

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 магістра
на тему:

«Проект підсистеми захисту мережної інфраструктури
підприємства, побудованої на базі обладнання Cisco та Mikrotik»

Виконав студент 2-го курсу, групи КБм-21-1
спеціальності 125 «Кібербезпека»

 Уваров М.С.

Керівник доктор технічних наук, доцент,
професор кафедри комп'ютерної інженерії та
кібербезпеки

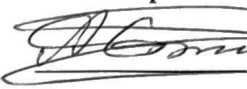
 Воротніков В.В.

Рецензент кандидат технічних наук, доцент,
завідувач кафедри комп'ютерної інженерії та
кібербезпеки

 Єфіменко А.А.

Житомир 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
 Єфіменко А. А.
«25» жовтня 2022 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу

Студента Уварова Микити Сергійовича

Тема роботи: Проект підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik
затверджена Наказом по університету від «25» жовтня 2022 р. № 501/С
Термін здачі студентом закінченої роботи – «19» грудня 2022 р.

Вихідні дані для роботи:

- 1. Фізична топологія мережі
- 2. Логічна топологія мережі
- 3. Маршрутизатори Cisco та MikroTik
- 4. Комутатори Cisco та MikroTik
- 5. Операційні системи Cisco IOS, RouterOS, Windows 7, Debian, Windows 8 Lite, TinyCore.
- 6. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Воротніков В.В		
2	Воротніков В.В		
3	Воротніков В.В		

Керівник  Воротніков В.В

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	25 жовтня 2022 – 30 жовтня 2022	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	30 жовтня 2022 – 3 листопада 2022	Виконано
3	Аналіз технологій захисту мережі за допомогою налаштувань на маршрутизаторах CISCO та MIKROTIK	4 листопада 2022 – 9 листопада 2022	Виконано
4	Аналіз можливостей мережного обладнання Cisco та MIKROTIK для гетерогенності мережі	10 листопада 2022 – 14 листопада 2022	Виконано
5	Розробка загального проекту мережі організації	15 листопада 2022 – 12 листопада 2022	Виконано
6	Проектування мережі та вибір обладнання для її реалізації	13 листопада 2022 – 19 листопада 2022	Виконано
7	Проектування таблиці маршрутизації	20 листопада 2022 – 24 листопада 2022	Виконано
8	Проектування сценарію тестування мережі	25 листопада 2022 – 29 листопада 2022	Виконано
9	Базове налагодження пристроїв мережі	30 листопада 2022 – 4 грудня 2022	Виконано
10	Налагодження гетерогенної мережі	4 грудня 2022 – 5 грудня 2022	Виконано
11	Тестування роботи гетерогенної мережі	6 грудня 2022 – 8 грудня 2022	Виконано
12	Аналіз результатів тестування	9 грудня 2022 – 11 грудня 2022	Виконано
13	Написання пояснювальної записки	12 грудня 2022 – 14 грудня 2022	Виконано
14	Підготовка презентації та виступу	15 грудня 2022 – 16 грудня 2022	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	17 грудня 2022 – 23 грудня 2022	Виконано
16	Захист	24 грудня 2022	Виконано

Студент  Уваров М.С.
Керівник  Воротніков В.В.

РЕФЕРАТ

Кваліфікаційна робота складається з Проект підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik та пояснювальної записки до нього. Пояснювальна записка містить 70 сторінки, 72 ілюстрації та 13 таблиць.

Кваліфікаційна робота присвячений розробці підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik. Метою проекту буде надійність, ефективність та захищеність комп'ютерної мережі. Наша мережа має забезпечувати безперервний обмін даними та постійний зв'язок з робочими машинами. Також для захисту на маршрутизаторах буде налаштовано користувачів з різними рівнями привілеїв для різних типів доступу і захист від BrutForce. Окремо буде показано захист домену від фішингових атак.

Кваліфікаційна робота буде складатися з трьох розділів, які включатимуть в себе розробку логічної та фізичної структури мережі, вибір мережевого обладнання та ПЗ, сценарій налаштування мережі та тестування проекту. В додатках буде вказано конфігурації маршрутизаторів та комутаторів мережі.

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

					КБ.КВ.Б – 125 – 22 – ПЗ			
Зм.	Арк.	№ докум	Підпис	Дата	Проект підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik Пояснювальна записка	Літ.	Арк.	Аркуші
Розроб.		Уваров М.С.		19.12				
Керівник		Воротников В.В.		19.12			4	70
Рецензент.		Байлюк С.М.		19.12		Державний університет «Житомирська політехніка», група КБм-21-1		
Зав. каф.		Ефіменко А. А.		19.12				

ABSTRACT

Qualifying work consists of the project of the subsystem for the protection of the enterprise`s network infrastructure, built on the basis of Cisco and Mikrotik network devices and explanatory note text. Explanatory note includes 70 pages, 72 pictures and 13 tables.

Qualifying work is devoted to the development project of a subsystem for the protection of the enterprise`s network infrastructure, built on the basis of Cisco and Mikrotik network devices. The goal of the project will be the reliability, efficiency and security of the computer network. Our network must provide continuous data exchange and constant communication with working machines. Also, for protection on routers, users with different levels of privileges will be configured for different types of access and protection against BrutForce. Domain protection against phishing attacks will be shown separately.

Qualifying work will consist of three sections, which will include the development of the logical and physical structure of the network, the selection of network devices and software, the network setup configuration, and project testing. The additions will indicate the configurations of routers and network switches.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ	4
ABSTRACT	5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ ТА ВИМОГИ ДО НЕЇ.....	10
1.1 Особливості побудови гетерогенної мережі.....	10
1.2 Протокол маршрутизації OSPF.....	11
1.3 Теоретичні відомості щодо можливих типів атак на мережу	13
1.4 Захист від можливих атак	19
РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ	25
2.1 Принципи роботи мережі.....	25
2.2 Розробка логічної структури мережі.....	27
2.3 Проект підсистеми, вибір обладнання та програмного забезпечення...	32
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА, ПОБУДОВАНОЇ НА БАЗІ ОБЛАДНАННЯ CISCO ТА МІКРОТІК.	38
3.1 Налаштування мережі.....	38
3.2 Тестування проекту підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik	52
3.3 Аналіз результатів тестування	60
ВИСНОВКИ	62
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	64
ДОДАТКИ.....	66

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

GNS3 – Graphical Network Simulator-3

AD – Active directory

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В сучасному світі без комп'ютерних мереж ні одна організація не зможе повноцінно та швидко функціонувати. Ефективність управління мережею комп'ютерів багато в чому залежить від правильності та грамотності її налаштування та складання коректної схеми маршрутизації та її захисту від зовнішніх загроз. Також для різних завдань не завжди буде підходити одна операційна система. Іноді виникає необхідність використання інших систем у зв'язку з вимогами різних програмних забезпечень.

Створення комп'ютерної мережі для різних організацій, компаній, підприємств є досить трудомістким процесом, який вимагає багато затраченого часу та сконцентрованості для правильної та злагодженої роботи всієї системи разом. Кожна компанія зазвичай має наявності в будь-якому випадку декілька комутаторів, маршрутизаторів, робочих станцій.

Оскільки комп'ютерна мережа буде використовуватися системою робочих станцій та мати вихід до мережі інтернет то необхідно буде також продумати можливі атаки на нашу мережу.

Також оскільки мережа буде складатися з великої кількості пристроїв, доцільним стане налаштування динамічної IP-адресації, оскільки також час від часу техніка може виходити з ладу або виникне необхідність у підключенні нових робочих станцій. Крім того, не зайвим буде використовувати різні привілеї доступу для різних рівнів працівників, оскільки не можна дозволяти будь-кому використовувати всі можливості комп'ютерної мережі. Мати доступ до всіх налаштувань комутаторів, маршрутизаторів, серверів та робочих станцій буде тільки одна-дві людини, які формуватимуть звіти та відповідатимуть за стан пристроїв в цілому.

Так як будь-яка система може викликати інтерес у зловмисників чи конкурентів, виникає необхідність у забезпеченні захисту даних організації. Відповідно нашу систему потрібно буде також захистити або мінімізувати збитки від зловмисного впливу за допомогою різних можливостей захисту від

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

компанії CISCO та MIKROTIK, так як комутатори та маршрутизатори саме цих фірм будуть використані під час налаштування схеми.

Для практичної реалізації підсистеми буде використовуватися графічний симулятор GNS3. Щоб забезпечити гетерогенність мережі використовуватимуться різні версії операційних систем Windows та Linux.

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

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 мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik.

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

В процесі виконання кваліфікаційної роботи був розроблений проект підсистеми захисту мережної інфраструктури підприємства, побудованої на базі обладнання Cisco та Mikrotik.

Апробація результатів:

1. Уваров М.С., Єфіменко А.А., Вакалюк Т.А. Проект підсистеми захисту гетерогенної мережі організації на базі пристроїв Mikrotik та CISCO // Тези IV Всеукраїнської науково-технічної конференції «Комп’ютерні технології: інновації, проблеми, рішення» «Комп’ютерна інженерія та кібербезпека», м. Житомир, 18-20 листопада 2021 року. – Житомир: Житомирська політехніка, 2021

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ ТА ВИМОГИ ДО НЕЇ

1.1 Особливості побудови гетерогенної мережі

Гетерогенна мережа з віддаленими робочими столами використовується для з'єднання між собою декількох LAN на невеликій території і надає можливість працювати з віддаленими мережами за допомогою віддалених робочих столів. Метою створення гетерогенної мережі є доступ до ресурсів всіх робочих станцій як і в LAN, так і в віддаленій мережі.[1]

До основних компонентів гетерогенної мережі будуть відноситися:

- робочі станції під управлінням різних ОС (Windows, Linux);
- комутатори;
- маршрутизатори;
- програмне забезпечення мережі.

В гетерогенній мережі використовується два види робочих станцій:

1. Клієнтська, яка буде отримувати через мережу доступ до інших робочих станцій і через віддалений доступ до головної робочої станції.
2. Головна(ядро), яка містить всі основні ресурси мережі і доступна лише користувачам, яким надано доступ[1].

Також мережа може бути одноранговою або з виділеним сервером, в залежності від того, який тип робочих станцій вона буде містити. Розглянемо всі переваги та недоліки таких мереж.

В одноранговій комп'ютерній мережі не буде якогось основного центру зберігання даних, керування мережею та забезпечення взаємодії між робочими станціями. Мережеве завдання буде розподілене між всіма пристроями. Кожний комп'ютер може виконувати як функції серверу, так і функції клієнта.

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

Він може приймати та обробляти дані, запити від інших робочих станцій, а також відправляти свої дані та запити до інших пристроїв.

До переваг однорангової комп'ютерної мережі належать:

- висока надійність;
- низька вартість.

Основними недоліками є:

- складність керування мережею - через те що в мережі немає як такого основного центру збору даних;
- складність в забезпеченні захисту інформації, оскільки налаштування будуть проводитися на всіх комутаторах, маршрутизаторах, робочих станціях окремо;
- працездатність, швидкість, ефективність роботи мережі напряму залежатимуть від кількості пристроїв і робочих станцій в мережі.

В комп'ютерній мережі з виділеним сервером вже буде робоча станція (сервер), яка виконуватиме функції збереження, керування, обробки і т.д.. Також вона призначена для використання всіма робочими станціями мережі.

Серед переваг можна виділити наступні:

- висока швидкість обробки інформації, оскільки все буде проходити через єдиний сервер;
- більш надійна система захисту інформації;
- відсутність обмеження по числу робочих станцій;
- простота адміністрування та керування системою.

До недоліків можна віднести:

- досить високу вартість, оскільки одна із станцій буде виділятися на сервер;
- швидкість та ефективність всієї системи буде залежати від потужності самого серверу.

1.2 Протокол маршрутизації OSPF

Протокол OSPF (Open Shortest Path First)[2] – це протокол найкоротшого шляху маршрутизації з виявленням маршрутів за станом зв'язку, розроблений

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк. 11
Змн.	Арк.	№ докум.	Підпис	Дата		

для IP мереж та працює на алгоритмі найкоротшого шляху, також являється протоколом внутрішніх шлюзів.

У мережах де використовується OSPF маршрутизатори підтримують одну і ту саму базу даних маршрутів, що описує топологію області. Кожен маршрутизатор або система в області створює свою базу даних інформації про стан каналів, яка складається з оголошень маршрутів, отриманих від усіх пристроїв в області за допомогою пакетів LSA. LSA – це пакет, що містить всі відомості про сусідні пристрої та оцінку шляху до кожного із них. Використовуючи бази даних із виявленням маршрутів за станом зв'язку, кожен маршрутизатор чи сервер з допомогою алгоритму пошуку найкоротшого шляху (SPF) будує остонове дерево шляхів, у якому коренем є сам маршрутизатор чи сервер.

Переваги протоколу OSPF

- Порівняно з іншими протоколами дистанційно-векторної маршрутизації, як протокол інформації про маршрутизацію (RIP), OSPF підходить до більших та неоднорідних мереж. OSPF дозволяє обчислювати шляхи маршрутизації за дуже короткий час, якщо змінюється топологія мережі.
- За допомогою протоколу OSPF можна розділити автономну систему (AS) на окремі області та обробляти їх топології окремо, щоб знизити потік маршрутизації OSPF та зменшити розмір бази даних маршрутів кожної області. OSPF забезпечує рівноцінну маршрутизацію з обхідними шляхами. За допомогою різних транзитних вузлів можна додавати додаткові маршрути до стек TCP.
- В протоколі OSPF відсутня обмеження досяжності пристроїв та він завжди обирає оптимальний шлях між пристроями.
- Протокол OSPF є також масштабованим і при додаванні нових пристроїв він просто будує нову таблицю маршрутизації.

Таймери протоколу

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

– HelloInterval — Інтервал часу в секундах після закінчення якого маршрутизатор відправляє наступний hello-пакет з інтерфейсу. Для широкомовних мереж і мереж точка-точка значення за замовчуванням, як правило, 10 секунд.

– RouterDeadInterval — Інтервал часу в секундах після закінчення якого сусід буде вважатися недосяжним. Цей інтервал повинен бути кратним значенню HelloInterval. Як правило, RouterDeadInterval дорівнює 4 інтервалам відправки hello-пакетів, тобто 40 секунд.

Принцип роботи протоколу OSPF

– Маршрутизатори відправляють один одному Hello-пакети.

– Після обміну Hello-пакетами кожен із маршрутизаторів додає сусіда в локальну таблицю мережі.

– Після створення локальних таблиць маршрутизатору відправляють посилення типу LSA (яке включає ідентифікатор самого маршрутизатору і його сусідів, метрику та тип мережі) сусідам та збирають інформацію з такими самими посиленнями від них.

– LSA відправляється кожному сусідові, який передає цей пакет далі по всій мережі.

– Після отримання пакету LSA кожен з маршрутизаторів додає свою інформацію яку він зібрав та передає далі по мережі і вносить зміни в локальну базу станів зв'язку між ними LSDB.

– Таблиця LSDB збирає та зберігає всі данні про всі пари маршрутизаторів всередині мережі.

– На основі всіх отриманих даних LSA будується повна карта мережі, яка в собі включає всі маршрутизатори та зв'язки між ними.

– Маючи таку карту мережі кожен з маршрутизаторів шукає найкоротший шлях до всіх мереж та підмереж і формує з них таблицю маршрутизації.

1.3 Теоретичні відомості щодо можливих типів атак на мережу

Розглянемо основні типи можливих атак на мережу

					КБ.КВ.Б – 125 – 22– ПЗ	Арк. 13
Змн.	Арк.	№ докум.	Підпис	Дата		

Credential Access (Доступ до облікових даних)[3]

Credential Access складається з методів викрадення облікових даних, таких як логіни облікових записів і паролі. Методи, які використовуються для отримання облікових даних, включають keylogin або скидання облікових даних. Використання законних облікових даних може надати хакеру доступ до систем, ускладнити їх виявлення та надати можливість створювати більше облікових записів, щоб допомогти досягти їхніх цілей.

Таблиця 1.1

Індекатор	Назва	Опис
T1557.003	DHCP Spoofing	Злочинці можуть перенаправляти мережевий трафік до систем, що належать їм, шляхом підміни трафіку динамічного протоколу конфігурації хоста (DHCP) і діючи як шкідливий DHCP-сервер у мережі жертв. Досягнувши позиції супротивника посередині (АіТМ), злочинець може збирати мережевий зв'язок, включаючи передані облікові дані, особливо ті, що надсилаються через незахищені, незашифровані протоколи. Це також може дозволити подальшу поведінку, таку як Network Sniffing або Transmitted Data Manipulation..
T1110	Brute Force	Злочинці можуть використовувати методи Brute Force, щоб отримати доступ до облікових записів, коли паролі невідомі. Не знаючи пароля для облікового запису або набору облікових записів, злочинець може систематично вгадувати пароль за допомогою повторюваного або ітераційного механізму. Перебір паролів може відбуватися через взаємодію зі службою, яка перевірить дійсність цих облікових даних в автономному режимі.
T1555	Credentials from Password Stores	Злочинці можуть шукати загальні місця зберігання паролів для отримання облікових даних користувача. Паролі зберігаються в декількох місцях системи, в

		залежності від операційної системи або програми, що містить облікові дані. Існують також спеціальні програми, які зберігають паролі, щоб полегшити користувачам керування. Після отримання облікових даних вони можуть бути використані для виконання для доступу до інформації з обмеженим доступом.
--	--	---

Discovery

Злочинець намагається з'ясувати ваше оточення. Відкриття складається з методів, які злочинець може використовувати для отримання знань про систему та внутрішню мережу. Ці методи допомагають супротивникам спостерігати за навколишнім середовищем і орієнтуватися, перш ніж вирішувати, як діяти. Вони також дозволяють злочинцям досліджувати, що вони можуть контролювати і що знаходиться навколо точки входу, щоб дізнатися, як це може принести користь їхній поточній меті. Вбудовані інструменти операційної системи часто використовуються для досягнення цієї мети збору інформації.

Таблиця 1.2

Індекатор	Назва	Опис
T1087	Account Discovery	Злочинці можуть намагатися отримати список облікових записів у системі. Ця інформація може допомогти злочинцям визначити, які облікові записи існують, щоб допомогти у подальших діях.
T1217	Browser Bookmark Discovery	Злочинці можуть перераховувати закладки браузера, щоб дізнатися більше про скомпрометовані хости. Закладки браузера можуть розкривати особисту інформацію про користувачів (наприклад, банківські сайти, соціальні мережі тощо), а також деталі про внутрішні мережеві ресурси, такі як сервери, інструменти / інформаційні панелі або інша пов'язана інфраструктура. Закладки браузера також можуть виділяти додаткові цілі після того, як

		супротивник отримає доступ до дійсних облікових даних, особливо облікових даних у файлах, пов'язаних із логінами, кешованими браузером. Конкретні місця зберігання залежать від платформи та/або програми.
T1083	File and Directory Discovery	Злочинці можуть перераховувати файли та каталоги або шукати в певних місцях хоста чи спільного доступу до мережі певну інформацію у файловій системі. Супротивники можуть використовувати інформацію з виявлення файлів і каталогів під час автоматичного виявлення для формування подальшої поведінки, включаючи те, чи повністю супротивник заражає ціль та/або намагається виконати конкретні дії. Для отримання цієї інформації можна використовувати багато утиліт командної оболонки.

Privilege Escalation

Ескалація привілеїв складається з методів, які злочинці використовують для отримання дозволів вищого рівня в системі або мережі. Злочинці часто можуть увійти в мережу з непривілейованим доступом і досліджувати її, але для досягнення своїх цілей потрібні розширені дозволи. Загальні підходи полягають у використанні переваг слабких місць системи, неправильних налаштувань та вразливостей. Приклади розширеного доступу включають:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

Таблиця 1.3

Індекатор	Назва	Опис
T1548	Abuse Elevation Control Mechanism	Злочинці можуть обходити механізми, призначені для контролю над підвищенням привілеїв, щоб отримати дозволи вищого рівня. Більшість сучасних систем містять нативні механізми контролю, які призначені для обмеження привілеїв, які користувач може виконувати на машині. Авторизація повинна бути надана конкретним користувачам, щоб виконувати завдання, які можна вважати більш ризикованими. Злочинець може виконувати кілька методів, щоб скористатися перевагами вбудованих механізмів управління з метою ескалації привілеїв у системі.
T1134	Access Token Manipulation	Злочинці можуть змінювати токени доступу, щоб вони працювали в іншому контексті безпеки користувача або системи, щоб виконувати дії та обходити контроль доступу. Windows використовує маркери доступу для визначення права власності на запущений процес. Користувач може маніпулювати маркерами доступу, щоб запущений процес виглядав так, ніби він є дочірнім елементом іншого процесу або належить комусь іншому, крім користувача, який розпочав процес. Коли це відбувається, процес також набуває контексту безпеки, пов'язаного з новим токеном.
T1547	Boot or Logon Autostart Execution	Злочинці можуть налаштувати параметри системи на автоматичне виконання програми під час завантаження системи або входу в систему, щоб отримати привілеї вищого рівня в скомпрометованих системах. Операційні системи можуть мати механізми автоматичного запуску

		програми під час завантаження системи або входу в обліковий запис.
--	--	--

Resource Development

Злочинець намагається створити ресурси, які вони можуть використовувати для підтримки операцій. Розробка ресурсів складається з методів, які передбачають створення, придбання або компрометацію/крадіжку ресурсів, які можуть бути використані для підтримки. Такі ресурси включають інфраструктуру, облікові записи. Злочинець може використовувати ці ресурси для допомоги на інших етапах життєвого циклу злочинця, наприклад, для використання придбаних доменів для підтримки командування і управління, облікових записів електронної пошти для фішингу в рамках початкового доступу або викрадення сертифікатів підпису коду, щоб допомогти з ухиленням від оборони.

Таблиця 1.4

Індекатор	Назва	Опис
T1583.001	Acquire Infrastructure: Domains	Злочинці можуть купувати домени, які можна використовувати під час націлювання. Доменні імена - це читабельні імена, які використовуються для представлення однієї або декількох IP-адрес. Їх можна придбати. Супротивники можуть використовувати придбані домени для різних цілей, зокрема для фішингу, компромісу з використанням дисків і командування й управління. Супротивники можуть вибирати домени, подібні до законних доменів, у тому числі шляхом використання іншого домену, саб-домену.
T1586.002	Compromise Accounts: Email Accounts	Злочинці можуть скомпрометувати облікові записи електронної пошти, які можна використовувати під час націлювання. Злочинці можуть використовувати скомпрометовані облікові записи електронної пошти для подальших операцій, наприклад,

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

		використовувати їх для фішингу. Використання існуючої особи з скомпрометованим обліковим записом електронної пошти може викликати рівень довіри до потенційної жертви, якщо вона має стосунки або знає про скомпрометовану особу. Скомпрометовані облікові записи електронної пошти також можна використовувати для придбання інфраструктури (наприклад, доменів).
T1584.001	Compromise Infrastructure: Domains	Злочинці можуть викрадати домени та/або субдомени, які можна використовувати під час націлювання. Викрадення реєстрації домену - це акт зміни реєстрації доменного імені без дозволу первісного реєстранта. Злочинці можуть отримати доступ до облікового запису електронної пошти для особи, зазначеної - як власник домену. Потім супротивник може стверджувати, що він забув свій пароль, щоб внести зміни в реєстрацію домену. Інші можливості включають соціальну інженерію, службу підтримки реєстрації домену, щоб отримати доступ до облікового запису або скористатися перевагами прогалин у процесі поновлення. Викрадення субдоменів може статися, коли організації мають записи DNS, які вказують на неіснуючі або депровізовані ресурси. У таких випадках супротивник може взяти під контроль субдомен для проведення операцій на користь довіри, пов'язаної з цим доменом.

1.4 Захист від можливих атак

З попереднього розділу де було розглянуто типи можливих загроз ми оббиратимемо декілька поширених типів атак.

– T1557.003 DHCP Spoofing

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

Як можна захиститися:

1. розглянути можливість фільтрації DHCP-трафіку на портах 67 і 68 до/з невідомих або ненадійних DHCP-серверів. Крім того, потрібно щоб було увімкнено стеження DHCP на 2 рівні комутаторів, оскільки це запобігатиме атакам підробки DHCP. Також необхідно вистежування доступних IP-адрес за допомогою сценарію або інструментів.
2. Крім того, потрібно блокувати трафік DHCPv6 і інформацію вхідних маршрутизаторів, особливо якщо IPv6 не використовується в мережі.

Перевірка і виявлення

Таблиця 1.5

Джерело даних	Компонент даних	Виявлення
Журнал додатків	Вміст журналу додатків	Відстежування журналу Windows (наприклад, EIDs 1341, 1342, 1020 та 1063) на предмет змін у налаштуваннях DHCP. Вони також можуть висвітлювати проблеми DHCP, такі як, розподіл IP-адрес може закінчитися.
Мережевий трафік	Вміст мережевого трафіку	Відстежування мережевого трафіку на предмет підозрілої/зловмисної поведінки, пов'язаної з DHCP, наприклад, зміни параметрів DNS та/або шлюзу. Крім того, відстежування мережевого трафіку для шахрайської активності DHCPv6
	Потік мережевого трафіку	Відстежування мережевого трафіку на наявність аномалій, пов'язаних з відомою поведінкою АІТМ. Розглядаємо моніторинг змін файлів конфігурації системи, що беруть участь у формуванні потоку мережевого трафіку.

— T1110 Brute Force

Як можна захиститися:

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк. 20
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Встановити політику блокування облікового запису після певної кількості невдалих спроб входу, щоб запобігти вгадуванню паролів. Занадто сувора політика може призвести до відмови в обслуговуванні та зробити середовище непридатним для використання.
2. Використовувати багатофакторну аутентифікацію. Де це можливо, також увімкніть багатофакторну автентифікацію на зовнішніх службах.
3. Примусове скидання облікових записів, які, як відомо, є частиною порушених облікових даних, або негайно, або після виявлення спроб Brute Force.

Перевірка і виявлення

Таблиця 1.6

Джерело даних	Компонент даних	Виявлення
Журнал додатків	Вміст журналу додатків	Відстежування журнали аутентифікації на наявність збоїв входу в систему. Якщо збої аутентифікації високі, то може бути спроба Brute Force отримати доступ до системи за допомогою облікових даних.
Команда	Виконання команд	Відстежування виконані команди та аргументи, які можуть використовувати методи Brute Force для отримання доступу до облікових записів, коли паролі невідомі або коли отримані хеші паролів.
Обліковий запис користувача	Автентифікація облікового запису користувача	Відстежування багато невдалих спроб автентифікації в різних облікових записах, які можуть бути результатом спроб введення пароля. Важко виявити, коли хеші зламані, оскільки це, як правило, робиться за межами цільової мережі.

- T1583.001 Acquire Infrastructure: Domains
- T1586.002 Compromise Accounts: Email Accounts

Як можна захиститися:

Змн.	Арк.	№ докум.	Підпис	Дата

Організації можуть навмисно реєструвати подібні домени на свої власні, щоб утримати супротивників від створення доменів, що порушують помилки. Інші аспекти цієї техніки не можуть бути легко пом'якшені превентивним контролем, оскільки вона базується на поведінці, що виконується поза сферою захисту та контролю підприємства.

Перевірка і виявлення

Таблиця 1.7

Джерело даних	Компонент даних	Виявлення
Доменне ім'я	Активний DNS	Відстежуйте дані реєстру системи доменних імен (DNS) для придбаних доменів, які можна використовувати під час можливих атак. Виявлення на основі репутації/категорії може бути складним. Зусилля з виявлення можуть бути зосереджені на суміжних етапах життєвого циклу злочинця, наприклад, під час початкового доступу та командування і управління.
	Реєстрація домену	Інформація про реєстрацію домену, за задумом, фіксується в публічних журналах реєстрації. Розглядати можливість використання сервісів, які можуть допомогти у відстеженні нових придбаних доменів, таких як бази даних WHOIS та/або пасивні DNS. У деяких випадках може бути можливим орієнтуватися на відомі фрагменти інформації про реєстрацію домену, щоб розкрити іншу інфраструктуру, придбану супротивником. Розглянути можливість моніторингу доменів, створених зі структурою, подібною до вашої власної, в тому числі під іншим TLD.
	Пасивний DNS	Відстежувати дані зареєстрованої системи доменних імен (DNS) для придбаних доменів, які можна використовувати під час атаки злочинця.

Цю методику не можна легко пом'якшити превентивним контролем, оскільки вона базується на поведінці, що виконується поза сферою захисту та контролю підприємства. Але можна перевіряти підозрілі e-mail листи на наявність налаштувань на домені відправника. Записи DNS такі як SPF, DKIM, DMARK.

SPF, DKIM, DMARK це є три стандарти аутентифікації всіх e-mail листів, які в свою чергу допомагають захистити електронні пошти організації від спуфінгу та фішингу.

SPF (Sender Policy Framework) – являється стандартним способом автентифікації електронної пошти. Цей запис DNS домагає захистити власний домен від підробки. SPF визначає поштові сервери, які зможуть відправляти листи від імені домену, і також поштові сервери які приймають листи також можуть перевіряти запис SPF для перевірки.[4]

DKIM (DomainKeys Identified Mail) – Це метод аутентифікації який являється цифровим підписом для електронних пошт. На серверах одержувачів пошти повідомлення, підписані за допомогою DKIM, вважаються надійними, оскільки DKIM гарантує фактичне надсилання повідомлень із вказаної адреси. DKIM також перевіряє, що вміст електронного листа не змінювався з моменту його надсилання.[5]

Використовуючи автентифікацію DKIM, ви збільшуєте ймовірність того, що законні повідомлення потраплять до папки "Вхідні" одержувача. Сервери на стороні одержувача отримують гарантію того, що електронні листи дійсно надсилаються з вашого домену.

DMARK (Domain-based Message Authentication, Reporting, and Conformance) – Спамери можуть надсилати підроблені електронні листи від імені вашого домену або вашої організації, видаючи себе за його

Змн.	Арк.	№ докум.	Підпис	Дата

представників. DMARC повідомляє поштовим серверам, що робити, коли вони отримують електронний лист, який, здається, був надісланий вашою організацією, але не автентифікований або не відповідає вимогам автентифікації у вашому записі правила DMARC. Якщо електронний лист не автентифіковано, можливо, його надіслали зловмисники від імені вашої організації або з підроблених серверів. DMARC завжди використовується разом з наступними двома методами аутентифікації: SPF та DKIM.[6]

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 та MIKROTİK.

Було розглянуто можливість встановлення різних типів захисту. Крім того, обрано протокол маршрутизації OSPF та протокол DHCP 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.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ

2.1 Принципи роботи мережі

При розробці мережі потрібно одразу логічно її структурувати. Дана підсистема буде складатися з декількох LAN.

При створенні даної мережі мають бути виконані наступні вимоги:

- створення підмережі з різними типами пристроїв від компанії CISCO та МІКТОТІК[7][8]
- використання різних операційних систем для гетерогенності мережі;
- забезпечення можливості працювати на віддалених робочих станціях;
- автоматичне отримання IP-адресації (DHCP) для кожної підмережі;
- захищеність підсистеми від дій зловмисників, конкурентів чи недбалості власних працівників.
- Налаштування DNS записів на домені для захисту від фішингу через пошту

При проектуванні схеми буде взято в розрахунок те що буде використовуватися мережі з середньою кількістю пристроїв, але будемо брати в розрахунок можливість масштабованості мережі. Потрібно забезпечити налаштування протоколу DHCP для автоматизації процесу IP-адресації, оскільки деякі робочі станції можуть як додаватися, так і виходити з ладу. Для цього буде розроблено декілька підмереж з різними DHCP-серверами та різними ОС (табл. 2.1).

Розподіл на підмережі буде здійснений за допомогою DHCP-серверів на базі маршрутизаторів. Окремі підмережі будуть налаштовані для зв'язку між маршрутизаторами рівня ядра.

Також потрібно розробити IP-топологию мережі. Оскільки в схемі буде досить багато підмереж, внутрішню адресацію забезпечуватиме протокол динамічного налаштування вузлів. Детальні параметри адресації наведено в табл. 2.2.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

Розподілення на підмережі пристроїв мережі

Назва мережі	Кількість робочих станцій	DHCP-сервер
LAN A	2 робочі станції (VPCS, Debian) (Можливість додавання робочих станцій)	Маршрутизатор
LAN B	2 робочі станції (VPCS, Win 8) (Можливість додавання робочих станцій)	Маршрутизатор
LAN C	2 робочі станції (VPCS, Tynucore) (Можливість додавання робочих станцій)	Маршрутизатор
LAN D	2 робочі станції (VPCS, Win 7) (Можливість додавання робочих станцій)	Маршрутизатор

Таблиця 2.2

Параметри адресації мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Підмережа A				
Комутатор SW-LAN-A	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC_1	E0	DHCP	255.255.255.0	/24
Робоча станція Debian	E0	DHCP	255.255.255.0	/24

Підмережа B				
Комутатор SW-LAN-B	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC_2	E0	DHCP	255.255.255.0	/24
Робоча станція Win-8	E0	DHCP	255.255.255.0	/24
Підмережа C				
Комутатор SW-LAN-C	Vlan 1	DHCP	255.255.255.0	/24
Робоча станція PC-3	E0	DHCP	255.255.255.0	/24
Робоча станція Tynucore	E0	DHCP	255.255.255.0	/24
Підмережа D				
Комутатор SW-LAN-D	Vlan 1	DHCP	255.255.255.0	/24

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		

Робоча станція PC-4	E0	DHCP	255.255.255.0	/24
Робоча станція Win-7	E0	DHCP	255.255.255.0	/24
Ядро мережі				
Маршрутизатор CISCO-R-1	E0/1	192.1.2.1	255.255.255.252	/30
	E0/2	192.1.1.1	255.255.255.252	/30
	E1/1	192.1.5.1	255.255.255.252	/30
	E1/2	192.1.6.1	255.255.255.252	/30
	E2/1	DHCP	255.255.255.0	/24
	E2/0	DHCP	255.255.255.0	/24
Маршрутизатор CISCO-R-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-R3	E1	192.1.3.1	255.255.255.252	/30
	E2	192.1.4.1	255.255.255.252	/30
	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
Маршрутизатор MIKROTIK-R4	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 буде використана трирівнева ієрархічна модель мережі, оскільки вона є надійною та високопродуктивною. Дана мережа складатиметься з 3-х рівнів: ядра, розподілу та доступу[11]. Перевагами такої структури є:

1. Масштабованість – можливість вдосконалювати систему в майбутньому.
2. Швидке усунення неполадок та швидке і просте управління.
3. Надійність – якщо з ладу виходить один із основних пристроїв то є запасний, який зможе виконувати його функції або якщо з ладу виходить один із зав'язків між маршрутизаторами на рівні ядра.
4. Швидка працездатність – ієрархічна структура дає можливість високої пропускної здатності.

Розберемо кожен з рівнів окремо. Рівень ядра відповідає за швидке транспортування між пристроями рівня розподілу, тобто між комутаторами мережі. На рівні ядра найчастіше використовують досить дорогі пристрої високого класу, і, якщо є можливість - високопродуктивні комутатори.

Рівень розподілу знаходиться посередині між рівнем ядра та доступу. Завдання даного рівня - забезпечувати маршрутизацію мережі, а також зв'язувати рівень ядра та доступу. Також на цьому рівні йде фільтрація ACLs та PBR. Основним завданням також є зменшення навантаження на мережу.

Рівень доступу зазвичай складається з комутаторів і точок доступу, які в свою чергу, дають можливість підключатися до робочих станцій, принтерів, IP-телефонів, серверів тощо. Щодо вимог до комутаторів, це, найчастіше, комутатори другого рівня через їх меншу вартість.

Загальний вигляд розробленої схеми разом із зазначенням вищевказаних рівнів наведено на рисунку 2.1.

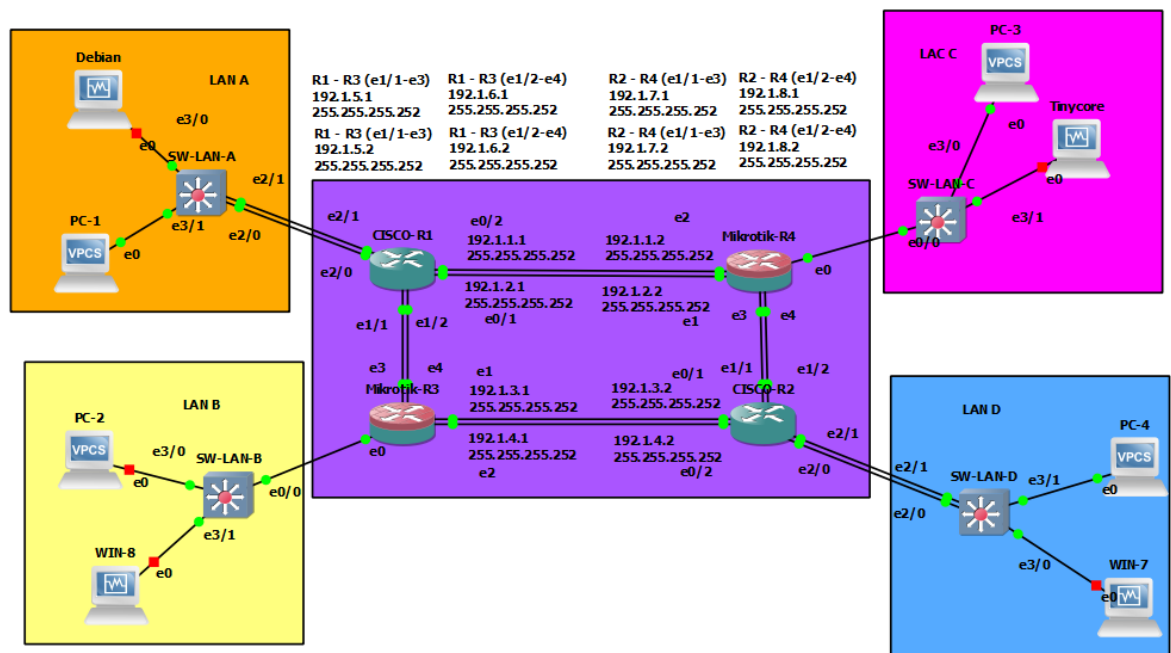


Рисунок 2.1. Трирівнева ієрархічна модель мережі

Детально розглянемо кожен з підмереж окремо. Зовнішній вигляд всіх LAN наведено на рисунках 2.2-2.6, пристрої, що входять до складу підмереж, зазначені в табл. 2.4-2.9.

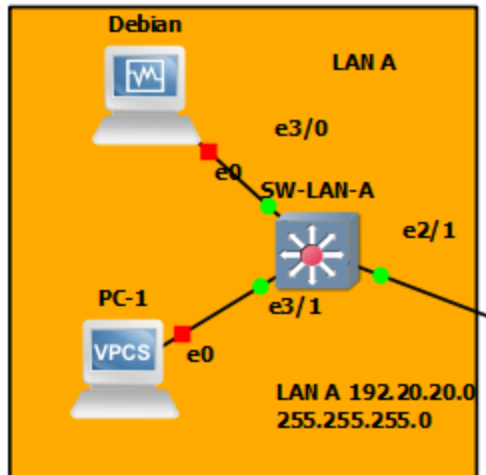


Рисунок2.2. Локальна мережа LAN А

Таблиця 2.3

Пристрої, що входять до складу LAN А

Робочі станції	Дві робочі станції - одна VPCS друга під управлінням ОС Debian
Комутатори	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

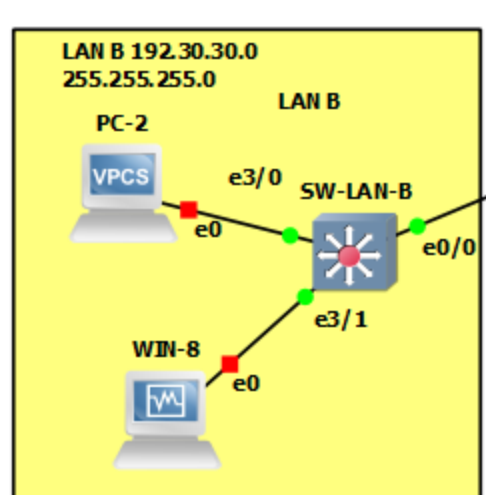


Рисунок2.3. Локальна мережа LAN В

Таблиця 2.4

Пристрої, що входять до складу LAN B

Робочі станції	Дві робочі станції - одна VPCS друга під управлінням ОС Windows 8 Lite
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

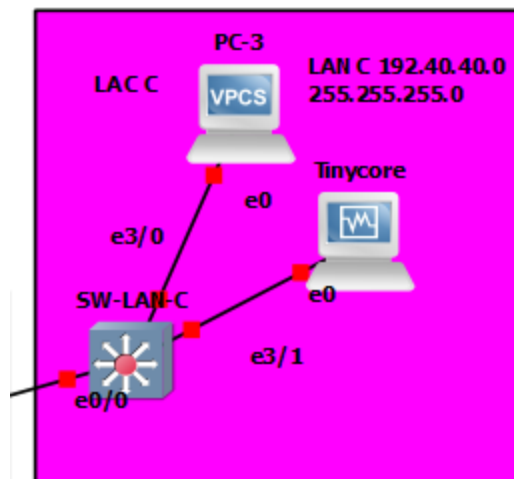


Рисунок2.4. Локальна мережа LAN C

Таблиця 2.5

Пристрої, що входять до складу LAN C

Робочі станції	Дві робочі станції - одна VPCS друга під управлінням ОС Tinycore
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

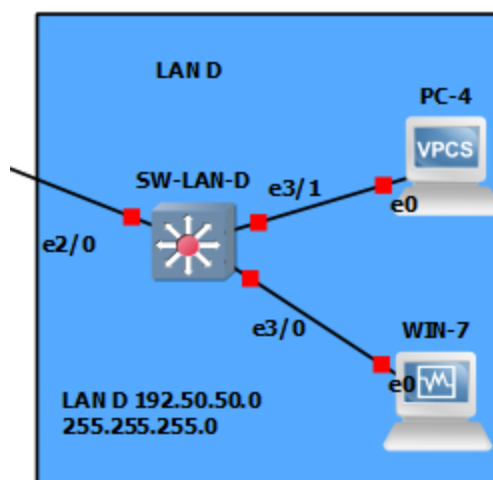


Рисунок2.5. Локальна мережа LAN D

Пристрої, що входять до складу LAN D

Робочі станції	Дві робочі станції - одна VPCS друга під управлінням ОС Windows 7
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

Окремо виділимо рівень ядра, що складається з двох маршрутизаторів CISCO (i86bi-linux-l3-adventerprisek9-15.2.2.03T.bin) та двох маршрутизаторів фірми Mikrotik (chr-6.39.2.img). Його зовнішній вигляд відображає рисунок 2.8.

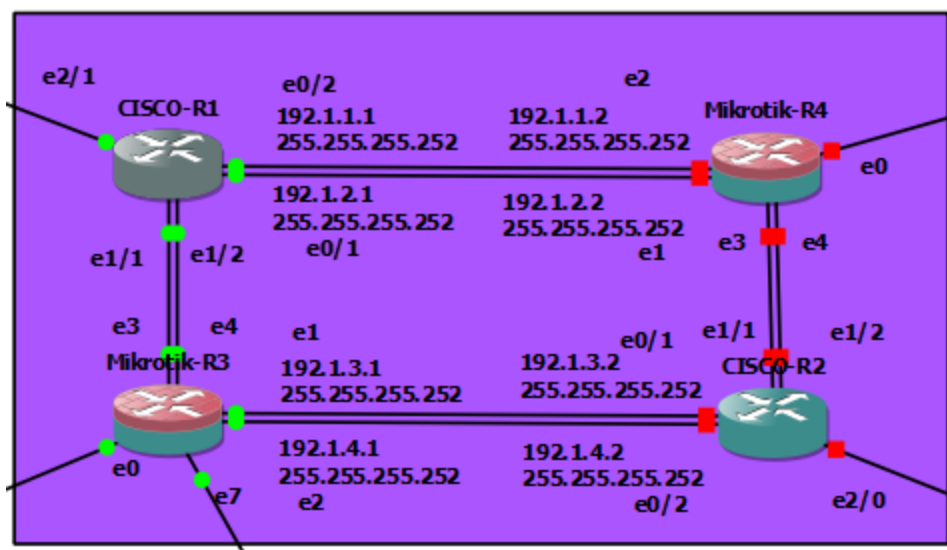


Рисунок2.6. Рівень ядра

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.

Для нормалізування роботи всієї мережі буде використано протокол зв'язку OSPF, оскільки він досить надійний, і при виникненні проблем із зв'язком досить швидко повідомляє про це інші пристрої в мережі та знаходить альтернативні шляхи до потрібного пристрою. До того ж на рівні

ядра будуть проведені додаткові зв'язки для забезпечення стабільної роботи якщо відмовить один з основних зав'язків.

2.3 Проект підсистеми, вибір обладнання та програмного забезпечення.

Відповідно до потреб, що зазначені вище, сформовано такі вимоги до програмно-апаратного забезпечення:

1. Вибір наступних операційних систем: Windows 7[12], Windows 8 Lite[13], Debian[14], Tinycore[15].
2. Наявність захисту від Credential Access, Privilege Escalation, Resource Development (тобто загроз розглянутих в розділі 1.3)

Для реалізації схеми будемо використовувати обладнання фірми CISCO та mikrotik. Основними перевагами CISCO перед іншими компаніями є:

1. Надійність обладнання – компанія CISCO перевірена роками і мільйонами трафіку інформації. Вона використовує лише якісні компоненти та матеріали починаючи від корпусу приладу і закінчуючи системою охолодження.
2. CISCO пропонує досить великий вибір приладів – рішення для малих компаній, бізнесів, а також для провайдерів інтернету та великих корпорацій [15].
3. Можливість різного налаштування – навіть на базі одного приладу є можливість реалізувати різні завдання, наприклад, маршрутизацію, комутацію, налаштування сервера, голосові сервіси, захист від різних типів атак. Найчастіше вистачає буквально декілька команд для того, щоб прилад міг виконувати ще якусь додаткову роботу, і вже не буде потреби в придбанні додаткового пристрою.
4. Рівень підтримки пристроїв CISCO – якщо потрібна допомога в налаштуванні пристроїв CISCO, то вся інформація є на офіційному сайті компанії CISCO.COM. Там можна знайти все, що буде потрібно системному адміністратору для налагодження: від опису моделі та її характеристик до повної документації щодо налаштувань різних можливостей

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

5. Рівень гарантії пристроїв – компанія CISCO пропонує гарантії на будь-які прилади, в тому числі і старі, і майже на будь-який термін. При покупці гарантії від CISCO, при несправності приладу компанія зробить повну заміну пристрою чи зламаної його частини протягом 4-8 годин. Для великих компаній, які користуються приладами CISCO, така гарантія є необхідною.

Основними перевагами фірми mikrotik є

1. Маршрутизатори фірми mikrotik мають свою власну ОС (Router OS)[19] і це можливість обирати модель тільки за апаратними характеристиками оскільки навіть найдешевший маршрутизатор зможе виконувати будь-які мережеві функції.
2. Маршрутизатори фірми mikrotik мають європейську якість складання та гарантує довгу та стабільну роботу без перебоїв.
3. Маршрутизатори фірми mikrotik мають різну цінову категорію що дає можливість обирати саме той варіант який підійде будь-якій за розміром та потребам компанії.
4. Навіть якщо модель маршрутизатора mikrotik була знята з виробництва все одно виробник буде забезпечувати її новими ПЗ.
5. Модельний ряд маршрутизаторів mikrotik містить в собі рішення для будь-якого сегмента мереж. Оскільки їх система забезпечує просту можливість перенесення конфігураційних файлів, а також простоту в налаштуванні.

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 невеликих бізнесів. Тому ми будемо використовувати образи маршрутизатора серії 4000(CISCO) [20] (Рисунок2.9), комутатора 9300(CISCO)[21](Рисунок2.10) та маршрутизатор MIKROTIK під управлінням RouterOS(6.39.2)(Рисунок2.11).

Для створення моделі комп'ютерної гетерогенної мережі з можливістю віддалених робочих столів будемо використовувати програму GNS3.

					КБ.КВ.Б – 125 – 22– ПЗ	Арк. 33
Змн.	Арк.	№ докум.	Підпис	Дата		

Додатково використовується програма VirtualBox[22], а також WireShark[23] для перевірки трафіку в нашій мережі.



Рисунок 2.7. Маршрутизатор останньої серії (Cisco 4000 Series Integrated Services Routers)



Рисунок 2.8. Комутатор останньої серії (Cisco Catalyst серії 9300)



Рисунок 2.9. Маршрутизатор останньої серії (MikroTik RB4011iGS)

GNS3 (Graphical Network Simulator) – це графічний симулятор мережі. Він дає можливість створювати різні мережі, проводити їх тестування, захищати і тощо прямо на комп’ютері. Головною перевагою є те, що GNS3 дозволяє розробляти саме гетерогенні мережі за рахунок додавання різного обладнання з різними образами, такими як Cisco, Juniper, Mikrotik, CheckPoint та ін. Тобто цей симулятор дає можливість запускати операційні системи різних виробників прямо в одній системі. Наприклад, при додаванні маршрутизатора Cisco або MikroTik в GNS3, запускається реальна операційна система Cisco IOS або RouterOS. Таким чином ми отримуємо повноцінний маршрутизатори Cisco та MikroTik. Тепер перерахуємо переваги та недоліки GNS3[25].

Головна перевага симулятора в тому, що він відтворює всі функції пристроїв. Тобто якщо додати маршрутизатор фірми Cisco, для нього будуть доступні всі команди, які працюватимуть і на реальному обладнанні, що дуже важливо. Якщо аналізувати Cisco Packet Tracer, то ця програма не підтримує всіх команд і не дає можливості продемонструвати гетерогенність мережі[24].

GNS3 дозволяє додавати та налаштовувати повноцінні робочі станції та сервери. Якщо розглядати Cisco Packet Tracer, то кінцевими пристроями будуть звичайні робочі станції з невеликим пакетом можливостей і дуже обмеженим функціоналом. Така ж ситуація і з серверами. Щодо GNS3, ми можемо додавати повноцінні робочі станції під керуванням ОС Windows 7, Windows 8 lite, Linux та інші.

Найбільший недолік GNS3 – це неможливість додавати повноцінні комутатори, тому потрібно користуватися саме стандартним комутатором від GNS3. Причиною є те, що в реальних комутаторах знаходяться ASIC мікросхеми, які неможливо відтворити в симуляторах на звичайних комп’ютерах. А комутатори мають таку велику передачу і обробку пакетів саме через ASIC мікросхеми.

Все ж таки симуляція реальних пристроїв та операційних систем тягне за собою ще один недолік – це великі потреби до параметрів та ресурсів

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

комп'ютера, на якому буде працювати GNS3. Наприклад, для гетерогенної мережі потрібно декілька віртуальних машин під управлінням операційних систем Windows та Linux. Але для запуску тільки однієї машини під управлінням Windows 10 потрібно 4 Гігабайти оперативної пам'яті.

VirtualBox – це програма для віртуалізації різних операційних систем і, що дуже важливо, вона працює майже на всіх операційних системах Windows, Linux, MAC OS та ін. VirtualBox має однаковий формат образів для віртуалізації, і, якщо брати, наприклад, створення віртуальної машини під управлінням ОС Linux, вона може бути переміщена на Windows і працювати далі без помилок.

Перевагами VirtualBox є досить зрозумілий та дружелюбний інтерфейс. Також програма підтримує досить багато форматів образів, тобто крім операційних систем також можна встановити образ маршрутизатора (наприклад Mikrotik) і також використовувати в GNS3. VirtualBox працює на основі віртуалізації різних ОС. Після створення віртуальної мережі користувач може встановити майже будь-яку ОС і працювати на ній, як на звичайному комп'ютері.

Можливості VirtualBox:

- запуск одразу декількох віртуальних машин;
- можливість налаштування параметрів та кількості ресурсів основного комп'ютера для кожної віртуальної машини;
- експорт та імпорт вже готових образів віртуальних машин;
- можливість “заморозити” стан віртуальної машини для зменшення втрати ресурсів на ту віртуальну машину, яка зараз не потрібна у використанні;
- можливість спільних папок та файлів для обміну даними як з основним комп'ютером, так і між віртуальними машинами;
- можливість робити скріншоти та захват відео з екрану віртуальних машин.

Wireshark – дуже потужна програма для аналізу та перехоплення мережевого трафіку. Дане ПЗ доступне на операційних системах Linux, Windows, NetBSD, MAC OS та ін. Ця програма потрібна для аналізу трафіку.

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

Також, якщо щось виходить з ладу, наприклад, протокол маршрутизації, можна за допомогою Wireshark перевірити, в чому проблема і де втрачаються пакети[21].

Можливості WinBox

- Налаштування конфігурації на маршрутизаторах MikroTik
- Простий в користуванні інтерфейс
- Налаштування всіх можливостей MikroTik через графічний інтерфейс що спрощує та прискорює роботу з MikroTik

Висновки до розділу 2

Була спроектована підсистема гетерогенної мережі, яка складається з 6 локальних підмереж та маршрутизаторів рівня ядра. Обґрунтовано необхідність використання трирівневої ієрархічної моделі. Сформовано таблицю параметрів інтерфейсів та адресації пристроїв мережі.

Обрано пристрої, які будуть використовуватися на рівні ядра як найпотужніші. Описані можливості обладнання, які можуть бути застосовані для поставлених завдань. Також обґрунтовано вибір програмного забезпечення, зокрема симулятора, в якому буде створена мережа, та операційних систем, що будуть використовуватися для забезпечення гетерогенності мережі.

					КБ.КВ.Б – 125 – 22– ПЗ	Арк.
						37
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

В даному пункті розглянуто основні налаштування пристроїв мережі. Спочатку повністю складемо схему, яку спроектували в попередньому розділі (Рисунок 3.1).

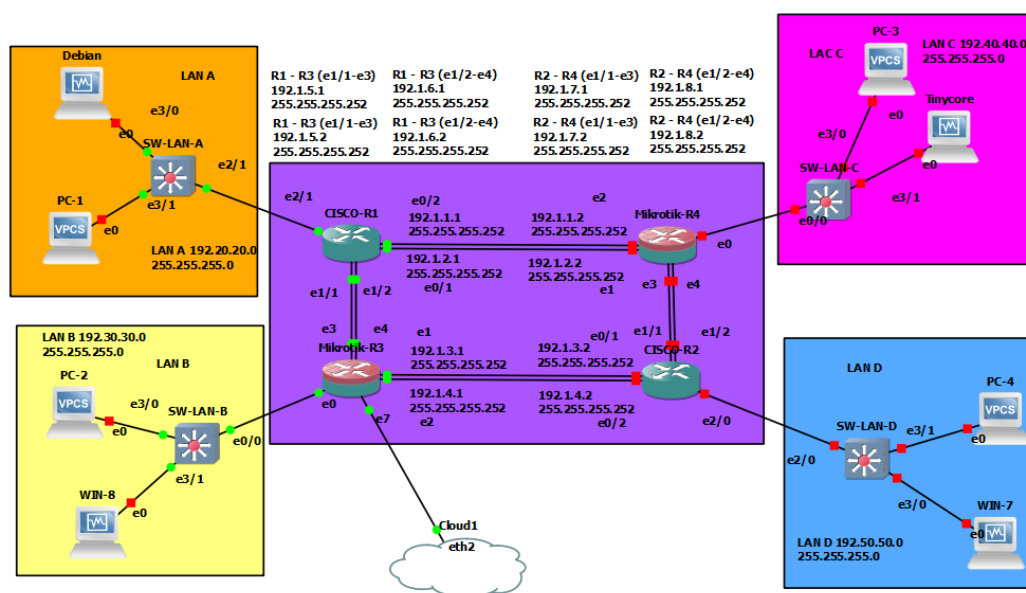


Рисунок 3.1 Повна схема мережі

Налаштуємо IP-адресацію та інші налаштування на всіх маршрутизаторах та комутаторах CISCO. На рисунку 3.2 наведено лістинг налаштування адресації на CISCO_R1. На інших пристроях мережі воно проводиться аналогічно.

```

CISCO-R1
*Dec 16 13:05:59.581: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to a
dministratively down
*Dec 16 13:05:59.590: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to a
dministratively down
CISCO-R1#
CISCO-R1#
CISCO-R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-R1(config)#int e0/2
CISCO-R1(config-if)#ip add 192.1.1.1 255.255.255.252
CISCO-R1(config-if)#no shut
CISCO-R1(config-if)#ex
CISCO-R1(config)#int e
*Dec 16 13:22:08.566: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Dec 16 13:22:09.567: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
CISCO-R1(config)#int e0/1
CISCO-R1(config-if)#ip add 192.1.2.1 255.255.255.252
CISCO-R1(config-if)#no shut
CISCO-R1(config-if)#ex
CISCO-R1(config)#int e/1
*Dec 16 13:22:23.443: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Dec 16 13:22:24.446: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
CISCO-R1(config)#int e1/1
CISCO-R1(config-if)#ip add 192.1.5.1 255.255.255.252
CISCO-R1(config-if)#no shut
CISCO-R1(config-if)#ex
CISCO-R1(config)#int e
*Dec 16 13:22:41.001: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
*Dec 16 13:22:42.012: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to up
CISCO-R1(config)#int e1/2
CISCO-R1(config-if)#ip add 192.1.6.1 255.255.255.252
CISCO-R1(config-if)#no shut
CISCO-R1(config-if)#ex
CISCO-R1(config)#
*Dec 16 13:23:02.401: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state to up
*Dec 16 13:23:03.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to up
CISCO-R1(config)#int e2/1
CISCO-R1(config-if)#ip add 192.20.20.1 255.255.255.0
CISCO-R1(config-if)#no shut
CISCO-R1(config-if)#end
CISCO-R1#
*Dec 16 13:23:19.194: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#
*Dec 16 13:23:20.429: %LINK-3-UPDOWN: Interface Ethernet2/1, changed state to up
*Dec 16 13:23:21.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1, changed state to up
CISCO-R1#

```

Рисунок 3.2. Налаштування IP-адресації на CISCO-R1

Тепер для зв'язку між маршрутизаторами, комутаторами та іншими приладами налаштуємо протокол маршрутизації. В нашому випадку це протокол OSPF (Рисунок 3.13)

```

CISCO-R1#
CISCO-R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-R1(config)#router ospf 1
CISCO-R1(config-router)#network 192.1.1.0 0.0.0.3 area 0
CISCO-R1(config-router)#network 192.1.2.0 0.0.0.3 area 0
CISCO-R1(config-router)#network 192.1.5.0 0.0.0.3 area 0
CISCO-R1(config-router)#network 192.1.6.0 0.0.0.3 area 0
CISCO-R1(config-router)#network 192.20.20.0 0.0.0.255 area 0
CISCO-R1(config-router)#exit
CISCO-R1(config)#exi
CISCO-R1#ro
*Dec 16 15:43:49.556: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#

```

Рисунок 3.3. Налаштування протоколу OSPF на CISCO-R1

Оскільки в нашій мережі використовується досить багато робочих станцій, то налаштуємо протокол DHCP на маршрутизаторах (Рисунок 3.14).

```

CISCO-R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-R1(config)#ip dhcp pool LAN-A
CISCO-R1(dhcp-config)#network 192.20.20.0 255.255.255.0
CISCO-R1(dhcp-config)#defa
CISCO-R1(dhcp-config)#default-router 192.20.20.1
CISCO-R1(dhcp-config)#end
CISCO-R1#
*Dec 16 14:11:01.758: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#

```

Рисунок 3.4 Налаштування протоколу DHCP на CISCO-R1

Після налаштувань маршрутизації та віддалених робочих столів потрібно також налаштувати безпеку пристроїв. Для початку захистимо наші маршрутизатори за допомогою створення користувачів з різними рівнями доступу (Рисунок 3.16-3.18).

```

CISCO-R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-R1(config)#privilege exec level 1 show run
CISCO-R1(config)#privilege exec level 1 show running-config
CISCO-R1(config)#privilege exec level 1 show interface
CISCO-R1(config)#privilege exec level 1 show ip interface
CISCO-R1(config)#privilege exec level 1 show ip route
CISCO-R1(config)#username NYKYTA privilege 1 secret cisco
CISCO-R1(config)#line cons
CISCO-R1(config)#line console 0
CISCO-R1(config-line)#exec-timeout 10
CISCO-R1(config-line)#end
CISCO-R1#
*Dec 17 14:10:42.310: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#

```

Рисунок 3.5. Налаштування користувачів на CISCO-R1

```

CISCO-R1#
*Dec 17 14:10:42.310: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-R1(config)#privilege exec level 4 configure terminal
CISCO-R1(config)#privilege configure level 4 interface
CISCO-R1(config)#privilege interface level 4 description
CISCO-R1(config)#privilege interface level 4 shutdown
CISCO-R1(config)#privilege interface level 4 write memory
% Unknown command 'write memory'
CISCO-R1(config)#username NYKYTA2 privilege 4 secret cisco
CISCO-R1(config)#line console 0
CISCO-R1(config-line)#exec-timeout 10
CISCO-R1(config-line)#end
CISCO-R1#
*Dec 17 14:12:56.270: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#

```

Рисунок 3.6. Налаштування користувачів на CISCO-R1

```

CISCO-R1(config)#banner login #=====
Enter TEXT message. End with the character '#'.
Device hostname -$(CISCO-R1)
Your connection is -$(line)
Enter Admin LOGIN and PSWD
=====#
CISCO-R1(config)#username admin privilege 15 secret cisco
CISCO-R1(config)#line local
^
% Invalid input detected at '^' marker.

CISCO-R1(config)#line console
% Incomplete command.

CISCO-R1(config)#line console 0
CISCO-R1(config-line)#login local
CISCO-R1(config-line)#exec-timeout 10
CISCO-R1(config-line)#end
CISCO-R1#
*Dec 17 14:17:28.186: %SYS-5-CONFIG_I: Configured from console by console
CISCO-R1#

```

Рисунок 3.7. Налаштування користувачів на CISCO-R1

І додатково налаштуємо параметри захисту на комутаторах, оскільки в нашій мережі досить багато DHCP-серверів. Якщо у зломисника буде можливість підключити свій DHCP-сервер, то ми можемо втратити дані, які будуть знаходитися на робочих станціях. Тому налаштуємо функцію довіреного порту на комутаторах (Рисунок 3.19).

```

SW-LAN-A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-LAN-A(config)#int vlan 1
SW-LAN-A(config-if)#ip add 192.20.20.210 255.255.255.0
SW-LAN-A(config-if)#no shut
SW-LAN-A(config-if)#exit
*Dec 17 14:23:08.892: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Dec 17 14:23:09.896: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW-LAN-A(config-if)#exit
SW-LAN-A(config)#ip dhcp snooping vlan 1
SW-LAN-A(config)#int e2/1
SW-LAN-A(config-if)#ip dhcp snooping trust
SW-LAN-A(config-if)#ip dhcp snooping limit rate 50
SW-LAN-A(config-if)#exit
SW-LAN-A(config)#no ip dhcp snooping information option
SW-LAN-A(config)#exit
SW-LAN-A#
*Dec 17 14:24:18.624: %SYS-5-CONFIG_I: Configured from console by console
SW-LAN-A#

```

Рисунок 3.8. Налаштування довіреного порту на комутаторі CISCO-R1

Також налаштуємо функцію Port Security на комутаторах (Рисунок 3.20).

```

Enter configuration commands, one per line. End with CNTL/Z.
SW-LAN-A(config)#int range e3/0-3
SW-LAN-A(config-if-range)#switchport mode access
SW-LAN-A(config-if-range)#switchport port-sec
SW-LAN-A(config-if-range)#switchport port-security maxi
SW-LAN-A(config-if-range)#switchport port-security maximum 100
SW-LAN-A(config-if-range)#switchport port-security mac-add
SW-LAN-A(config-if-range)#switchport port-security mac-address sticky
SW-LAN-A(config-if-range)#end
SW-LAN-A#
*Dec 17 14:25:44.442: %SYS-5-CONFIG_I: Configured from console by console
SW-LAN-A#

```

Рисунок 3.9. Налаштування Port Security на комутаторі CISCO-R1

```

CISCO-R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-R1(config)#login block ?
<1-65535> Time period in seconds

CISCO-R1(config)#login block-for 60 attempts 3 within 20
CISCO-R1(config)#login delay 5
CISCO-R1(config)#login on-failure log
CISCO-R1(config)#login in-success log
^
% Invalid input detected at '^' marker.

CISCO-R1(config)#login on-success log
CISCO-R1(config)#

```

Рисунок 3.10. Налаштування захисту від BrutForce на CISCO-R1

Тепер налаштуємо IP-адресацію та інші налаштування на всіх маршрутизаторах MikroTik за допомогою WinBox. На рисунку 3.11-13 наведено налаштування адресації на CISCO_R1. На інших пристроях мережі воно проводиться аналогічно.

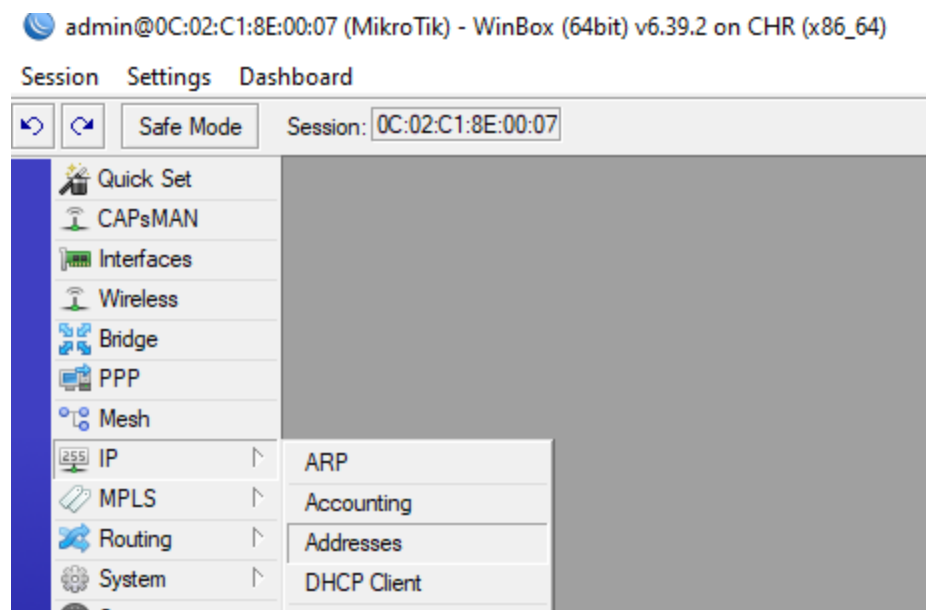


Рисунок 3.11. Налаштування IP-адресації на MikroTik-R3

					КБ.КВ.Б – 125 – 22– ПЗ	Арк. 42
Змн.	Арк.	№ докум.	Підпис	Дата		

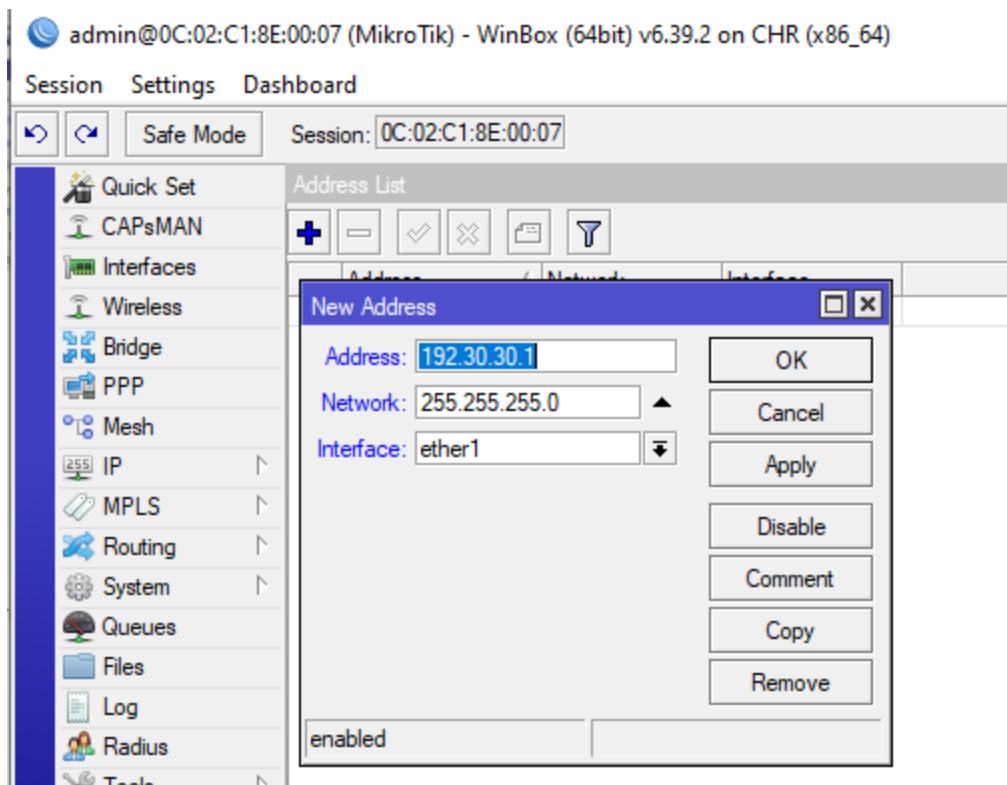


Рисунок 3.12. Налаштування IP-адресації на MikroTik-R3

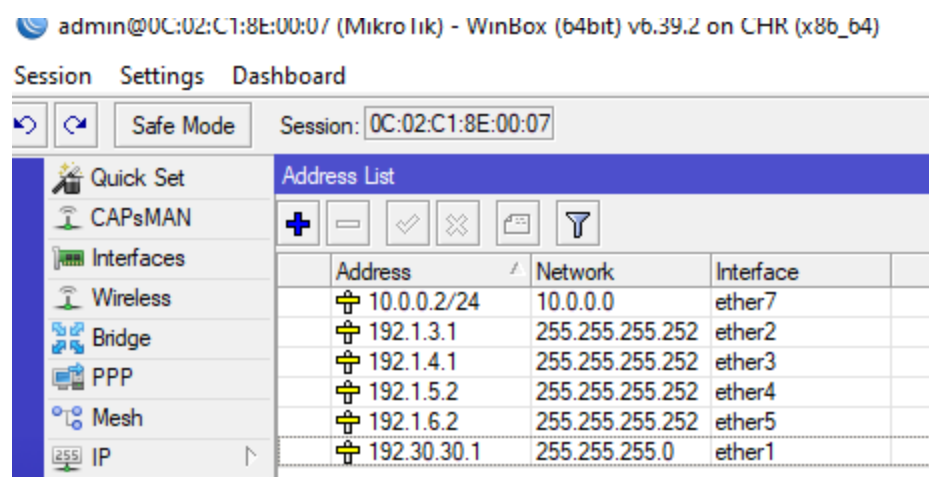


Рисунок 3.13. Налаштування IP-адресації на MikroTik-R3

Тепер для зв'язку між маршрутизаторами, комутаторами та іншими приладами налаштуємо протокол маршрутизації. В нашому випадку це протокол OSPF (Рисунок 3.13)

OSPF		
Instances	Networks	Areas
+ - ✓ ✗ 📄 🔍		
Network	Area	
192.1.3.0/30	backbone	
192.1.4.0/30	backbone	
192.1.5.0/30	backbone	
192.1.6.0/30	backbone	
192.30.30.0/24	backbone	

Рисунок 3.14. Налаштування протоколу OSPF на MikroTik-R3

Оскільки в нашій мережі використовується досить багато робочих станцій, то налаштуємо протокол DHCP на маршрутизаторах (Рисунок 3.14).

admin@0C:02:C1:8E:00:07 (MikroTik) - WinBox (64bit) v6.39.2 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 0C:02:C1:8E:00:07

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log

Address List

Address	Network	Interface
10.0.0.2/24	10.0.0.0	ether7
192.30.30.1	255.255.255.0	ether1

- ARP
- Accounting
- Addresses
- DHCP Client
- DHCP Relay
- DHCP Server
- DNS

Рисунок 3.15. Налаштування протоколу DHCP на MikroTik-R3

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+

-

✓

✗

🔍

DHCP Config

DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
DHCP Setup Select network for DHCP addresses DHCP Address Space: 192.30.30.0/24 Back Next Cancel					

Рисунок 3.16. Налаштування протоколу DHCP на MikroTik-R3

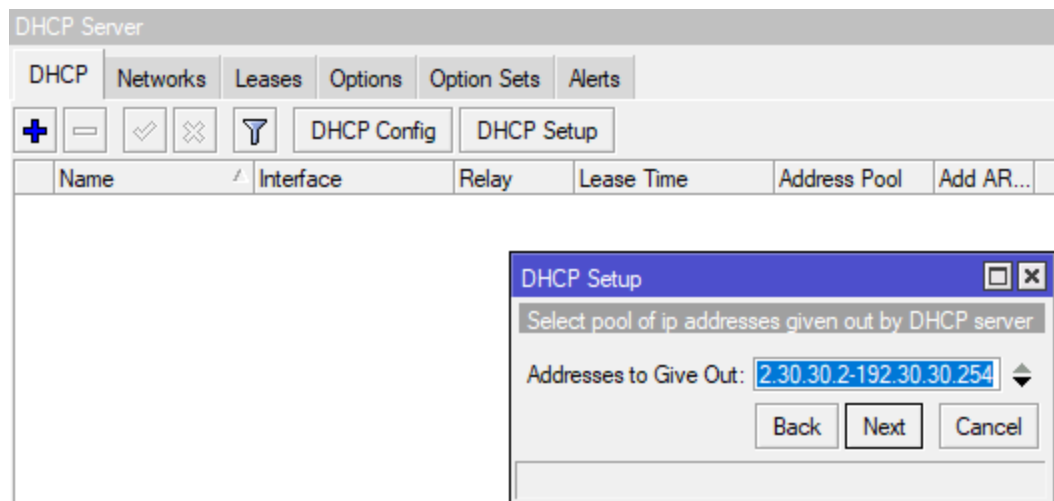


Рисунок 3.17. Налаштування протоколу DHCP на MikroTik-R3

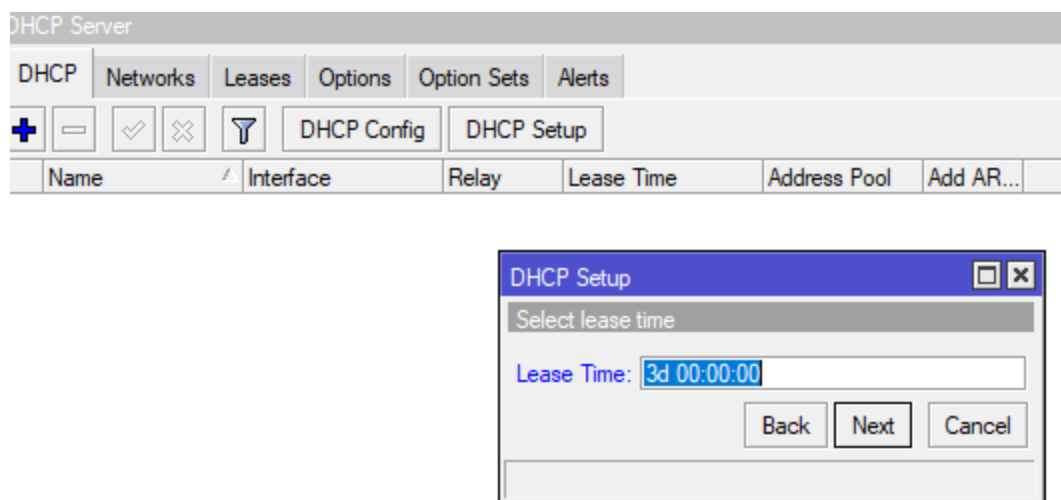


Рисунок 3.18. Налаштування протоколу DHCP на MikroTik-R3

Після налаштувань маршрутизації потрібно також налаштувати безпеку пристроїв. Для початку захистимо наші маршрутизатори за допомогою створення користувачів з різними рівнями доступу (Рисунок 3.16-3.18).

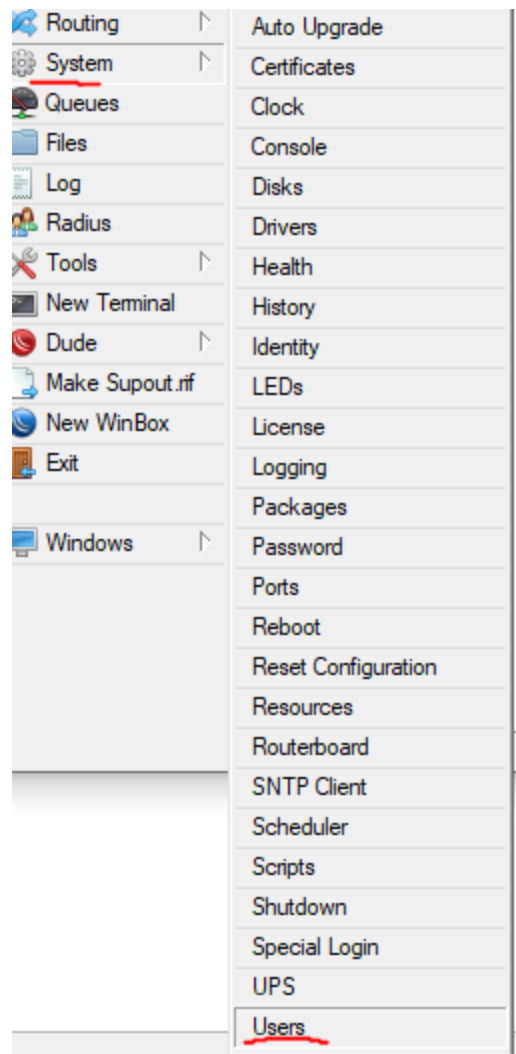


Рисунок 3.19. Налаштування користувачів на МікроТік-РЗ

Рисунок 3.20. Налаштування користувачів на МікроТік-РЗ

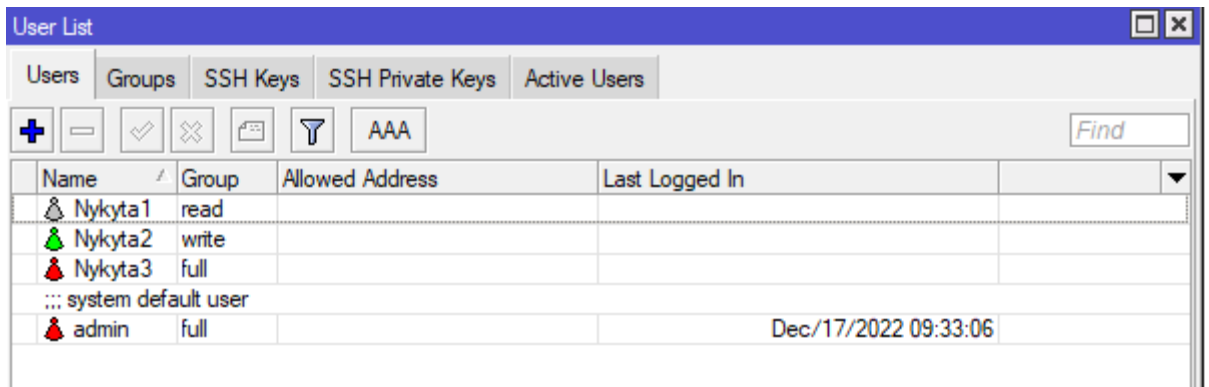


Рисунок 3.21. Налаштування користувачів на Mikrotik-R3

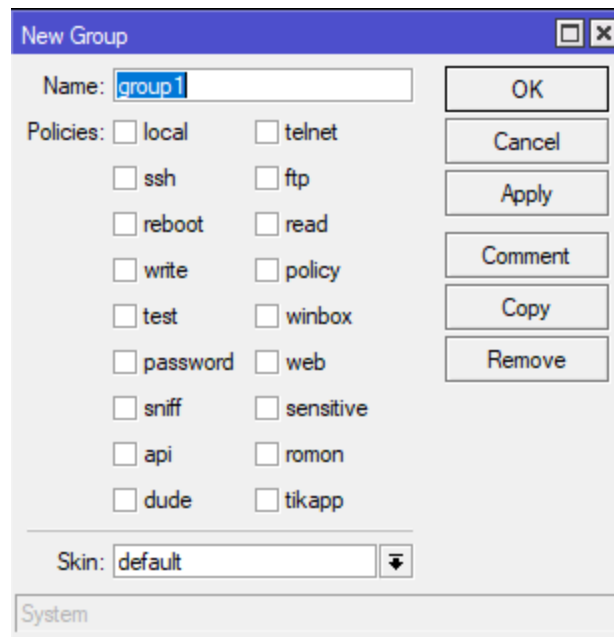


Рисунок 3.22. Налаштування користувачів на Mikrotik-R3

На маршрутизаторі Mikrotik було налаштовано захист від BrutForce відразу різних можливих сторонах.

```
[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 BrutForce на Mikrotik-R3

```
[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 BrutForce на Mikrotik-R3

```
[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 BrutForce на Mikrotik-R3

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

Рисунок 3.26. Налаштування захисту від BrutForce на MikroTik-R3

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

Рисунок 3.27. Налаштування захисту від BrutForce на MikroTik-R3

Також було налаштовано захист домену та пошти від фішингових атак

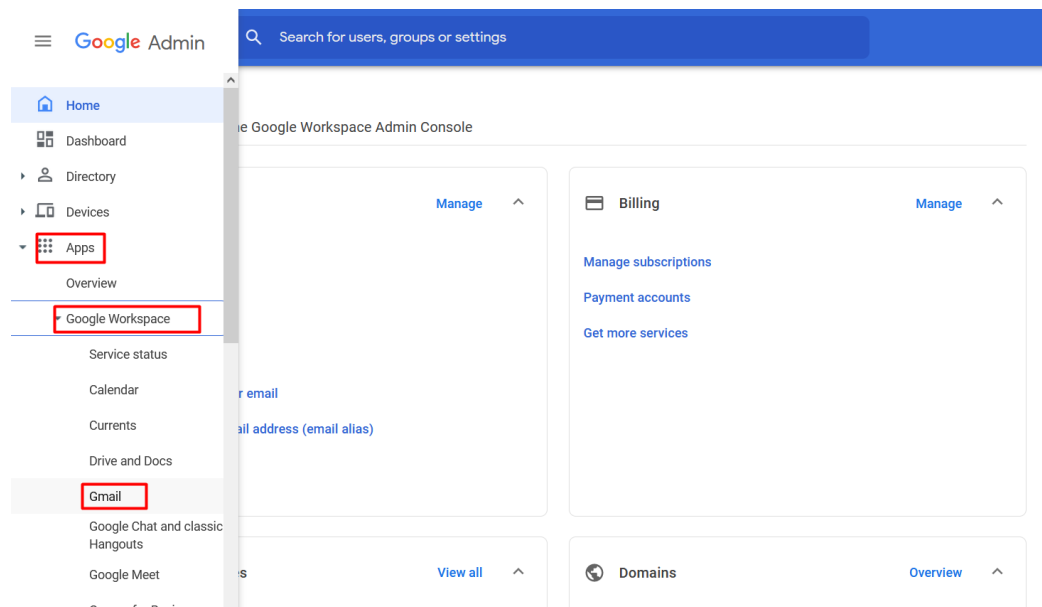


Рисунок 3.28. Налаштування захисту від Fishing домену DKIM

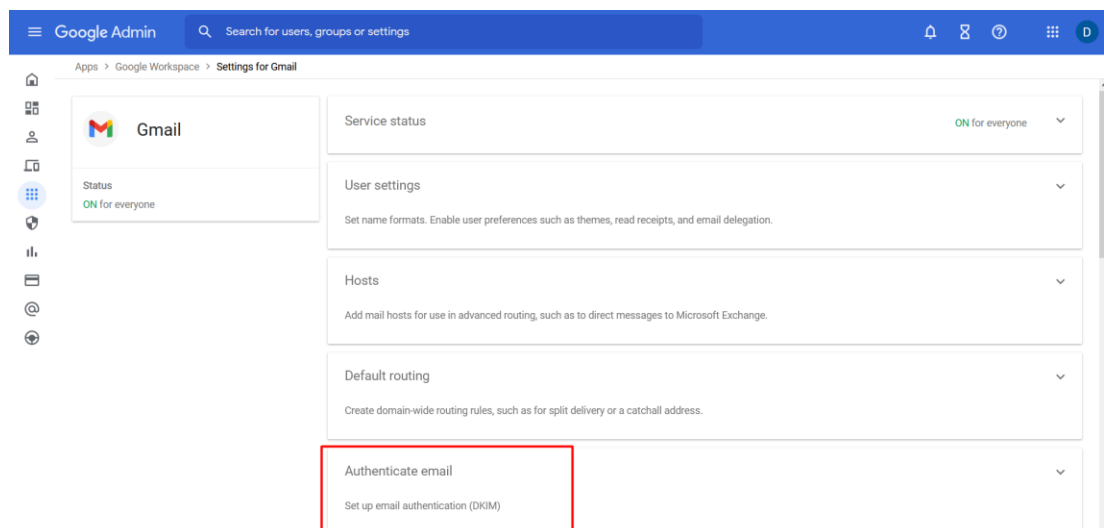


Рисунок 3.29. Налаштування захисту від Fishing домену DKIM

Authenticate email

DKIM authentication

Selected domain

salesstaff.info

The domains you select will use the DKIM (DomainKeys Identified Mail) protocol for authenticating outgoing emails. [Learn more](#)

Status: Not authenticating email

You must update the DNS records for this domain.

To start authenticating email for the domain selected above, enter the following DNS TXT record into your domain provider's DNS settings page. Then click "Start authentication."

DNS Host name (TXT record name):

google._domainkey

TXT record value:

v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0RI4VZyy0lksvA+AHUQ08Bm2RNx/R8QDa1sNL4B7vJRN4k4bhTm7BAVTzCD202ZUQwFM+yBgfm/0nYGlaUiXgGFqcYfFu6J2rUpym/IWPAUGoYkeyZVrenP1SE9VPxwFNeErBjojrUj6c5pwpCqHBD43/YBjaQlJ0LpoGoG8dzgf2Se3zY1WuTypdVxfvEI"drn4lugwIAGbHI48HGH/+69BTIXYH1WnYdlE6o+hdEb6l8fJrIB0YFx+CsnmXNCqTtTb1p/IL4leOIPdxWOv1TQoIl01M4jxdqRb9mGMR3AZbeNTIS092NLMBtbxGV48jdpZ6lJevrNJva+u2vwIDAQAB

GENERATE NEW RECORD

Рисунок 3.30. Налаштування захисту від Fishing домену DKIM

DNS Records

DNS Records define how your domain behaves, like showing your website content and delivering your email.

Delete

Copy

Filter

Add

...

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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0RI4VZyy0lksvA+AHUQ08Bm2RNx/R8QDa1sNL4B7vJRN4k4bhTm7BAVTzCD202ZUQwFM+yBgfm/0nYGlaUiXgGFqcYfFu6J2rUpym/IWPAUGoYkeyZVrenP1SE9VPxwFNeErBjojrUj6c5pwpCqHBD43/YBjaQlJ0LpoGoG8dzgf2Se3zY1WuTypdVxfvEI"drn4lugwIAGbHI48HGH/+69BTIXYH1WnYdlE6o+hdEb6l8fJrIB0YFx+CsnmXNCqTtTb1p/IL4leOIPdxWOv1TQoIl01M4jxdqRb9mGMR3AZbeNTIS092NLMBtbxGV48jdpZ6lJevrNJva+u2vwIDAQAB

1/2 Hour

Add record

Clear

Type

Name

Data

TTL

Delete

Edit

A

@

Parked

600 seconds

Delete

Edit

Рисунок 3.31. Налаштування захисту від Fishing домену DKIM

s2._domainkey

CNAME

3600

s2._domainkey.u25481426.wl177.sendgrid.net.

google._domainkey

TXT

3600

"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0RI4VZyy0lksvA+AHUQ08Bm2RNx/R8QDa1sNL4B7vJRN4k4bhTm7BAVTzCD202ZUQwFM+yBgfm/0nYGlaUiXgGFqcYfFu6J2rUpym/IWPAUGoYkeyZVrenP1SE9VPxwFNeErBjojrUj6c5pwpCqHBD43/YBjaQlJ0LpoGoG8dzgf2Se3zY1WuTypdVxfvEI"drn4lugwIAGbHI48HGH/+69BTIXYH1WnYdlE6o+hdEb6l8fJrIB0YFx+CsnmXNCqTtTb1p/IL4leOIPdxWOv1TQoIl01M4jxdqRb9mGMR3AZbeNTIS092NLMBtbxGV48jdpZ6lJevrNJva+u2vwIDAQAB"

+ Add more to this record

Create new record

Cancel

Save

Required

Informational only records

Рисунок 3.32. Налаштування захисту від Fishing домену DKIM

					КБ.КВ.Б – 125 – 22– ПЗ	Арк. 49
Змн.	Арк.	№ докум.	Підпис	Дата		

DNS Records

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

Delete

Copy

Filter

Add

[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

Add record

Clear

Type	Name	Data	TTL		
	A	@	Parked	600 seconds	Delete Edit

Рисунок 3.33. Налаштування захисту від Fishing домену SPF

salesstaff.info

Global DNS set

Default name servers (Active) Custom name servers

These DNS settings are active. Changes are published immediately, but may take time to propagate

Resource records

Export DNS records

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"

Рисунок 3.34. Налаштування захисту від Fishing домену SPF

/IL4leOIPdxW0v1TQoIl01M4jxdqRb9mGMR3AZbeNTIS
O92NLMBtbxGV48jdpZ6lJevrNJva+u2vwiDAQAB"

+ 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.	

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

DNS Records

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

Delete

Copy

Filter ▾

Add

⋮

	Type ?	Name ?	Data ?	TTL ?		
☐	A	@	Parked	600 seconds	Delete	Edit
☐	NS	@	ns35.domaincontrol.com.	1 Hour	Can't delete	Can't edit
☐	NS	@	ns36.domaincontrol.com.	1 Hour	Can't delete	Can't edit
☐	CNAME	em2291	u25363915.wl166.sendgrid.net.	1/2 Hour	Delete	Edit
☐	CNAME	s1._domainkey	s1.domainkey.u25363915.wl166.sendgrid.net.	1/2 Hour	Delete	Edit

Рисунок 3.36. Налаштування захисту від Fishing домену DMARC

DNS Records

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

Delete

Copy

Filter ▾

Add

⋮

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

Type

Name

Value

TTL

TXT ▾

_dmarc

v=DMARC1; p=none

1/2 Hour ▾

Add record

Clear

	Type ?	Name ?	Data ?	TTL ?		
☐	A	@	Parked	600 seconds	Delete	Edit
☐	NS	@	ns35.domaincontrol.com.	1 Hour	Can't delete	Can't edit

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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0

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 не виникає при цьому конфліктів (Рисунок 3.27-3.28).

```
PC-1> ip dhcp
DDORA IP 192.20.20.2/24 GW 192.20.20.1
PC-1> █
```

Рисунок 3.40. Перевірка DHCP серверу на CISCO-R1

```

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-R1

```

PC-2> ip dhcp
DORA IP 192.30.30.3/24 GW 192.30.30.1
PC-2>

```

Рисунок 3.42. Перевірка DHCP серверу на МІКРОТІК-R3

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2010 Microsoft Corporation. All rights reserved.

C:\Users\nykyta.WIN7>ipconfig

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

C:\Users\nykyta.WIN7>

```

Рисунок 3.43. Перевірка DHCP серверу на МІКРОТІК-R3

Тепер спробуємо зайти під користувачем admin на маршрутизаторі CISCO-R1 і перевіримо результат хешування у перехопленому повідомленні (Рисунок 3.29-3.30).

```

=====
Device hostname -(CISCO-R1)
Your connection is -0
Enter Admin LOGIN and PSWD
=====

User Access Verification

Username: Nykyta
Password:
CISCO-R1>

```

Рисунок 3.44. Перевірка налаштувань користувачів на CISCO-R1

```

=====
Device hostname -$(CISCO-R1)
Your connection is -0
Enter Admin LOGIN and PSWD
=====

User Access Verification

Username: admin
Password:
CISCO-R1#
CISCO-R1#
CISCO-R1#
CISCO-R1#

```

Рисунок 3.45. Перевірка налаштувань користувачів на CISCO-R1

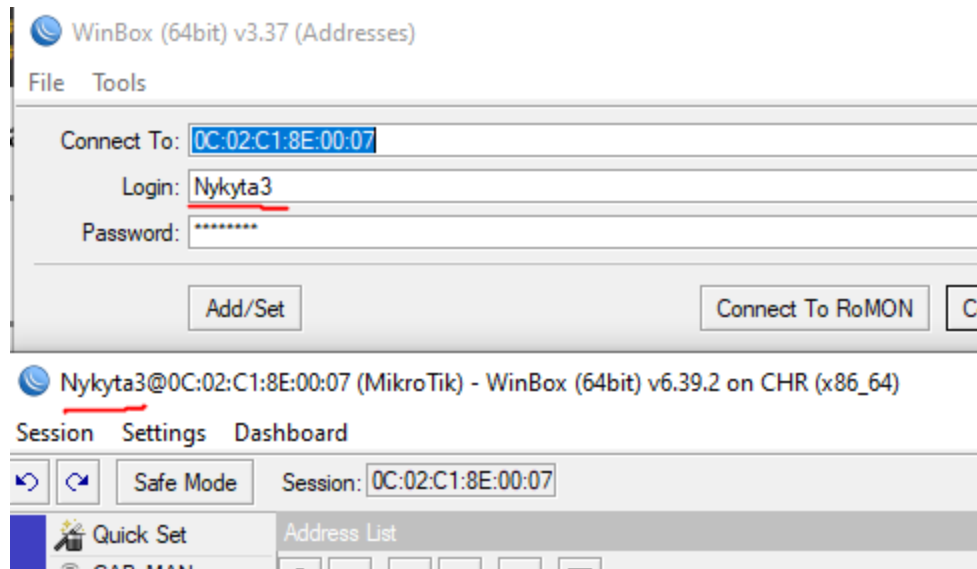


Рисунок 3.46. Перевірка налаштувань користувачів на МІКРОТІК-R3

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

```

PC1> ping 192.30.30.2
84 bytes from 192.30.30.2 icmp_seq=1 ttl=64 time=0.610 ms
84 bytes from 192.30.30.2 icmp_seq=2 ttl=64 time=0.567 ms
84 bytes from 192.30.30.2 icmp_seq=3 ttl=64 time=0.535 ms
84 bytes from 192.30.30.2 icmp_seq=4 ttl=64 time=0.604 ms
84 bytes from 192.30.30.2 icmp_seq=5 ttl=64 time=0.618 ms

PC1>

```

Рисунок 3.47. Перевірка зв'язку між LAN A та LAN B

```

PC1> ping 192.40.40.2
84 bytes from 192.40.40.2 icmp_seq=1 ttl=64 time=0.558 ms
84 bytes from 192.40.40.2 icmp_seq=2 ttl=64 time=0.628 ms
84 bytes from 192.40.40.2 icmp_seq=3 ttl=64 time=0.623 ms
84 bytes from 192.40.40.2 icmp_seq=4 ttl=64 time=0.580 ms
84 bytes from 192.40.40.2 icmp_seq=5 ttl=64 time=0.620 ms

PC1>

```

Рисунок 3.48. Перевірка зв'язку між LAN A та LAN C

PC1>

Рисунок 3.49. Перевірка зв'язку між LAN A та LAN D

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 підключені до нього буде працювати DHCP-сервер. Створимо додатковий маршрутизатор і налаштуємо його як DHCP-сервер(Рисунок3.42).

 Hacker
Hacker(config)#ip dhcp pool LAN_HACK
Hacker(dhcp-config)#network 200.1.1.0 255.255.255.0
Hacker(dhcp-config)#defa
Hacker(dhcp-config)#default-router 200.1.1.1
Hacker(dhcp-config)#end
Hacker#
*Dec 18 11:58:43.384: %SYS-5-CONFIG_I: Configured from
Hacker#

Рисунок 3.50. Налаштування додаткового ДНСР-серверу

Підключимо його до довіреного порту e2/1 і спробуємо отримати IP-адресу від нього (рис 3.43).

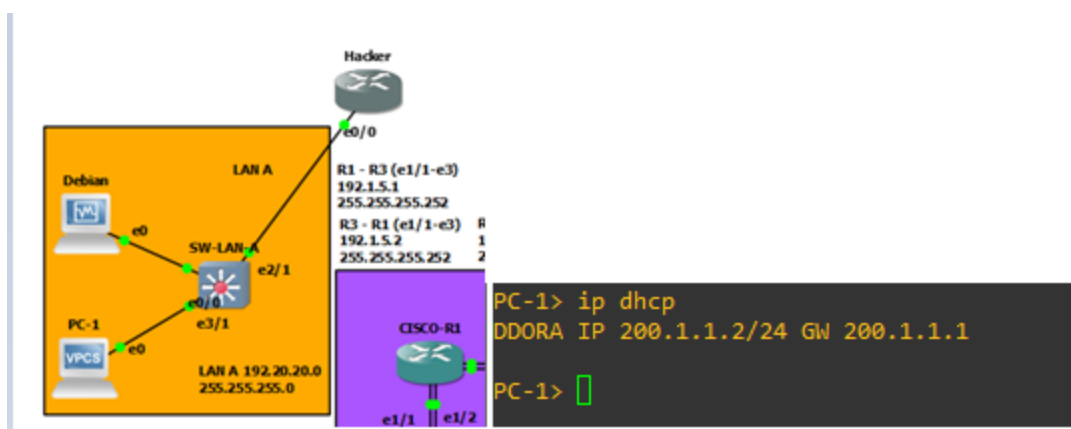


Рисунок 3.51. Отримання IP-адреси від сервера-зловмисника

Як бачимо, саме через порт e2/1 ми отримаємо IP-адресу. Підключимо його тепер до будь-якого іншого порту (Рисунок 3.44).

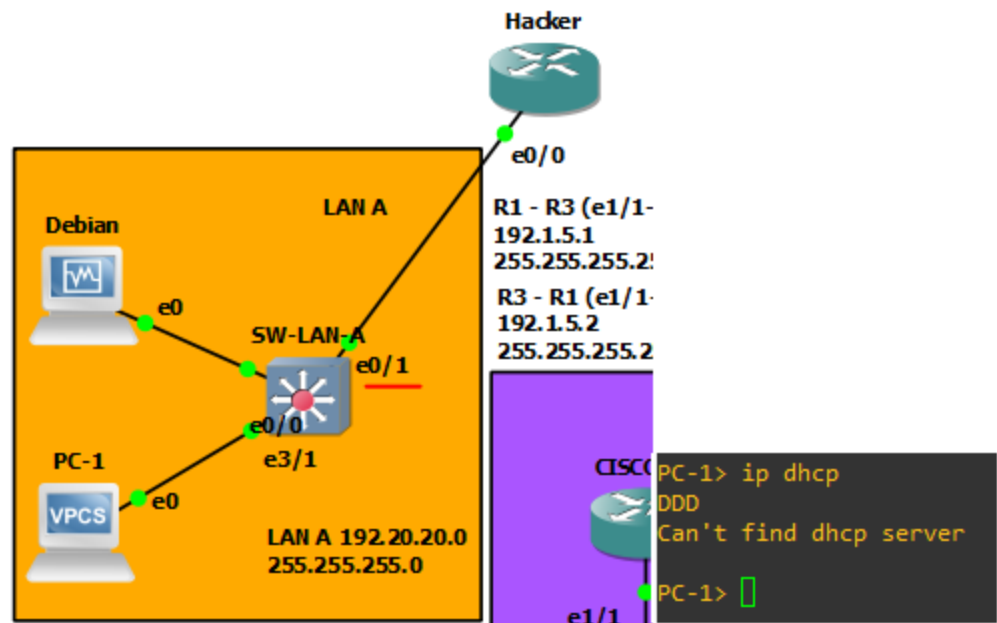


Рисунок 3.52. Підключення сервера-зловмисника до недовіреного порту комутатора.

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 BrutForce

```

=====
Device hostname -(CISCO-R1)
Your connection is -0
Enter Admin LOGIN and PSWD
=====

User Access Verification

Username: nykyta
Password:
% Login invalid

Username: nykyta
Password:
% Login invalid

Username: nykyta

```

Рисунок 3.53. Перевірка захисту від BrutForce на CISCO-R1.

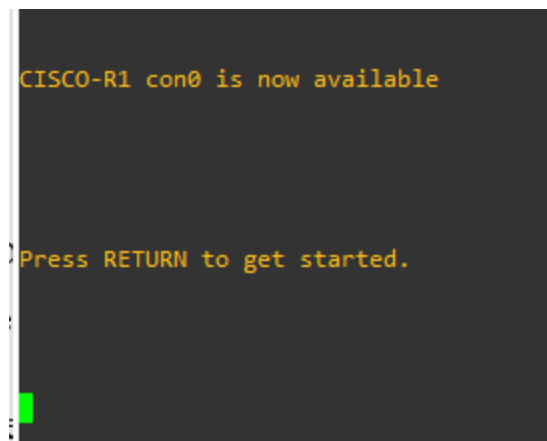


Рисунок 3.54. Перевірка захисту від BrutForce на CISCO-R1.

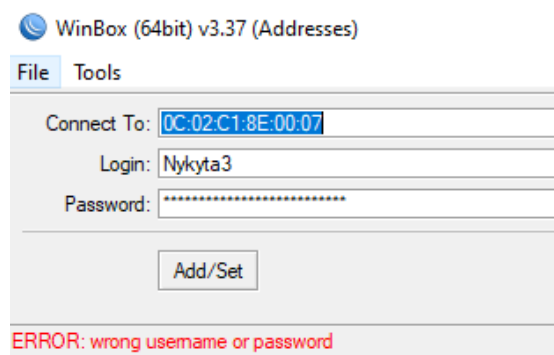


Рисунок 3.55. Перевірка захисту від BrutForce на МІКРОТІК-R3

Після декількох некоректних введів паролю WinBox вимикається.

Перевірка налаштувань домену.

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

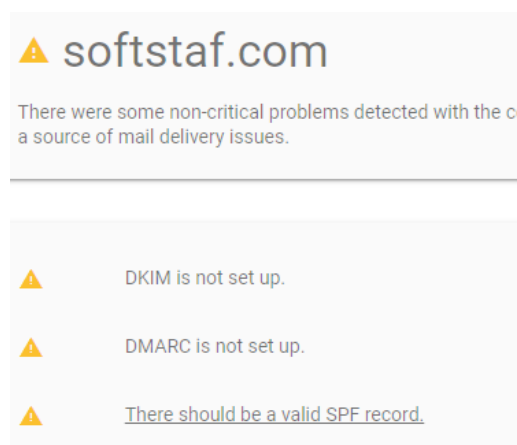


Рисунок 3.56. Перевірка налаштувань домену

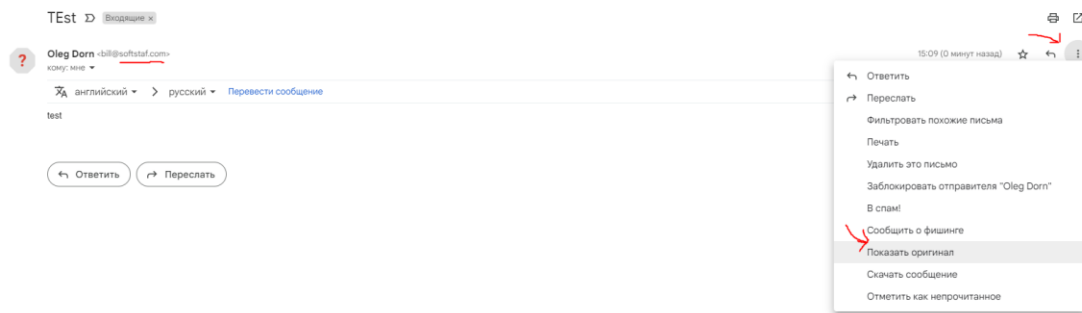


Рисунок 3.57. Перевірка налаштувань домену

Исходное сообщение

Идентификатор сообщения	<CAA3a7FDxDts_WheniuZ3GWG5Bw2iaYBK0fgKGerwvxh8czYWQw@mail.gmail.com>
Создано:	18 декабря 2022 г., 15:09 (доставлено через 13 секунд)
От:	Oleg Dorn <bill@softstaf.com>
Кому:	zeus15032000@gmail.com
Тема:	TEst
SPF:	NEUTRAL с IP-адресом 209.85.220.41. Подробнее...
DKIM:	'FAIL', домен softstaf.com Подробнее...

[Скачать оригинал](#)

Рисунок 3.58. Перевірка налаштувань домену

```
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=to:subject:message-id:date:from:mime-version:dkim-signature;
bh=hDoM3XnbQp3mgIxxmKu3DY57KeorooocQ10R+cI=;
b=F6vismtuazjgZn8M/yE50+9qGcota+3M26XQ9190D1P/VB012XdYntxspE5TjMw0
g-18hKkK7ummsJH2R7GT/cxf5mW5u0201m00R0R0N3Q1aigAgJ2uXVtOCfntquH
j369Y9xdnK8Hxkdj3Q1Kz3seplX6vPvSwH8j0Z1gK0IVzzBvYugq3KNU8FW/GZyc
wAD1MXCSr2AD/gpWGBdNLZkkjckE3fN+dbM+JH3V1Z1ZbrahZHYRtbrsL5j30VLDhAr
O+c3czuKebKPH540ugEB5p+Z5s131Atssm4zq0m2My+L9hMKZn2IpcgvH6G6R9RL7yqQ
WeSA==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=tempperror (no key for signature) header.i=@softstaf.com header.s=google header.b=MH5QGEXe;
spf=neutral (google.com: 209.85.220.41 is neither permitted nor denied by best guess record for domain of bill@softstaf.com) smtp.mailfrom=bill@softstaf.com
Return-Path: <bill@softstaf.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
by mx.google.com with SMTPS id n2-20020a19d60200000b004b5969925afsor13603751fg.148.2022.12.18.05.09.31
for <zeus15032000@gmail.com>
(Google Transport Security);
Sun, 18 Dec 2022 05:09:31 -0800 (PST)
Received-SPF: neutral (google.com: 209.85.220.41 is neither permitted nor denied by best guess record for domain of bill@softstaf.com) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
dkim=tempperror (no key for signature) header.i=@softstaf.com header.s=google header.b=MH5QGEXe;
spf=neutral (google.com: 209.85.220.41 is neither permitted nor denied by best guess record for domain of bill@softstaf.com) smtp.mailfrom=bill@softstaf.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=softstaf.com; s=google;
h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
:date:message-id:reply-to;
bh=hDoM3XnbQp3mgIxxmKu3DY57KeorooocQ10R+cI=;
b=MH5QGEXeCTBjp4Xx8RyBQ5Hs7KBYFvU//IumQU6nn/tvKxkEknzJXkeelQk/xunzR
x2me2rG6eW0xH1yH19FK9cfQ71aw2PQ0tf34g0nK03447DDfzK3eP+KST1MB481
c/pRPhqwt4x31F0ny/rCFEQ8939xkd/ukJ2KZr0uqBf3/01b/G8nu9/3Dhwacz0+180
MAtN02We5CC08dHeuzut118i0HdGRKYV11dTN3Qam1ZnmnBvqHryumF80pUbiIQ0a
g23+214H0yFxnva4iocj/ypQP8eA15RpP2K55/YkV1v13pk+Q0xp2Dm07EFf1N80HxVw
HFAA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Рисунок 3.59. Перевірка налаштувань домену

Після чого було перевірено лист від домена на якому налаштовано всі записи DNS (SPF, DKIM, DMARK)

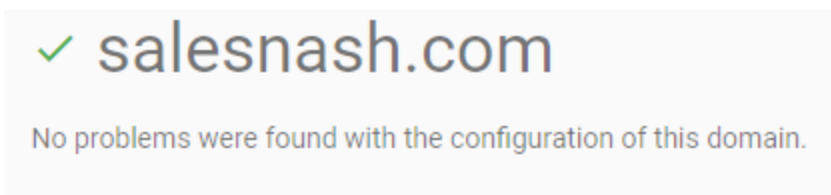


Рисунок 3.60. Перевірка налаштувань домену

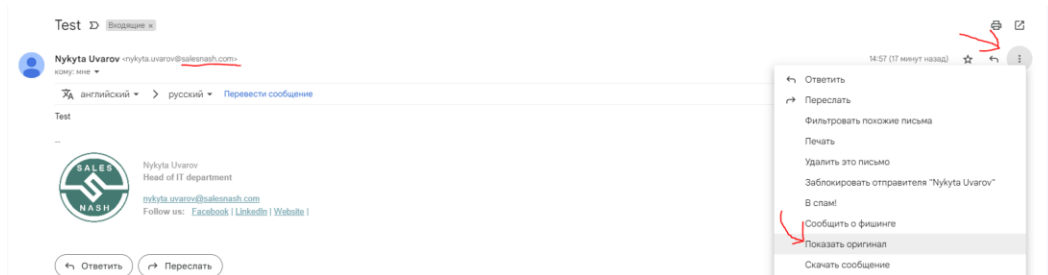


Рисунок 3.61. Перевірка налаштувань домену

Исходное сообщение

Идентификатор сообщения	<CAF3js9LSTDJ940b8nbHJQw_xP48xjXJC_E0Wm-RDOXF_yk8LQ@mail.gmail.com>
Создано:	18 декабря 2022 г., 14:56 (доставлено через 12 секунд)
От:	Nykyta Uvarov <nykyta.uvarov@salesnash.com>
Кому:	zeus15032000@gmail.com
Тема:	Test
SPF:	<u>PASS</u> с IP-адресом 209.85.220.41. Подробнее...
DKIM:	<u>'PASS'</u> , домен salesnash.com Подробнее...
DMARC:	<u>'PASS'</u> Подробнее...

Рисунок 3.62. Перевірка налаштувань домену

```
ARC-Authentication-Results: i=1; mx.google.com;
  dkim=pass header.i=@salesnash.com header.s=google header.b=e02UgINf;
  spf=pass (google.com: domain of nykyta.uvarov@nectardesk.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=nykyta.uvarov@nectardesk.com;
  dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=salesnash.com
Return-Path: <nykyta.uvarov@nectardesk.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
  by mx.google.com with SMTPS id 1133-20020a25cc8b000000b07071b8a1c6dsor2796291ybf.135.2022.12.18.04.57.02
  for <zeus15032000@gmail.com>
  (Google Transport Security);
  Sun, 18 Dec 2022 04:57:02 -0800 (PST)
Received: SPF: pass (google.com: domain of nykyta.uvarov@nectardesk.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
  dkim=pass header.i=@salesnash.com header.s=google header.b=e02UgINf;
  spf=pass (google.com: domain of nykyta.uvarov@nectardesk.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=nykyta.uvarov@nectardesk.com;
  dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=salesnash.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=salesnash.com; s=google;
  h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
```

Рисунок 3.63. 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.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						60
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 BrutForce і захист домену від фішингу.

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

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						61
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 створено гетерогенну мережу на базі протоколу OSPF.

Для початку було проведено аналіз та вибір існуючих технологій побудови сучасних гетерогенних мереж. Зокрема було обрано графічний симулятор GNS3, Debian, Tinycore, Windows 7, Windows 8 Lite, протокол маршрутизації OSPF, а також технології прикладного рівня DHCP.

На етапі розробки мережі було визначено, що комп'ютерна мережа міститиме досить багато робочих станцій, тому була розроблена топологія мережі. Щоб мережа використовувала досить багато IP-адрес для масштабованості в майбутньому і для комфорту налаштувань підключень нових робочих станцій та приладів було використано автоматичну видачу IP-адрес за допомогою DHCP.

Далі було спроектовано логічну ієрархічну модель комп'ютерної мережі трьох рівнів, яка складається з рівнів ядра, розподілу і доступу.

Це дозволяє забезпечити зміни мережі в майбутньому – масштабованість та надійність роботи. Комп'ютерна мережа має в собі вісім робочих станцій з яких:

- дві робочих станції під управлінням Windows 7, Windows 8;
- дві робочі станції під управлінням TinyCore, Debian;
- чотири робочих станцій під управлінням влаштованих в програму GNS3 образів робочих станцій VPCS.

Для масштабованості мережі в майбутньому використовувалися образи комутатора другого рівня з шістнадцятьма портами (образ i86bi-linux-l2-adventerprise-15.1b.bin), адже звичайний комутатор, який знаходиться в GNS3, неможливо налаштувати необхідним нам чином. Для ядра мережі використовувалися образи досить потужних та гнучких в налаштуванні

маршрутизаторів третього рівня фірми CISCO (образ i86bi-linux-13-adventerprisek9-15.2.2.03T.bin) і для фірми MIKROTIK(обра RouterOS 6.39.2).

В третьому розділі було обрано обладнання на програмне забезпечення. Образи маршрутизаторів та комутаторів обрані від компанії CISCO та MIKROTIK через їх надійність та гнучкість в налаштуваннях. Також ще через те, що протокол OSPF підтримується і використовується обома фірмами. Це ще раз доводить те, що система буде досить надійною. Програма, в якій виконувався дипломний проект (GNS3) була обрана через, те що вона дозволяє створити саме гетерогенну мережу за допомогою VirtualBox, яка, в свою чергу, дозволяє використовувати різні операційні системи, зокрема Windows, Linux, Ubuntu, Tinycore.

Проведено налаштування пристроїв та аналіз результатів, сформовано висновки стосовно модернізації та вдосконалення роботи. Реалізована мережа є готовим макетом реальної реалізації проекту, а конфігурації можуть застосовуватися для реального обладнання.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						63
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гетерогенна комп'ютерна мережа [Електронний ресурс] – [Гетерогенні комп'ютерні мережі — Вікіпедія \(wikipedia.org\)](#)
2. Протокол OSPF [Електронний ресурс] – <https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf>
3. Існуючі типи атак [Електронний ресурс] – [MITRE ATT&CK®](#)
4. SPF [Електронний ресурс] – [Help prevent spoofing and spam with SPF - Google Workspace Admin Help](#)
5. DKIM [Електронний ресурс] – [Help prevent spoofing and spam with DKIM - Google Workspace Admin Help](#)
6. DMARC [Електронний ресурс] – [Help prevent spoofing and spam with DMARC - Google Workspace Admin Help](#)
7. Mikrotik [Електронний ресурс] – [MikroTik Routers and Wireless](#)
8. Cisco [Електронний ресурс] – [Networking, Cloud, and Cybersecurity Solutions - Cisco](#)
9. Налаштування CISCO DHCP [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html
10. Налаштування MIKROTIK DHCP [Електронний ресурс] – [Search - MikroTik Documentation](#)
11. Ієрархічна модель мережі від Cisco [Електронний ресурс] – <http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
12. Windows 7 [Електронний ресурс] – https://ru.wikipedia.org/wiki/Windows_7
13. Windows 8.1 [Електронний ресурс] – https://ru.wikipedia.org/wiki/Windows_8.1
14. Debian [Електронний ресурс] – [Debian -- The Universal Operating System](#)
15. Tinycore [Електронний ресурс] – [Tiny Core Linux, Micro Core Linux, 12MB Linux GUI Desktop, Live, Frugal, Extendable](#)

16. Credential Access [Електронний ресурс] – [Credential Access, Tactic TA0006 - Enterprise | MITRE ATT&CK®](#)
17. Privilege Escalation [Електронний ресурс] – [Credential Access, Tactic TA0006 - Enterprise | MITRE ATT&CK®](#)
18. Resource Development [Електронний ресурс] – [Credential Access, Tactic TA0006 - Enterprise | MITRE ATT&CK®](#)
19. Router OS [Електронний ресурс] – [MikroTik Routers and Wireless - Software](#)
20. Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet [Електронний ресурс] – https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html
21. Керівництво CISCO по захисту пристроїв CISCO IOS [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/ip/access-lists/13608-21.html#anc2
22. VirtualBox [Електронний ресурс] - <https://www.virtualbox.org/>
23. Wireshark User Guide [Електронний ресурс] - https://www.wireshark.org/docs/wsug_html/
24. Cisco IOS - Privilege Levels [Електронний ресурс] - <https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels>
25. GNS3 [Електронний ресурс] - <https://habr.com/ru/post/266503/>
26. -https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

ДОДАТКИ

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор CISCO-R1

CISCO-R1

CISCO-R1#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-R1

!

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-A

network 192.20.20.0 255.255.255.0

default-router 192.20.20.1

!

!

no ip domain lookup

ip cef

no ip v6 cef

!

multilink bundle-name authenticated

!

crypto pki token default removal timeout

!

username NYKYTA2 privilege 4 secret 5
\$1\$SpNS\$9bdC3KMGf2U8y5cdPBF41

username NYKYTA secret 5
\$1\$5BBh\$jFB43ilvsm/VEMrxe2BSP.

username admin privilege 15 secret 5
\$1\$kMkB\$9mdAltLY4iDyRAO/Q5WfY1

!

redundancy

!

!

ip tcp synwait-time 5

!

!

interface Ethernet0/0

no ip address

shutdown

!

<pre> interface Ethernet0/1 ip address 192.1.2.1 255.255.255.252 ! interface Ethernet0/2 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 </pre>	<pre> banner login ^C===== Device hostname -\$(CISCO-R1) 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 line vty 0 4 login transport input all ! ! end </pre>
--	--

Комутатор SW_1

SW_1

SW-LAN-A#show running-config

Building configuration...

Current configuration : 1455 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname SW-LAN-A

!

boot-start-marker

boot-end-marker

!

logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

no ip icmp rate-limit unreachable

!

ip cef

!

no ip domain-lookup

no ip v6 cef

ip v6 multicast rpf use-bgp

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

!

interface Ethernet0/0

duplex auto

!

interface Ethernet0/1

duplex auto

!

interface Ethernet0/2

duplex auto

!

interface Ethernet0/3

duplex auto

!

interface Ethernet1/0

duplex auto

!

interface Ethernet1/1

duplex auto

!

interface Ethernet1/2

duplex auto

!

interface Ethernet1/3

duplex auto

!

					КБ.КБ.Б – 125 – 22 – ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet2/0
!
duplex auto
line con 0
!
exec-timeout 0 0
interface Ethernet2/1
privilege level 15
duplex auto
logging synchronous
!
line aux 0
interface Ethernet2/2
exec-timeout 0 0
duplex auto
privilege level 15
!
logging synchronous
interface Ethernet2/3
line vty 0 4
duplex auto
login
!
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
no ip address
shutdown
!
no ip http server
!
control-plane

```

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		