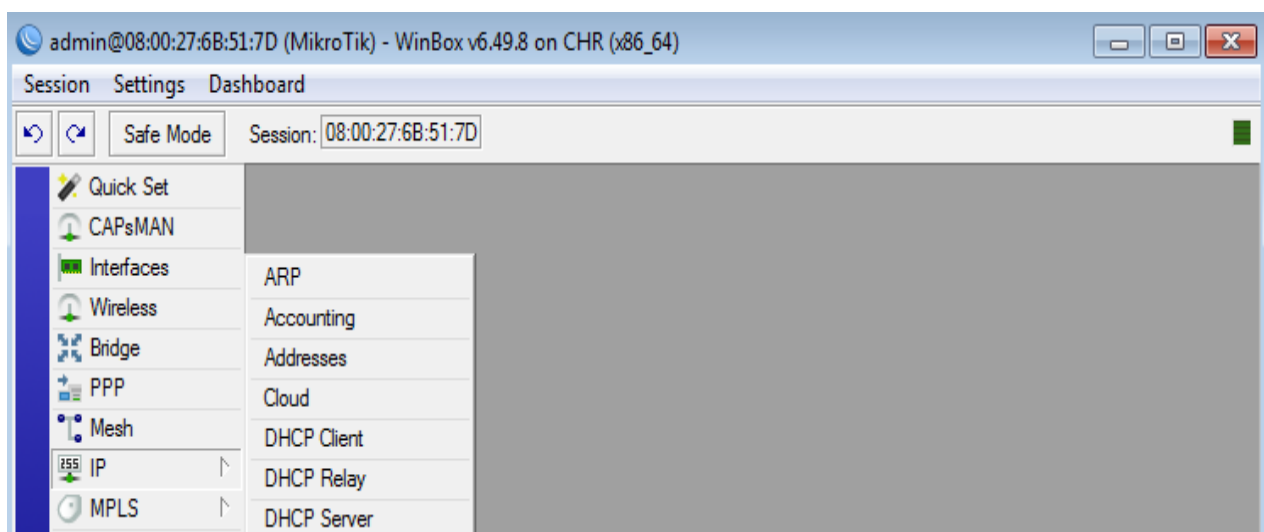


Рисунок 3.11. Налаштування IP-адресації на Mikrotik-1

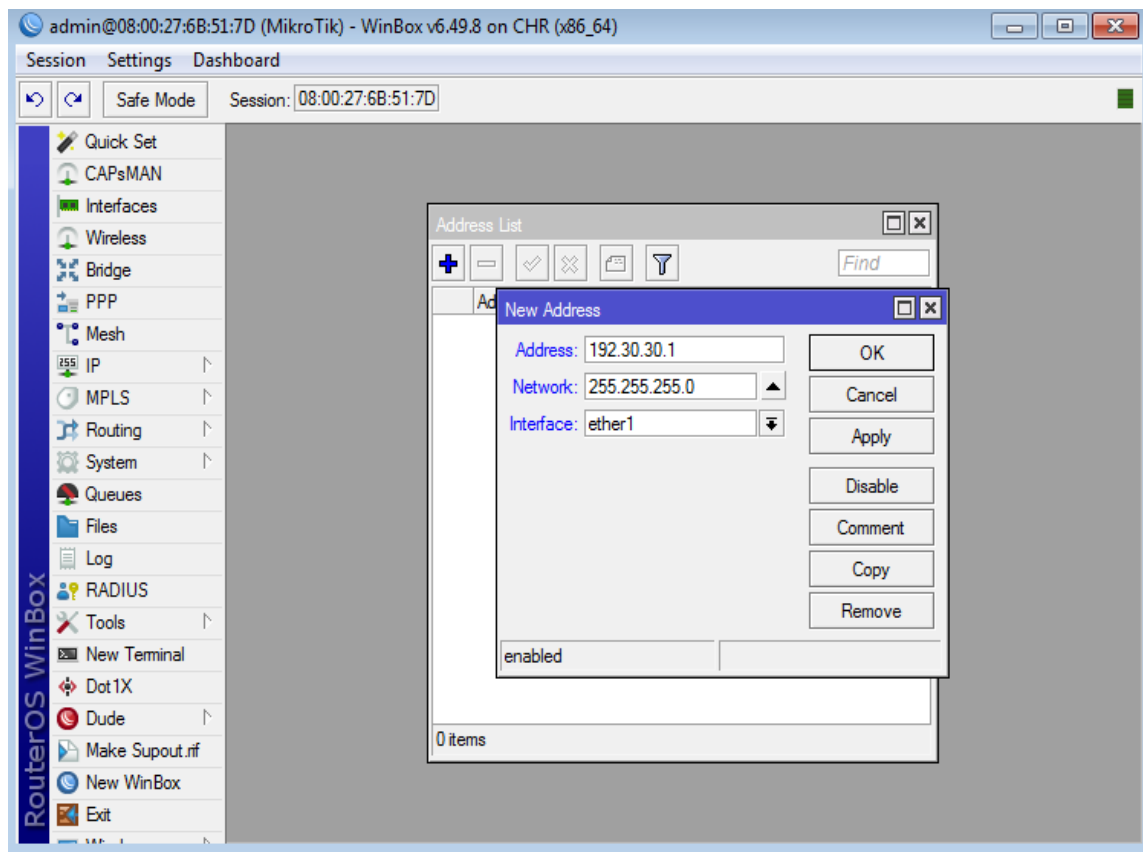


Рисунок 3.12. Налаштування IP-адресації на Mikrotik-1

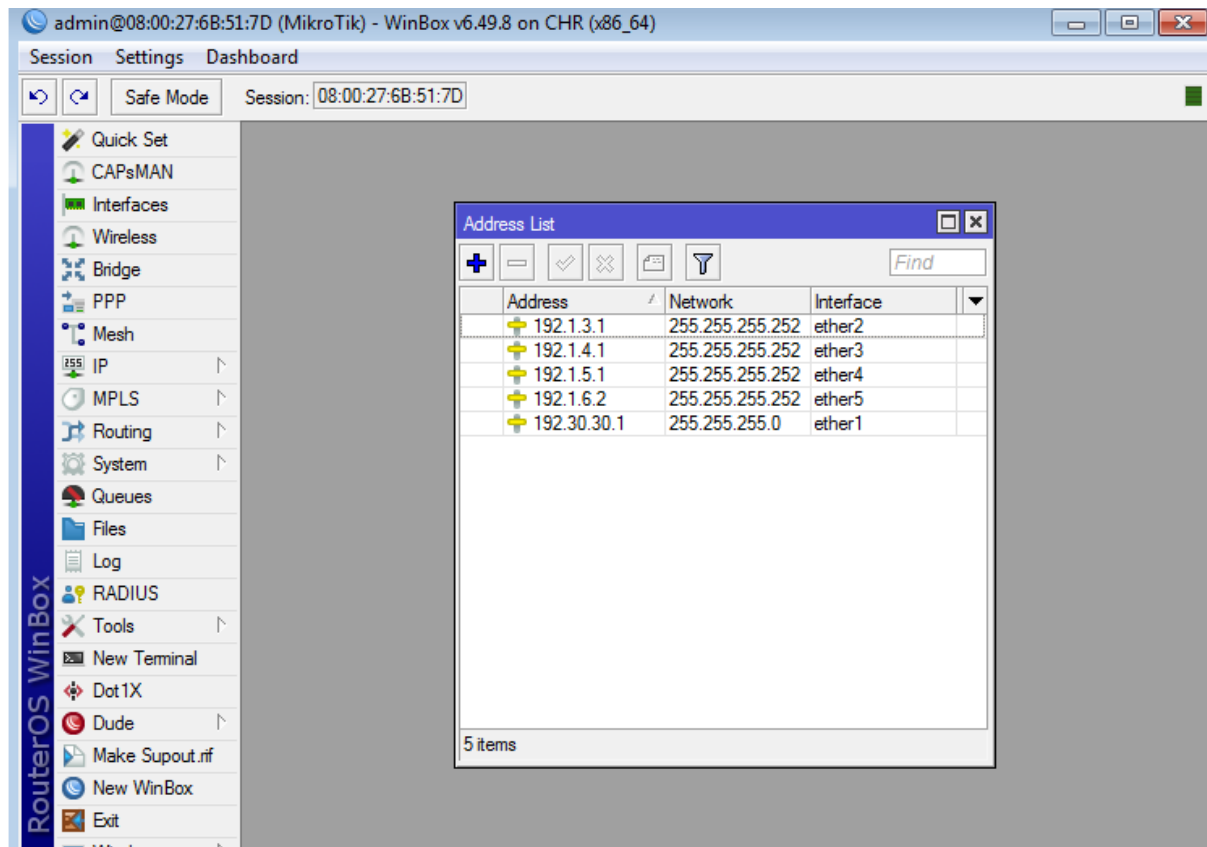


Рисунок 3.13. Налаштування IP-адресації на Mikrotik-1

Тепер для зв'язку між маршрутизаторами, комутаторами та іншими приладами налаштуємо протокол маршрутизації. В нашому випадку це протокол OSPF, рис.3.14.

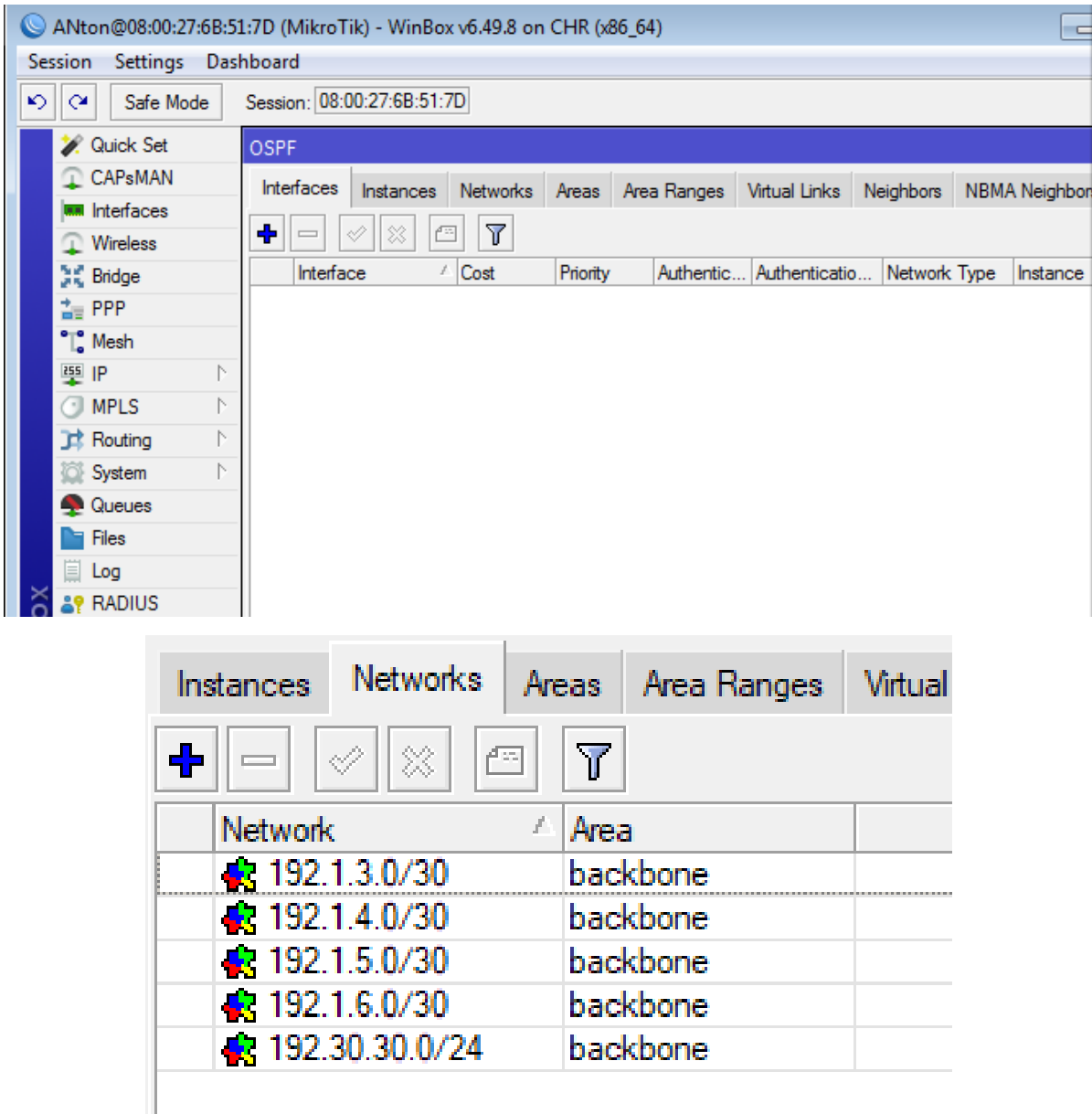


Рисунок 3.14. Налаштування протоколу OSPF на Mikrotik-1

Оскільки в нашій мережі використовується значна кількість робочих станцій, ми налаштуємо протокол DHCP на маршрутизаторах. Це дозволить автоматично призначати IP-адреси робочим станціям для забезпечення зручності в налаштуванні та масштабованості мережі, рис.3.15–3.18.

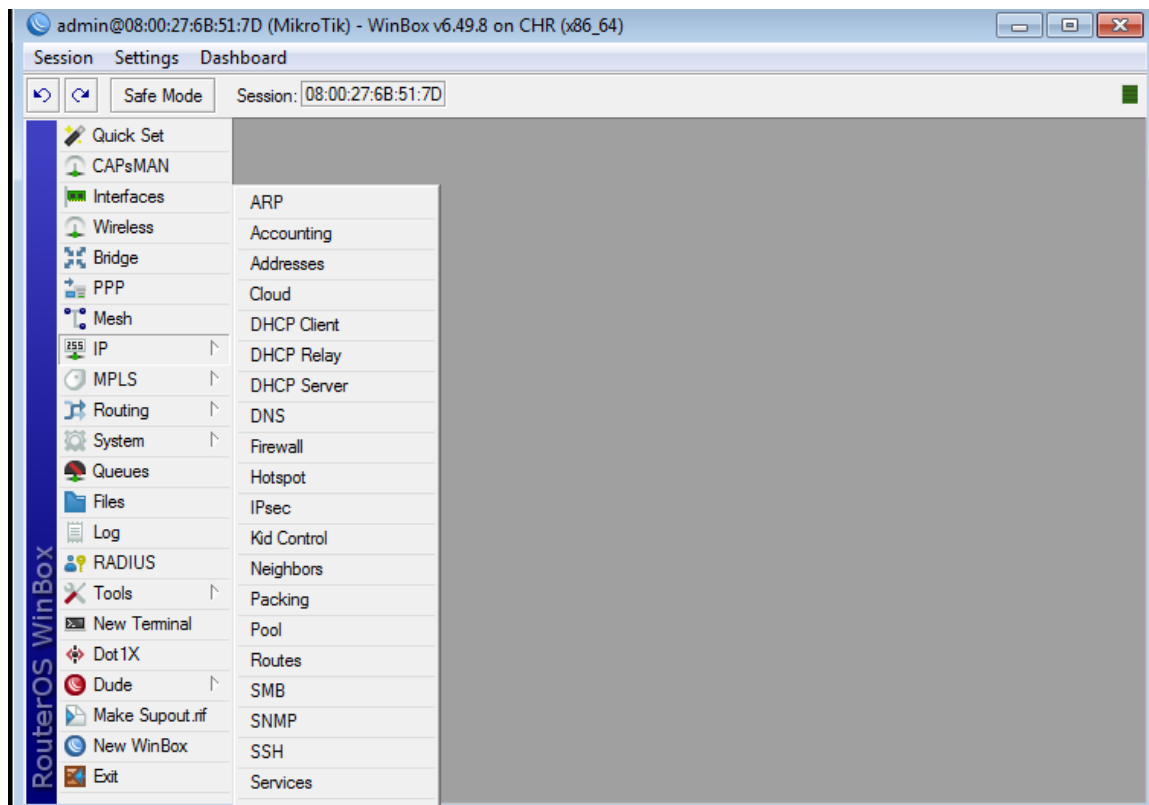


Рисунок 3.15. Налаштування протоколу DHCP на Mikrotik-1

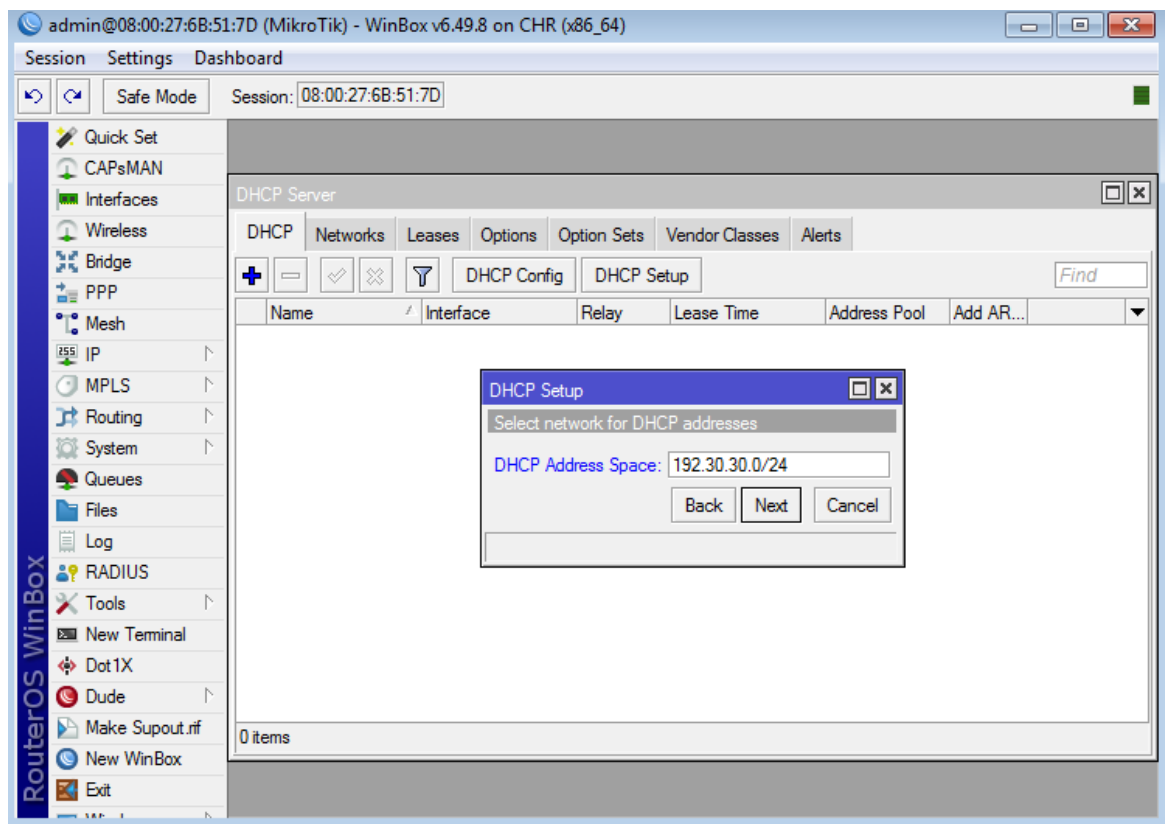


Рисунок 3.16. Налаштування протоколу DHCP на Mikrotik-1

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

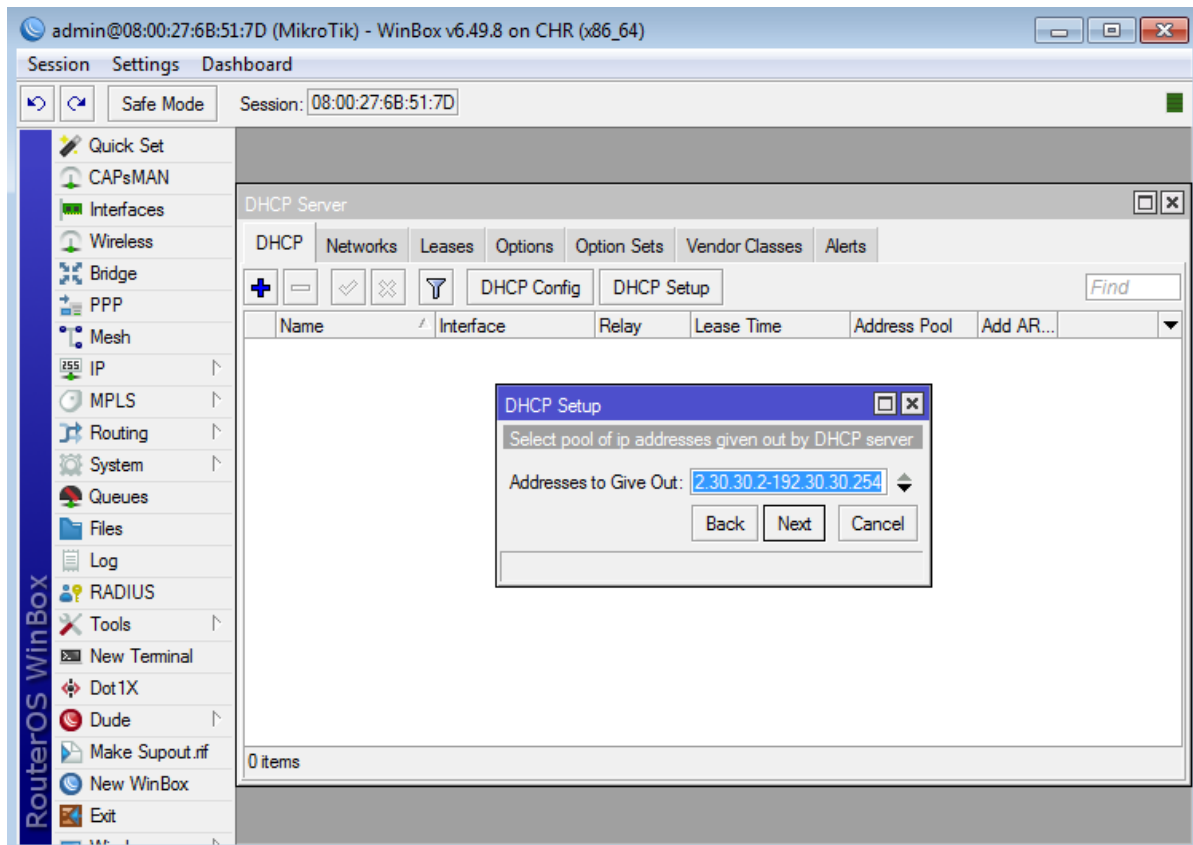


Рисунок 3.17. Налаштування протоколу DHCP на Mikrotik-1

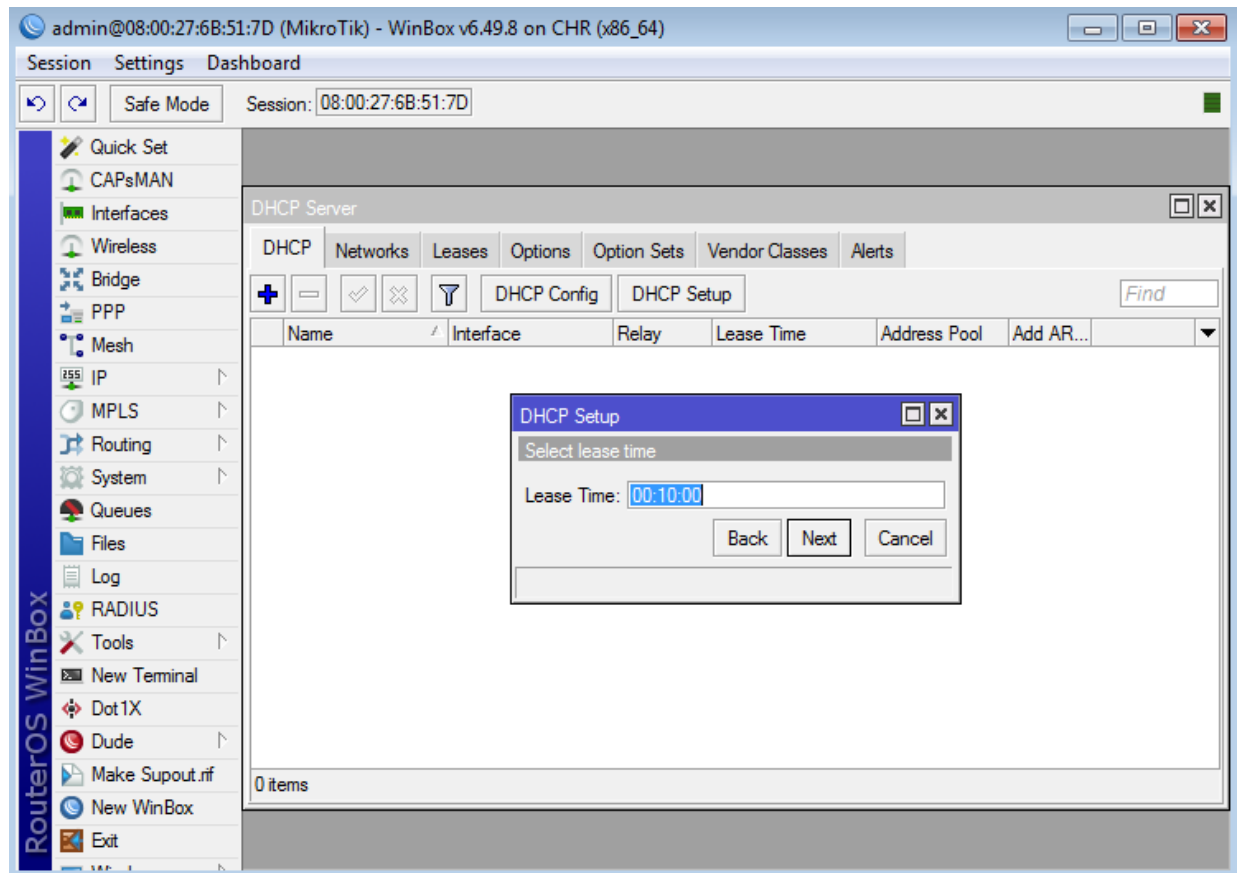


Рисунок 3.18. Налаштування протоколу DHCP на Mikrotik-1

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

Після налаштувань маршрутизації потрібно також налаштувати безпеку пристроїв. Для початку захистимо наші маршрутизатори за допомогою створення користувачів з різними рівнями доступу, рис.3.19–3.22.

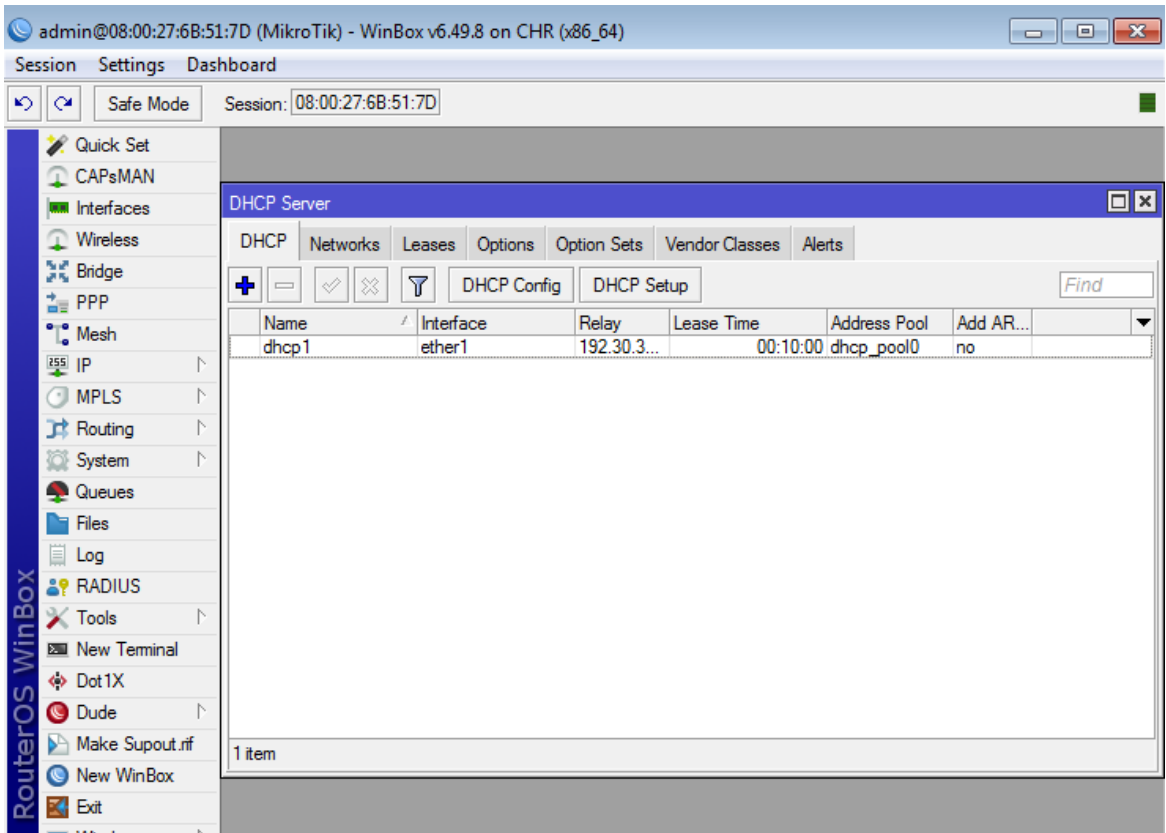


Рисунок 3.19 – Створений сервер DHCP на Mikrotik-1

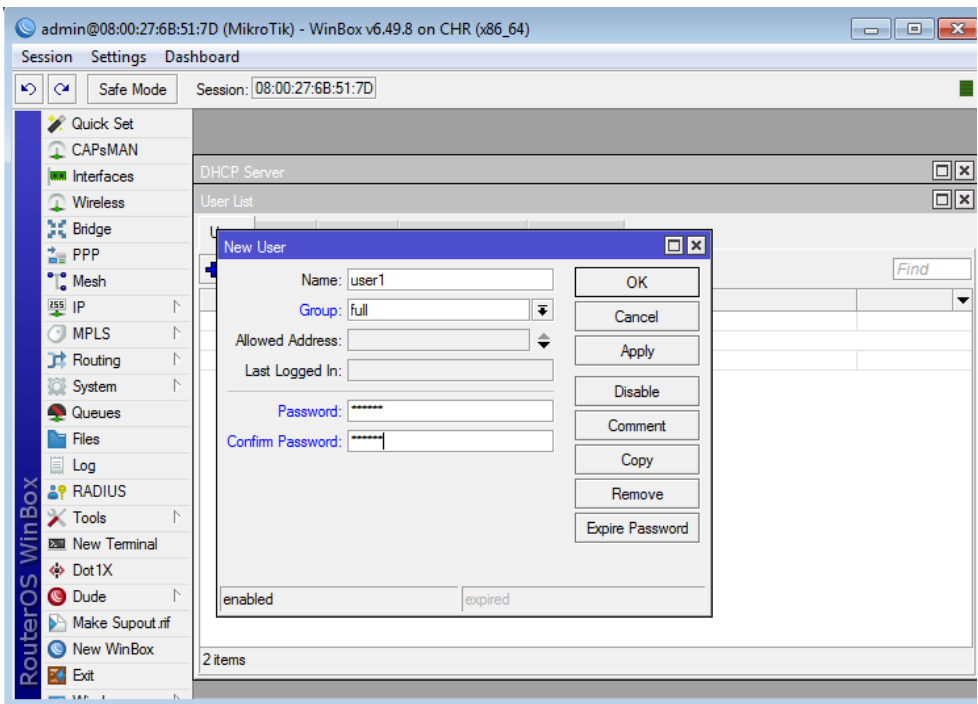


Рисунок 3.20 – Налаштування користувачів на Mikrotik-1

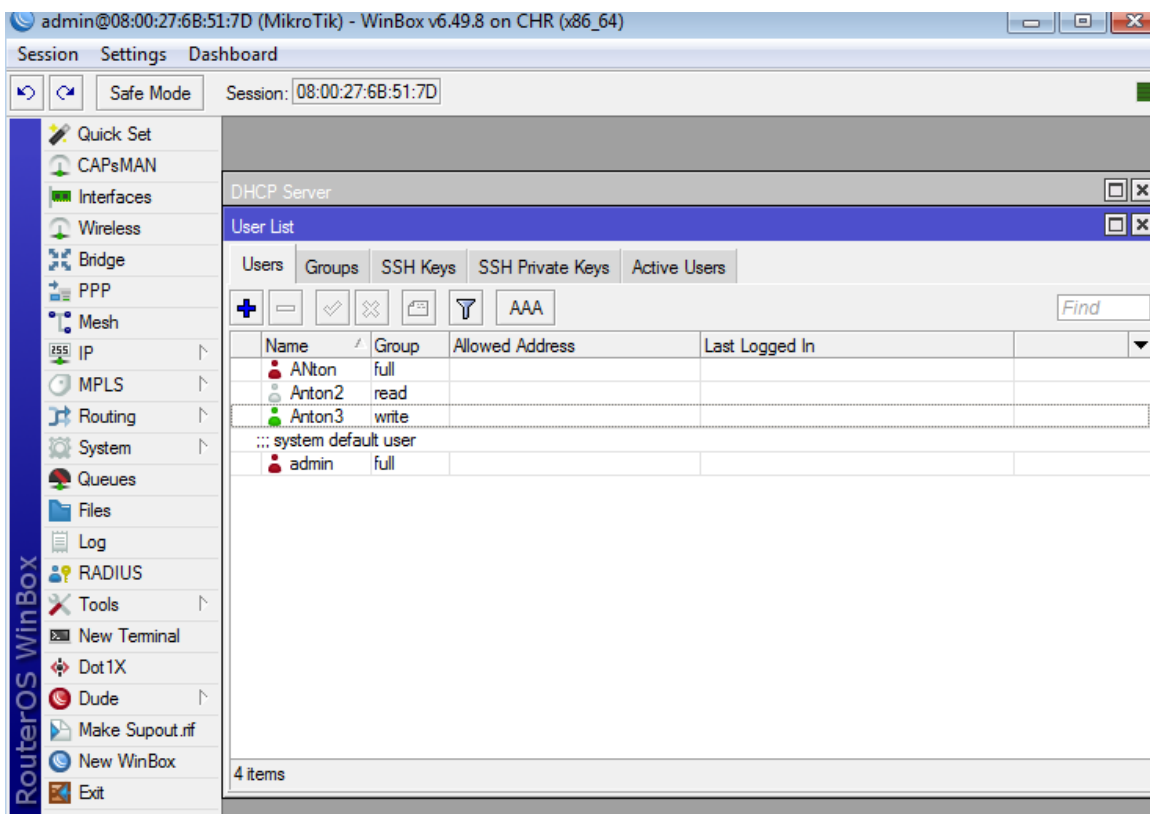


Рисунок 3.21 – Налаштування користувачів на Mikrotik-1

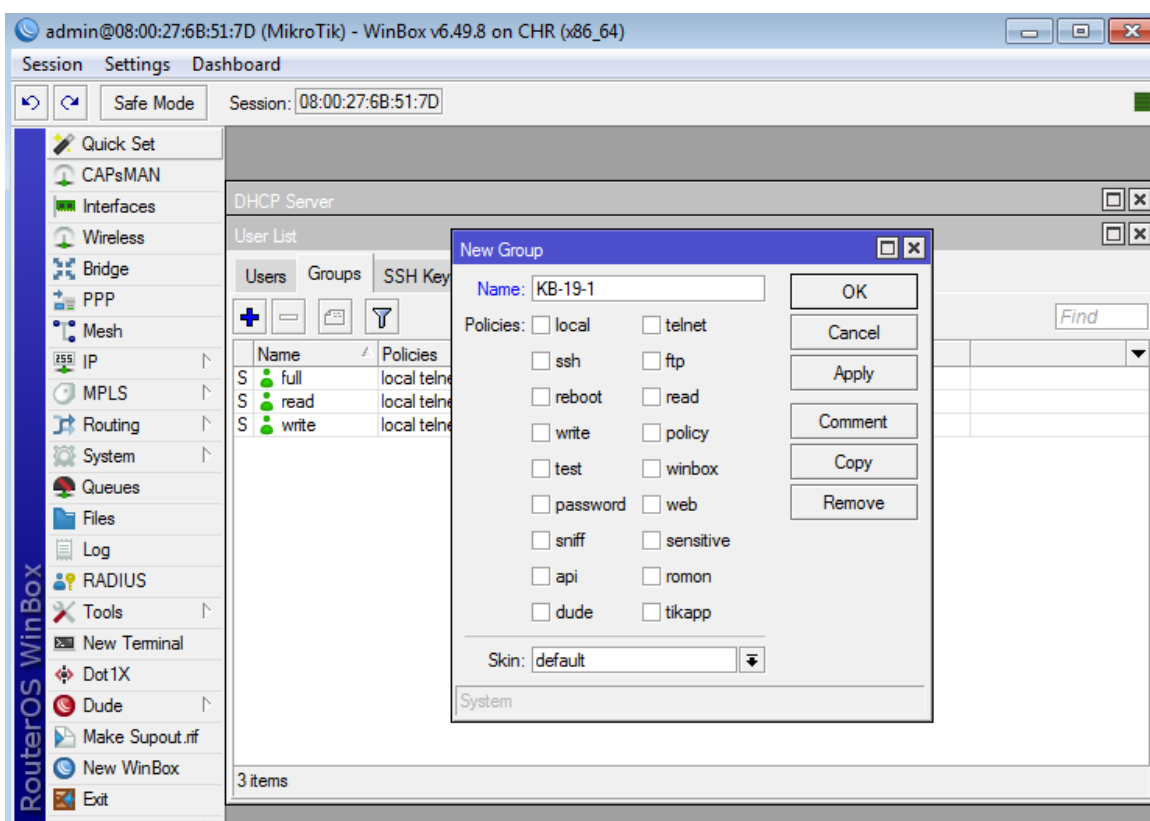


Рисунок 3.22 – Можливе додавання груп користувачів на Mikrotik-1

На маршрутизаторі Mikrotik-1 було налаштовано захист від Bruteforce відразу різних можливих сторонах, рис.3.23–3.27.

```
[admin@MikroTik] > /ip firewall filter add action=add-src-to-address-list address-list=BlackList address-list-timeout=10m chain=input comment="F2B SSH: Login Failure -> BlackList" connection-state=established dst-port=22 packet-size=304 protocol=tcp
```

Рисунок 3.23 – Налаштування захисту від Bruteforce на Mikrotik-1

```
[admin@MikroTik] > /ip firewall filter add action=add-dst-to-address-list address-list=BlackList address-list-timeout=10m chain=output comment="F2B Web: Login Failure -> BlackList" connection-state=established content="Error 403" protocol=tcp src-port=90
```

Рисунок 3.24 – Налаштування захисту від Bruteforce на Mikrotik-1

```
[admin@MikroTik] > /ip firewall filter add action=add-dst-to-address-list address-list=BlackList address-list-timeout=10m chain=output comment="F2B Winbox: Login Failure -> BlackList" content="invalid user name or password" protocol=tcp src-port=8291
```

Рисунок 3.25 – Налаштування захисту від Bruteforce на Mikrotik-1

```
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="drop invalid" connection-state=invalid
```

Рисунок 3.26 – Налаштування захисту від Bruteforce на Mikrotik-1

```
[admin@MikroTik] /ip firewall filter> add action=accept chain=input comment="accept ICMP" protocol=icmp
[admin@MikroTik] /ip firewall filter>
```

Рисунок 3.27 – Налаштування захисту від Bruteforce на Mikrotik-1

Також було виконано налаштування захисту домену та пошти від фішингових атак, рис.3.28–рис.3.39.

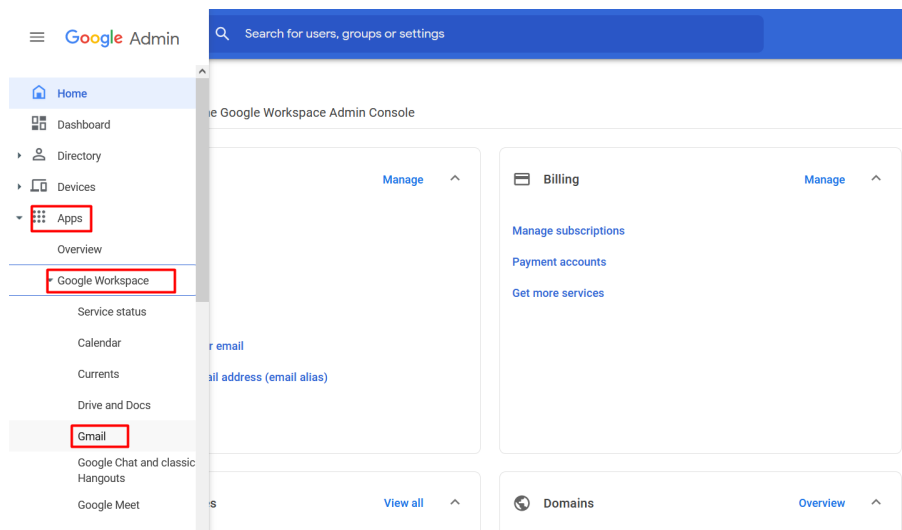


Рисунок 3.28. Налаштування захисту від Fishing домену DKIM

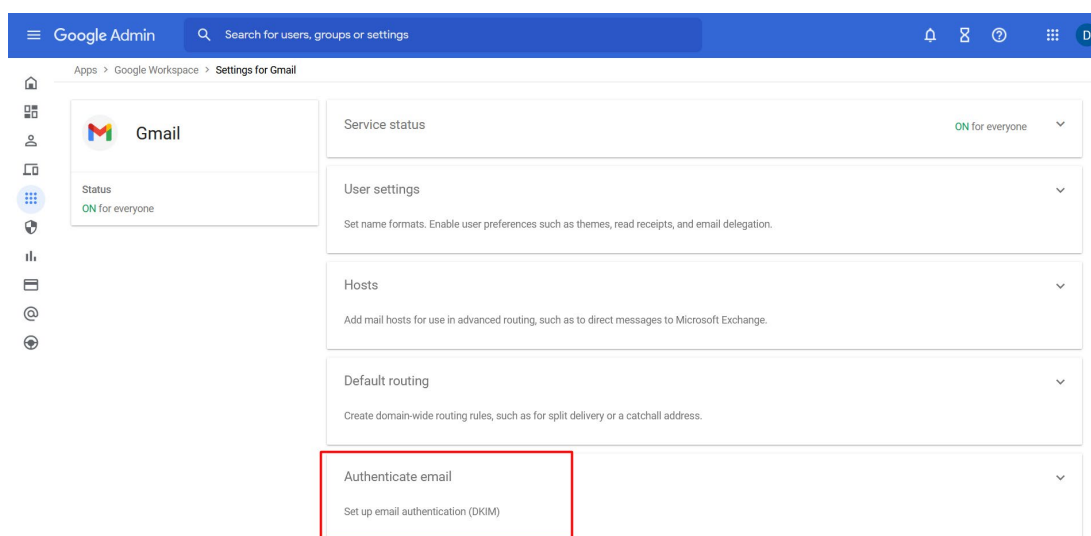


Рисунок 3.29 – Налаштування захисту від Fishing домену DKIM

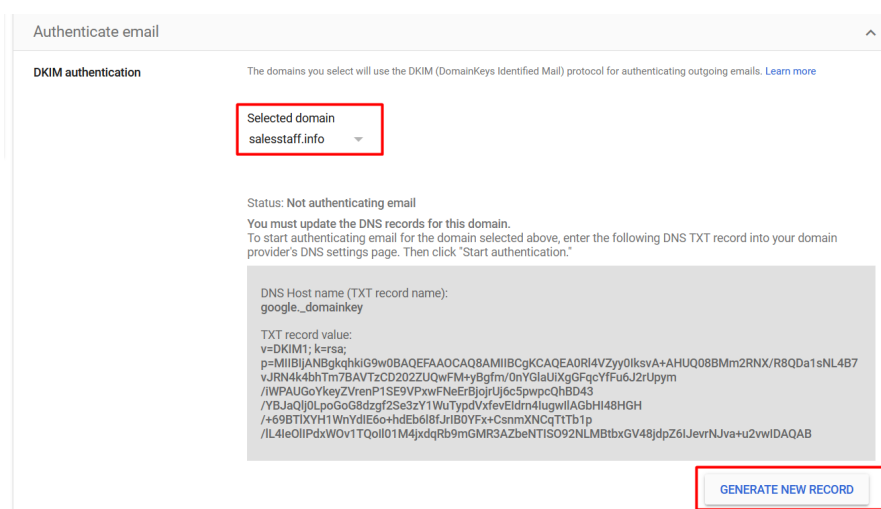


Рисунок 3.30 – Налаштування захисту від Fishing домену DKIM

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

DNS Records

[DNS Records](#) define how your domain behaves, like showing your website content and delivering your email.

Filter

[TXT records](#) are most commonly used to verify domain ownership, SSL verification, and [email sender policies](#). ✕

Type	Name	Value	TTL
TXT	google._domainkey	v=DKIM1; k=rsa; p=MIIIBjANBgkqhkiG9w0I...	1/2 Hour

Type	Name	Data	TTL	
☐	A	@	Parked	600 seconds Delete Edit

Рисунок 3.31 – Налаштування захисту від Fishing домену DKIM

Required
Informational only records

Рисунок 3.32 – Налаштування захисту від Fishing домену DKIM

DNS Records

[DNS Records](#) define how your domain behaves, like showing your website content and delivering your email.

Filter

[TXT records](#) are most commonly used to verify domain ownership, SSL verification, and [email sender policies](#). ✕

Type	Name	Value	TTL
TXT	@	v=spf1 include:_spf.google.com ~all	1/2 Hour

Type	Name	Data	TTL	
☐	A	@	Parked	600 seconds Delete Edit

Рисунок 3.33 – Налаштування захисту від Fishing домену SPF^[4]

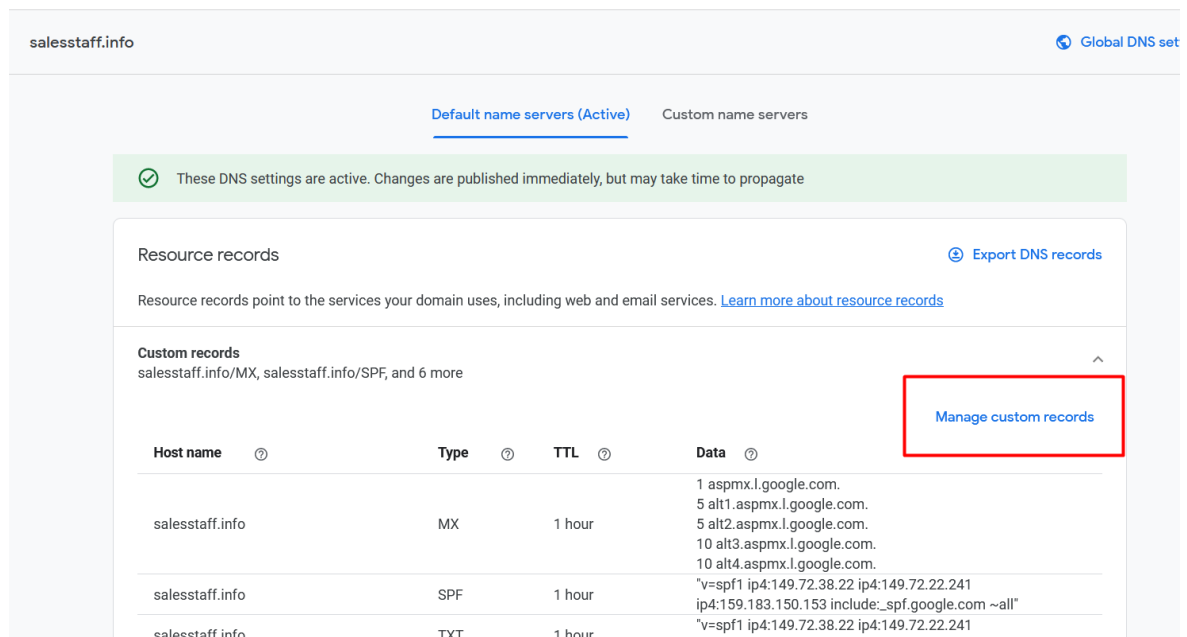


Рисунок 3.34. Налаштування захисту від Fishing домену SPF

/IL4leOIPdxW0v1TQoII01M4jxdqRb9mGMR3AZbeNTIS
O92NLMBtbxGV48jdpZ6IJevrNJva+u2vwIDAQAB"

+ Add more to this record

s1__domainkeyCNAME3600s1.domainkey.u25481426.wl177.sendgrid.net

s2__domainkeyCNAME3600s2.domainkey.u25481426.wl177.sendgrid.net

TXT

3600

v=spf1 include:_spf.google.com ~all

+ Add more to this record

SPF

3600

v=spf1 include:_spf.google.com ~all

+ Add more to this record

Create new record

Cancel

Save

Required
Informational only records

Рисунок 3.35 – Налаштування захисту від Fishing домену SPF

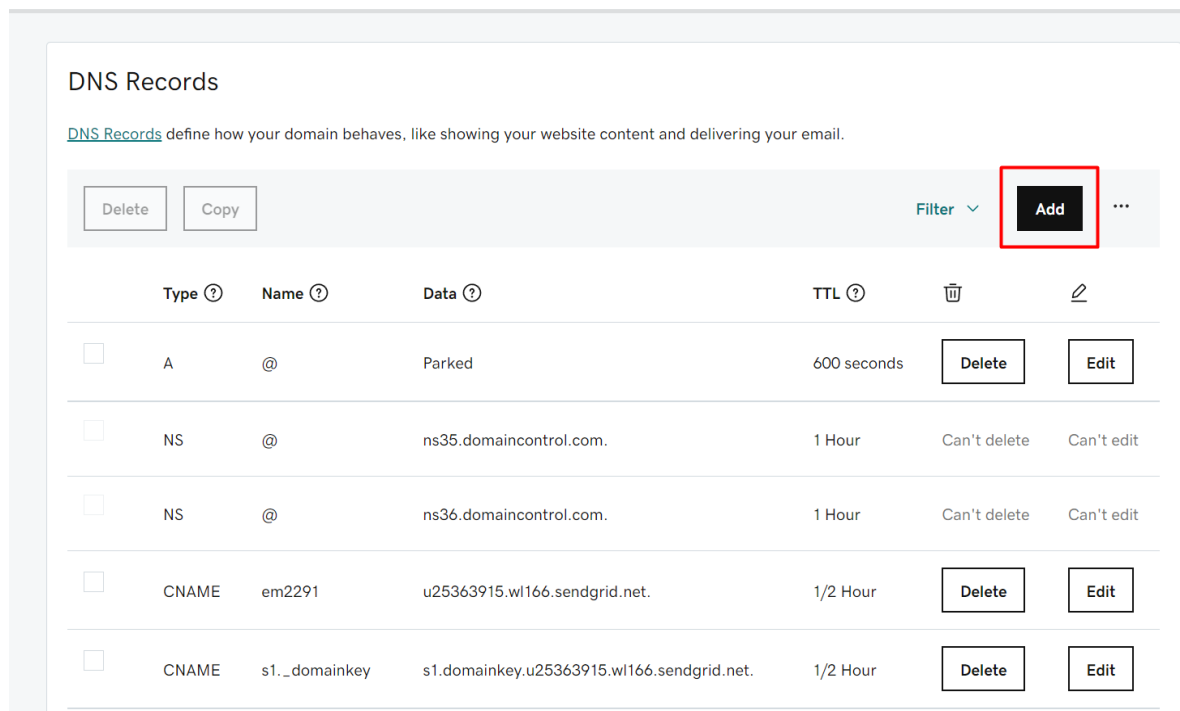


Рисунок 3.36 – Налаштування захисту від Fishing домену DMARC

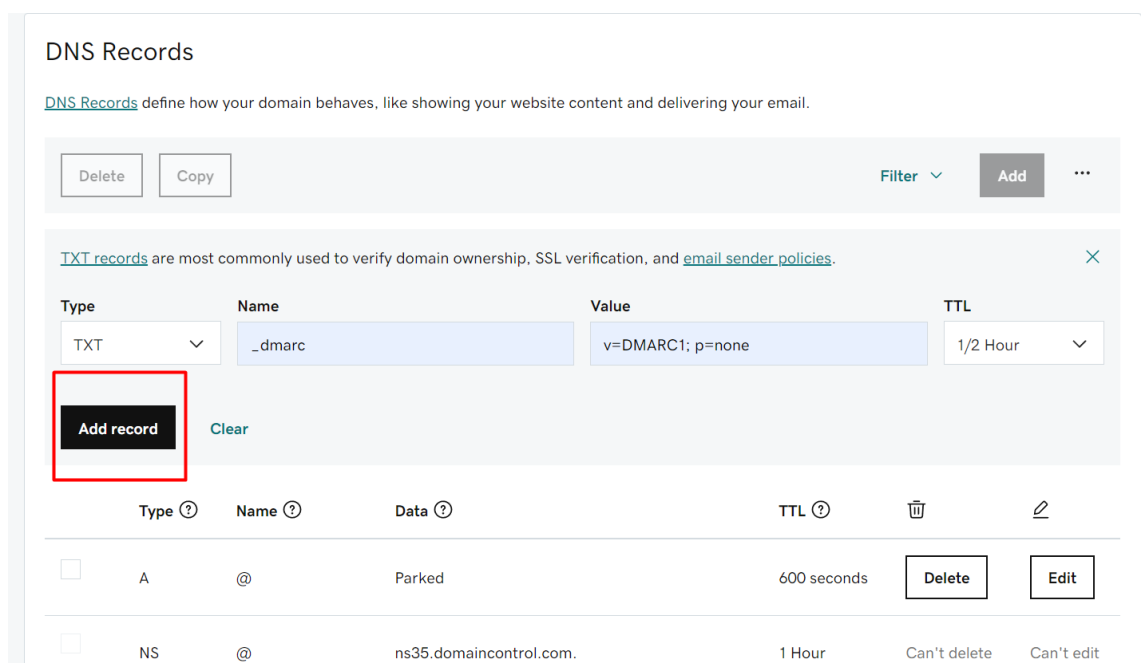


Рисунок 3.37 – Налаштування захисту від Fishing домену DMARC

resource records point to the services your domain uses, including web and email services. [Learn more about resource records](#)

Custom records
salesstaff.info/MX, salesstaff.info/SPF, and 6 more

[Manage custom records](#)

Host name	Type	TTL	Data
salesstaff.info	MX	1 hour	1 aspmx.l.google.com. 5 alt1.aspmx.l.google.com. 5 alt2.aspmx.l.google.com. 10 alt3.aspmx.l.google.com. 10 alt4.aspmx.l.google.com.
salesstaff.info	SPF	1 hour	"v=spf1 ip4:149.72.38.22 ip4:149.72.22.241 ip4:159.183.150.153 include:_spf.google.com ~all"
salesstaff.info	TXT	1 hour	"v=spf1 ip4:149.72.38.22 ip4:149.72.22.241 ip4:159.183.150.153 include:_spf.google.com ~all"
_dmarc.salesstaff.info	TXT	1 hour	"v=DMARC1; p=none; rua=mailto:dana@salesstaff.info; ruf=mailto:dana@salesstaff.info; fo=1:d:s"
em9224.salesstaff.info	CNAME	1 hour	u25481426.wl177.sendgrid.net. "v=DKIM1; k=rsa; p=MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0

Рисунок 3.38 – Налаштування захисту від Fishing домену DMARC

[+ Add more to this record](#)

s1._domainkey	CNAME	3600	s1._domainkey.u25481426.wl177.sendgrid.net.	
s2._domainkey	CNAME	3600	s2._domainkey.u25481426.wl177.sendgrid.net.	
_dmarc	TXT	3600	v=DMARC1; p=none	

[+ Add more to this record](#)

[Create new record](#) [Cancel](#) [Save](#)

Рисунок 3.39 – Налаштування захисту від Fishing домену DMARC

3.2 Тестування проекту підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik

Тестування підсистеми захисту гетерогенної мережі організації проводиться з метою перевірки налаштувань на відповідність поставленим завданням.

Перевіримо роботу інших DHCP серверів, зокрема чи видають вони адреси робочим станціям і чи виникає при цьому конфліктів, рис.3.40-3.43.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

```

PC1> IP DHCP
Bad command: "IP DHCP". Use ? for help.

PC1> ip dhcp
DORA IP 192.20.20.2/24 GW 192.20.20.1 D

```

Рисунок 3.40 – Перевірка DHCP серверу на CISCO-1

```

root@debian8-3:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:d0:38 brd ff:ff:ff:ff:ff:ff
    inet 192.20.20.2/24 brd 192.20.20.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed7:d038/64 scope link
        valid_lft forever preferred_lft forever
root@debian8-3:~#

```

Рисунок 3.41 – Перевірка DHCP серверу на CISCO-1

```

PC8> ip dhcp
DORA IP 192.30.30.3/24 GW 192.30.30.1

```

Рисунок 3.42 – Перевірка DHCP серверу на МІКРОТІК-1

```

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4187:8f6d:a7a2:28f5%13
    IPv4 Address. . . . . : 192.30.30.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.30.30.1

```

Рисунок 3.43 – Перевірка DHCP серверу на МІКРОТІК-1

Тепер спробуємо зайти під користувачем admin на маршрутизаторі CISCO-1 і перевіримо результат хешування у перехопленому повідомленні, рис.3.44–3.47.

```
=====
Device hostname -$(Cisco-1)
Your connection is -0
Enter Admin LOGIN and PSWD
=====

User Access Verification

Username: Anton
Password:
Cisco-1>
```

Рисунок 3.44 – Перевірка налаштувань користувачів на CISCO-1

```
=====
Device hostname -$(Cisco-1)
Your connection is -0
Enter Admin LOGIN and PSWD
=====

User Access Verification

Username: Administrator
Password:
Cisco-1>
```

Рисунок 3.45 – Перевірка налаштувань користувачів на CISCO-1

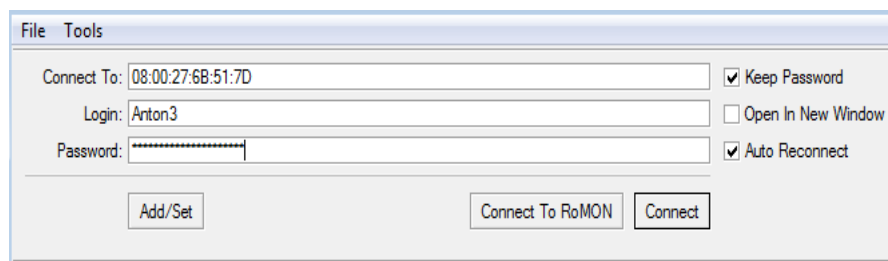


Рисунок 3.46 – Перевірка налаштувань користувачів на МІКРОТІК-1

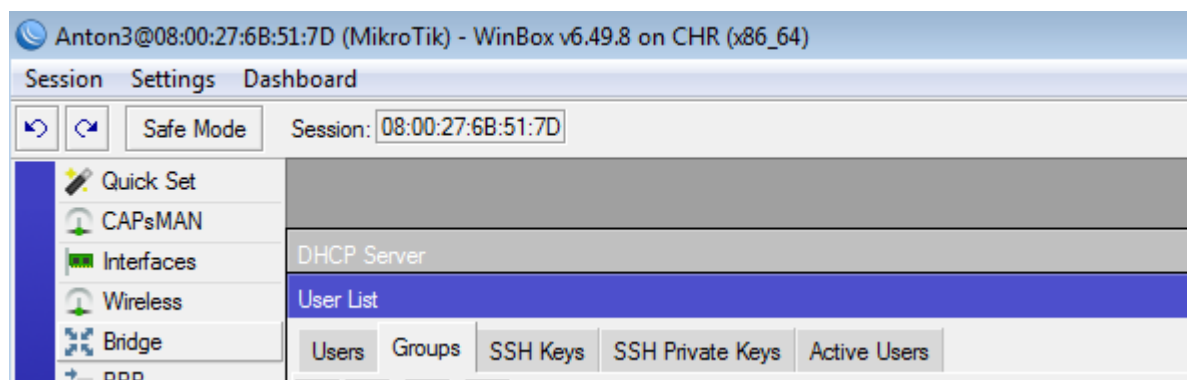


Рисунок 3.47 – Коректний вхід користувача на МІКРОТІК-1

Тепер перевіримо протокол маршрутизації OSPF за допомогою перевірки зв'язку між віддаленими мережами.

 PC1 - PuTTY

```

PC1> ping 192.30.30.2

84 bytes from 192.30.30.2 icmp_seq=1 ttl=64 time=0.629
84 bytes from 192.30.30.2 icmp_seq=2 ttl=64 time=0.573
84 bytes from 192.30.30.2 icmp_seq=3 ttl=64 time=0.586
84 bytes from 192.30.30.2 icmp_seq=4 ttl=64 time=0.602
84 bytes from 192.30.30.2 icmp_seq=5 ttl=64 time=0.584

```

Рисунок 3.48 – Перевірка зв'язку між LAN 1 та LAN 2

 PC1 - PuTTY

```

PC1> ping 192.40.40.2

84 bytes from 192.40.40.2 icmp_seq=1 ttl=64 time=0.596
84 bytes from 192.40.40.2 icmp_seq=2 ttl=64 time=0.630
84 bytes from 192.40.40.2 icmp_seq=3 ttl=64 time=0.560
84 bytes from 192.40.40.2 icmp_seq=4 ttl=64 time=0.559
84 bytes from 192.40.40.2 icmp_seq=5 ttl=64 time=0.585

```

Рисунок 3.49 – Перевірка зв'язку між LAN 1 та LAN 3

 PC1 - PuTTY

```

PC1> ping 192.50.50.2

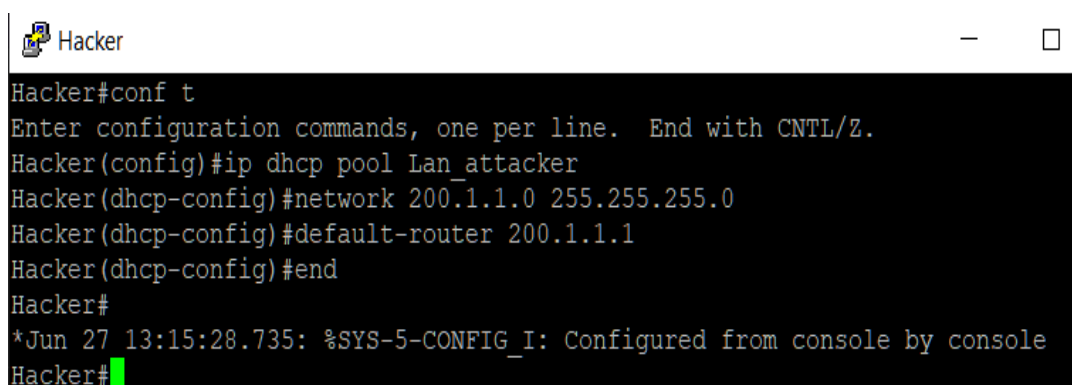
84 bytes from 192.50.50.2 icmp_seq=1 ttl=64 time=0.611
84 bytes from 192.50.50.2 icmp_seq=2 ttl=64 time=0.632
84 bytes from 192.50.50.2 icmp_seq=3 ttl=64 time=0.604
84 bytes from 192.50.50.2 icmp_seq=4 ttl=64 time=0.598
84 bytes from 192.50.50.2 icmp_seq=5 ttl=64 time=0.582

```

Рисунок 3.50 – Перевірка зв'язку між LAN 1 та LAN 4

Після всіх налаштувань захисту гетерогенної мережі потрібно перевірити їх правильність. Оскільки раніше вже перевіряли налаштування щодо користувачів, тепер потрібно протестувати налаштування довіреного порту.

Тепер перевіримо налаштування довіреного порту. Оскільки у нас довірений інтерфейс налаштований саме на e0/0, то тільки при підключенні до нього буде працювати DHCP-сервер. Створимо додатковий маршрутизатор і налаштуємо його як DHCP-сервер, рис.3.51.



```
Hacker#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Hacker(config)#ip dhcp pool Lan_attacker
Hacker(dhcp-config)#network 200.1.1.0 255.255.255.0
Hacker(dhcp-config)#default-router 200.1.1.1
Hacker(dhcp-config)#end
Hacker#
*Jun 27 13:15:28.735: %SYS-5-CONFIG_I: Configured from console by console
Hacker#
```

Рисунок 3.51 – Налаштування додаткового DHCP-серверу

Підключимо його до довіреного порту e2/1 і спробуємо отримати IP-адресу від нього. Як бачимо, саме через порт e2/1 ми отримуємо IP-адресу. Підключимо його тепер до будь-якого іншого порту, рис.3.52.



```
PC1> ip dhcp
DDD
Can't find dhcp server
PC1>
```

Рисунок 3.52 – Підключення сервера-зловмисника до недовіреного порту комутатору.

Як можна побачити, при підключенні до порту e0/1, який не є довіреним, комутатор не буде пропускати IP-адреси від серверу-зловмисника.

Перевірка захисту від Bruteforce, рис.3.53–3.55.

```
=====
Device hostname -$(Cisco-1)
Your connection is -0
Enter Admin LOGIN and PSWD
=====

User Access Verification

Username: Antin
Password:
% Login invalid
```

Рисунок 3.53. Перевірка захисту від Bruteforce на CISCO-1.

```
CISCO-1 con0 is now available

Press RETURN to get Started.
```

Рисунок 3.54. Перевірка захисту від Bruteforce на CISCO-1.

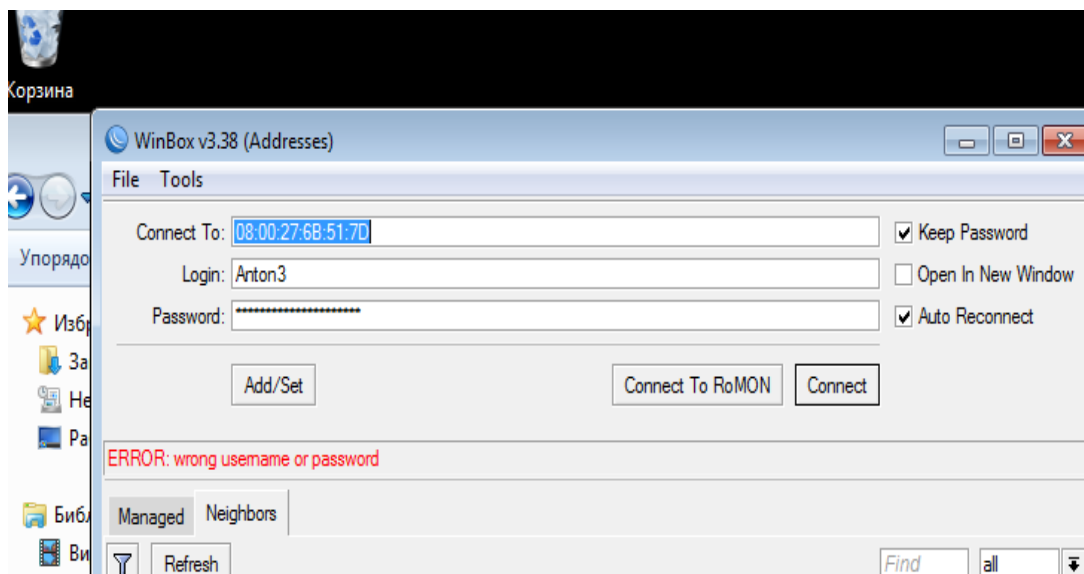


Рисунок 3.55 – Перевірка захисту від Bruteforce на МІКРОТІК-1

Після декількох некоректних введів паролю WinBox вимикається.
Перевірка налаштувань домену.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

При отриманні листа від неналаштованого домену при розборі листа можна побачити чи налаштовані всі записи (SPF, DKIM, DMARC), рис.3.56.

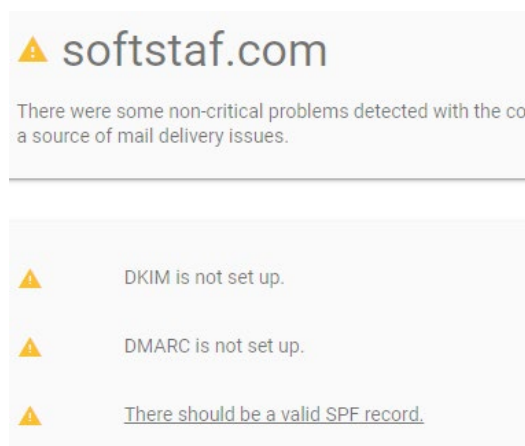


Рисунок 3.56 – Перевірка налаштувань домену

Після чого було перевірено лист від домена на якому налаштовано всі записи DNS (SPF, DKIM, DMARC), рис.3.57–3.58.



Рисунок 3.57 – Перевірка налаштувань домену

Исходное сообщение	
Идентификатор сообщения	<CAF3js9LSTDJ940b8nbHJQw_xP48xjrXJC_E0Wm-RDOXF_uk8LQ@mail.gmail.com>
Создано:	27 июня 2023 г., 12:22 (доставлено через 18 секунд)
От:	Anton Hryhorus <anton.hryhorus@salesnash.com>
Кому:	vovapet234@gmail.com
Тема:	Test
SPF:	PASS с IP-адресом 209.85.220.41 Подробнее...
DKIM:	'PASS', домен salesnash.com Подробнее...
DMARC:	'PASS' Подробнее...

Рисунок 3.58 – Перевірка налаштувань домену

3.3 Аналіз результатів тестування

Як і планувалося, всі вимоги, які ставились раніше, були успішно виконані. В майбутньому дана мережа може бути збільшена та покращена під якісь певні завдання. Для цього є всі можливості. DHCP допоможе при встановленні нових робочих станцій та пристроїв, рівень ядра, так як використовуються маршрутизатори фірми CISCO та MIKROTIK, є досить гнучкий для майбутніх налаштувань.

Щодо захисту, оскільки наша мережа використовує досить багато DHCP серверів, в нагоді став захист портів, оскільки при бажанні зловмисник міг би приєднатися до комутатору та давати свої IP-адреси, що призвело б до пошкодження мережі та тягнуло б за собою втрату даних з робочих станцій та мережі в цілому. Також захист на маршрутизаторах буде доцільний, якщо у зловмисника вийде приєднатися до маршрутизатора напямую. Це може тягнути за собою як втрату даних, так і знищення пристрою, підміну даних та інше.

Ще одна перевага мережі в тому, що на рівні ядра є 4 маршрутизатори, які з'єднані між собою і якщо один з них виходить з ладу, то за допомогою протоколу OSPF досить швидко знаходиться новий маршрут до потрібної мережі.

Щодо недоліків даної мережі, чим більш професійне та якісне обладнання, тим воно буде дорожче. Тобто комутатори та маршрутизатори від компанії CISCO є досить дорогими через їх надійність, якість, гарантію на заміну пристрою чи його компонентів при неполадках в малі строки, що досить вигідно великим компаніям, коли кожна хвилина коштує грошей. Також для налаштування та моніторингу стану приладів буде потрібно наймати працівника із знаннями цих пристроїв, тобто чим складніший та дорожчий пристрій, тим більше буде потрібна заробітна плата працівнику. Тому для невеликих компаній чи організацій мережа з використанням комутаторів та маршрутизаторів CISCO буде не вигідною і тому також використовуються маршрутизатори MIKROTIK.

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до розділу 3

В даному розділі було описано базові налаштування всіх пристроїв даної мережі. Була налаштована статична та динамічна (DHCP) маршрутизація. Для зручності використання та налаштування пристроїв було надано кожному особисту назву.

Для зв'язку між всіма підмережами схеми було використано протокол маршрутизації OSPF. Для захисту було налаштовано довірені порти, користувачів з різними привілеями, захист від Bruteforce і захист домену від фішингу.

Було проведено аналіз тестування та описано можливості масштабування та покращення мережі.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У дипломному проекті була спроектована ієрархічна модель комп'ютерної гетерогенної мережі на базі протоколу маршрутизації OSPF. Для побудови мережі використовувалися технології від компаній Cisco та MikroTik. При розробці були враховані всі вимоги до проекту, і було створено гетерогенну мережу на базі протоколу OSPF.

Для початку був проведений аналіз та вибір існуючих технологій побудови сучасних гетерогенних мереж. В результаті, були обрані графічний симулятор GNS3, операційні системи Debian, Ubuntu, Windows 7, Windows 10, протокол маршрутизації OSPF, а також технології прикладного рівня DHCP.

На етапі розробки мережі була визначена топологія мережі, враховуючи наявність багатьох робочих станцій. Для забезпечення масштабованості в майбутньому і зручності налаштування нових пристроїв було використано автоматичну видачу IP-адрес за допомогою DHCP.

Була спроектована логічна ієрархічна модель комп'ютерної мережі трьох рівнів, що складається з рівнів ядра, розподілу і доступу. Це дозволяє забезпечити масштабованість та надійність роботи мережі. Комп'ютерна мережа включає в себе вісім робочих станцій, з яких дві працюють під управлінням Windows 7 та Windows 10, дві - під управлінням Ubuntu та Debian, і вісім - у віртуальних робочих станцій VPCS, що запущені в програмі GNS3.

Для забезпечення масштабованості мережі в майбутньому використовуються образи комутаторів другого рівня з шістнадцятьма портами (образ i86bi-linux-l2-adventerprise-15.1b.bin). Для ядра мережі використовуються образи потужних та гнучких маршрутизаторів третього рівня від Cisco (образ i86bi-linux-l3-adventerprisek9-15.2.2.03T.bin) та MikroTik (образ RouterOS 6.39.2).

На третьому етапі проекту було обрано обладнання на програмне забезпечення. Були вибрані образи маршрутизаторів та комутаторів від компаній Cisco та MikroTik через їх надійність та гнучкість налаштувань. Також, оскільки протокол OSPF підтримується та використовується обома

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

фірмами, це забезпечує додаткову надійність системи. Програма GNS3 була обрана для виконання дипломного проекту через її можливість створення гетерогенних мереж за допомогою VirtualBox, що дозволяє використовувати різні операційні системи, такі як Windows, Linux та Ubuntu.

Були проведені налаштування пристроїв та аналіз результатів, і були сформовані висновки щодо модернізації та вдосконалення роботи мережі. Реалізована мережа є готовим макетом реальної реалізації проекту, а конфігурації можуть бути застосовані для реального обладнання.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гетерогенна комп'ютерна мережа [Електронний ресурс]. – https://uk.wikipedia.org/wiki/Гетерогенні_комп%27ютерні_мережі
2. Протокол OSPF [Електронний ресурс]. – <https://ru.wikipedia.org/wiki/OSPF>
3. Віддалена мережева атака [Електронний ресурс]. – https://uk.wikipedia.org/wiki/Віддалені_мережеві_атаки#Класифікація_атак
4. SPF [Електронний ресурс]. – <https://support.google.com/a/answer/33786?hl=en>
5. Mikrotik [Електронний ресурс]. – <https://uk.wikipedia.org/wiki/MikroTik>
6. Cisco [Електронний ресурс] – <https://ru.wikipedia.org/wiki/Cisco>
7. Налаштування DHCP [Електронний ресурс]. – <https://blog.sedicomm.com/2018/03/19/konfiguratsiya-dhcp-cisco/>
8. Трирівнева ієрархічна модель мережі [Електронний ресурс]. – <https://rci-c.com/technology/yerarkhycheskaia-model-sety/>
9. Windows 7 [Електронний ресурс]. – <https://learn.ztu.edu.ua/course/view.php?id=1898>
10. Windows 10 [Електронний ресурс]. – <https://learn.ztu.edu.ua/course/view.php?id=4144>
11. Debian [Електронний ресурс]. – <https://learn.ztu.edu.ua/course/view.php?id=1898>
12. Ubuntu [Електронний ресурс]. – <https://learn.ztu.edu.ua/course/view.php?id=1898>
13. Налаштування Mikrotik [Електронний ресурс]. – <https://настройка-микротик.укр/kak-nastroit-router-mikrotik-bazovaya-konfiguracziya/>
14. VirtualBox [Електронний ресурс]. – <https://www.virtualbox.org>
15. GNS3 [Електронний ресурс]. – <https://www.gns3.com>
16. WinBox [Електронний ресурс]. – <https://mikrotik.com/download>

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

17. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. Том 2. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
18. Тарнавський Ю. А., Кузьменко І. М. Організація комп'ютерних мереж / Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.
19. Todd Lamle. CCNA Routing and Switching Complete Study Guide, 2016
20. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco: навчальний посібник. [Текст] / А.А. Єфіменко. – Житомир : Державний університет «Житомирська політехніка», 2021. – 116 с.

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор CISCO-1

```

# CISCO-1#show running-config
Building configuration...

Current configuration : 5792 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CISCO-1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip icmp rate-limit unreachable
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
!
!
ip dhcp pool LAN-1
network 192.20.20.0 255.255.255.0
default-router 192.20.20.1
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout
!
username Anton2 privilege 4 secret 5 $1$S2NS$p9b6C3KdGf2U8y5cdPBF41
username Anton secret 5 $1$5Bhh$jFa43ilv4m/VEaxe2BSP.
username Administrator privilege 15 secret 5 $1$kMhB$9mdAltLY4daR60/Q5WfY1
!
redundancy
!
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 192.1.2.1 255.255.255.252
!
interface Ethernet0/2

```

		Григорусь А.М.			KIK.KP.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

router OSPF 1
network 192.1.1.0 0.0.0.3 area 0
network 192.1.2.0 0.0.0.3 area 0
network 192.1.5.0 0.0.0.3 area 0
network 192.1.6.0 0.0.0.3 area 0
network 192.20.20.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
privilege interface level 4 shutdown
privilege interface level 4 description
privilege configure level 4 interface
privilege exec level 4 configure
privilege exec level 1 show ip route
privilege exec level 1 show ip
privilege exec level 1 show running-config
privilege exec level 1 show interfaces
privilege exec level 1 show
banner login ^C=====
Device hostname -$(CISCO-1)
Your connection is -$(line)
Enter Admin LOGIN and PSWD
=====^C
!
line con 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4 login

```

		Григорусь А.М.			КІК.КР.Б - 125 - 04 - ПЗ	Арк.
		Воротніков В.В.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики віртуальної машини Mikrotik

Общие

Имя: Mikrotik
ОС: Turbolinux (64-bit)

Система

Оперативная память: 512 МБ
Порядок загрузки: Гибкий диск, Оптический диск, Жёсткий диск
Ускорение: Nested Paging, Паравиртуализация KVM

Дисплей

Видеопамять: 16 МБ
Графический контроллер: VMSVGA
Сервер удалённого дисплея: Выключен
Запись: Выключена

Носители

Контроллер: IDE
Вторичное устройство IDE 0: [Оптический привод] Пусто
Контроллер: SATA
SATA порт 0: chr-6.49.8.vdi (Обычный, 64,00 МБ)

Пreview

Microtik

Технічні характеристики віртуальної машини Ubuntu

Общие

Имя: Ubuntu-22-04
ОС: Ubuntu (64-bit)

Система

Оперативная память: 3072 МБ
Процессоры: 2
Порядок загрузки: Гибкий диск, Оптический диск, Жёсткий диск
Ускорение: Nested Paging, Паравиртуализация KVM

Дисплей

Видеопамять: 32 МБ
Графический контроллер: VMSVGA
Ускорение: 3D-ускорение
Сервер удалённого дисплея: Выключен
Запись: Выключена

Носители

Контроллер: IDE
Вторичное устройство IDE 0: [Оптический привод] Пусто
Контроллер: SATA
SATA порт 0: Ubuntu-22-04-disk001.vdi (Обычный, 25,00 ГБ)

Пreview

Ubuntu-22-04

Технічні характеристики віртуальної машини Debian

Общие

Имя: Debian8-3
ОС: Debian (32-bit)

Система

Оперативная память: 1024 МБ
Порядок загрузки: Гибкий диск, Оптический диск, Жёсткий диск
Ускорение: Nested Paging, Паравиртуализация KVM

Дисплей

Видеопамять: 16 МБ
Графический контроллер: VBoxVGA
Сервер удалённого дисплея: Выключен
Запись: Выключена

Носители

Контроллер: IDE
Первичное устройство IDE 1: [Оптический привод] Пусто
Контроллер: SATA
SATA порт 0: Debian8-3-disk1.vdi (Обычный, 8,00 ГБ)

Пreview

Debian8-3

		Григорусь А.М.			KIK.KP.B - 125 - 04 - ПЗ	Арк.
		Воротников В.В.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики віртуальної машини Windows7

Общие

Имя: Windows_7-32
ОС: Windows 7 (32-bit)

Система

Оперативная память: 1024 МБ
Порядок загрузки: Гибкий диск, Оптический диск, Жесткий диск
Ускорение: Nested Paging, Паравиртуализация Hyper-V

Дисплей

Видеопамять: 27 МБ
Графический контроллер: VBoxVGA
Сервер удаленного дисплея: Выключен
Запись: Выключена

Носители

Контроллер: SATA
SATA порт 0: Windows_7-32-disk001.vdi (Обычный, 100,00 ГБ)
SATA порт 1: [Оптический привод] VBoxGuestAdditions.iso (51,01 МБ)

Пreview

Windows_7-32

Технічні характеристики віртуальної машини Windows10

Общие

Имя: Windows_10_64_bits
ОС: Windows 10 (64-bit)

Система

Оперативная память: 2048 МБ
Порядок загрузки: Гибкий диск, Оптический диск, Жесткий диск
Ускорение: Nested Paging, Паравиртуализация Hyper-V

Дисплей

Видеопамять: 128 МБ
Графический контроллер: VBoxSVGA
Сервер удаленного дисплея: Выключен
Запись: Выключена

Носители

Контроллер: SATA
SATA порт 0: Windows_10_64_bit-disk001.vdi (Обычный, 20,00 ГБ)
SATA порт 1: [Оптический привод] Пусто

Пreview

Windows_10_64_bits