

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми периметрового захисту ге-
терогенної мережі освітнього закладу на базі роутерів
Mikrotik та Cisco»

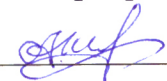
Виконав студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»

 Олександр ДМИТРИЄВ

Керівник старший викладач кафедри КІ та КБ

 Олександра ПОКОТИЛО

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

 Олексій ШЕЛУХА

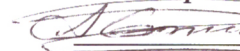
Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Дмитрієв Олександр Геннадійович

Тема роботи: «Проект підсистеми периметрового захисту гетерогенної мережі освітнього закладу на базі роутерів Mikrotik та Cisco»

затверджена Наказом університету від 5 березня 2024 р. №98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

Вихідні дані роботи:

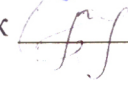
Об'єктом дослідження є процес проектування підсистеми периметрового захисту гетерогенної мережі освітнього закладу на базі роутерів Mikrotik та Cisco

Предметом дослідження є технологія інтеграції роутерів Mikrotik та Cisco в рамках освітнього закладу Обладнання та програмне забезпечення:

- Мережевий емулятор GNS3
- Oracle VM VirtualBox
- Образ маршрутизатора Cisco
- Образ маршрутизатора Mikrotik chr-6.49.15
- Операційна система Linux Ubuntu 22
- Операційна система Windows 10
- FileZilla Client 3.67.0
- Visual Syslog Server 1.6.4

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Морозов Д.С.	05.03.2024	05.03.2024
2	Морозов Д.С.	15.04.2024	15.04.2024
3	Морозов Д.С.	15.05.2024	15.05.2024

Студент  Олександр Дмитрієв
Керівник  Олександра Покотило

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	01.06.24	виконано
2	Аналіз літературних джерел	03.06.24	виконано
3	Аналіз об'єкта дослідження	05.06.24	виконано
4	Постановка задачі дослідження	06.06.24	виконано
5	Розробка структурної моделі	07.06.24	виконано
6	Розрахунок параметрів адресації	08.06.24	виконано
7	Виконання налаштувань	15.06.24	виконано
8	Перевірка працездатності	16.06.24	виконано
9	Оформлення пояснювальної записки	18.06.24	виконано
10	Оформлення презентації	19.06.24	виконано
11	Захист	29.06.24	виконано

Студент  Олександр Дмитрієв
Керівник  Олександра Покотило

АНОТАЦІЯ

У межах кваліфікаційної роботи було розроблено проект підсистеми периметрового захисту для гетерогенної мережі освітнього закладу, використовуючи ресурс від Mikrotik та Cisco. Проект включає в себе перелік умовних скорочень, вступ, три розділи, висновки, список використаної літератури, додатки. Текстова частина викладена на 79 сторінках, кількість рисунків використаних в записці 78 та кількість таблиць 12. Список використаних джерел: 20 найменувань на 2 сторінках. Загальний обсяг роботи – 109 сторінок.

Метою випускної кваліфікаційної роботи є розробка та впровадження ефективної підсистеми периметрового захисту для гетерогенної мережі освітнього закладу, що забезпечує високий рівень інтеграції маршрутизаторів Cisco та Mikrotik та базовий рівень захисту.

Основні результати роботи:

- Проведено аналіз найвідоміших атак та надані варіанти їх запобігання.
- Описано мережеве обладнання, за допомогою якого створено та налаштовано проект.
- Розроблено проект підсистеми периметрового захисту гетерогенної мережі освітнього закладу.
- Створено схему адресації для побудованої мережі.
- Проведено тестування роботи створеного проекту.

КЛЮЧОВІ СЛОВА: ГЕТЕРОГЕННА МЕРЕЖА, ОСВІТНІЙ ЗАКЛАД, ПЕРИМЕТРОВИЙ ЗАХИСТ, ROUTER CISCO, ROUTER MIKROTIK

					ККІК<.КР.Б – 125 – 6– ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Прокт підсистеми периметрового захи- хисту гетерогенної мережі освітнього закла-ду на базі роутерів Mikrotik та Cisco.	Лім.	Арк.	Аркуші	
Розроб.		Дмитрієв О.Г.		28.06					
Керівник		Покотило О.А.		28.06			4	109	
Реценз.		Шелуха О.О.		28.06					
Н. контр.		Покотило О.А.		28.06					
Затверд.		Єфіменко А.А.		28.06					
						ФІКТ, Гр. КБ-20-2			

ANNOTATION

As part of the qualification work, a project for the perimeter security subsystem for the heterogeneous network of an educational institution was developed using resources from Mikrotik and Cisco. The project includes a list of conditional abbreviations, an introduction, three chapters, conclusions, a list of references, and appendices. The text part is presented on 79 pages, the number of figures used in the report is 78, and the number of tables is 12. The list of references contains 20 items spread over 2 pages. The total volume of the work is 109 pages.

The aim of the final qualification work is to develop and implement an effective perimeter security subsystem for the heterogeneous network of an educational institution, ensuring a high level of integration of Cisco and Mikrotik routers and a basic level of security.

The main results of the work:

- An analysis of the most famous attacks was carried out and options for their prevention were provided.
- The network equipment used to create and configure the project is described.
- The project of the perimeter protection subsystem of the heterogeneous network of the educational institution was developed.
- An addressing scheme has been created for the constructed network.
- Testing of the work of the created project was carried out.

KEYWORDS: HETEROGENEOUS NETWORK, EDUCATIONAL INSTITUTION, PERIMETER SECURITY, CISCO ROUTER, MIKROTIK ROUTER.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Cisco IOS - Internetwork Operating System

DDoS - Distributed Denial of Service

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DoS - Denial of Service

EduNet - Educational Network

EIGRP - Enhanced Interior Gateway Routing Protocol

ISI - Integrated Security Infrastructure

MROS - MikroTik RouterOS

NAC - Network Access Control

OSPF - Open Shortest Path First

PSS - Perimeter Security System

QoS - Quality of Service

SSH - Secure Shell

VLAN - Virtual LAN

VPN - Virtual Private Network

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ЗМІСТ

РОЗДІЛ 1. АНАЛІЗ ТА СИСТЕМАТИЗАЦІЯ ОСНОВНИХ ТЕОРИТИЧНИХ ВІДОМОСТЕЙ ПОВ'ЯЗАНИХ З ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ ...	10
1.1 Особливості побудови комп'ютерних гетерогенних мереж	10
1.2 Принципи побудови та функціонування обладнання Cisco та Mikrotik .	11
1.3 Найбільш поширені атаки на гетерогенні комп'ютерні мережі та аналіз загроз мережевої безпеки	15
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖІ ОСВІТНЬОГО ЗАКЛАДУ	21
2.1 Розробка топології комп'ютерної мережі	21
2.2 Розробка схеми адресації мережі	27
2.3 Технології, які налаштовувались в проєкті	33
РОЗДІЛ 3. ПОБУДОВА , НАЛАГОДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ТЕСТУВАННЯ ФУНКЦІОНУВАННЯ МЕРЕЖІ, ЗАСОБІВ ЇЇ ЗАХИСТУ	44
3.1. Вибір обладнання та програмного забезпечення.....	44
3.2. Налагодження обладнання мережі	58
3.3 Тестування функціонування мережі та засобів її захисту	69
ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	79
ДОДАТКИ.....	81

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. В сучасному світі кіберзагрози, стають все більш складними та частими. Освітні заклади є особливо вразливими через великий обсяг даних студентів та співробітників, а також через широкий спектр пристроїв, підключених до мережі. Проєкт підсистеми периметрового захисту допомагає запобігти несанкціонованому доступу, зменшити ризики витоку даних та забезпечити безпеку інформації. Освітні заклади часто використовують різноманітні пристрої та технології для забезпечення навчального процесу. Гетерогенна мережа, що включає обладнання від різних виробників (наприклад, Mikrotik та Cisco), вимагає уніфікованого підходу до захисту, який враховує специфіку кожного типу обладнання та забезпечує сумісність і ефективність захисту. Використання роутерів Mikrotik та Cisco забезпечує високу надійність та продуктивність мережі. Ці пристрої відомі своєю стабільністю, широкими можливостями конфігурації та потужними засобами захисту, що робить їх ідеальними для впровадження в навчальних закладах..

Мета і завдання роботи. Метою роботи є проектування підсистеми периметрового захисту гетерогенної мережі освітнього закладу на базі роутерів Mikrotik та Cisco.

Досягнення поставленої мети потребує вирішення наступних задач:

- Проведення аналізу поняття гетерогенних мереж, принципів роботи
- Розробки мережної структури освітнього закладу
- Проведення тестування безпеки та розробка рішень безпеки на основі цього тестування.
- Перевірка ефективності та якості розробленої структури, проведених тестувань

Об’єктом дослідження є процес проектування підсистеми периметрового захисту гетерогенної мережі освітнього закладу на базі роутерів Mikrotik та Cisco

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Предметом дослідження є технологія інтеграції роутерів Mikrotik та Cisco в рамках освітнього закладу.

Практичне значення роботи. У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми периметрового захисту гетерогенної мережі освітнього закладу на базі роутерів Mikrotik та Cisco, що включає аналіз загроз, проектування мережевої інфраструктури та впровадження засобів захисту з використанням сучасних ресурсів. Рішення на базі Mikrotik та Cisco легко масштабуються відповідно до зростаючих потреб освітнього закладу.

Інтеграція роутерів Mikrotik та Cisco дозволяє ефективно управляти мережевими ресурсами, розподіляти трафік, забезпечувати якість обслуговування (QoS) та здійснювати моніторинг мережевої активності, що сприяє підвищенню ефективності використання мережевих ресурсів та зниженню експлуатаційних витрат

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. АНАЛІЗ ТА СИСТЕМАТИЗАЦІЯ ОСНОВНИХ ТЕОРИТИЧНИХ ВІДОМОСТЕЙ ПОВ'ЯЗАНИХ З ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

1.1 Особливості побудови комп'ютерних гетерогенних мереж

Гетерогенна мережа — це мережа, яка поєднує різні типи комп'ютерних пристроїв, операційних систем та протоколів. Наприклад, локальні мережі (LAN), які з'єднують комп'ютери на базі Windows, Linux та macOS, є гетерогенними[1]. Такі мережі забезпечують інтеграцію різноманітних технологій для забезпечення широкого спектра мережевих послуг та підвищення загальної продуктивності мережі.

Основні характеристики гетерогенних мереж:

- Інтероперабельність: гетерогенні мережі забезпечують взаємодію між різними мережевими пристроями та системами, що використовують різні протоколи та стандарти. Це дозволяє об'єднувати ресурси різних виробників і платформ, забезпечуючи ефективне управління та доступ до них з будь-якої точки мережі.
- Масштабованість: завдяки використанню гетерогенних мереж можливо легко масштабувати мережу, додаючи нові пристрої та технології без необхідності значних змін в існуючій інфраструктурі. Це особливо важливо для великих корпоративних мереж, де потрібна гнучкість і адаптивність до зростаючих вимог.
- Безпека: гетерогенні мережі часто включають різні механізми безпеки, що дозволяє забезпечити захист даних і зменшити ризики атак. Наприклад, використання різних методів аутентифікації та шифрування даних допомагає забезпечити безпеку інформації при її передачі між різними системами.
- Висока доступність та надійність: завдяки можливості використовувати різні типи з'єднань і технологій, гетерогенні мережі забезпечують високу доступність та надійність сервісів. Наприклад, при

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

відмові одного з компонентів мережі, інші компоненти можуть продовжувати роботу, забезпечуючи безперервний доступ до критичних ресурсів.

– Оптимізація трафіку: гетерогенні мережі можуть використовувати різні методи для оптимізації трафіку, такі як балансування навантаження між різними типами мережевих з'єднань (наприклад, Wi-Fi, Ethernet). Це дозволяє забезпечити ефективне використання мережевих ресурсів і підвищити загальну продуктивність мережі.

Виклики при побудові гетерогенних мереж:

– Сумісність: забезпечення сумісності між різними мережевими пристроями та системами може бути складним завданням, оскільки вони можуть використовувати різні протоколи та стандарти. Це вимагає використання спеціальних шлюзів та конвертерів для забезпечення коректної взаємодії.

– Управління та моніторинг: управління гетерогенною мережею може бути складнішим через різноманітність використовуваних технологій та пристроїв. Необхідно використовувати інтегровані системи управління та моніторингу, які здатні забезпечити централізоване управління всіма компонентами мережі[2].

– Безпека: змішування різних технологій та платформ може створювати додаткові ризики для безпеки, тому необхідно ретельно планувати та впроваджувати політики безпеки, що враховують специфіку кожної з використаних технологій.

1.2 Принципи побудови та функціонування обладнання Cisco та Mikrotik

Cisco Systems є одним з провідних виробників мережевого обладнання, яке використовується в різних мережах по всьому світу. Обладнання Cisco відоме своєю надійністю, функціональністю та високою продуктивністю.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11



Рисунок 1.1 - Логотип обладнання Cisco

Основні принципи побудови та функціонування:

- Архітектура та модульність: обладнання Cisco побудоване на модульній архітектурі, що дозволяє легко адаптуватися до змін у мережі. Наприклад, комутатори та маршрутизатори Cisco мають різні слоти для додаткових модулів, таких як порти Ethernet, оптичні інтерфейси та інші[3].

- Протоколи та стандарти: Cisco підтримує широкий спектр мережевих протоколів і стандартів, таких як OSPF, BGP, EIGRP, VLAN, QoS та багато інших. Це забезпечує сумісність з іншими виробниками та гнучкість у налаштуванні мережі.

- Безпека: обладнання Cisco інтегрує розширені функції безпеки, включаючи міжмережеві екрани, VPN, захист від атак DDoS та інші засоби безпеки. Це дозволяє забезпечити високий рівень захисту мережевих інфраструктур.

- Управління та моніторинг: Cisco надає різноманітні інструменти для управління та моніторингу мережі, такі як Cisco Network Assistant, Cisco Prime та інші. Ці інструменти дозволяють адміністраторам ефективно керувати мережами, відслідковувати продуктивність та швидко реагувати на проблеми.

Mikrotik є виробником мережевого обладнання та програмного забезпечення, відомого своєю доступністю та потужними функціями для мережевих адміністраторів. Основні продукти компанії включають маршрутизатори RouterBOARD та операційну систему RouterOS.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12



Рисунок 1.2 - Логотип обладнання MikroTik

Основні принципи побудови та функціонування:

- RouterOS: RouterOS є операційною системою, розробленою для маршрутизаторів Mikrotik, яка надає широкий набір функцій для маршрутизації, управління мережею та безпеки. Вона підтримує різноманітні протоколи та сервіси, такі як OSPF, BGP, MPLS, VPN та інші.
- Гнучкість налаштувань: обладнання Mikrotik дозволяє гнучко налаштовувати мережеві параметри через інтерфейс командного рядка (CLI), графічний інтерфейс WinBox або веб-інтерфейс. Це забезпечує зручність у конфігурації та управлінні мережами.
- Безпека: Mikrotik інтегрує різні функції безпеки, включаючи фільтрацію трафіку, NAT, IPsec VPN та інші засоби захисту. Це допомагає захистити мережі від зовнішніх загроз і забезпечити безпеку даних.
- Ціна та продуктивність: однією з ключових переваг Mikrotik є висока продуктивність за доступною ціною. Це робить обладнання Mikrotik привабливим варіантом для малих і середніх підприємств, які шукають ефективні мережеві рішення.

Ці принципи та можливості роблять обладнання Cisco та Mikrotik потужними інструментами для побудови та управління сучасними мережевими інфраструктурами.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Порівняння Cisco та Mikrotik

Характеристика	Cisco	Mikrotik
Асортимент продукції	Широкий асортимент для підприємств, операторів зв'язку та малих бізнесів (комутатори, маршрутизатори, брандмауери, точки доступу Wi-Fi, мережеві контролери)	В основному маршрутизатори, комутатори та точки доступу Wi-Fi, орієнтовані на малі та середні підприємства
Операційна система	IOS (Internetwork Operating System), NX-OS, IOS-XE, IOS-XR	RouterOS
Простота налаштування	Потребує глибоких знань, часто використовується CLI для конфігурації, наявні GUI та web-інтерфейси для спрощення налаштування	Більш зручна для новачків завдяки інтуїтивно зрозумілому інтерфейсу Winbox, також доступний CLI та web-інтерфейс
Функціональні можливості	Високий рівень функціональності, підтримка багатьох протоколів і технологій, потужні засоби управління та безпеки	Хороший набір функцій для маршрутизації, VPN, брандмауера, QoS, підтримка основних протоколів
Безпека	Високий рівень безпеки, інтегровані функції безпеки, підтримка advanced security features (брандмауери, IPS/IDS, VPN, TrustSec)	Надійний базовий рівень безпеки, вбудовані функції безпеки (брандмауери, VPN), регулярні оновлення безпеки
Ціна	Висока, особливо для підприємницьких рішень та великих мереж	Відносно низька, приваблива для малого та середнього бізнесу
Підтримка та документація	Високоякісна технічна підтримка, обширна документація та навчальні матеріали, сертифікаційні програми (CCNA, CCNP, CCIE)	Хороша підтримка та документація, активна спільнота користувачів, форум, менш розвинені сертифікаційні програми

Порівняння Cisco та Mikrotik

Характеристика	Cisco	Mikrotik
Масштабованість	Висока, рішення для масштабування від малих мереж до великих корпоративних та операторських мереж	Добра для малих та середніх мереж, обмежена масштабованість для великих корпоративних мереж
Інтеграція з іншими системами	Добра інтеграція з іншими мережевими та системами безпеки, підтримка широкого спектру стандартів та протоколів	Підтримка основних стандартів та протоколів, але менш розвинена інтеграція з іншими системами у порівнянні з Cisco

1.3 Найбільш поширені атаки на гетерогенні комп'ютерні мережі та аналіз загроз мережевої безпеки

Найбільш поширені атаки на комп'ютерні мережі

– Malware, або шкідливе програмне забезпечення, включає віруси, черви, трояни, шпигунські програми та програми-вимагачі. Воно може пошкодити або викрасти дані, а також використовувати комп'ютерні ресурси для незаконних цілей.[4] Зокрема, віруси та черви здатні швидко поширюватися через мережі, заражаючи пристрої без участі користувача.



Рисунок 1.3 - Схематичне зображення Malware

– Фішинг – це метод соціальної інженерії, який обманом змушує користувачів надавати конфіденційну інформацію, таку як логіни та паролі,

через підроблені електронні листи або вебсайти. Види фішингу включають spear phishing, який орієнтований на конкретних осіб, та whale phishing, що спрямований на керівників компаній.[5].



Рисунок 1.4 - Схематичне зображення Фішингу

– Атака "людина посередині" (MitM) відбувається, коли зломисник перехоплює та змінює комунікацію між двома сторонами, не підозрюючими про його присутність. Це може призвести до викрадення конфіденційних даних або підробки повідомлень.

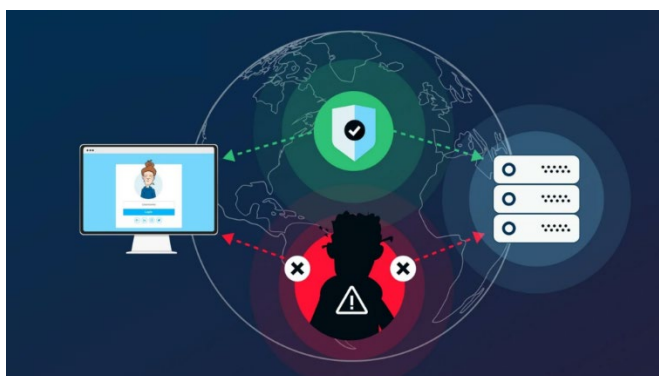


Рисунок 1.5 - Схематичне зображення MitM

– Атаки DoS і DDoS спрямовані на перевантаження системи або мережі надмірним трафіком, що робить її недоступною для законних користувачів. DoS атака виконується одним джерелом, тоді як DDoS атака залучає кілька зломаних комп'ютерів для одночасної атаки на систему.



Рисунок 1.6 - Схематичне зображення DDoS

– SQL-ін'єкція дозволяє зловмисникам виконувати небажані SQL-запити через введення спеціально сформованих даних у вебформи. Це може призвести до викрадення або знищення даних у базі даних.

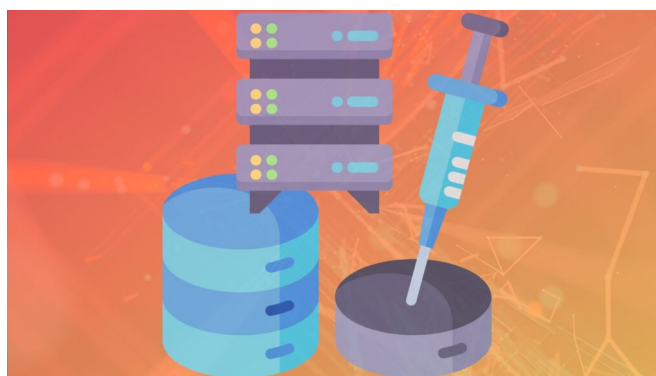


Рисунок 1.7 - Схематичне зображення SQL-ін'єкція

– Експлойт "нульового дня" використовує нещодавно виявлені вразливості у програмному забезпеченні до того, як розробники випустять оновлення для їхнього виправлення. Це дає зловмисникам можливість атакувати системи, які ще не встигли оновитися.

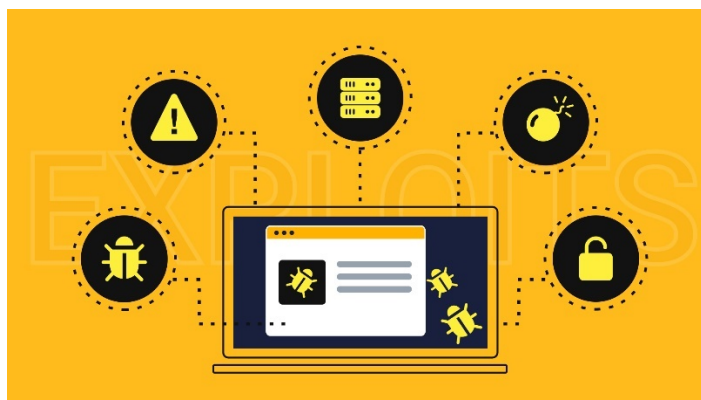


Рисунок 1.8 - Схематичне зображення експлойту "нульового дня"

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

– Програми-вимагачі шифрують файли на заражених системах і вимагають викуп за їх розшифрування. Вони можуть суттєво порушити роботу організацій, блокуючи доступ до важливих даних.[6].



Рисунок 1.9 - Схематичне зображення програм-вимагачів

– АРТ – це тривалі та добре сплановані атаки, які спрямовані на проникнення в мережу і збір конфіденційної інформації протягом тривалого часу. Вони часто використовуються для шпигунства або викрадення даних великих корпорацій та урядів.



Рисунок 1.10 - Схематичне зображення АРТ

– Внутрішні загрози походять від співробітників організації, які мають доступ до її систем і можуть зловживати своїми правами для завдання шкоди. Це можуть бути як навмисні дії, так і ненавмисні помилки.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

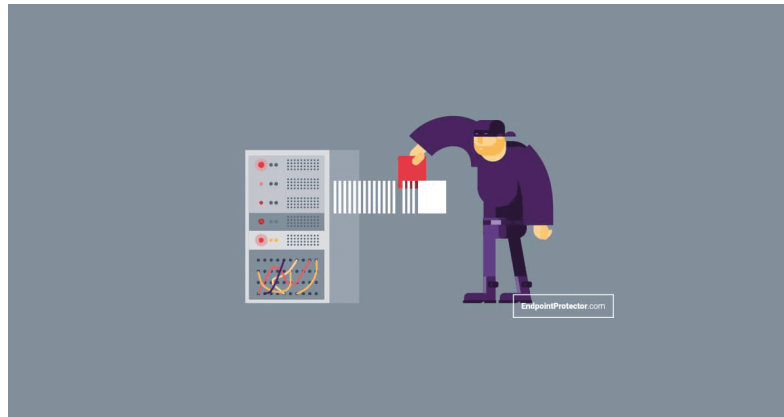


Рисунок 1.11 - Схематичне зображення внутрішніх загроз яку надходять від співробітників

Захист мережі від вищезазначених загроз вимагає комплексного підходу, включаючи впровадження різних технологій і політик безпеки, таких як використання антивірусного програмного забезпечення, налаштування брандмауерів, навчання співробітників правилам безпеки, і постійний моніторинг мережевої активності.

– Використання антивірусного програмного забезпечення: антивірусне програмне забезпечення є ключовим елементом захисту від шкідливого ПЗ, включаючи віруси, черви та програми-вимагачі. Регулярні оновлення баз даних вірусів і систем сканування допомагають виявляти та нейтралізувати загрози до того, як вони можуть завдати шкоди системам.

– Налаштування брандмауерів: брандмауери контролюють вхідний і вихідний трафік у мережі, забезпечуючи бар'єр між довіреними внутрішніми мережами і ненадійними зовнішніми мережами. Вони можуть бути налаштовані для блокування підозрілого трафіку, що може містити шкідливий код або представляти загрозу безпеці.

– Навчання співробітників: людський фактор є однією з найслабших ланок у мережевій безпеці. Регулярне навчання співробітників методам розпізнавання фішингових атак, правильному використанню паролів і інших аспектів кібербезпеки є критично важливим для зменшення ризиків.

– Моніторинг мережевої активності: постійний моніторинг мережевої активності дозволяє виявляти аномалії та підозрілу поведінку, які

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

можуть свідчити про спроби атак або порушення безпеки. Використання систем виявлення вторгнень (IDS) і систем запобігання вторгнень (IPS) допомагає швидко реагувати на інциденти безпеки.

– Використання багатофакторної аутентифікації (MFA): багатофакторна аутентифікація забезпечує додатковий рівень захисту, вимагаючи від користувачів підтвердження їхньої особи за допомогою кількох методів аутентифікації, таких як паролі, мобільні пристрої або біометричні дані. Це значно ускладнює зловмисникам доступ до систем навіть у випадку компрометації одного з факторів.

– Шифрування даних: шифрування конфіденційних даних як під час передачі, так і в стані спокою допомагає захистити інформацію від несанкціонованого доступу. Використання протоколів HTTPS, TLS та інших методів шифрування забезпечує безпечну передачу даних між клієнтами і серверами.

– Регулярне оновлення та патчинг систем: регулярне встановлення оновлень і виправлень програмного забезпечення допомагає усунути відомі вразливості, які можуть бути використані зловмисниками для проведення атак. Автоматизація цього процесу може значно підвищити ефективність захисту.

– Застосування політики мінімальних привілеїв: надання користувачам лише тих доступів і прав, які необхідні для виконання їхніх обов'язків, зменшує ризик внутрішніх загроз і зловживань. Регулярні аудити прав доступу допомагають підтримувати актуальність цієї політики.

Висновки до першого розділу

Під час виконання першого розділу було приведено теоретична інформація щодо особливостей гетерогенних мереж. Проаналізовано найпопулярніші атаки на комп'ютерні мережі та запропоновано захист від цих атак.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ МЕРЕЖІ ОСВІТНЬОГО ЗАКЛАДУ

2.1 Розробка топології комп'ютерної мережі

Більшість атак на мережі спрямовані на такі об'єкти, як мережеві сервіси та додатки, маршрутизатори, комутатори, сервери та дані, що передаються. Ці напади можуть відбуватися на різних рівнях моделі OSI, таких як фізичний, каналний, мережевий, транспортний, сеансовий, рівень представлення та рівень прикладних програм[7].

Тому під час проектування мережі була використана трирівнева структура. Ця структура є логічною та надійною завдяки використанню надмірного апаратного забезпечення.

Таким чином, мережа розподіляється на три рівні:

- Рівень ядра (Core Layer): Цей рівень забезпечує швидкий та ефективний пересилання даних між різними частинами мережі. Він зазвичай має високу пропускну здатність і мінімальну затримку.
- Рівень розподілу (Distribution Layer): На цьому рівні здійснюється маршрутизація і фільтрація трафіку між різними сегментами мережі. Він дозволяє збалансувати навантаження мережі і забезпечити надійність підключення[8].
- Рівень доступу (Access Layer): Цей рівень забезпечує підключення кінцевих пристроїв (наприклад, комп'ютерів, принтерів) до мережі. Він контролює доступ до мережі та забезпечує безпеку на рівні локального підключення.

Ця архітектурна модель дозволяє оптимізувати мережеві ресурси, підвищити ефективність і надійність мережі, а також спростити її керування і підтримку[9].

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

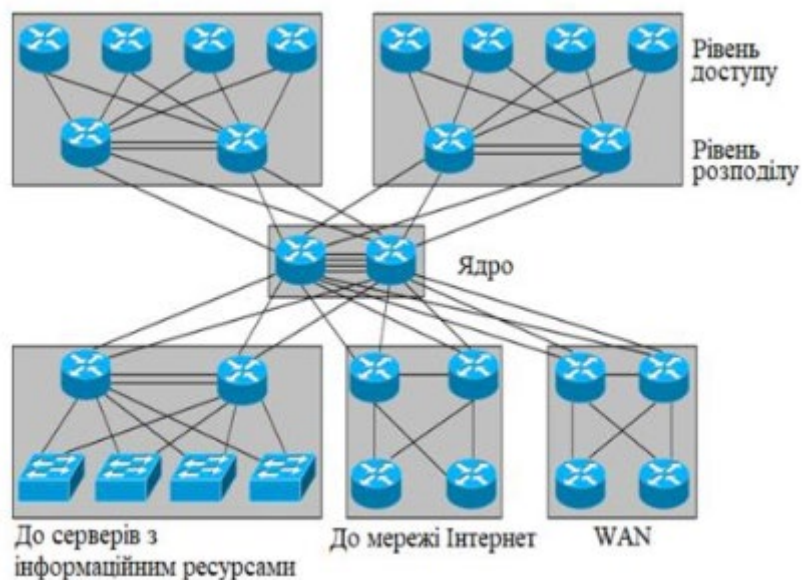


Рисунок 2.1 - Приклад трирівневої структури мережі

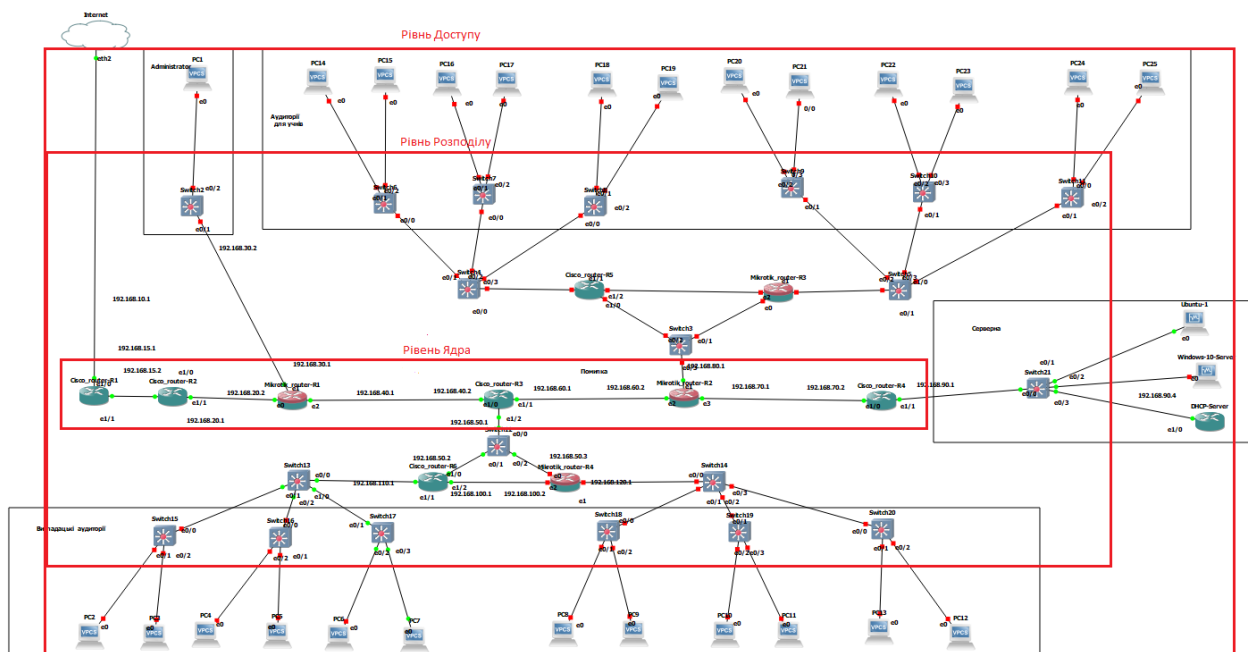


Рисунок 2.2 - Топологія розробленої мережі

Детально розглянемо кожну підмережу, зовнішній вид всіх підмереж зображено на рис 2.3-2.15.

Для підмережі 192.168.150.0 використовується маршрутизатор Cisco, 4 комутатора, 3 робочі станції, одна з яких Windows 10.

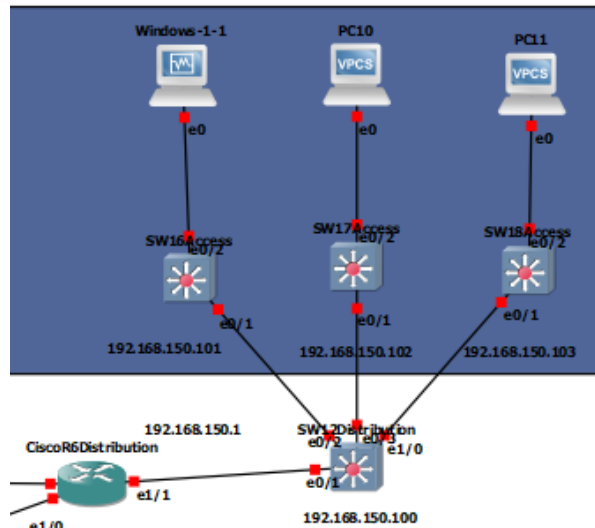


Рисунок 2.3 - Підмережа 192.168.150.0

Для підмережі 192.168.140.0 використовується маршрутизатор Cisco, 4 комутатора, 3 робочі станції, одна з яких Ubuntu Linux.

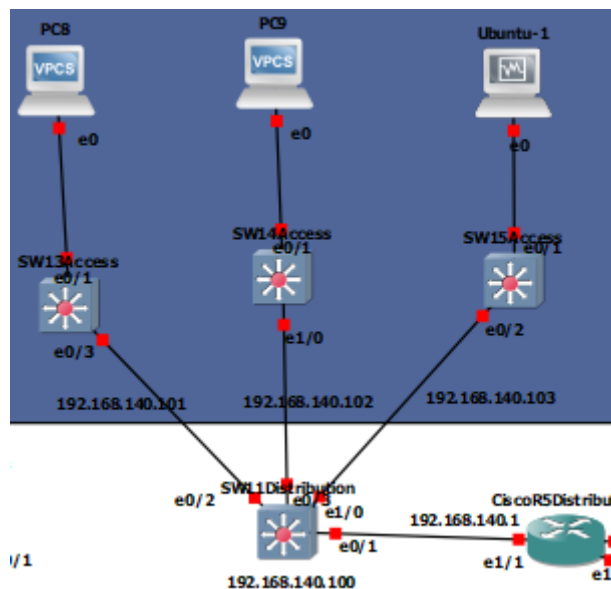


Рисунок 2.4 - Підмережа 192.168.140.0

Для підмережі 192.168.120.0 використовується маршрутизатор Mikrotik, 4 комутатора, 3 робочі станції.

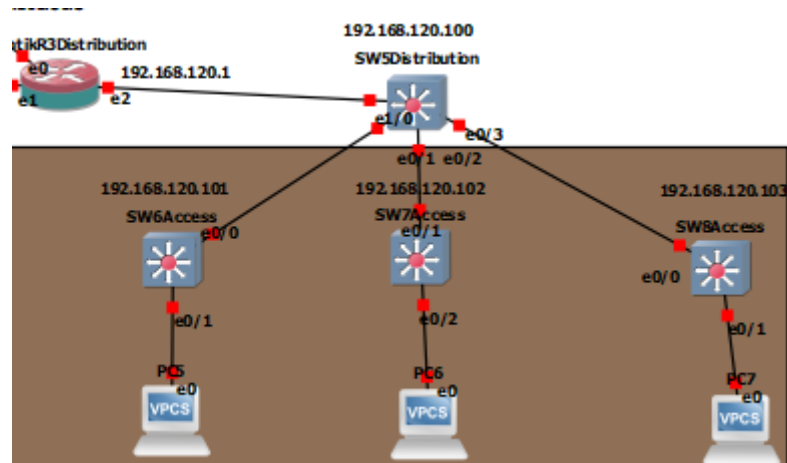


Рисунок 2.5 - Підмережа 192.168.120.0

Для підмережі 192.168.110.0 використовується маршрутизатор Cisco, 4 комутатора, 3 робочі станції.

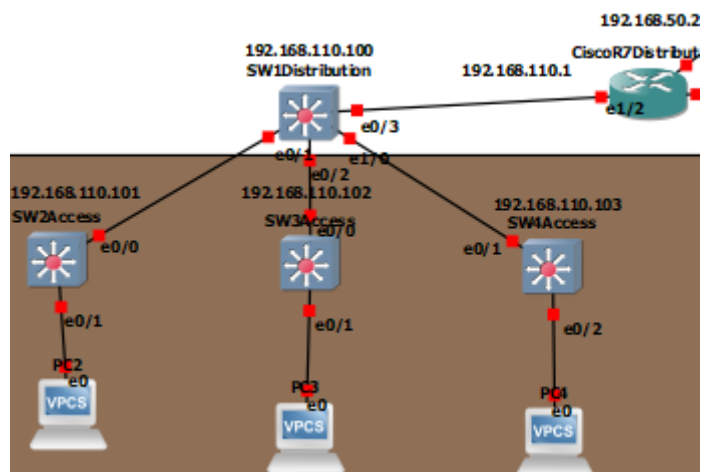


Рисунок 2.6 - Підмережа 192.168.110.0

Для підмережі 192.168.90.0 використовується маршрутизатор Cisco, 1 комутатор, 1 робоча станція Windows 10, яка налаштована в якості сервера.

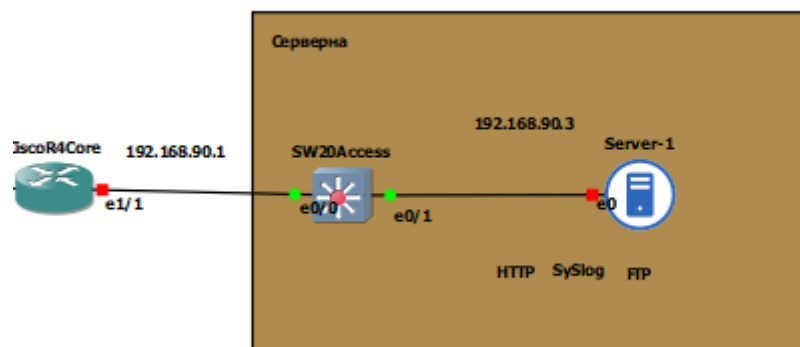


Рисунок 2.7 - Підмережа 192.168.90.0

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Для підмережі 192.168.30.0 використовується маршрутизатор Mikrotik, 1 комутатор, 1 робоча станція.

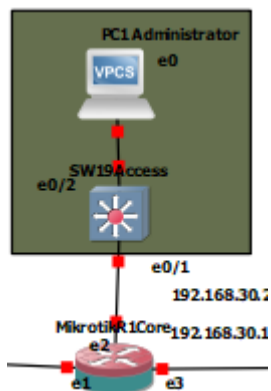


Рисунок 2.8 - Підмережа 192.168.30.0

Для підмережі 192.168.80.0 використовується маршрутизатор Mikrotik та 2 маршрутизатора Cisco, 1 комутатор.

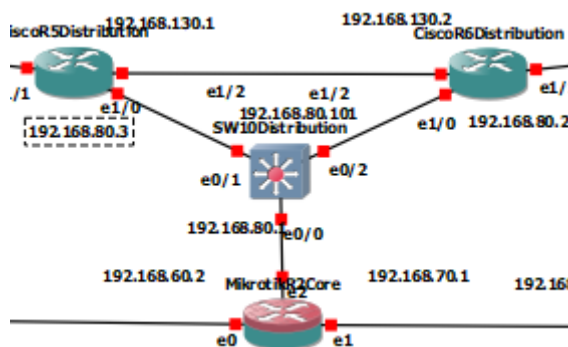


Рисунок 2.9 - Підмережа 192.168.80.0

Для підмережі 192.168.50.0 використовується маршрутизатор Mikrotik та 2 маршрутизатора Cisco, 1 комутатор.

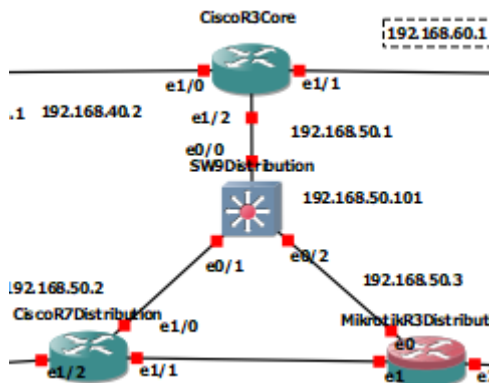


Рисунок 2.10 - Підмережа 192.168.50.0

Для підмережі 192.168.15.0 використовується 3 маршрутизатора Cisco.

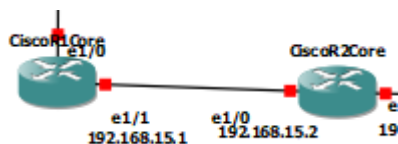


Рисунок 2.11 - Підмережа 192.168.15.0

Для підмережі 192.168.20.0 використовується 1 маршрутизатор Cisco та 1 маршрутизатор Mikrotik.

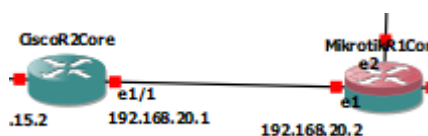


Рисунок 2.12 - Підмережа 192.168.20.0

Для підмережі 192.168.40.0 використовується 1 маршрутизатор Cisco та 1 маршрутизатор Mikrotik.

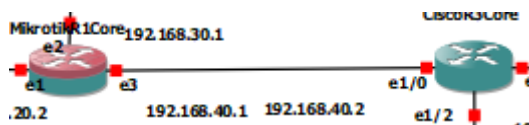


Рисунок 2.13 - Підмережа 192.168.40.0

Для підмережі 192.168.60.0 використовується 1 маршрутизатор Cisco та 1 маршрутизатор Mikrotik.

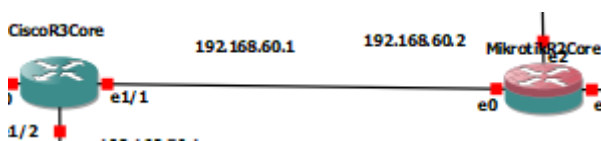


Рисунок 2.14 - Підмережа 192.168.60.0

Для підмережі 192.168.70.0 використовується 1 маршрутизатор Cisco та 1 маршрутизатор Mikrotik.

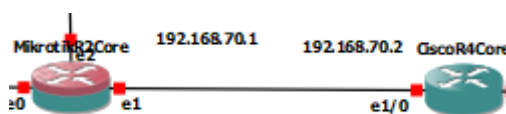


Рисунок 2.15 - Підмережа 192.168.70.0

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

2.2 Розробка схеми адресації мережі

Нижче приведена таблиця адресації мережі.

Таблиця 2.1

Таблиця адресації мережі

Назва пристрою	Підмережа	Інтерфейс	Адреса	Маска	Шлюз
CiscoR1 Core	192.168.10.0	e1/0	192.168.10.1	/30	192.168.10.0
	192.168.15.0	e1/1	192.168.15.1	/30	
CiscoR2 Core	192.168.15.0	e1/0	192.168.15.2	/30	192.168.10.0
	192.168.20.0	e1/1	192.168.20.1	/30	
CiscoR3 Core	192.168.40.0	e1/0	192.168.40.2	/30	192.168.10.0
	192.168.50.0	e1/2	192.168.50.1	/24	
	192.168.60.0	e1/1	192.168.60.1	/30	
CiscoR4 Core	192.168.70.0	e1/0	192.168.70.2	/30	192.168.10.0
	192.168.90.0	e1/1	192.168.90.1	/28	
CiscoR5 Distribution	192.168.80.0	e1/0	192.168.80.3	/24	192.168.10.0
	192.168.130.0	e1/2	192.168.130.1	/30	
	192.168.140.0	e1/1	192.168.140.1	/24	
CiscoR6 Distribution	192.168.80.0	e1/0	192.168.80.2	/24	192.168.10.0
	192.168.130.0	e1/2	192.168.130.2	/30	
	192.168.150.0	e1/1	192.168.150.1	/24	
CiscoR7 Distribution	192.168.50.0	e1/0	192.168.50.2	/24	
	192.168.100.0	e1/1	192.168.100.1	/30	
	192.168.110.0	e1/2	192.168.110.1	/24	

Таблиця адресації мережі

Назва пристрою	Підмережа	Інтерфейс	Адреса	Маска	Шлюз
MikrotikR1 Core	192.168.20.0	ether1	192.168.20.2	/30	192.168.10.0
	192.168.30.0	ether2	192.168.30.1	/28	
	192.168.40.0	ether3	192.168.40.1	/30	
MikrotikR2 Core	192.168.60.0	ether1	192.168.60.2	/30	192.168.10.0
	192.168.70.0	ether2	192.168.70.1	/30	
	192.168.80.0	ether3	192.168.80.1	/24	
MikrotikR3 Distribution	192.168.50.0	ether1	192.168.50.3	/24	192.168.10.0
	192.168.100.0	ether2	192.168.100.2	/30	
	192.168.120.0	ether3	192.168.120.0	/24	

Дана підмережа слугує для розміщення робочих станцій та комутаторів, розташована на рівні доступу та розподілу.

Таблиця 2.2

Параметри адресації підмережі 192.168.140.0

Призначення	ІР-адреса
Адреса мережі	192.168.140.0
Маска мережі	255.255.255.0
Префікс мережі	24
Обернена маска	0.0.0.255
Мінімальна адреса	192.168.140.1
Максимальна адреса	192.168.140.254
Широкомовна	192.168.140.255
Шлюз за замовчуванням	192.168.140.1
Діапазон адрес комутаторів	192.168.140.100-192.168.140.254
Діапазон адрес ПК	192.168.140.2-192.168.140.99

Дана підмережа слугує для розміщення робочих станцій та комутаторів, розташована на рівні доступу та розподілу.

Таблиця 2.3

Параметри адресації підмережі 192.168.150.0

Призначення	ІР-адреса
Адреса мережі	192.168.150.0
Маска мережі	255.255.255.0
Префікс мережі	24
Обернена маска	0.0.0.255
Мінімальна адреса	192.168.150.1
Максимальна адреса	192.168.150.254
Широкомовна	192.168.150.255
Шлюз за замовчуванням	192.168.150.1
Діапазон адрес комутаторів	192.168.150.100-192.168.150.254
Діапазон адрес ПК	192.168.150.2-192.168.150.90

Дана підмережа слугує для розміщення робочих станцій та комутаторів, розташована на рівні доступу та розподілу.

Таблиця 2.4

Параметри адресації підмережі 192.168.120.0

Призначення	ІР-адреса
Адреса мережі	192.168.120.0
Маска мережі	255.255.255.0
Префікс мережі	24
Мінімальна адреса	192.168.120.1
Максимальна адреса	192.168.120.254
Широкомовна	192.168.120.255
Шлюз за замовчуванням	192.168.120.1
Діапазон адрес комутаторів	192.168.120.100-192.168.120.254
Діапазон адрес ПК	192.168.120.2-192.168.120.99

Дана підмережа слугує для розміщення робочих станцій та комутаторів, розташована на рівні доступу та розподілу.

Таблиця 2.5

Параметри адресації підмережі 192.168.110.0

Призначення	ІР-адреса
Адреса мережі	192.168.110.0
Маска мережі	255.255.255.0
Префікс мережі	24
Обернена маска	0.0.0.255
Мінімальна адреса	192.168.110.1
Максимальна адреса	192.168.110.254
Широкомовна	192.168.110.255
Шлюз за замовчуванням	192.168.110.1
Діапазон адрес комутаторів	192.168.110.100-192.168.110.254
Діапазон адрес ПК	192.168.110.2-192.168.110.99

Данна підмережа слугує для з'єднання мережі, знаходиться на рівні ядра

Таблиця 2.6

Параметри адресації підмережі 192.168.30.0

Призначення	ІР-адреса
Адреса мережі	192.168.30.0
Маска мережі	255.255.255.240
Префікс мережі	28
Обернена маска	0.0.0.16
Мінімальна адреса	192.168.30.1
Максимальна адреса	192.168.30.15
Широкомовна	192.168.30.16
Шлюз за замовчуванням	192.168.30.1
Діапазон адрес ПК	192.168.30.3-192.168.30.15

Дана підмережа слугує для з'єднання мережі та розміщення гілки аудиторій викладачів, знаходиться на рівні ядра.

Таблиця 2.7

Параметри адресації підмережі 192.168.50.0

Призначення	ІР-адреса
Адреса мережі	192.168.50.0
Маска мережі	255.255.255.0
Префікс мережі	24
Обернена маска	0.0.0.255
Мінімальна адреса	192.168.50.1
Максимальна адреса	192.168.50.254
Широкомовна	192.168.50.255
Діапазон адрес комутаторів	192.168.50.101-192.168.50.254

Дана підмережа слугує для з'єднання мережі та розміщення гілки аудиторій учнів, знаходиться на рівні ядра.

Таблиця 2.8

Параметри адресації підмережі 192.168.80.0

Призначення	ІР-адреса
Адреса мережі	192.168.80.0
Маска мережі	255.255.255.0
Префікс мережі	24
Обернена маска	0.0.0.255
Мінімальна адреса	192.168.80.1
Максимальна адреса	192.168.80.254
Широкомовна	192.168.80.255
Діапазон адрес комутаторів	192.168.80.101-192.168.110.254

Данна підмережа слугує для та розміщення гілки серверної, знаходиться на частково на всіх рівнях.

Таблиця 2.9

Параметри адресації підмережі 192.168.90.0

Призначення	ІР-адреса
Адреса мережі	192.168.90.0
Маска мережі	255.255.255.240
Префікс мережі	28
Обернена маска	0.0.0.16
Мінімальна адреса	192.168.90.1
Максимальна адреса	192.168.90.15
Широкомовна	192.168.90.16
Шлюз за замовчуванням	192.168.90.1
Діапазон адрес комутаторів	192.168.90.10-192.168.90.15
Діапазон адрес ПК	192.168.90.2-192.168.90.9

Данна підмережа слугує для з'єднання мережі, знаходиться на рівні розподілу.

Таблиця 2.10

Параметри адресації підмережі 192.168.100.0

Призначення	ІР-адреса
Адреса мережі	192.168.100.0
Маска мережі	255.255.255.252
Префікс мережі	30
Обернена маска	0.0.0.3
Мінімальна адреса	192.168.100.1
Максимальна адреса	192.168.100.15
Широкомовна	192.168.100.16

Данна підмережа слугує для з'єднання мережі, знаходиться на рівні розподілу.

Параметри адресації підмережі 192.168.130.0

Призначення	ІР-адреса
Адреса мережі	192.168.130.0
Маска мережі	255.255.255.252
Префікс мережі	30
Обернена маска	0.0.0.3
Мінімальна адреса	192.168.130.1
Максимальна адреса	192.168.130.15
Широкомовна	192.168.130.16

2.3 Технології, які налаштовувались в проєкті

Open Shortest Path First (OSPF) — це протокол маршрутизації, який використовується для обміну маршрутизаційною інформацією між маршрутизаторами всередині однієї автономної системи. OSPF є інтер'єрним протоколом шлюзу (IGP) і базується на алгоритмі стану каналу (Link-State Routing Protocol). Він забезпечує швидке відновлення мережі після змін у топології, таких як відмова лінії зв'язку або додавання нового маршрутизатора

Основні характеристики

- Алгоритм SPF (Shortest Path First): OSPF використовує алгоритм Дейкстри для обчислення найкоротшого шляху до кожного вузла у мережі. Це дозволяє швидко адаптуватися до змін у мережевій топології і забезпечувати ефективну маршрутизацію даних
- Використання метрики "вартість шляху": метрика "вартість" в OSPF зазвичай розраховується на основі пропускної здатності інтерфейсу. Шлях з найменшою вартістю вважається оптимальним для передачі даних. Висока пропускна здатність інтерфейсу знижує його вартість, роблячи його привабливим для маршрутизації

- Мультикаст комунікація: OSPF використовує мультикаст-адреси (224.0.0.5 і 224.0.0.6) для обміну маршрутизаційною інформацією між маршрутизаторами. Це дозволяє знижувати навантаження на інші вузли мережі
- Аутентифікація: OSPF підтримує аутентифікацію, що дозволяє обмінюватися LSAs (Link-State Advertisements) лише між легітимними маршрутизаторами, підвищуючи таким чином безпеку мережі.[10]
- Ієрархічна структура: OSPF використовує концепцію областей (areas) для зменшення кількості маршрутів та оптимізації використання ресурсів. Основною областю є Area 0 (backbone), до якої підключаються всі інші області через маршрутизатори прикордонної області (ABRs - Area Border Routers) (Wikipedia)

Переваги OSPF

- Швидка конвергенція: OSPF швидко адаптується до змін у мережі завдяки тригерним оновленням, що зменшує ймовірність помилок у таблицях маршрутизації та запобігає утворенню петель
- Підтримка VLSM (Variable Length Subnet Mask): це дозволяє ефективніше використовувати IP-адреси та здійснювати більш гнучку маршрутизацію
- Маршрутизація рівного вартості (ECMP - Equal Cost Multi-Path): OSPF може балансувати навантаження між декількома маршрутами однакової вартості, що покращує пропускну здатність і надійність мережі[10].

Недоліки

- Високе навантаження на процесор та пам'ять: через складність алгоритму OSPF вимагає більше ресурсів у порівнянні з простішими протоколами, такими як RIP.

OSPF є потужним протоколом маршрутизації, який забезпечує надійність і гнучкість мережі завдяки своїм розширеним можливостям. Його використання вимагає ретельного планування адресації та налаштувань для досягнення оптимальної продуктивності.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

SSH (Secure Shell) – це криптографічний мережевий протокол, який забезпечує безпечне з'єднання між клієнтом і сервером через небезпечну мережу. Основні функції SSH включають безпечний віддалений доступ до серверів, передачу файлів і тунелювання.

Основні компоненти SSH

– Клієнт та Сервер. SSH використовує модель клієнт-сервер. Клієнт ініціює з'єднання, а сервер приймає запити. Сервер прослуховує на визначеному TCP порту, зазвичай це порт 22, чекаючи на запити від клієнтів.

– Аутентифікація. Для встановлення з'єднання SSH використовує методи асиметричної криптографії, які включають пари публічних та приватних ключів. Клієнт та сервер взаємно аутентифікуються за допомогою цих ключів. Після цього може знадобитися додаткова аутентифікація користувача, яка зазвичай здійснюється введенням паролю або використанням SSH ключів без паролю[11].

– Шифрування. Після аутентифікації клієнт та сервер використовують симетричне шифрування для захисту всієї сесії. Алгоритм обміну ключами Діффі-Геллмана допомагає встановити спільний симетричний ключ, який використовується для шифрування даних під час сесії.

– Тунелювання. SSH дозволяє використовувати тунелювання (або перенаправлення портів), що дозволяє безпечно передавати дані між локальними та віддаленими хостами. Це особливо корисно для доступу до ресурсів у приватних мережах або обхід обмежень брандмауера.

Використання SSH

– Віддалене керування серверами: SSH дозволяє адміністраторам безпечно керувати віддаленими серверами, виконуючи команди так, ніби вони працюють безпосередньо на локальній машині.

– Безпечна передача файлів: SSH використовує протоколи SCP (Secure Copy) і SFTP (SSH File Transfer Protocol) для безпечної передачі файлів між клієнтом і сервером.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

– З'єднання з хмарними сервісами: SSH забезпечує безпечний доступ до хмарних сервісів, захищаючи від експонування локальних портів у Інтернеті[11].

Переваги SSH

– Безпека: Використання сильного шифрування для захисту даних під час передачі.

– Гнучкість: Підтримка різних методів аутентифікації, включаючи паролі та ключі SSH.

– Універсальність: працює на всіх основних операційних системах, включаючи Unix, Linux, MacOS та Windows.

SSH є критично важливим інструментом для безпечного керування та обслуговування віддалених серверів і мережевих ресурсів. Завдяки своїм широким можливостям і високому рівню безпеки, SSH широко використовується в IT-індустрії для забезпечення конфіденційності та цілісності даних.

DHCP (Dynamic Host Configuration Protocol) — це мережевий протокол, який автоматично надає пристроям в мережі IP-адреси та інші параметри конфігурації мережі, такі як маска підмережі, шлюз за замовчуванням і DNS-сервери. Основна мета DHCP — спростити адміністрування мережі, автоматизуючи процес призначення IP-адрес і зменшуючи кількість конфліктів IP-адрес.

Як працює DHCP-сервер:

– DHCP Discover: клієнт надсилає широкомовне повідомлення DHCP Discover, щоб знайти доступні DHCP-сервери.

– DHCP Offer: кожен DHCP-сервер, який отримує запит, відповідає повідомленням DHCP Offer, пропонуючи IP-адресу та інші параметри мережі.

– DHCP Request: Клієнт вибирає одну з пропозицій і надсилає запит DHCP Request на підтвердження вибору.

– DHCP Acknowledgment: вибраний сервер підтверджує присвоєння IP-адреси клієнту повідомленням DHCP Acknowledgment, завершуючи процес.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні компоненти:

- IP-адреси: DHCP автоматично надає IP-адреси з визначеного пулу.
- Маска підмережі: вказує, яка частина IP-адреси належить до мережі, а яка до хоста.
- Шлюз за замовчуванням: IP-адреса маршрутизатора, через який клієнти отримують доступ до інших мереж.
- DNS-сервери: сервери, які перетворюють доменні імена на IP-адреси.

Syslog (System Logging Protocol) — це стандартний протокол для збору і зберігання логів з різних пристроїв у мережі[12]. Використовуючи Syslog, системні адміністратори можуть централізовано зберігати і аналізувати події з різних пристроїв, таких як маршрутизатори, комутатори, сервери та інші мережеві елементи.

Основні функції Syslog-сервера:

- Збір логів: Syslog-сервер отримує логи від різних пристроїв через мережу за допомогою протоколів UDP або TCP.
- Фільтрація і зберігання: сервер може фільтрувати повідомлення на основі різних критеріїв, таких як пріоритет, IP-адреса джерела, зміст повідомлення тощо. Логи зберігаються у файлах на диску, з можливістю ротації за розміром або датою.
- Реагування на події: система може виконувати різні дії при отриманні певних повідомлень, такі як показ попереджень, відправлення електронних листів або виконання зовнішніх програм.

FTP (File Transfer Protocol) — це стандартний мережевий протокол, який використовується для передачі файлів між клієнтом і сервером через TCP/IP мережі. Він дозволяє користувачам завантажувати та завантажувати файли на віддалений сервер. Для налаштування FTP-сервера на Windows 10 було використано Internet Information Services (IIS).

Основні функції FTP:

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докum.	Підпис	Дата		37

– Передача файлів: FTP дозволяє користувачам завантажувати (upload) файли на сервер та завантажувати (download) файли з сервера. Це забезпечує ефективний обмін даними між клієнтом і сервером.

– Аутентифікація та безпека: FTP підтримує різні методи аутентифікації, включаючи використання імені користувача та пароллю. Деякі сервери також дозволяють анонімний доступ, але з обмеженими правами. Для підвищення безпеки використовуються варіанти FTP з шифруванням, такі як FTPS і SFTP[13].

– Відновлення перерваних передач: якщо передача файлів була перервана, FTP дозволяє відновити її з того місця, де вона зупинилася. Це зменшує втрату часу та ресурсів на повторну передачу файлів з самого початку.

– Підтримка різних режимів передачі: FTP працює в активному або пасивному режимі передачі даних. Активний режим використовується, коли клієнт слухає вхідні з'єднання від сервера, а пасивний режим — коли сервер слухає вхідні з'єднання від клієнта, що корисно при роботі за фаєрволами.

– Можливість чергового завантаження: FTP підтримує чергове завантаження файлів, що дозволяє користувачам додавати файли до черги передач і виконувати їх послідовно. Це оптимізує використання мережевих ресурсів та підвищує ефективність передачі даних.

– Взаємодія з файловою системою сервера: користувачі можуть навігувати по файловій системі сервера, використовуючи команди для зміни каталогів, перерахування файлів, створення та видалення каталогів, а також для переміщення і видалення файлів.

HTTP (HyperText Transfer Protocol) — це протокол для обміну інформацією в Інтернеті. IIS (Internet Information Services) — це веб-сервер від Microsoft, який дозволяє налаштовувати та керувати веб-сайтами та веб-додатками на Windows.

Основні функції HTTP:

– Запити та відповіді (Request and Response): HTTP використовує модель запит-відповідь, де клієнт надсилає запити, а сервер повертає відповіді.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Клієнт може запитувати різні ресурси, такі як HTML-документи, зображення, відео, скрипти тощо. Сервер обробляє ці запити і повертає відповідний ресурс або інформацію про статус виконання запиту

- **Методи HTTP (HTTP Methods):** HTTP підтримує різні методи запитів, які вказують на тип дії, яку клієнт хоче виконати на сервері.

- **Заголовки HTTP (HTTP Headers):** заголовки надають додаткову інформацію про запит або відповідь. Вони можуть вказувати на тип контенту, мову, довжину даних, якість з'єднання тощо. Наприклад, заголовок Content-Type вказує тип даних, що передаються, а Authorization може містити токен для аутентифікації користувача.

- **Статуси відповідей (Response Status Codes):** сервери повертають коди статусів для вказівки результату обробки запиту. Наприклад, код 200 OK вказує на успішне виконання запиту, 404 Not Found означає, що ресурс не знайдено, а 500 Internal Server Error сигналізує про внутрішню помилку сервера.[14]

- **Безпека та аутентифікація:** HTTP може використовуватися разом з іншими протоколами, такими як HTTPS, для забезпечення безпечного шифрованого з'єднання. Аутентифікація здійснюється за допомогою заголовків Authorization, де можуть передаватися облікові дані користувачів або токени безпеки

NAT (Network Address Translation) — це мережевий метод, який дозволяє кільком пристроям у приватній мережі використовувати один публічний IP-адрес для виходу в Інтернет. Це здійснюється за допомогою зміни інформації про IP-адресу у заголовках пакетів під час їх проходження через маршрутизатор або інший пристрій NAT.

Основні принципи роботи NAT:

- **Перетворення адреси і порту (NAPT):** NAT дозволяє багатьом пристроям у приватній мережі використовувати один публічний IP-адрес. Під час виходу в Інтернет, маршрутизатор змінює приватні IP-адреси на один

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

публічний IP-адрес, додатково змінюючи номери портів, щоб відстежувати, які відповіді належать якому пристрою.

- Статичний NAT: статичний NAT забезпечує постійне співвідношення між приватним і публічним IP-адресами. Це корисно для серверів, які мають бути доступні з Інтернету за постійною IP-адресою.

- Динамічний NAT: динамічний NAT призначає публічний IP-адрес із пулу доступних адрес на тимчасовій основі, коли пристрій у приватній мережі ініціює з'єднання з Інтернетом.

Налаштування NAT на Cisco ASA:

- Auto NAT (Network Object NAT): цей тип NAT конфігурується всередині об'єктів мережі. NAT-перетворення визначаються всередині конфігурації мережевих об'єктів, що робить процес налаштування простішим і швидшим. Auto NAT часто використовується для статичного NAT, коли локальні сервери мають бути доступні з Інтернету.

- Manual NAT (Twice NAT): цей тип NAT дозволяє більш гнучке налаштування, включаючи політики, що залежать від адреси призначення пакета. Manual NAT використовується для складних сценаріїв, де потрібні специфічні правила перетворення для IP-адрес і портів.

- Dynamic PAT (Port Address Translation): це багатопортова трансляція, яка дозволяє багатьом приватним IP-адресам використовувати один публічний IP-адрес одночасно, використовуючи різні порти для кожного з'єднання. Це знижує витрати на публічні IP-адреси, оскільки один публічний адрес може обслуговувати багато внутрішніх пристроїв.

Port Security — це функція безпеки, яка дозволяє обмежити доступ до портів комутатора на основі MAC-адрес. Вона забезпечує захист від несанкціонованого доступу до мережі, обмежуючи кількість MAC-адрес, які можуть бути асоційовані з портом комутатора.

Основні можливості Port Security:

Обмеження кількості MAC-адрес. Port Security дозволяє встановлювати максимальну кількість MAC-адрес, які можуть бути пов'язані з конкретним

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

портом комутатора. Якщо кількість перевищується, застосовуються заходи безпеки, такі як блокування порту.

Види порушень:

- Protect: дискардує трафік від неавторизованих MAC-адрес, але залишає порт активним і не надсилає повідомлення SNMP.
- Restrict: дискардує трафік від неавторизованих MAC-адрес, залишає порт активним і надсилає повідомлення SNMP.
- Shutdown: дискардує трафік від неавторизованих MAC-адрес, надсилає повідомлення SNMP і відключає порт.

Налаштування статичних і динамічних MAC-адрес. Можна вручну вказати MAC-адреси, дозволені на порту, або дозволити комутатору динамічно навчатися MAC-адресам за допомогою команди "sticky".

DHCP Snooping — це функція безпеки мережі, яка запобігає атакам на основі DHCP, таких як атаки «людина посередині» та несанкціоноване використання DHCP-серверів. Ця технологія працює на комутаторах і забезпечує моніторинг та контроль DHCP-повідомлень, які проходять через мережу.

Основні можливості DHCP Snooping:

- Фільтрація DHCP-повідомлень. DHCP Snooping перевіряє всі DHCP-повідомлення, що надходять через комутатор, та дозволяє або блокує їх залежно від конфігурації портів як довірених або недовірених.
- Запобігання атакам DHCP. Ця функція захищає мережу від несанкціонованих DHCP-серверів, які можуть надсилати підроблені IP-адреси клієнтам, змушуючи їх надсилати трафік через зловмисний сервер.
- DHCP Snooping Binding Database. Комутатор створює і підтримує базу даних DHCP Snooping, яка містить інформацію про призначені IP-адреси, MAC-адреси, порти комутатора і час оренди IP-адрес. Це допомагає у відстеженні і перевірці правильності DHCP-запитів і відповідей.
- Опція 82 (DHCP Relay Agent Information Option). DHCP Snooping може додавати опцію 82 до DHCP-повідомлень, що допомагає ідентифікувати

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

джерело запиту. Це забезпечує додатковий рівень безпеки і контроль над DHCP-трафіком.

BPDU (Bridge Protocol Data Unit) — це тип мережевого пакету, який використовується протоколом Spanning Tree Protocol (STP) для запобігання петлям у мережі. На маршрутизаторах та комутаторах Cisco BPDU відіграє критичну роль в управлінні та забезпеченні стабільності мережевої інфраструктури.

BPDU передаються між комутаторами для обміну інформацією про топологію мережі. STP використовує цю інформацію для визначення оптимального шляху передачі даних і для виявлення та запобігання петлям у мережі. Існують два основні типи BPDU:

- Configuration BPDUs: використовуються для обміну інформацією про структуру мережі та для визначення кореневого комутатора.
- Topology Change Notification (TCN) BPDUs: використовуються для інформування інших комутаторів про зміни в топології мережі.

Основні функції BPDU на маршрутизаторах Cisco:

- Запобігання мережевим петлям: BPDU допомагають STP виявляти та запобігати петлям, які можуть виникнути в мережі, що призводить до зменшення продуктивності мережі або її повного збої.
- Визначення кореневого комутатора: STP використовує BPDUs для обрання кореневого комутатора (root bridge), який стає центральною точкою керування трафіком у мережі.
- Вибірка шляхів та портів: BPDU допомагають визначити, які порти будуть активними (forwarding) та які будуть заблоковані (blocking) для забезпечення петлі-free топології.
- Інформування про зміни в топології: коли в мережі відбуваються зміни, такі як підключення або відключення комутатора, TCN BPDU повідомляють інші комутатори про ці зміни, щоб вони могли відповідно оновити свої таблиці маршрутизації.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докum.	Підпис	Дата		42

Забезпечення стабільності мережі: Регулярний обмін BPDUs між комутаторами забезпечує постійну перевірку та оновлення інформації про топологію мережі, що дозволяє швидко виявляти та реагувати на проблеми.

Висновки до другого розділу

Під час виконання другого розділу було розроблено проект глобальної мережі організації та наведено обґрунтування структури мережі та зв'язків між підмережами. Розроблено схему адресації для побудованої глобальної мережі. Ця схема дозволить досить легке управління ір-адресами пристроїв та дозволить в подальшому можливість розширити мережу. Наведено список налаштованих технологій в мережі

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

РОЗДІЛ 3. ПОБУДОВА , НАЛАГОДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ТЕСТУВАННЯ ФУНКЦІОНУВАННЯ МЕРЕЖІ, ЗАСОБІВ ЇЇ ЗАХИСТУ

3.1. Вибір обладнання та програмного забезпечення



Рисунок 3.1 – Маршрутизатор MikroTik версії chr-6.49.15

Маршрутизатор MikroTik версії chr-6.49.15 є віртуальним маршрутизатором, який використовується у програмному комплексі GNS3 для моделювання мережних топологій. Ось основні характеристики цієї версії MikroTik:

- Версія: chr-6.49.15. Це означає, що вона базується на версії RouterOS 6.49.15, яка має свої унікальні функції і вдосконалення.
- Тип: віртуальний маршрутизатор. Використовується для емуляції реального обладнання MikroTik у віртуальних середовищах, таких як GNS3.
- Функціональність. MikroTik RouterOS надає широкий спектр мережних сервісів, таких як маршрутизація, фаєрвол, VPN, DHCP, моніторинг мережі тощо.
- Використання. Використовується для моделювання складних мережних топологій. Він інтегрується з GNS3 як віртуальний образ, що дозволяє імітувати різні сценарії мережі перед їх реалізацією в реальних умовах.

- Конфігурування. Для налаштування MikroTik RouterOS потрібно використовувати консольне або веб-інтерфейси, зазвичай доступні через SSH або веб-браузер.
- Властивості. Підтримує широкі можливості маршрутизації, VLAN, безпеки, управління bandwidth, моніторингу мережі та інших сучасних функцій. Загалом, MikroTik RouterOS у версії chr-6.49.15 є потужним інструментом для віртуалізації мережного обладнання, що дозволяє ефективно тестувати розробляти різні мережні сценарії без реального обладнання.



Рисунок 3.2 – Маршрутизатор Cisco 7200

Cisco 7200 є одним із серійних маршрутизаторів Cisco, призначеним для використання в середніх і великих мережах. Ось основні характеристики цього маршрутизатора:

- Модель. Cisco 7200 Series Router. Це маршрутизатор серії 7200, що випускається Cisco Systems.
- Функціонал. Cisco 7200 пропонує високопродуктивну маршрутизацію і доступ до мережі. Підтримує широкий спектр протоколів маршрутизації, включаючи OSPF, EIGRP, BGP, RIP. Підтримує VPN (Virtual Private Network), QoS (Quality of Service), NAT (Network Address Translation) і багато інших мережних сервісів.
- Продуктивність. В залежності від моделі і конфігурації, Cisco 7200 може обробляти великі обсяги мережевого трафіку і має високу швидкість обробки пакетів.

- Використання. Використовується в середніх і великих корпоративних мережах, провайдерських мережах та для розробки рішень з управління мережами.
- Конфігурація. Для налаштування Cisco 7200 використовуються CLI (Command Line Interface) та GUI інтерфейси, такі як Cisco IOS.
- Інтеграція з GNS3; В GNS3 Cisco 7200 може бути використаний як віртуальний маршрутизатор для моделювання різних мережних топологій.

Загалом, Cisco 7200 є потужним маршрутизатором з широким спектром функціоналу і високою продуктивністю, що робить його популярним вибором для великих мереж і мережних додатків.

Мережевий емулятор GNS3 (Graphical Network Simulator-3) є потужним інструментом, який широко використовується для моделювання та тестування мережевих конфігурацій. Ось вигляд його інтерфейсу:

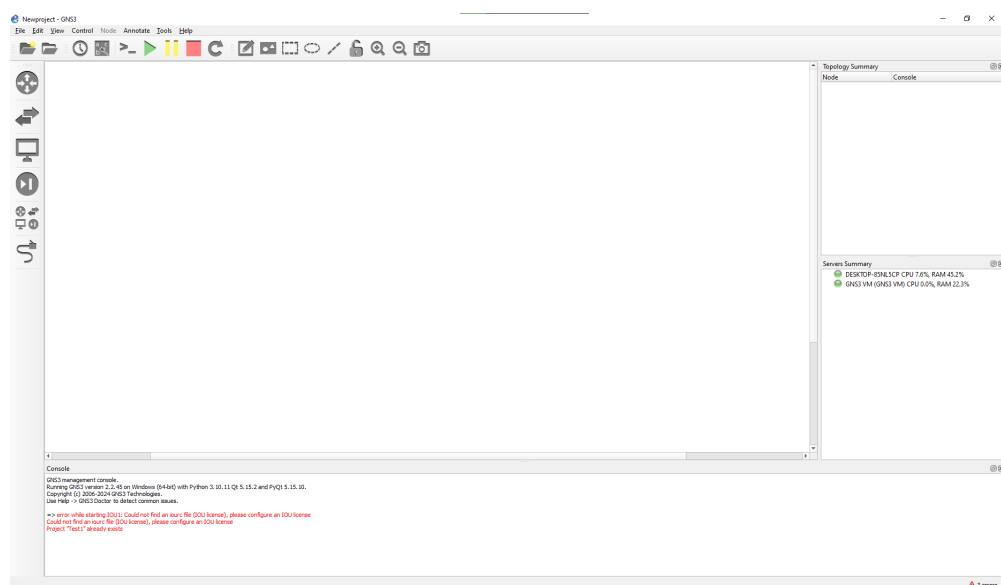


Рисунок 3.3 Вигляд інтерфейсу GNS3

Це програмне забезпечення дозволяє створювати складні мережеві топології, комбінуючи віртуальні пристрої з реальними, що дозволяє значно спростити процес навчання та тестування нових технологій без необхідності придбання дорогого обладнання.

GNS3 забезпечує можливість емуляції реальних мережевих пристроїв, таких як маршрутизатори та комутатори Cisco, а також пристроїв інших виробників, включаючи Mikrotik. Це досягається завдяки використанню

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

емуляційних движків, таких як Dynamips, QEMU та VirtualBox, які дозволяють запускати операційні системи цих пристроїв у віртуальному середовищі.

Однією з основних переваг GNS3 є його інтеграція з реальними пристроями та іншими емуляторами, що дозволяє створювати гібридні мережі[15]. Це особливо корисно для тестування нових конфігурацій перед їх впровадженням у реальному середовищі, що мінімізує ризик виникнення проблем та збоїв у роботі мережі.

GNS3 також підтримує функції трасування пакетів та аналізу мережевого трафіку, що дозволяє детально досліджувати поведінку мережі та ідентифікувати потенційні проблеми. Завдяки цьому, студенти та професіонали мають можливість отримати глибокі знання та практичні навички в налаштуванні та управлінні мережами.

При створенні підсистеми периметрового захисту гетерогенної мережі освітнього закладу, GNS3 є незамінним інструментом. Він дозволяє моделювати мережеву топологію, що складається з маршрутизаторів Mikrotik та Cisco, налаштовувати та тестувати політики безпеки, аналізувати їх ефективність та знаходити оптимальні рішення для забезпечення надійного захисту мережі.

Таким чином, використання GNS3 в ході роботи над дипломним проектом надає можливість створити реалістичну модель мережі, випробувати різні конфігурації та налаштування без ризику вплинути на роботу реальних систем, що є критично важливим для забезпечення високого рівня безпеки та надійності мережі освітнього закладу.

VirtualBox — це потужний програмний продукт, який дозволяє користувачам створювати і управляти віртуальними машинами на своєму комп'ютері. Розроблений компанією Oracle, VirtualBox підтримує широкий спектр операційних систем, включаючи Windows, Linux, macOS та інші, що робить його універсальним інструментом для тестування і розробки. Ось вигляд його інтерфейсу:

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

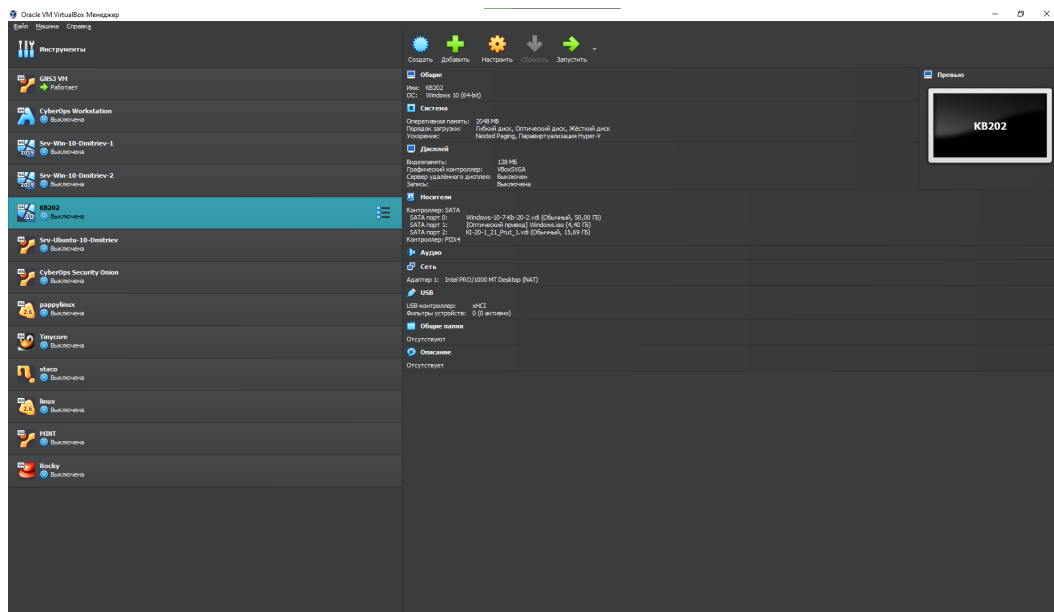


Рисунок 3.4 Вигляд інтерфейсу VirtualBox

Основні можливості VirtualBox включають:

- підтримка багатьох гостей ОС; VirtualBox дозволяє запускати різні операційні системи одночасно на одному фізичному комп'ютері, що особливо корисно для тестування програмного забезпечення в різних середовищах[16];
- безшовна інтеграція; за допомогою функції безшовного режиму, користувачі можуть інтегрувати вікна гостьової ОС у свою основну робочу середу, що робить роботу з віртуальними машинами більш природною і зручною;
- мережеві можливості; VirtualBox підтримує різні режими мережевого підключення, включаючи NAT, Bridged, Host-only та інші, що дозволяє створювати складні мережеві топології і тестувати мережеві налаштування;
- знімки системи; користувачі можуть створювати знімки стану віртуальної машини, що дозволяє легко повертатися до попереднього стану системи у разі виникнення проблем або помилок;
- підтримка загального буферу обміну і спільних папок; ці функції спрощують обмін даними між гостьовою і хостовою ОС, що підвищує продуктивність і зручність використання.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

При розробці підсистеми периметрового захисту гетерогенної мережі освітнього закладу, VirtualBox відіграє ключову роль у створенні і тестуванні віртуальних середовищ. Завдяки можливості запускати різні операційні системи і налаштовувати їх мережеві параметри, VirtualBox дозволяє моделювати і перевіряти роботу мережевих пристроїв, таких як маршрутизатори Mikrotik та Cisco, у віртуальному середовищі.

Загалом, використання VirtualBox у ході роботи над дипломним проектом забезпечує гнучкість та ефективність процесу тестування і розробки, дозволяючи створювати реалістичні моделі мереж і перевіряти їхню функціональність без ризику для реального обладнання.

Операційна система маршрутизаторів Cisco та компанія Cisco



Рисунок 3.5 Логотип Cisco ios

Cisco IOS (Internetwork Operating System) — це операційна система, яка використовується в більшості маршрутизаторів і комутаторів Cisco; вона є ключовим компонентом мережевого обладнання Cisco, забезпечуючи основні функції для керування та маршрутизації трафіку в мережі.

Основні можливості та характеристики Cisco IOS включають:

- різноманітність функцій; Cisco IOS підтримує широкий спектр мережевих функцій, включаючи маршрутизацію, комутацію, забезпечення безпеки, управління трафіком та багато інших; це дозволяє створювати складні і надійні мережеві архітектури;
- масштабованість; Cisco IOS може використовуватися на різних типах мережевих пристроїв, від невеликих маршрутизаторів для домашніх і

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

офісних мереж до потужних комутаторів і маршрутизаторів для великих корпоративних і провайдерських мереж;

- інтерфейс командного рядка (CLI) основним засобом управління пристроями з Cisco IOS є інтерфейс командного рядка (CLI); CLI дозволяє адміністратору виконувати різноманітні налаштування та управлінські завдання за допомогою текстових команд. це забезпечує високу гнучкість та контроль над конфігурацією пристроїв;

- безпека; Cisco IOS підтримує широкий спектр функцій безпеки, включаючи доступ на основі ролей (Role-Based Access Control, RBAC), VPN (Virtual Private Network), фаєрволи, захист від DDoS атак, фільтрацію трафіку та інші механізми захисту;

- мережеві протоколи; Cisco IOS підтримує всі основні мережеві протоколи, такі як OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol), BGP (Border Gateway Protocol), MPLS (Multiprotocol Label Switching) та багато інших. це забезпечує сумісність з різноманітними мережевими інфраструктурами і дозволяє ефективно маршрутизувати трафік;

- оновлення та підтримка; Cisco регулярно випускає оновлення для IOS, що включають нові функції, покращення продуктивності та виправлення безпекових вразливостей; це забезпечує постійне вдосконалення та адаптацію операційної системи до змін у мережевих технологіях.

При створенні підсистеми периметрового захисту гетерогенної мережі освітнього закладу, Cisco IOS є ключовим компонентом для налаштування та управління маршрутизаторами Cisco; використання можливостей цієї операційної системи дозволяє ефективно забезпечити маршрутизацію трафіку, налаштувати політики безпеки та забезпечити надійний захист мережі.

В роботі використано маршрутизатор c7200-adventerprisek9-mz.124-24.T5

Загалом, Cisco IOS є важливим інструментом для побудови надійних та безпечних мереж, що робить його незамінним у ході роботи над дипломним проектом.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Операційна система маршрутизаторів MikroTik



Рисунок 3.6 Логотип MikroTik

RouterOS — це операційна система, яка використовується на маршрутизаторах Mikrotik; вона забезпечує широкий спектр функцій для управління та налаштування мережевих пристроїв, що дозволяє створювати потужні та гнучкі мережеві інфраструктури[16].

Основні можливості та характеристики RouterOS включають:

- широкий набір функцій; RouterOS підтримує різноманітні мережеві функції, такі як маршрутизація, комутація, управління смугою пропускання, забезпечення безпеки, VPN, брандмауер, QoS (Quality of Service) та інші; це дозволяє створювати складні мережеві конфігурації, адаптовані під конкретні потреби;
- графічний інтерфейс користувача (GUI); RouterOS має інтуїтивно зрозумілий графічний інтерфейс користувача, що дозволяє легко налаштовувати та управляти пристроями; крім того, доступний інтерфейс командного рядка (CLI) для більш просунутих користувачів, які віддають перевагу налаштуванню через текстові команди;
- безпека. RouterOS включає різноманітні функції безпеки, такі як фільтрація трафіку, брандмауер, захист від DoS-атак, підтримка VPN (PPTP, L2TP, IPsec), аутентифікація користувачів та контроль доступу; це забезпечує надійний захист мережевої інфраструктури від зовнішніх та внутрішніх загроз;
- гнучкість у налаштуванні; RouterOS дозволяє детально налаштовувати мережеві параметри та адаптувати пристрій до конкретних умов

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

експлуатації; це включає налаштування маршрутизації, управління смугою пропускання, налаштування безпекових політик та інші аспекти;

- підтримка різних мережевих протоколів; RouterOS підтримує всі основні мережеві протоколи, включаючи OSPF, BGP, RIP, MPLS та інші; це забезпечує сумісність з іншими мережевими пристроями та системами, дозволяючи інтегрувати маршрутизатори Mikrotik у вже існуючі мережеві інфраструктури;

- моніторинг та аналіз; RouterOS надає потужні інструменти для моніторингу мережевого трафіку, аналізу продуктивності та виявлення проблем; це включає можливості логування, графіки трафіку, аналізатор пакетів та інші інструменти для детального дослідження роботи мережі.

При розробці підсистеми периметрового захисту гетерогенної мережі освітнього закладу, RouterOS є ключовим компонентом для налаштування та управління маршрутизаторами Mikrotik; завдяки своїй гнучкості, широкому набору функцій та інтуїтивно зрозумілому інтерфейсу, RouterOS дозволяє ефективно забезпечити захист мережі, налаштовувати політики безпеки та управляти трафіком у складній мережевій інфраструктурі.

В роботі використано Mikrotik chr-6.49.15.img.

Загалом, RouterOS є важливим інструментом для створення надійних та безпечних мереж, що робить його незамінним у ході роботи над дипломним проектом.

Windows 10, розроблена компанією Microsoft, є однією з найпопулярніших операційних систем для персональних комп'ютерів. Незважаючи на те, що вона переважно призначена для настільного використання, її також можна використовувати для налаштування серверів у невеликих і середніх мережах завдяки її гнучкості та широкому набору функцій. У середовищі GNS3 Windows 10 може бути використана як віртуальна машина для моделювання серверних функцій.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52



Рисунок 3.7 Логотип Windows 10

Основні можливості Windows 10 для налаштування серверів включають:

- користувацький інтерфейс; зручний графічний інтерфейс, що дозволяє легко налаштовувати серверні параметри навіть користувачам з обмеженими технічними знаннями;
- сумісність з програмним забезпеченням, підтримка широкого спектру програмного забезпечення, яке може використовуватися для управління мережею, моніторингу та налаштування серверних служб;
- безпека. вбудовані засоби безпеки, такі як Windows Defender, BitLocker та регулярні оновлення безпеки, що забезпечують захист серверних систем;
- дистанційне управління. підтримка функцій віддаленого робочого столу та Windows PowerShell, які дозволяють керувати серверами дистанційно; у середовищі GNS3 Windows 10 може бути використана для моделювання серверних ролей, таких як DNS, DHCP, та інших мережевих служб.
- розгортання та налаштування. За допомогою інструментів, таких як Windows Deployment Services (WDS) та Microsoft Deployment Toolkit (MDT), можна автоматизувати процес розгортання Windows 10 на серверах та налаштовувати їх відповідно до вимог мережі[19].

Ubuntu Linux — це популярний дистрибутив операційної системи Linux з відкритим вихідним кодом, який широко використовується в серверних середовищах завдяки своїй надійності, гнучкості та безпеці. Ubuntu має різні

версії, які можуть використовуватися для різних завдань, включаючи серверні застосування.



Рисунок 3.8 Логотип Linux Ubuntu

Основні можливості Ubuntu для налаштування серверів включають:

- Гнучкість та налаштованість. Ubuntu дозволяє користувачам налаштовувати систему відповідно до їхніх потреб, що робить його ідеальним для різних серверних застосувань. Користувачі можуть легко налаштувати конфігураційні файли, встановлювати та видаляти програмне забезпечення і модифікувати системні параметри.
- Безпека: Високий рівень безпеки завдяки регулярним оновленням, багаторівневій системі прав доступу та активній спільноті розробників. Ubuntu часто отримує оновлення безпеки і має вбудовані механізми для захисту від загроз, таких як AppArmor та брандмауер UFW (Uncomplicated Firewall).
- Продуктивність: Ubuntu є менш ресурсомістким порівняно з деякими іншими операційними системами, що забезпечує високу продуктивність навіть на менш потужних системах. Це робить Ubuntu ідеальним вибором для серверів, які потребують ефективного використання ресурсів.
- Віддалене управління: Широкий набір інструментів для віддаленого управління, таких як SSH, що дозволяє ефективно керувати серверами з будь-якої точки світу. SSH забезпечує безпечний доступ до серверів, дозволяючи адміністраторам виконувати команди, передавати файли і налаштовувати системи віддалено.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

– Сумісність з мережевими сервісами: Ubuntu підтримує всі основні мережеві протоколи та сервіси, що робить його ідеальним вибором для налаштування серверних ролей, таких як веб-сервери (Apache, Nginx), бази даних (MySQL, PostgreSQL), поштові сервери та інші. Це забезпечує гнучкість та інтеграцію з існуючими мережевими інфраструктурами[18].

У середовищі GNS3 Ubuntu може бути використаний для моделювання серверних середовищ і налаштування різноманітних мережеслужб. Це дозволяє тестувати та відпрацьовувати конфігурації у віртуальному середовищі перед впровадженням у реальну мережу, що знижує ризики помилок та підвищує ефективність впровадження нових технологій.

FileZilla — це популярний клієнт FTP з відкритим вихідним кодом, який використовується для передачі файлів між комп'ютером користувача та віддаленим сервером. Він підтримує різні протоколи, включаючи FTP, FTPS (FTP Secure), і SFTP (SSH File Transfer Protocol), що робить його універсальним інструментом для адміністраторів мереж та користувачів, які потребують простого способу керування файлами на сервері.



Рисунок 3.9 Логотип FileZilla

FileZilla розробляється та підтримується спільнотою розробників з використанням відкритого вихідного коду. Вперше програма була випущена в 2001 році і з того часу отримала численні оновлення та покращення. Вона доступна для основних операційних систем, таких як Windows, macOS та Linux, що забезпечує широку доступність для користувачів по всьому світу.

Основні функції FileZilla:

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

- Підтримка декількох протоколів: FileZilla підтримує FTP, FTPS і SFTP, що дозволяє користувачам безпечно передавати файли через різні мережі.
- Менеджер сайтів: ця функція дозволяє користувачам зберігати дані про свої FTP-сервери, включаючи ім'я хоста, порт, тип входу та дані для аутентифікації, що значно спрощує підключення до різних серверів.
- Черга передачі файлів: FileZilla забезпечує можливість створення черги для передачі файлів, що дозволяє користувачам бачити, які файли передаються в даний момент, і які заплановані для передачі.
- Підтримка великих файлів: програма підтримує передачу файлів розміром до 4 ГБ, що робить її придатною для професійного використання, де часто потрібна робота з великими обсягами даних.
- Редагування файлів на сервері: FileZilla дозволяє редагувати файли прямо на сервері. Після редагування файл автоматично завантажується назад на сервер.
- Інтуїтивно зрозумілий інтерфейс: FileZilla має зручний графічний інтерфейс користувача з підтримкою перетягування файлів, що спрощує навігацію та керування файлами.
- Можливість відновлення перерваних завантажень: програма підтримує функцію відновлення передачі файлів, що була перервана, дозволяючи користувачам продовжувати передачу з місця зупинки.
- Конфігурація швидкісних обмежень: користувачі можуть налаштувати швидкісні обмеження для передачі файлів, що дозволяє контролювати використання мережевих ресурсів.

FileZilla є відмінним вибором для тих, хто шукає надійний та багатофункціональний FTP-клієнт з відкритим вихідним кодом. Його широкі можливості та зручність у використанні роблять його популярним серед як початківців, так і досвідчених користувачів[19].

Visual Syslog — це легкий та зручний інструмент для моніторингу журналів системних подій в режимі реального часу. Він є простим у

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

використанні та забезпечує зручний графічний інтерфейс для аналізу системних логів, що робить його корисним інструментом для адміністраторів систем[20].

Visual Syslog Server for Windows розроблено для прийому та відображення повідомлень від різних пристроїв та додатків, що підтримують протокол Syslog. Програма є безкоштовною і доступною для операційної системи Windows. Вона дозволяє отримувати та аналізувати події, допомагаючи швидко реагувати на потенційні проблеми в системі.

Основні функції Visual Syslog

- Реальний час: Visual Syslog забезпечує моніторинг журналів у реальному часі, що дозволяє швидко реагувати на події, що відбуваються в системі.
- Зручний інтерфейс: програма має простий та інтуїтивно зрозумілий інтерфейс, що робить її доступною для користувачів різного рівня підготовки.
- Фільтрація та пошук: Visual Syslog дозволяє налаштовувати фільтри для відображення лише тих повідомлень, які вас цікавлять, а також здійснювати пошук за конкретними критеріями.
- Архівація логів: можливість зберігання та архівації системних логів для подальшого аналізу та звітності.
- Підтримка Syslog протоколу: програма підтримує стандартний протокол Syslog, що дозволяє інтегрувати її з широким спектром мережевих пристроїв та додатків.
- Налаштовані сповіщення: Visual Syslog може відправляти сповіщення при виникненні певних подій, що дозволяє швидко реагувати на критичні ситуації.
- Легкість у використанні: завдяки простоті встановлення та налаштування, Visual Syslog є зручним рішенням для моніторингу логів навіть у невеликих мережах.

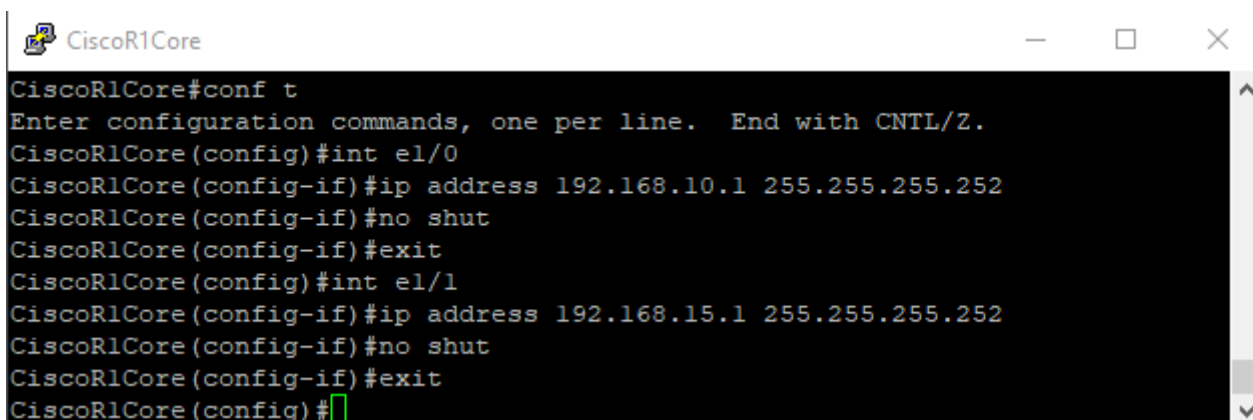
Visual Syslog є відмінним інструментом для тих, хто потребує простого та ефективного рішення для моніторингу системних подій на базі протоколу

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

Syslog. Він забезпечує необхідні функції для ефективного аналізу та управління системними логами, допомагаючи підтримувати стабільність та безпеку мережі.

3.2. Налаштування обладнання мережі

Проведемо базове налаштування інтерфейсів маршрутизатора Cisco. Додамо адреси за допомогою команди `ip address`, до інтерфейсів `e1/0` та `e1/1` з відповідними масками, на кожному інтерфейсі також задається параметр `no shut` для активації його (інші маршрутизатори налагоджені аналогічним способом)



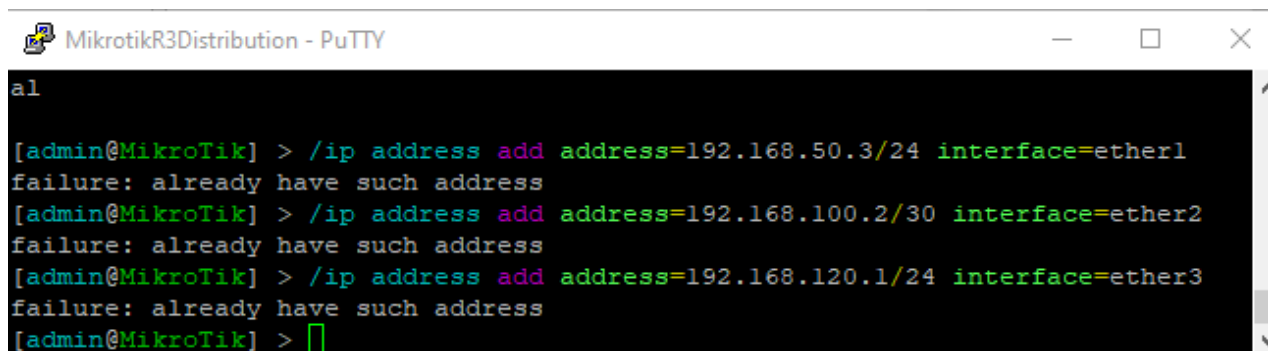
```

CiscoR1Core#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CiscoR1Core(config)#int e1/0
CiscoR1Core(config-if)#ip address 192.168.10.1 255.255.255.252
CiscoR1Core(config-if)#no shut
CiscoR1Core(config-if)#exit
CiscoR1Core(config)#int e1/1
CiscoR1Core(config-if)#ip address 192.168.15.1 255.255.255.252
CiscoR1Core(config-if)#no shut
CiscoR1Core(config-if)#exit
CiscoR1Core(config)#

```

Рисунок 3.10 - Базове налаштування інтерфейсів маршрутизатора Cisco

Базове налаштування інтерфейсів на маршрутизаторах Mikrotik виглядає наступним чином, за допомогою команди `ip address add` додаємо до інтерфейсів `ether1`, `ether2`, `ether3` адреси з відповідними масками. (інші маршрутизатори налагоджені аналогічним способом)



```

al
[admin@MikroTik] > /ip address add address=192.168.50.3/24 interface=ether1
failure: already have such address
[admin@MikroTik] > /ip address add address=192.168.100.2/30 interface=ether2
failure: already have such address
[admin@MikroTik] > /ip address add address=192.168.120.1/24 interface=ether3
failure: already have such address
[admin@MikroTik] >

```

Рисунок 3.11- Базове налаштування інтерфейсів маршрутизатора Mikrotik

Налаштовуємо маршрутизацію OSPF на маршрутизаторі Cisco. Вказуємо номер процесу OSPF, в даному випадку це 1, оголошуємо підмережі, які

додаємо до маршрутизації, та вказуємо унікальне ID роутера (інші маршрутизатори налагоджені аналогічним способом).

```

Cisco_router-R3
Cisco_router-R3(config)#router ospf 1
Cisco_router-R3(config-router)#network 192.168.40.0 0.0.0.3 area 0
Cisco_router-R3(config-router)#network 192.168.50.0 0.0.0.255 area 0
Cisco_router-R3(config-router)#network 192.168.60.0 0.0.0.3 area 0
Cisco_router-R3(config-router)#router-id 4.4.4.4
Cisco_router-R3(config-router)#
  
```

Рисунок 3.12 - Налаштування маршрутизації OSPF Cisco

Налаштовуємо маршрутизацію OSPF на маршрутизаторі Mikrotik вказуємо назву OSPF роутера вданому випадку default, задаєм стандартні налаштування вказуємо унікальне ID роутера. Додаєм підмережі в зону backbone (це аналог area 0) (інші маршрутизатори налагоджені аналогічним способом)

```

Mikrotik_router-R4 - PuTTY
[admin@MikroTik] > /routing ospf instance set [ find default=yes ] distribute-de
fault=never name=default router-id=5.5.5.5
[admin@MikroTik] > /routing ospf network add area=backbone network=192.168.70.0/
30
[admin@MikroTik] > /routing ospf network add area=backbone network=192.168.80.0/
24
[admin@MikroTik] > 
  
```

Рисунок 3.13 - Налаштування маршрутизації OSPF Mikrotik

Після цього налаштовуємо DHCP-server для автоматичного отримання адрес, задаємо назву DHCP пулу, видаляєм з цього пула першу адресу, додаєм мережу в якій буде надаватись адреси, призначаєм адресу маршрутизатора по замовченню і назву домену (інші маршрутизатори налагоджені аналогічним способом)

```

CiscoR5Distribution
CiscoR5Distribution#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CiscoR5Distribution(config)#ip dhcp excluded 192.168.140.1
CiscoR5Distribution(config)#ip dhcp pool Subnet140
CiscoR5Distribution(dhcp-config)#network 192.168.140.0 255.255.255.0
CiscoR5Distribution(dhcp-config)#default-router 192.168.140.1
CiscoR5Distribution(dhcp-config)#domain-name my.net
CiscoR5Distribution(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
CiscoR5Distribution(dhcp-config)#exit
CiscoR5Distribution(config)#
  
```

Рисунок 3.14 - Налаштування DHCP серверу

Робочим станціям яким не передбачено автоматичного присвоювання IP-адрес, надаємо статично за допомогою команди ip вказуємо відповідну адресу, маску та шлюз (інші робочі станції налагоджені аналогічним способом).

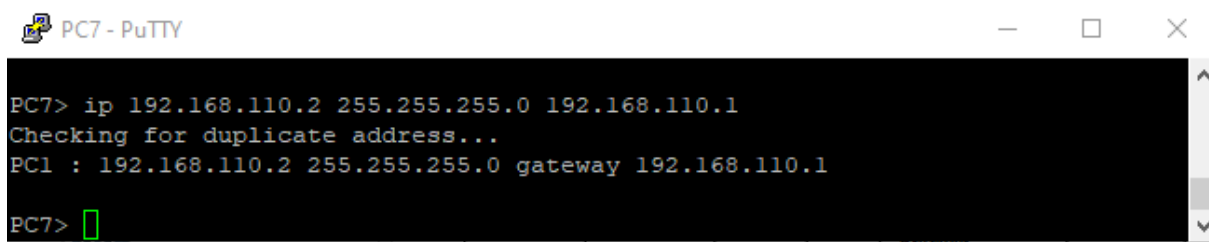


Рисунок 3.15 - Статичне присвоювання адреси робочій станції

За допомогою графічного інтерфейсу на робочій станції Ubuntu-1 присвоюємо адресу 192.168.110.3 з маскою 255.255.255.0, шлюзом слугує адреса роутера 192.168.110.1

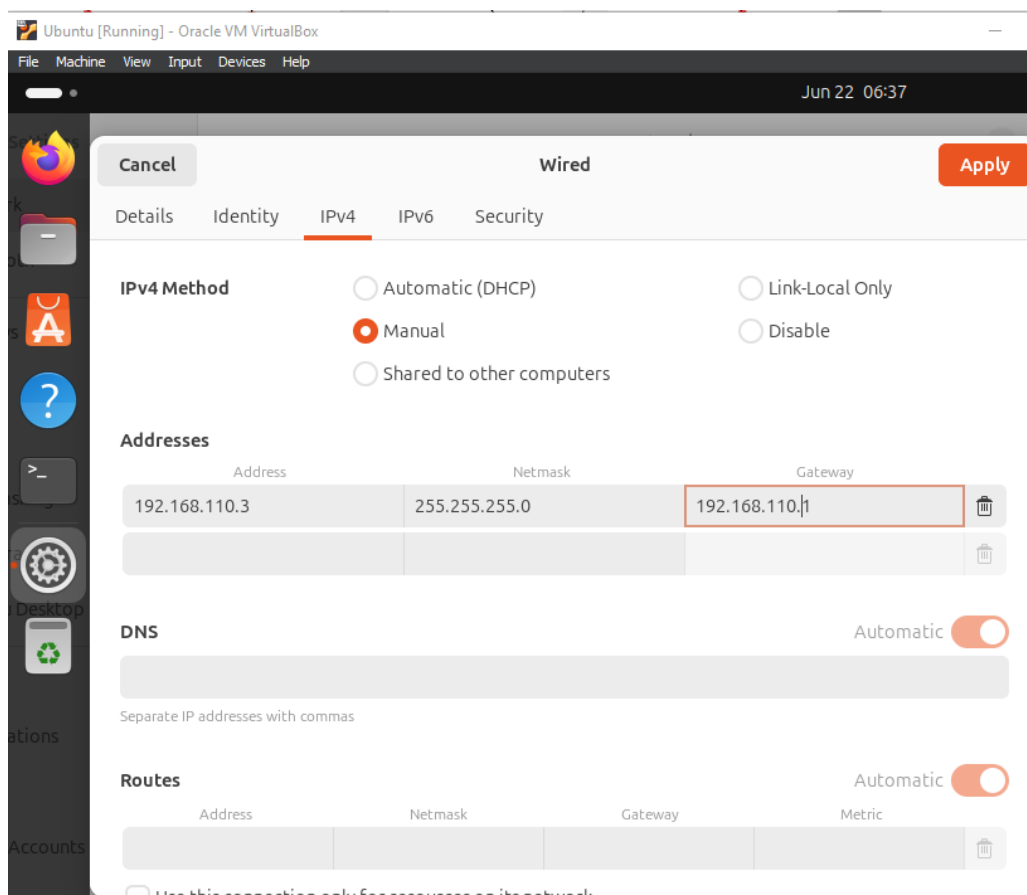


Рисунок 3.16 - Статичне присвоювання адреси робочій станції

Налаштовуємо списки доступу для забезпечення захисту підмереж аудиторій викладачів, забороняємо зв'язок аудиторії учнів з аудиторіями викладачів, забороняючи відповідні підмережі (інші маршрутизатори налагоджені аналогічним способом).

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

```

CiscoR5Distribution#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CiscoR5Distribution(config)#t icmp any 192.168.140.0 0.0.0.255 echo
CiscoR5Distribution(config)#t icmp 192.168.140.0 0.0.0.255 any echo-reply
CiscoR5Distribution(config)# 140 deny ip 192.168.110.0 0.0.0.255 any
CiscoR5Distribution(config)# 140 deny ip 192.168.120.0 0.0.0.255 any
CiscoR5Distribution(config)#access-list 140 permit ip any any
CiscoR5Distribution(config)#interface e1/1
CiscoR5Distribution(config-if)#ip access-group 140 out
CiscoR5Distribution(config-if)#exit
CiscoR5Distribution(config)#

```

Рисунок 3.17 - Налаштування списків доступу ACL

Налаштовуємо протокол віддаленого доступу SSH для маршрутизаторів Cisco, присвоюємо доменне ім'я, створюємо додаткового користувача, задаємо параметри підключення (інші маршрутизатори налагоджені аналогічним способом).

```

CiscoR2Core#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CiscoR2Core(config)#
CiscoR2Core(config)#username admin privilege 15 secret admin
CiscoR2Core(config)#
CiscoR2Core(config)#username user privilege 1 secret user
CiscoR2Core(config)#
CiscoR2Core(config)#ip domain-name my.com
CiscoR2Core(config)#
CiscoR2Core(config)#crypto key generate rsa modulus 2048
The name for the keys will be: CiscoR2Core.my.com

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

CiscoR2Core(config)#
CiscoR2Core(config)#ip ssh version 2
CiscoR2Core(config)#
CiscoR2Core(config)#line vty 0 4
CiscoR2Core(config-line)# transport input ssh
CiscoR2Core(config-line)# login local
CiscoR2Core(config-line)# exit
CiscoR2Core(config)#line console 0
CiscoR2Core(config-line)# login local
CiscoR2Core(config-line)# exit
CiscoR2Core(config)#end
CiscoR2Core#write memory
*Jun 24 17:28:18.651: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jun 24 17:28:19.423: %SYS-5-CONFIG_I: Configured from console by console
CiscoR2Core#write memory

```

Рисунок 3.18 - Налаштування SSH Cisco і додаткових користувачів

```

MikrotikR1Core - PuTTY
[admin@MikroTik] > /user set admin password=admin

[admin@MikroTik] > /user add name=user group=read password=user
failure: user with the same name already exists
[admin@MikroTik] >

```

Рисунок 3.19 - Налаштування користувачів Mikrotik

Налаштовуємо протокол віддаленого доступу ssh для маршрутизаторів Mikrotik, достатньо задати порт 22 як SSH (інші маршрутизатори налагоджені аналогічним способом).

```

Mikrotik_router-R1 - PuTTY
load command name exit (line 1 column 1)
[superadmin@MikroTik] /ip service> set ssh port=22
[superadmin@MikroTik] /ip service>

```

Рисунок 3.20 - Налаштування SSH Cisco

Виконуємо базові налаштування комутатора задаємо пароль, створюємо користувача, задаємо правила підключення через SSH, генеруємо ключ RSA, призначаємо адресу Vlan1 (інші комутатори налагоджені аналогічним способом).

```

SW5Distribution - PuTTY
Enter configuration commands, one per line. End with CNTL/Z.
Switch14(config)#hostname SW2Distribution
SW2Distribution(config)#enable secret admin
SW2Distribution(config)#line console 0
SW2Distribution(config-line)#password mypassword
SW2Distribution(config-line)#login
SW2Distribution(config-line)#exit
SW2Distribution(config)#username admin privilege 15 secret admin
SW2Distribution(config)#line vty 0 4
SW2Distribution(config-line)#login local
SW2Distribution(config-line)#transport input ssh
SW2Distribution(config-line)#exit
SW2Distribution(config)#ip domain-name my.com
SW2Distribution(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
SW2Distribution(config)#crypto key generate rsa
The name for the keys will be: SW2Distribution.my.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

SW2Distribution(config)#
*Jun 23 08:28:33.001: %SSH-5-ENABLED: SSH 2.0 has been enabled
SW2Distribution(config)#interface vlan 1
SW2Distribution(config-if)#ip address 192.168.120.100 255.255.255.0
SW2Distribution(config-if)#no shutdown
SW2Distribution(config-if)#exit
SW2Distribution(config)#
*Jun 23 08:28:41.545: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun 23 08:28:42.552: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to up
SW2Distribution(config)#

```

Рисунок 3.21 - Базові налаштування комутатора

Для захисту комутаторів, налаштовуємо port-security, вмикаємо захист порту, задаємо максимальну кількість адрес, вмикаємо збереження інформації про адреси, та задаємо налаштування на видалення застарілих адрес (інші комутатори налагоджені аналогічним способом).

```

SW4Access(config)#int e0/2
SW4Access(config-if)#switchport mode access
SW4Access(config-if)#switchport port-security
SW4Access(config-if)#switchport port-security maximum 2
SW4Access(config-if)#switchport port-security mac-address sticky
SW4Access(config-if)#switchport port-security aging time 10
SW4Access(config-if)#switchport port-security aging type inactivity
SW4Access(config-if)#exit
SW4Access(config)#exit
SW4Access#write memory
Building configuration...
Compressed configuration from 2003 bytes to 1195 bytes[OK]
SW4Access#
*Jun 23 09:32:16.974: %SYS-5-CONFIG_I: Configured from console by console
SW4Access#

```

Рисунок 3.22 - Налаштування port-security

Налаштовуємо DHCP snooping на комутаторах для захисту мережі від атак шкідливих DHCP-серверів, вказуємо довірений інтерфейс, всі інші вважатимуться не довіреними (інші комутатори налагоджені аналогічним способом).

```

SW14Access#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW14Access(config)#ip dhcp snooping
SW14Access(config)#ip dhcp snooping vlan 1
SW14Access(config)#interface e0/1
SW14Access(config-if)#switchport mode access
SW14Access(config-if)#ip dhcp snooping trust
SW14Access(config-if)#exit
SW14Access(config)#

```

Рисунок 3.23 - Налаштування DHCP snooping

Для захисту мережі на маршрутизаторі Cisco налаштовуємо NAT, вказуємо зовнішню адресу до інтернету, та внутрішню до мережі.

```

CiscoR1Core#
CiscoR1Core#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CiscoR1Core(config)#ip nat inside source static 192.168.15.2 10.0.0.1
CiscoR1Core(config)#ip nat inside source static 192.168.20.2 10.0.0.2
CiscoR1Core(config)#ip nat inside source static 192.168.40.2 10.0.0.3
CiscoR1Core(config)#interface Ethernet1/0
CiscoR1Core(config-if)#ip address 192.168.10.1 255.255.255.252
CiscoR1Core(config-if)#ip nat outside
CiscoR1Core(config-if)#no shutdown
CiscoR1Core(config-if)#exit
CiscoR1Core(config)#interface Ethernet1/1
CiscoR1Core(config-if)#ip address 192.168.15.1 255.255.255.252
CiscoR1Core(config-if)#ip nat inside
CiscoR1Core(config-if)#no shutdown
CiscoR1Core(config-if)#exit
CiscoR1Core(config)#

```

Рисунок 3.24 - Налаштування NAT на маршрутизаторі Cisco

```

SW15Access(config)#interface e0/1
SW15Access(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/1 but will only
have effect when the interface is in a non-trunking mode.
SW15Access(config-if)#spanning-tree bpduguard enable
SW15Access(config-if)#
SW15Access#
*Jun 24 12:05:50.100: %SYS-5-CONFIG_I: Configured from console by console
SW15Access#

```

Рисунок 3.25 Налаштування BPDU на маршрутизаторі Cisco

Створюємо HTTP сервер за допомогою Windows 10, задаємо назву, адресу, місце знаходження, далі в папку, яка вказувалась раніше, додаємо файл index.html з нашим Web-сайтом.

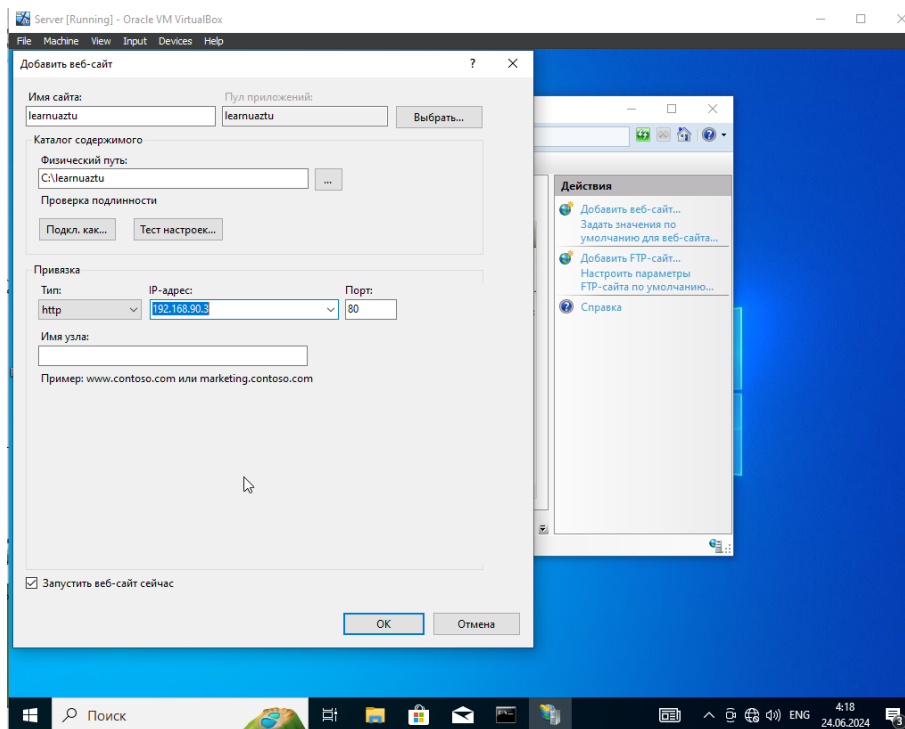


Рисунок 3.26 - Налаштування HTTP серверу (частина 1)

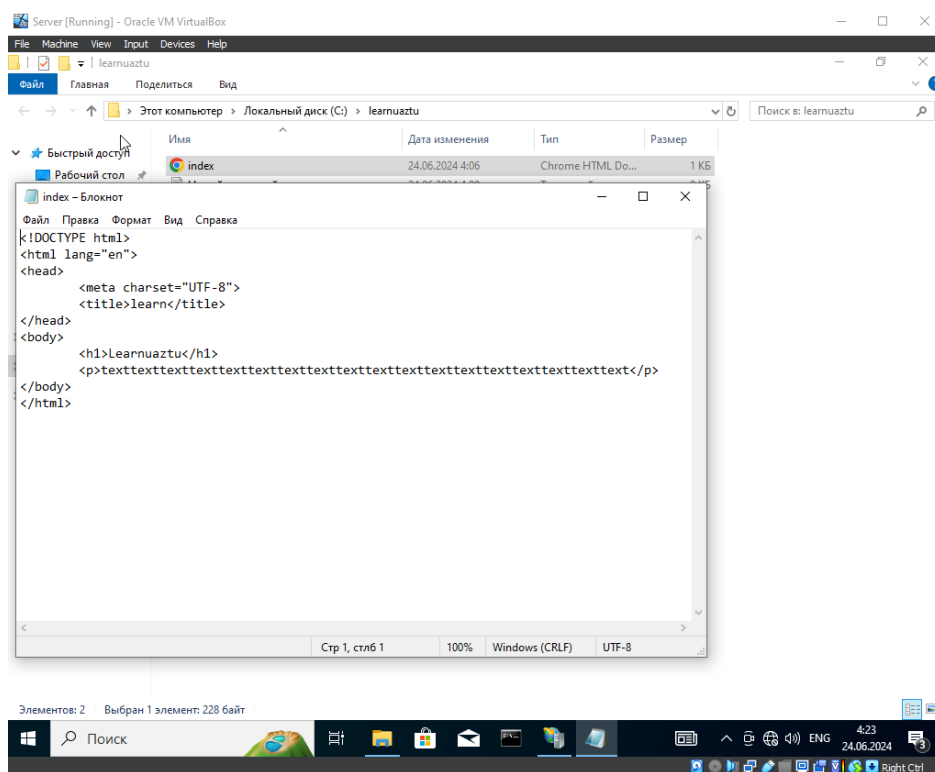


Рисунок 3.27 - Налаштування HTTP серверу (частина 2)

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

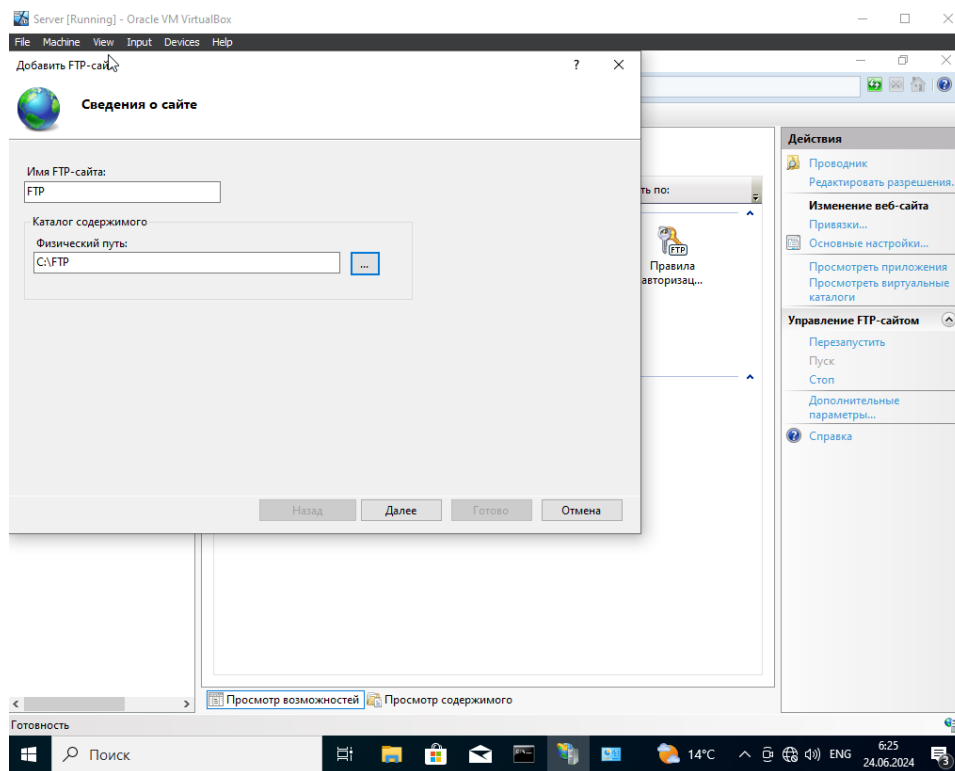


Рисунок 3.28 - Наляштування FTP серверу (частина 1)

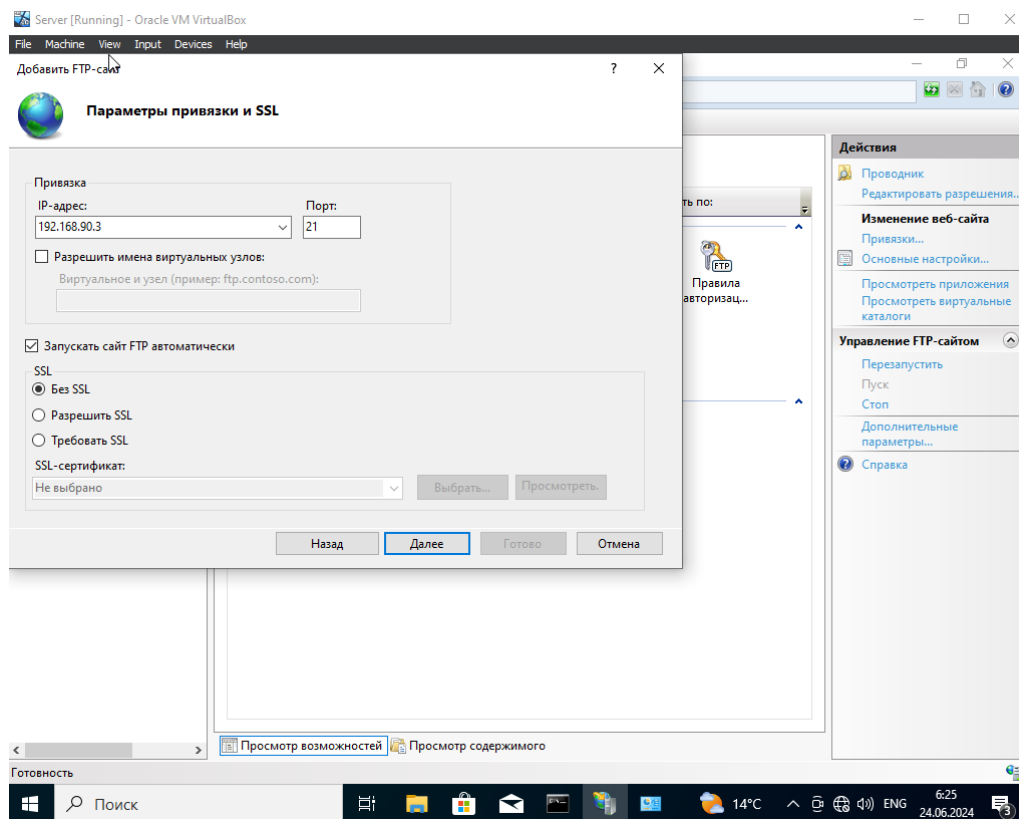


Рисунок 3.29 - Наляштування FTP серверу (частина 2)

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

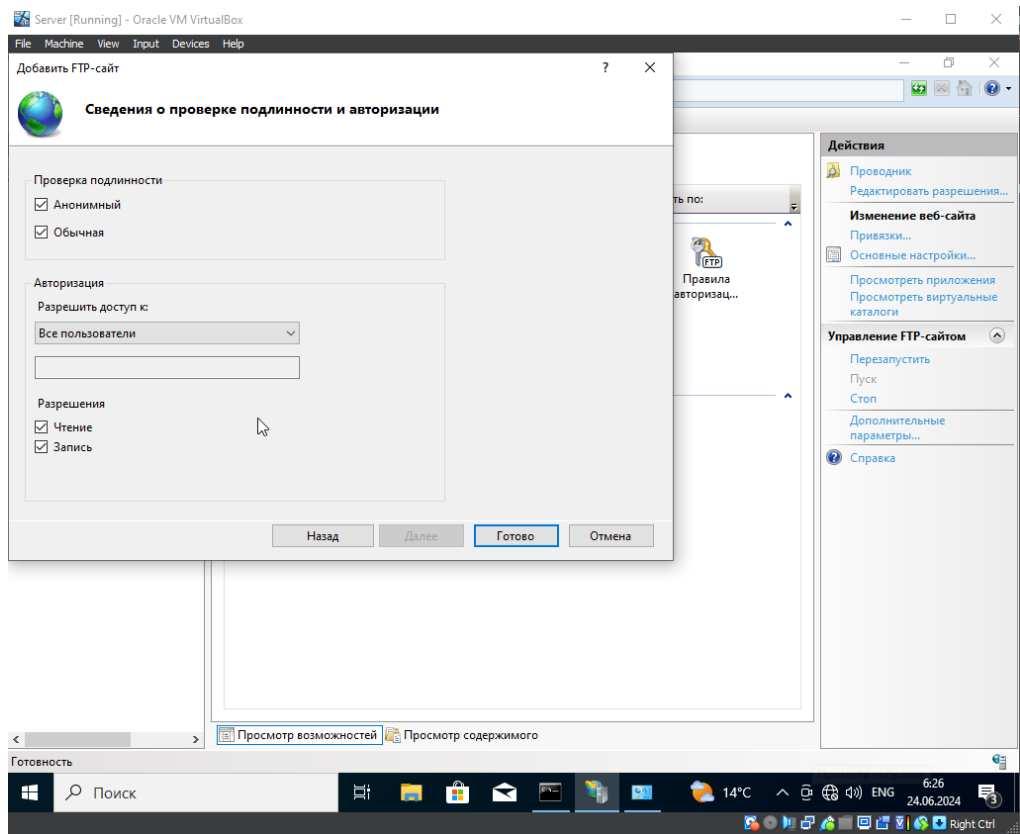


Рисунок 3.30 - Налаштування FTP серверу (частина 3)

Додаємо деякі файли до папки FTP серверу.

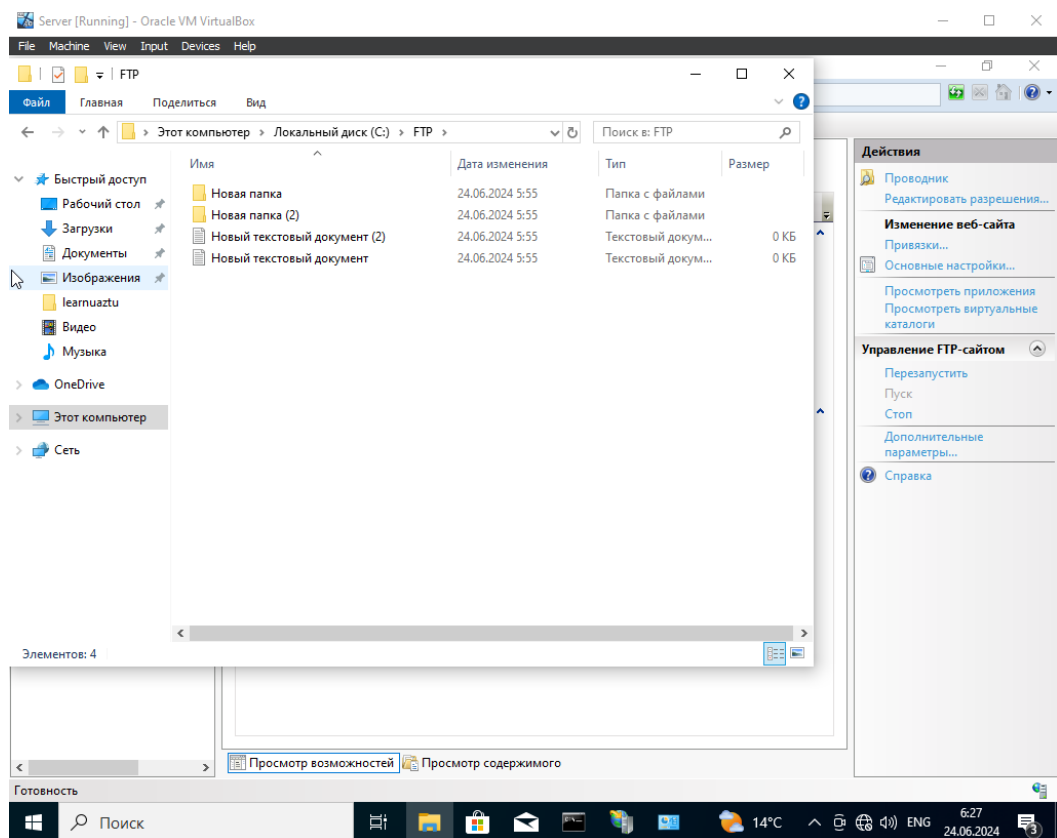


Рисунок 3.31 - Налаштування FTP серверу (частина 4)

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

```

CiscoR4Core#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CiscoR4Core(config)#logging 192.168.90.3
CiscoR4Core(config)#logging trap informational
CiscoR4Core(config)#service timestamps log datetime localtime
CiscoR4Core(config)#end
CiscoR4Core#write memory
*Jun 24 15:24:20: %SYS-5-CONFIG_I: Configured from console by console
CiscoR4Core#write memory
Building configuration...
[OK]
CiscoR4Core#
*Jun 24 15:24:21: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.90.3 port
514 started - CLI initiated
CiscoR4Core#

```

Рисунок 3.32 - Налаштування syslog серверу на маршрутизаторі Cisco

```

[admin@MikroTik] > /system logging action add name=remote2 target=remote remote=
192.168.90.3
[admin@MikroTik] > /system logging add action=remote topics=info

```

Рисунок 3.33 - Налаштування syslog серверу на маршрутизаторі Mikrotik

Server [Роботаєт] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Setup

Main Files E-mail

UDP syslog server

☒ Enable UDP listener

UDP listener interface and port 192.168.90.3 514

TCP syslog server

☒ Enable TCP listener

TCP listener interface and port 192.168.90.3 514

Launch

☐ Automatic start with windows

Highlighting

☒ 3D fill

Working

☐ Write all received messages to a file "raw" for diagnostic purposes

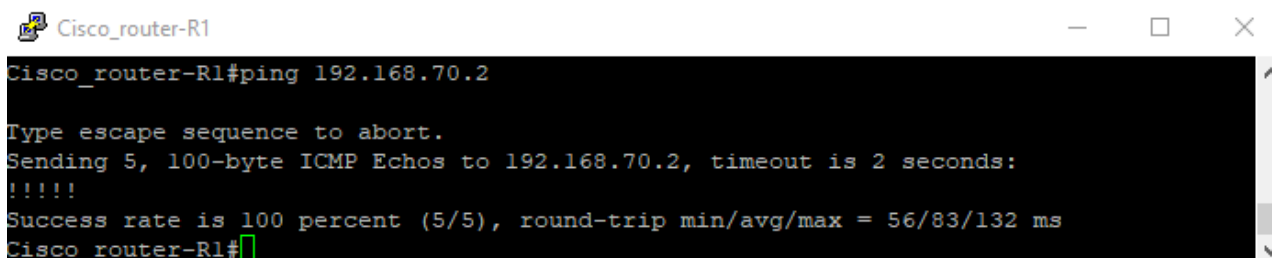
☐ Receive messages encoded in UTF8

OK Cancel

Рисунок 3.34 - Налаштування syslog серверу на Windows 10

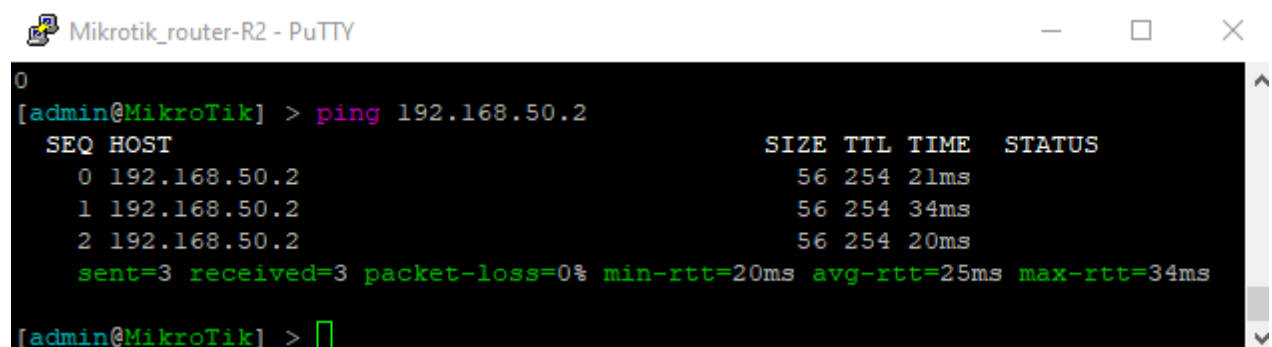
3.3 Тестування функціонування мережі та засобів її захисту

Проведемо тестування командую ping.



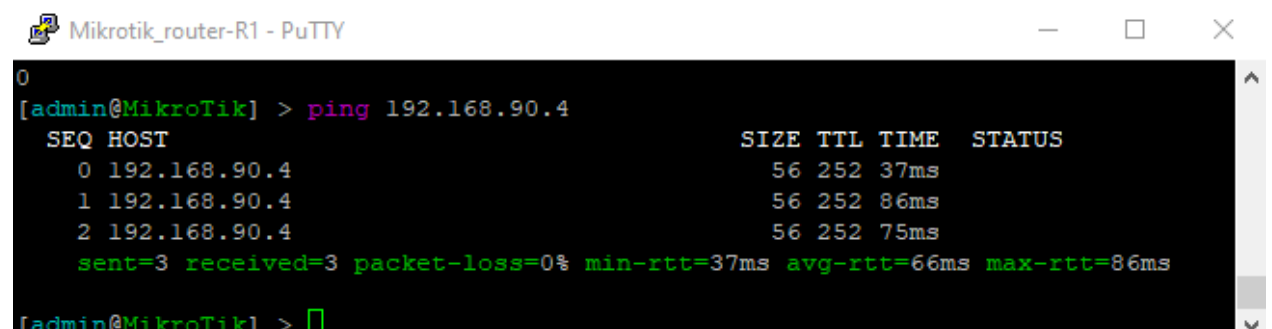
```
Cisco_router-R1#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/83/132 ms
Cisco_router-R1#
```

Рисунок 3.35 - Виконання команди ping 192.168.70.2 з маршрутизатора R1cisco



```
0
[admin@MikroTik] > ping 192.168.50.2
  SEQ HOST                SIZE TTL TIME  STATUS
  0 192.168.50.2           56 254 21ms
  1 192.168.50.2           56 254 34ms
  2 192.168.50.2           56 254 20ms
  sent=3 received=3 packet-loss=0% min-rtt=20ms avg-rtt=25ms max-rtt=34ms
[admin@MikroTik] >
```

Рисунок 3.36 - Виконання команди ping 192.168.50.2 з маршрутизатора R2mikrotik



```
0
[admin@MikroTik] > ping 192.168.90.4
  SEQ HOST                SIZE TTL TIME  STATUS
  0 192.168.90.4           56 252 37ms
  1 192.168.90.4           56 252 86ms
  2 192.168.90.4           56 252 75ms
  sent=3 received=3 packet-loss=0% min-rtt=37ms avg-rtt=66ms max-rtt=86ms
[admin@MikroTik] >
```

Рисунок 3.37 - Виконання команди ping 192.168.90.4 з маршрутизатора R1mikrotik

Результат показує, що зв'язок по всі мережі працює справно.

Проведемо тестування DHCP-серверу. Отримаємо автоматично адресу від DHCP-серверу для Linux Ubuntu.

Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

IPv4 Method

☒ Automatic (DHCP)
☐ Link-Local Only
☐ Manual
☐ Disable
☐ Shared to other computers

DNS

Automatic ☒

Separate IP addresses with commas

Routes

Automatic ☒

Address

Netmask

Gateway

Metric

☐ Use this connection only for resources on its network

Рисунок 3.38 - Автоматичне присвоювання адреси Linux Ubuntu (частина 1)

Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

Link speed

1000 Mb/s

IPv4 Address

192.168.140.3

IPv6 Address

fe80::a23d:63c3:94e6:9029

Hardware Address

08:00:27:53:29:86

Default Route

192.168.140.1

☒ Connect automatically

☒ Make available to other users

☐ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

Remove Connection Profile...

Рисунок 3.39 - Автоматичне присвоювання адреси Linux Ubuntu (частина 2)

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

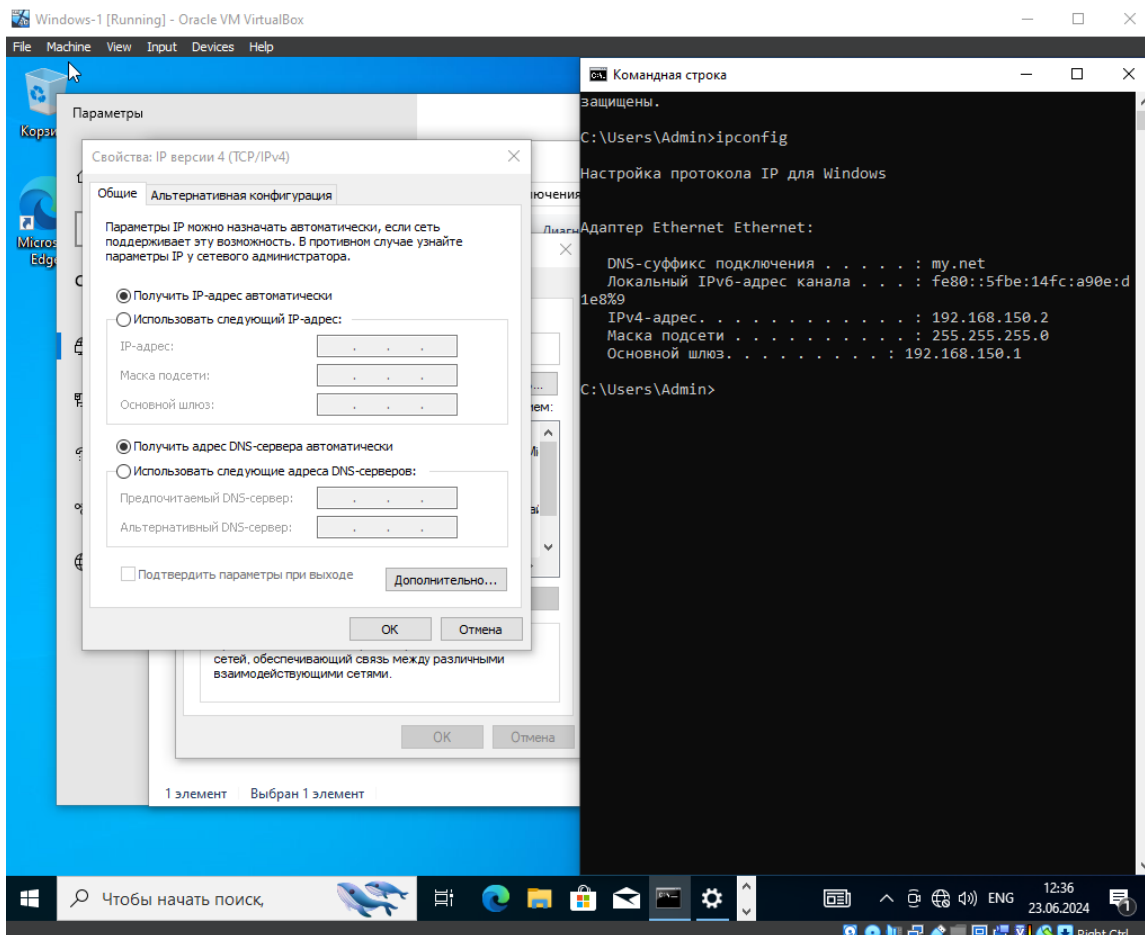


Рисунок 3.40 - Автоматичне присвоювання адреси

Отримаємо автоматично адресу для решти станцій.

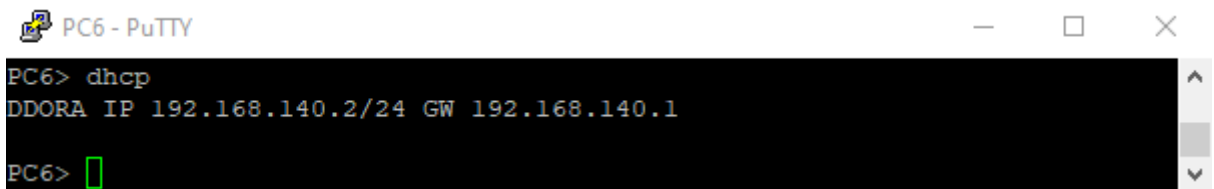


Рисунок 3.41 - Автоматичне присвоювання адреси робочій станції

Результат показує, що DHCP-сервер справно, надає адреси робочим станціям

Проведемо тестування серверів.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

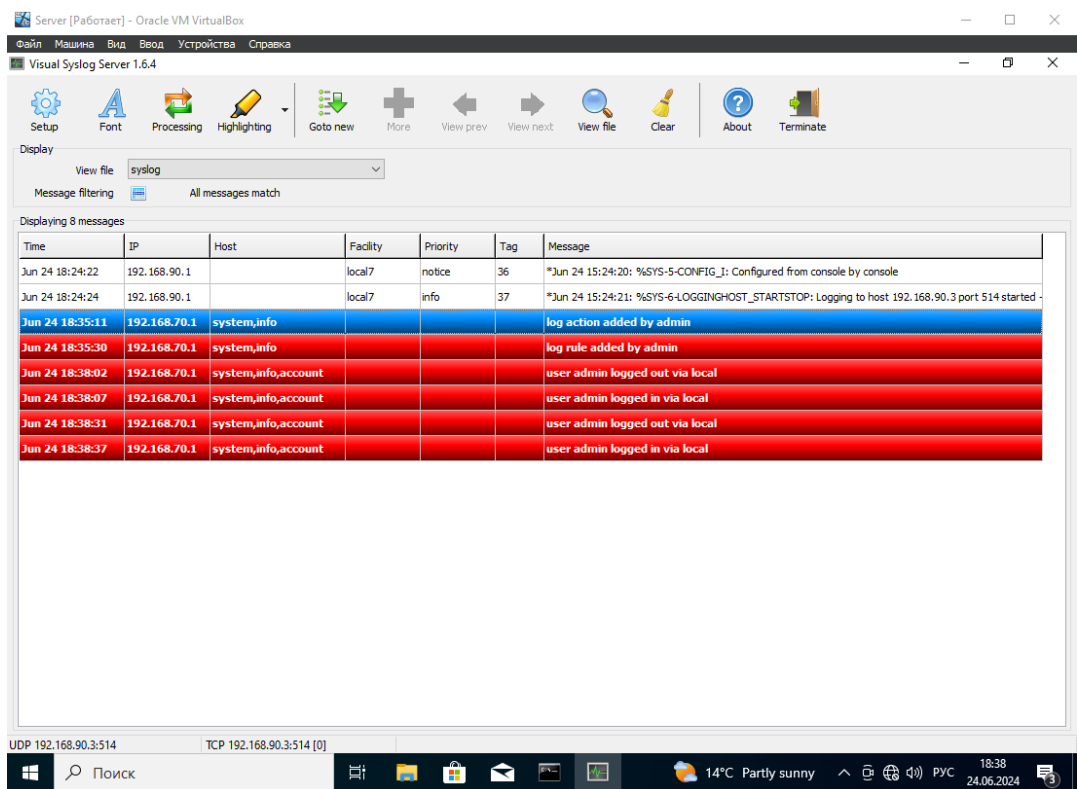


Рисунок 3.44 - Перевірка роботи syslog серверу

Виведемо таблицю маршрутизації для перевірки.

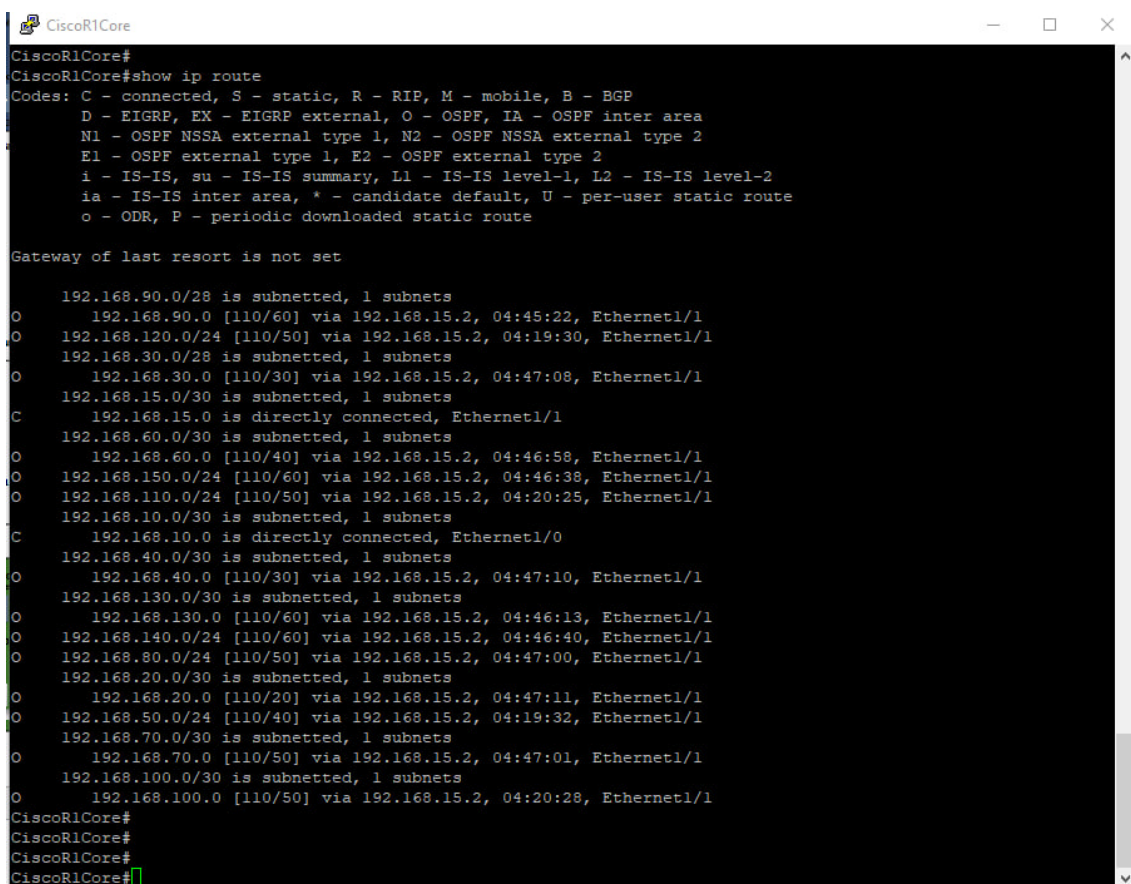


Рисунок 3.45 - Таблиця маршрутизації

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Протестуємо списки доступу:

```

PC8> ping 192.168.120.2

192.168.120.2 icmp_seq=1 timeout
192.168.120.2 icmp_seq=2 timeout
192.168.120.2 icmp_seq=3 timeout
192.168.120.2 icmp_seq=4 timeout
192.168.120.2 icmp_seq=5 timeout

PC8>
  
```

Рисунок 3.46 - Спроба виконати команду ping до підмережі аудиторій викладачів з підмережі аудиторій учнів

```

PC5> ping 192.168.140.3

84 bytes from 192.168.140.3 icmp_seq=1 ttl=60 time=148.736 ms
84 bytes from 192.168.140.3 icmp_seq=2 ttl=60 time=31.202 ms
84 bytes from 192.168.140.3 icmp_seq=3 ttl=60 time=39.081 ms
84 bytes from 192.168.140.3 icmp_seq=4 ttl=60 time=48.549 ms
84 bytes from 192.168.140.3 icmp_seq=5 ttl=60 time=42.501 ms

PC5>
  
```

Рисунок 3.47 - Спроба виконати команду ping до підмережі аудиторій учнів з підмережі аудиторій викладачів

Протестуємо SSH:

```

SW5Distribution - PuTTY

Compressed configuration from 1790 bytes to 1077 bytes[OK]
SW2Distribution#ssh -l admin 192.168.120.1
Password:

MMM      MMM      KKK                      TTTTTTTTTT      KKK
MMMMM    MMMM      KKK                      TTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK KKK  RRRRRR   OOOOOO      TTT      III  KKK KKK
MMM MM  MMM  III  KKKKK  RRR RRR  OOO OOO      TTT      III  KKKKK
MMM  MMM  III  KKK KKK  RRRRRR   OOO OOO      TTT      III  KKK KKK
MMM      MMM  III  KKK KKK  RRR RRR  OOOOOO      TTT      III  KKK KKK

MikroTik RouterOS 6.49.15 (c) 1999-2024      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..           Move up one level
/command     Use command at the base level

[admin@MikroTik] >
  
```

Рисунок 3.48 - Підключення до MikrotukR3Distribution по SSH через комутатор

```

CiscoR5Distribution
*Jun 24 01:52:33.931: %SYS-5-CONFIG_I: Configured from console by console
CiscoR5Distribution#ssh -l admin 192.168.140.100

Password:

SW11Distribution#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW11Distribution(config)#

```

Рисунок 3.49 - Підключення до SW11Distribution по SSH через маршрутизатор

Протестуємо port-security:

```

SW15Access(config)#
*Jun 24 12:31:39.377: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/2, putting Et0/2 in err-disable state
SW15Access(config)#
*Jun 24 12:31:39.378: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.2727.d113 on port Ethernet0/2.
*Jun 24 12:31:40.378: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
SW15Access(config)#
*Jun 24 12:31:41.386: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to down
SW15Access(config)#
SW15Access#
*Jun 24 12:31:53.237: %SYS-5-CONFIG_I: Configured from console by console
SW15Access#

```

Рисунок 3.50 - Перевірка роботи port-security

Протестуємо NAT:

```

CiscoR1Core
CiscoR1Core(config)#exit
CiscoR1Core#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside glob
al
--- 10.0.0.1            192.168.15.2      ---                ---
--- 10.0.0.2            192.168.20.2      ---                ---
--- 10.0.0.3            192.168.40.2      ---                ---
CiscoR1Core#
*Jun 24 18:36:55.263: %SYS-5-CONFIG_I: Configured from console by console
CiscoR1Core#show ip nat statistics
Total active translations: 3 (3 static, 0 dynamic; 0 extended)
Peak translations: 3, occurred 00:12:14 ago
Outside interfaces:
  Ethernet1/0
Inside interfaces:
  Ethernet1/1
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
  Appl doors: 0
  Normal doors: 0
Queued Packets: 0
CiscoR1Core#

```

Рисунок 3.51 Перевірка роботи NAT

Протестуємо DHCP-snooping:

```

SW14Access#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0500 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/1              yes       yes             unlimited
  Custom circuit-ids:
SW14Access#

```

Рисунок 3.52 Перевірка роботи DHCP snooping

Висновки до третього розділу

Під час виконання третього розділу були наведені обґрунтування та технічні характеристики вибраного для глобальної мережі обладнання та програмного забезпечення. Було побудовано та налагоджено мережу в GNS3. Також було протестовано мережу на правильність налаштування та особливості роботи протоколів маршрутизації.

ВИСНОВКИ

У процесі проведення дослідження, метою якого було розробити підсистему периметрового захисту мережі освітнього закладу, було досягнуто значних результатів. Основним результатом роботи стало створення ефективної підсистеми периметрового захисту, яка забезпечує достатній рівень безпеки та стабільність функціонування мережевої інфраструктури.

Під час реалізації цього проекту вдалося забезпечити інтероперабельність між різними мережевими пристроями та системами, що використовують різні протоколи та стандарти. Це дозволило об'єднувати ресурси різних виробників і платформ, забезпечуючи ефективне управління та доступ до них з будь-якої точки мережі. Масштабованість системи досягнуто завдяки гнучкому додаванню нових пристроїв та технологій без значних змін в існуючій інфраструктурі.

Особливу увагу було приділено принципам побудови та функціонування обладнання Cisco та Mikrotik. Cisco Systems пропонує надійне, функціональне та високопродуктивне обладнання, яке підтримує широкий спектр протоколів і стандартів, інтегрує розширені функції безпеки та забезпечує ефективне управління мережами. Mikrotik, з іншого боку, відомий своєю доступністю та потужними функціями для мережевих адміністраторів, пропонуючи гнучкі налаштування та надійну безпеку за доступною ціною

Проаналізовані різні механізми захисту, включаючи використання антивірусного програмного забезпечення, брандмауерів, VPN, аутентифікацію та шифрування даних.

Для реалізації захисту налаштовано NAT, port-security, DHCP-snooping

Практична цінність результатів дослідження полягає у підвищенні рівня безпеки та надійності мережевої інфраструктури освітнього закладу, що забезпечує захист від кіберзагроз. Це сприяє безперебійній роботі інформаційних систем і безпеці даних.

Подальші наукові дослідження можуть включати вдосконалення механізмів виявлення і реагування на нові види загроз, розвиток методів автоматичного оновлення безпекових політик, а також інтеграцію систем

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

штучного інтелекту для прогнозування і запобігання потенційним атакам. Вдосконалення програмного комплексу може включати розширення його функціональних можливостей, оптимізацію продуктивності та підвищення зручності користування для адміністраторів мережі.

В результаті виконання кваліфікаційної роботи були виконані всі поставлені завдання. Розглянуто теоретичні аспекти безпеки комп'ютерних мереж, розроблено проєкт захищеної комп'ютерної мережі на базі обладнання Cisco, налаштовано та протестовано систему. Всі ці заходи сприяли створенню надійної та безпечної мережевої інфраструктури, яка надає достатній рівень захисту інформації.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

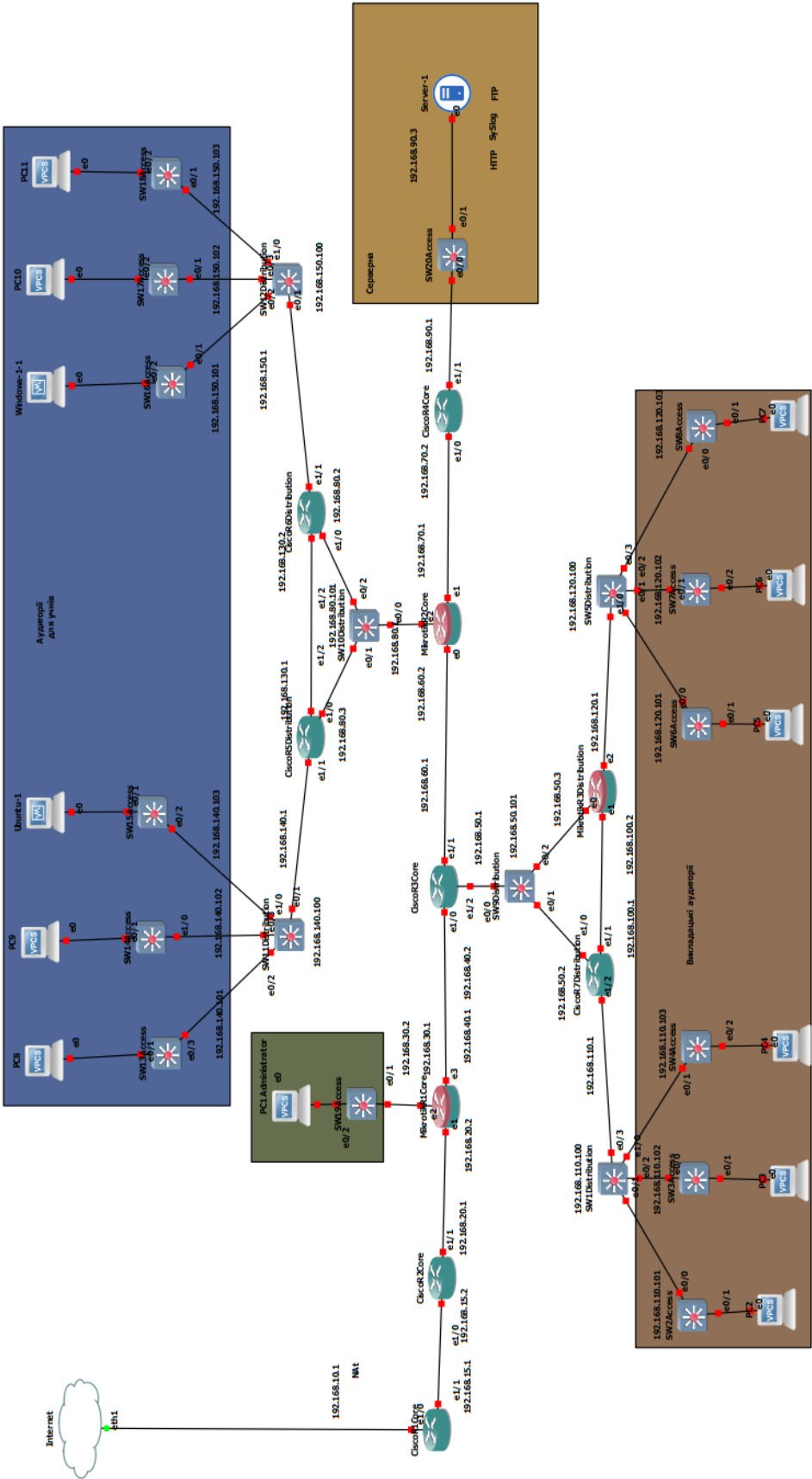
1. Heterogeneous network [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Heterogeneous_network.
2. Networking Solutions for Integrated Heterogeneous Wireless Ecosystem [Електронний ресурс] – Режим доступу до ресурсу: <https://www.intechopen.com/chapters/53772>.
3. Cisco Networking Academy Connecting Networks Companion [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>.
4. Top 10 Most Common Types of Network Attacks [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lepide.com/blog/common-types-of-network-attacks/>.
5. Malware, Phishing, and Ransomware [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>.
6. Types of cyberthreats [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/think/topics/cyberthreats-types>.
7. The OSI Model – The 7 Layers of Networking Explained in Plain English [Електронний ресурс] – Режим доступу до ресурсу: <https://www.freecodecamp.org/news/osi-model-networking-layers-explained-in-plain-english/>.
8. Common Security Attacks in the OSI Layer Model [Електронний ресурс] – Режим доступу до ресурсу: <https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/>.
9. The OSI Model's 7 Layers, Explained [Електронний ресурс] – Режим доступу до ресурсу: <https://builtin.com/articles/osi-model-layers>.
10. OSPF Features, Advantages, Disadvantages [Електронний ресурс] – Режим доступу до ресурсу: <https://www.computernetworkingnotes.com/ccna-study-guide/ospf-features-advantages-disadvantages.html>.

		Дмитрієв О.Г.			ККІКБ.КР.Б – 125 – 6– ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

- 11.What is SSH? | Secure Shell (SSH) protocol [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cloudflare.com/ru-ru/learning/access-management/what-is-ssh/>.
- 12.Syslog [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/Syslog>.
- 13.File Transfer Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/File_Transfer_Protocol.
- 14.HTTP [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/HTTP>.
- 15.GNS3 Graphical Network Simulator [Електронний ресурс] – Режим доступу до ресурсу: <https://www.networkstraining.com/gns3-graphical-network-simulator/>.
- 16.Mikrotik [Електронний ресурс] – Режим доступу до ресурсу: <https://mikrotik.com/>.
- 17.Windows 10 deployment scenarios and tools [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools>.
- 18.Ubuntu Server how-to guides [Електронний ресурс] – Режим доступу до ресурсу: <https://ubuntu.com/server/docs/how-to>.
- 19.FileZilla [Електронний ресурс] – Режим доступу до ресурсу: <https://filezilla-project.org/>.
- 20.Visual Syslog Server for Windows [Електронний ресурс] – Режим доступу до ресурсу: <https://maxbelkov.github.io/visualsyslog/>.

ДОДАТКИ

Схема побудованої мережі



Лістинг налаштування роутерів

hostname CiscoR1Core	!
!	!
boot-start-marker	username admin privilege 15 secret 5
boot-end-marker	\$1\$CeHB\$.oWUjY.RjW5xKoWYXCXtB1
!	username user secret 5
	\$1\$nLzs\$gB839fRihuGs6pjzyCeP91
logging message-counter syslog	archive
!	log config
no aaa new-model	hidekeys
ip source-route	!
no ip icmp rate-limit unreachable	!
ip cef	!
!	!
!	!
!	ip tcp synwait-time 5
!	ip ssh version 2
no ip domain lookup	!
ip domain name my.com	!
no ipv6 cef	!
!	!
multilink bundle-name authenticated	interface FastEthernet0/0
!	no ip address
!	shutdown
!	duplex half
!	!
!	interface Ethernet1/0
!	ip address 192.168.10.1 255.255.255.252
!	ip nat outside
!	ip virtual-reassembly
!	duplex half
!	!
!	interface Ethernet1/1
!	ip address 192.168.15.1 255.255.255.252
!	ip nat inside
!	ip virtual-reassembly

duplex half	!
!	ip forward-protocol nd
interface Ethernet1/2	no ip http server
no ip address	no ip http secure-server
shutdown	!
duplex half	!
!	ip nat inside source static 192.168.15.2 10.0.0.1
interface Ethernet1/3	ip nat inside source static 192.168.20.2 10.0.0.2
no ip address	ip nat inside source static 192.168.40.2 10.0.0.3
shutdown	!
duplex half	logging 192.168.90.3
!	no cdp log mismatch duplex
interface Ethernet1/4	!
no ip address	!
shutdown	!
duplex half	!
!	!
interface Ethernet1/5	!
no ip address	control-plane
shutdown	!
duplex half	!
!	!
interface Ethernet1/6	!
no ip address	!
shutdown	!
duplex half	!
!	gatekeeper
interface Ethernet1/7	shutdown
no ip address	!
shutdown	!
duplex half	line con 0
!	exec-timeout 0 0
router ospf 1	privilege level 15
router-id 1.1.1.1	logging synchronous
log-adjacency-changes	login local
network 192.168.10.0 0.0.0.3 area 0	stopbits 1
network 192.168.15.0 0.0.0.3 area 0	line aux 0

exec-timeout 0 0	!
privilege level 15	!
logging synchronous	!
stopbits 1	!
line vty 0 4	!
login local	!
transport input ssh	!
!	!
end	username admin privilege 15 secret 5
hostname CiscoR2Core	\$1\$ENmI\$KgJ3IclxgJOi3Mvt4Dott/
!	username user secret 5
boot-start-marker	\$1\$K.lp\$K8YbO1D/.C9JBxEQsr1Yq.
boot-end-marker	archive
!	log config
logging message-counter syslog	hidekeys
!	!
no aaa new-model	!
ip source-route	!
no ip icmp rate-limit unreachable	!
ip cef	ip tcp synwait-time 5
!	ip ssh version 2
!	!
!	!
!	!
no ip domain lookup	!
ip domain name my.com	interface FastEthernet0/0
no ipv6 cef	no ip address
!	shutdown
multilink bundle-name authenticated	duplex half
!	!
!	interface Ethernet1/0
!	ip address 192.168.15.2 255.255.255.252
!	duplex half
!	!
!	interface Ethernet1/1
!	ip address 192.168.20.1 255.255.255.252
!	duplex half

!	ip forward-protocol nd
interface Ethernet1/2	no ip http server
no ip address	no ip http secure-server
shutdown	!
duplex half	!
!	!
interface Ethernet1/3	logging 192.168.90.3
no ip address	no cdp log mismatch duplex
shutdown	!
duplex half	!
!	!
interface Ethernet1/4	!
no ip address	!
shutdown	!
duplex half	control-plane
!	!
interface Ethernet1/5	!
no ip address	!
shutdown	!
duplex half	!
!	!
interface Ethernet1/6	!
no ip address	gatekeeper
shutdown	shutdown
duplex half	!
!	!
interface Ethernet1/7	line con 0
no ip address	exec-timeout 0 0
shutdown	privilege level 15
duplex half	logging synchronous
!	login local
router ospf 1	stopbits 1
router-id 2.2.2.2	line aux 0
log-adjacency-changes	exec-timeout 0 0
network 192.168.15.0 0.0.0.3 area 0	privilege level 15
network 192.168.20.0 0.0.0.3 area 0	logging synchronous
!	stopbits 1

line vty 0 4	!
login local	!
transport input ssh	!
!	!
End	username admin privilege 15 secret 5
hostname CiscoR3Core	\$1\$I0MO\$tKnkG26Y9UNUgtqqTDvOI/
!	username user secret 5
boot-start-marker	\$1\$rqhC\$2q0TNBhduRtaS0I4tetge1
boot-end-marker	archive
!	log config
logging message-counter syslog	hidekeys
!	!
no aaa new-model	!
ip source-route	!
no ip icmp rate-limit unreachable	!
ip cef	ip tcp synwait-time 5
!	ip ssh version 2
!	!
!	!
!	!
no ip domain lookup	!
ip domain name my.com	interface FastEthernet0/0
no ipv6 cef	no ip address
!	shutdown
multilink bundle-name authenticated	duplex half
!	!
!	interface Ethernet1/0
!	ip address 192.168.40.2 255.255.255.252
!	duplex half
!	!
!	interface Ethernet1/1
!	ip address 192.168.60.1 255.255.255.252
!	duplex half
!	!
!	interface Ethernet1/2
!	ip address 192.168.50.1 255.255.255.0
!	duplex half

!	!
interface Ethernet1/3	!
no ip address	logging 192.168.90.3
shutdown	no cdp log mismatch duplex
duplex half	!
!	!
interface Ethernet1/4	!
no ip address	!
shutdown	!
duplex half	!
!	control-plane
interface Ethernet1/5	!
no ip address	!
shutdown	!
duplex half	!
!	!
interface Ethernet1/6	!
no ip address	!
shutdown	gatekeeper
duplex half	shutdown
!	!
interface Ethernet1/7	!
no ip address	line con 0
shutdown	exec-timeout 0 0
duplex half	privilege level 15
!	logging synchronous
router ospf 1	login local
router-id 4.4.4.4	stopbits 1
log-adjacency-changes	line aux 0
network 192.168.40.0 0.0.0.3 area 0	exec-timeout 0 0
network 192.168.50.0 0.0.0.255 area 0	privilege level 15
network 192.168.60.0 0.0.0.3 area 0	logging synchronous
!	stopbits 1
ip forward-protocol nd	line vty 0 4
no ip http server	login local
no ip http secure-server	transport input ssh
!	!

End	!
hostname SW9Distribution	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	!
logging buffered 50000	interface Ethernet0/0
logging console discriminator EXCESS	duplex auto
enable secret 4	!
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	interface Ethernet0/1
!	duplex auto
username admin privilege 15 secret 4	!
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	interface Ethernet0/2
no aaa new-model	duplex auto
no ipv6 cef	!
ipv6 multicast rpf use-bgp	interface Ethernet0/3
no ip icmp rate-limit unreachable	duplex auto
!	!
no ip domain-lookup	interface Ethernet1/0
ip domain-name my.com	duplex auto
no ip cef	!
!	interface Ethernet1/1
!	duplex auto
!	!
!	interface Ethernet1/2
spanning-tree mode pvst	duplex auto
spanning-tree extend system-id	!
!	interface Ethernet1/3
!	duplex auto
!	!
!	interface Ethernet2/0
vlan internal allocation policy ascending	duplex auto
!	!
ip tcp synwait-time 5	interface Ethernet2/1
ip ssh version 2	duplex auto
!	

```

!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    ip address 192.168.50.101 255.255.255.0
!
!
no ip http server
!
!
!
!
!
!
control-plane
!
!
line con 0
    exec-timeout 0 0
    privilege level 15
    password mypassword
    logging synchronous

```

```

login
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login local
    transport input ssh
!
End
MikrotilR1Core
/interface ethernet
    set [ find default-name=ether2 ] name=ether1
    set [ find default-name=ether3 ] name=ether2
    set [ find default-name=ether4 ] name=ether3
    set [ find default-name=ether1 ] name=ether4
/interface wireless security-profiles
    set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
    set [ find default=yes ] router-id=3.3.3.3
/system logging action
    add name=remote2 remote=192.168.90.3
    target=remote
/ip address
    add address=192.168.20.2/30 interface=ether1
    network=192.168.20.0
    add address=192.168.30.1/28 interface=ether2
    network=192.168.30.0
    add address=192.168.40.1/30 interface=ether3
    network=192.168.40.0
/ip dhcp-client
    add disabled=no interface=ether1
/routing ospf network
    add area=backbone network=192.168.20.0/30
    add area=backbone network=192.168.30.0/28
    add area=backbone network=192.168.40.0/30
/system logging
    add action=remote topics=info

```

hidekeys

!

!

!

!

!

```
ip tcp synwait-time 5
```

!

!

!

!

```
interface FastEthernet0/0
```

no ip address

shutdown

duplex half

!

```
interface Ethernet1/0
```

```
ip address 192.168.50.2 255.255.255.0
```

duplex half

!

```
interface Ethernet1/1
```

ip address 192.168.100.1 255.255.255.252

duplex half

!

```
interface Ethernet1/2
```

```
ip address 192.168.110.1 255.255.255.0
```

duplex half

!

```
interface Ethernet1/3
```

no ip address

shutdown

duplex half

!

```
interface Ethernet1/4
```

no ip address

shutdown

duplex half

!	control-plane
interface Ethernet1/5	!
no ip address	!
shutdown	!
duplex half	!
!	!
interface Ethernet1/6	!
no ip address	!
shutdown	gatekeeper
duplex half	shutdown
!	!
interface Ethernet1/7	!
no ip address	line con 0
shutdown	exec-timeout 0 0
duplex half	privilege level 15
!	logging synchronous
router ospf 1	stopbits 1
router-id 9.9.9.9	line aux 0
log-adjacency-changes	exec-timeout 0 0
network 192.168.50.0 0.0.0.255 area 0	privilege level 15
network 192.168.100.0 0.0.0.3 area 0	logging synchronous
network 192.168.110.0 0.0.0.255 area 0	stopbits 1
!	line vty 0 4
ip forward-protocol nd	login
no ip http server	!
no ip http secure-server	end
!	
!	hostname CiscoR4Core
!	!
logging 192.168.90.3	boot-start-marker
no cdp log mismatch duplex	boot-end-marker
!	!
!	logging message-counter syslog
!	!
!	no aaa new-model
!	ip source-route
!	no ip icmp rate-limit unreachable


```

duplex half
!
interface Ethernet1/6
no ip address
shutdown
duplex half
!
interface Ethernet1/7
no ip address
shutdown
duplex half
!
router ospf 1
router-id 6.6.6.6
log-adjacency-changes
network 192.168.70.0 0.0.0.3 area 0
network 192.168.90.0 0.0.0.15 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging 192.168.90.3
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!

```

```

!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
end

MikrotikR3Distribution

/interface ethernet
set [ find default-name=ether4 ] name=ether1
set [ find default-name=ether1 ] name=ether2
set [ find default-name=ether2 ] name=ether3
set [ find default-name=ether3 ] name=ether4
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=10.10.10.10
/ip address

```

```

add address=192.168.50.3/24 interface=ether1
network=192.168.50.0

add address=192.168.100.2/30 interface=ether2
network=192.168.100.0

add address=192.168.120.1/24 interface=ether3
network=192.168.120.0

/ip dhcp-client

add disabled=no interface=ether1

/routing ospf network

add area=backbone network=192.168.50.0/24

add area=backbone network=192.168.100.0/30

add area=backbone network=192.168.120.0/24

MikrotikR2Core

/interface ethernet

set [ find default-name=ether4 ] name=ether1

set [ find default-name=ether1 ] name=ether2

set [ find default-name=ether2 ] name=ether3

set [ find default-name=ether3 ] name=ether4

/interface wireless security-profiles

set [ find default=yes ] supplicant-identity=MikroTik

/routing ospf instance

set [ find default=yes ] router-id=5.5.5.5

/system logging action

set 3 remote=192.168.90.3

add name=remote2 remote=192.168.90.3
target=remote

/ip address

add address=192.168.60.2/30 interface=ether1
network=192.168.60.0

add address=192.168.70.1/30 interface=ether2
network=192.168.70.0

add address=192.168.80.1/24 interface=ether3
network=192.168.80.0

/ip dhcp-client

add disabled=no interface=ether1

/routing ospf network

add area=backbone network=192.168.60.0/30

add area=backbone network=192.168.70.0/30

add area=backbone network=192.168.80.0/24

/system logging

```

```

add action=remote topics=info

add action=remote topics=info

add action=remote topics=info

hostname SW10Distribution

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

enable secret 4
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU

!

username admin privilege 15 secret 4
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU

no aaa new-model

no ipv6 cef

ipv6 multicast rpf use-bgp

no ip icmp rate-limit unreachable

!

no ip domain-lookup

ip domain-name my.com

no ip cef

!

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

!

!

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

```

```
ip ssh version 2
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
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
```

```
!
```

```
interface Ethernet2/0
```

```
duplex auto
```

```
!
```

```
interface Ethernet2/1
```

```
duplex auto
```

```
!
```

```
interface Ethernet2/2
```

```
duplex auto
```

```
!
```

```
interface Ethernet2/3
```

```
duplex auto
```

```
!
```

```
interface Ethernet3/0
```

```
duplex auto
```

```
!
```

```
interface Ethernet3/1
```

```
duplex auto
```

```
!
```

```
interface Ethernet3/2
```

```
duplex auto
```

```
!
```

```
interface Ethernet3/3
```

```
duplex auto
```

```
!
```

```
interface Vlan1
```

```
ip address 192.168.80.101 255.255.255.0
```

```
!
```

```
!
```

```
no ip http server
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
control-plane
```

```
!
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

password mypassword	multilink bundle-name authenticated
logging synchronous	!
login	!
line aux 0	!
exec-timeout 0 0	!
privilege level 15	!
logging synchronous	!
line vty 0 4	!
login local	!
transport input ssh	!
!	!
End	!
hostname CiscoR5Distribution	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
logging message-counter syslog	archive
!	log config
no aaa new-model	hidekeys
ip source-route	!
no ip icmp rate-limit unreachable	!
ip cef	!
!	!
!	!
ip dhcp excluded-address 192.168.140.1	ip tcp synwait-time 5
!	!
ip dhcp pool Subnet140	!
network 192.168.140.0 255.255.255.0	!
default-router 192.168.140.1	!
domain-name my.net	interface FastEthernet0/0
dns-server 8.8.8.8 8.8.4.4	no ip address
!	shutdown
!	duplex half
no ip domain lookup	!
no ipv6 cef	interface Ethernet1/0
!	ip address 192.168.80.3 255.255.255.0

!	no ip domain lookup
line con 0	no ipv6 cef
exec-timeout 0 0	!
privilege level 15	multilink bundle-name authenticated
logging synchronous	!
stopbits 1	!
line aux 0	!
exec-timeout 0 0	!
privilege level 15	!
logging synchronous	!
stopbits 1	!
line vty 0 4	!
login	!
!	!
End	!
hostname CiscoR6Distribution	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
logging message-counter syslog	archive
!	log config
no aaa new-model	hidekeys
ip source-route	!
no ip icmp rate-limit unreachable	!
ip cef	!
!	!
!	!
ip dhcp excluded-address 192.168.150.1	ip tcp synwait-time 5
!	!
ip dhcp pool Subnet150	!
network 192.168.150.0 255.255.255.0	!
default-router 192.168.150.1	!
domain-name my.net	interface FastEthernet0/0
dns-server 8.8.8.8 8.8.4.4	no ip address
!	shutdown
!	duplex half

!	duplex half
interface Ethernet1/0	!
ip address 192.168.80.2 255.255.255.0	router ospf 1
duplex half	router-id 8.8.8.8
!	log-adjacency-changes
interface Ethernet1/1	network 192.168.80.0 0.0.0.255 area 0
ip address 192.168.150.1 255.255.255.0	network 192.168.130.0 0.0.0.3 area 0
ip access-group 150 out	network 192.168.150.0 0.0.0.255 area 0
duplex half	!
!	ip forward-protocol nd
interface Ethernet1/2	no ip http server
ip address 192.168.130.2 255.255.255.252	no ip http secure-server
duplex half	!
!	!
interface Ethernet1/3	!
no ip address	logging 192.168.90.3
shutdown	access-list 150 permit icmp any 192.168.150.0 0.0.0.255 echo
duplex half	access-list 150 permit icmp 192.168.150.0 0.0.0.255 any echo-reply
!	access-list 150 deny ip 192.168.110.0 0.0.0.255 any
interface Ethernet1/4	access-list 150 deny ip 192.168.120.0 0.0.0.255 any
no ip address	access-list 150 permit ip any any
shutdown	no cdp log mismatch duplex
duplex half	!
!	!
interface Ethernet1/5	!
no ip address	!
shutdown	!
duplex half	!
!	!
interface Ethernet1/6	control-plane
no ip address	!
shutdown	!
duplex half	!
!	!
interface Ethernet1/7	!
no ip address	!
shutdown	!

gatekeeper	ip domain-name my.com
shutdown	no ip cef
!	!
!	!
line con 0	!
exec-timeout 0 0	!
privilege level 15	spanning-tree mode pvst
logging synchronous	spanning-tree extend system-id
stopbits 1	!
line aux 0	!
exec-timeout 0 0	!
privilege level 15	!
logging synchronous	vlan internal allocation policy ascending
stopbits 1	!
line vty 0 4	ip tcp synwait-time 5
login	ip ssh version 2
!	!
End	!
hostname SW11Distribution	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	!
logging buffered 50000	interface Ethernet0/0
logging console discriminator EXCESS	duplex auto
enable secret 4	!
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	interface Ethernet0/1
!	duplex auto
username admin privilege 15 secret 4	!
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	interface Ethernet0/2
no aaa new-model	duplex auto
no ipv6 cef	!
ipv6 multicast rpf use-bgp	interface Ethernet0/3
no ip icmp rate-limit unreachable	duplex auto
!	spanning-tree bpduguard enable
no ip domain-lookup	

```

!
interface Ethernet1/0
    duplex auto
!
interface Ethernet1/1
    duplex auto
!
interface Ethernet1/2
    duplex auto
!
interface Ethernet1/3
    duplex auto
!
interface Ethernet2/0
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!

interface Vlan1
    ip address 192.168.140.100 255.255.255.0
!
!
no ip http server
!
!
logging host 192.168.90.3
!
!
!
control-plane
!
!
line con 0
    exec-timeout 0 0
    privilege level 15
    password mypassword
    logging synchronous
    login
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login local
    transport input ssh
!
End
hostname SW13Access
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000

```

logging console discriminator EXCESS

enable secret 4

X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU

!

username admin privilege 15 secret 4

X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU

no aaa new-model

no ipv6 cef

ipv6 multicast rpf use-bgp

no ip icmp rate-limit unreachable

!

no ip domain-lookup

ip domain-name my.com

no ip cef

!

!

ip dhcp snooping

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

!

!

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

ip ssh version 2

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

duplex auto

!

interface Ethernet0/1

switchport mode access

switchport port-security maximum 2

switchport port-security

switchport port-security aging time 10

switchport port-security aging type inactivity

switchport port-security mac-address sticky

duplex auto

ip dhcp snooping trust

!

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

!

interface Ethernet2/0

duplex auto

!

interface Ethernet2/1

duplex auto

!

```
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 192.168.140.101 255.255.255.0
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
password mypassword
logging synchronous
login
```

```
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
End
hostname SW14Access
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
!
username admin privilege 15 secret 4
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip domain-name my.com
no ip cef
!
!
ip dhcp snooping vlan 1
ip dhcp snooping
!
!
spanning-tree mode pvst
```

```

spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
    duplex auto
!
interface Ethernet0/1
    switchport mode access
    switchport port-security maximum 2
    switchport port-security
    switchport port-security aging time 10
    switchport port-security aging type inactivity
    switchport port-security mac-address sticky
    duplex auto
    ip dhcp snooping trust
!
interface Ethernet0/2
    switchport mode access
    switchport port-security maximum 2
    switchport port-security
    switchport port-security aging time 10
    switchport port-security aging type inactivity

```

```

switchport port-security mac-address sticky
duplex auto
!
interface Ethernet0/3
    duplex auto
!
interface Ethernet1/0
    duplex auto
    spanning-tree bpduguard enable
!
interface Ethernet1/1
    duplex auto
!
interface Ethernet1/2
    duplex auto
!
interface Ethernet1/3
    duplex auto
!
interface Ethernet2/0
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!

```

interface Ethernet3/2	boot-end-marker
duplex auto	!
!	!
interface Ethernet3/3	logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
duplex auto	logging buffered 50000
!	logging console discriminator EXCESS
interface Vlan1	enable secret 4
ip address 192.168.140.102 255.255.255.0	X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
!	!
!	username admin privilege 15 secret 4
no ip http server	X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
!	no aaa new-model
!	no ipv6 cef
!	ipv6 multicast rpf use-bgp
!	no ip icmp rate-limit unreachable
!	!
control-plane	no ip domain-lookup
!	ip domain-name my.com
!	no ip cef
line con 0	!
exec-timeout 0 0	!
privilege level 15	ip dhcp snooping vlan 1
password mypassword	ip dhcp snooping
logging synchronous	!
login	!
line aux 0	spanning-tree mode pvst
exec-timeout 0 0	spanning-tree extend system-id
privilege level 15	!
logging synchronous	!
line vty 0 4	!
login local	!
transport input ssh	vlan internal allocation policy ascending
!	!
End	ip tcp synwait-time 5
hostname SW15Access	!
!	!
boot-start-marker	!
	!

```

!
!
!
!
!
interface Ethernet0/0
    duplex auto
!
interface Ethernet0/1
    switchport mode access
    switchport port-security maximum 2
    switchport port-security
    switchport port-security aging time 10
    switchport port-security aging type inactivity
    switchport port-security mac-address sticky
    switchport port-security mac-address sticky
    aabb.cc00.1301
    switchport port-security mac-address sticky
    ca01.1067.001d
    duplex auto
    ip dhcp snooping trust
!
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
!
interface Ethernet2/0
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    ip address 192.168.140.103 255.255.255.0
!
!
no ip http server
!
!
!
!
!
control-plane

```

!	no ip cef
!	!
line con 0	!
exec-timeout 0 0	!
privilege level 15	!
password mypassword	spanning-tree mode pvst
logging synchronous	spanning-tree extend system-id
login	!
line aux 0	!
exec-timeout 0 0	!
privilege level 15	!
logging synchronous	vlan internal allocation policy ascending
line vty 0 4	!
login local	ip tcp synwait-time 5
transport input ssh	ip ssh version 2
!	!
End	!
hostname SW12Distribution	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	!
logging buffered 50000	interface Ethernet0/0
logging console discriminator EXCESS	duplex auto
enable secret 4	!
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	interface Ethernet0/1
!	duplex auto
username admin privilege 15 secret 4	!
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	interface Ethernet0/2
no aaa new-model	duplex auto
no ipv6 cef	!
ipv6 multicast rpf use-bgp	interface Ethernet0/3
no ip icmp rate-limit unreachable	duplex auto
!	!
no ip domain-lookup	interface Ethernet1/0
ip domain-name my.com	

duplex auto	!
!	!
interface Ethernet1/1	no ip http server
duplex auto	!
!	!
interface Ethernet1/2	!
duplex auto	!
!	!
interface Ethernet1/3	control-plane
duplex auto	!
!	!
interface Ethernet2/0	line con 0
duplex auto	exec-timeout 0 0
!	privilege level 15
interface Ethernet2/1	password mypassword
duplex auto	logging synchronous
!	login
interface Ethernet2/2	line aux 0
duplex auto	exec-timeout 0 0
!	privilege level 15
interface Ethernet2/3	logging synchronous
duplex auto	line vty 0 4
!	login local
interface Ethernet3/0	transport input ssh
duplex auto	!
!	End
interface Ethernet3/1	hostname SW16Access
duplex auto	!
!	boot-start-marker
interface Ethernet3/2	boot-end-marker
duplex auto	!
!	!
interface Ethernet3/3	logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
duplex auto	logging buffered 50000
!	logging console discriminator EXCESS
interface Vlan1	enable secret 4
ip address 192.168.150.100 255.255.255.0	X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU

```
!  
username admin privilege 15 secret 4  
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU  
no aaa new-model  
no ipv6 cef  
ipv6 multicast rpf use-bgp  
no ip icmp rate-limit unreachable  
!  
no ip domain-lookup  
ip domain-name my.com  
no ip cef  
!  
!  
ip dhcp snooping vlan 1  
ip dhcp snooping  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
vlan internal allocation policy ascending  
!  
ip tcp synwait-time 5  
ip ssh version 2  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
duplex auto
```

```
!  
interface Ethernet0/1  
duplex auto  
!  
interface Ethernet0/2  
switchport mode access  
switchport port-security maximum 2  
switchport port-security  
switchport port-security aging time 10  
switchport port-security aging type inactivity  
switchport port-security mac-address sticky  
duplex auto  
ip dhcp snooping trust  
!  
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  
!  
interface Ethernet2/0  
duplex auto  
!  
interface Ethernet2/1  
duplex auto  
!  
interface Ethernet2/2  
duplex auto
```

```

!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    ip address 192.168.150.101 255.255.255.0
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
    exec-timeout 0 0
    privilege level 15
    password mypassword
    logging synchronous
    login
line aux 0
    exec-timeout 0 0

privilege level 15
logging synchronous
line vty 0 4
    login local
    transport input ssh
!
End
hostname SW17Access
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
!
username admin privilege 15 secret 4
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip domain-name my.com
no ip cef
!
!
ip dhcp snooping vlan 1
ip dhcp snooping
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!

```

```

!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
    duplex auto
!
interface Ethernet0/1
    duplex auto
!
interface Ethernet0/2
    switchport mode access
    switchport port-security maximum 2
    switchport port-security
    switchport port-security aging time 10
    switchport port-security aging type inactivity
    switchport port-security mac-address sticky
    duplex auto
    ip dhcp snooping trust
!
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
!
interface Ethernet2/0
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    ip address 192.168.150.102 255.255.255.0
!

```

!	username admin privilege 15 secret 4
no ip http server	X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU
!	no aaa new-model
!	no ipv6 cef
!	ipv6 multicast rpf use-bgp
!	no ip icmp rate-limit unreachable
!	!
control-plane	no ip domain-lookup
!	ip domain-name my.com
!	no ip cef
line con 0	!
exec-timeout 0 0	!
privilege level 15	ip dhcp snooping vlan 1
password mypassword	ip dhcp snooping
logging synchronous	!
login	!
line aux 0	spanning-tree mode pvst
exec-timeout 0 0	spanning-tree extend system-id
privilege level 15	!
logging synchronous	!
line vty 0 4	!
login local	!
transport input ssh	vlan internal allocation policy ascending
!	!
End	ip tcp synwait-time 5
hostname SW18Access	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	!
logging buffered 50000	!
logging console discriminator EXCESS	interface Ethernet0/0
enable secret 4	duplex auto
X4ZqtPJ///KxuEWxHSsJrv3beQVnz2ise/xj8fF6eFU	!
!	interface Ethernet0/1

```

duplex auto
!
interface Ethernet0/2
switchport mode access
switchport port-security maximum 2
switchport port-security
switchport port-security aging time 10
switchport port-security aging type inactivity
switchport port-security mac-address sticky
duplex auto
ip dhcp snooping trust
!
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
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3

```

```

duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 192.168.150.103 255.255.255.0
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
password mypassword
logging synchronous
login
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

line vty 0 4

!

login local

end

transport input ssh