

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

ПОЯСНЮВАЛЬНА ЗАПISKA

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної гетерогенної мережі організації з використанням технологій VPN»

Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Іван СЕРДІЙЧУК

Керівник: старший викладач кафедри КІ та КБ

 Олександра ПОКОТИЛО

Рецензент: Професор кафедри КІ та КБ, д.т.н., доцент

 Володимир ВОРОТНИКОВ

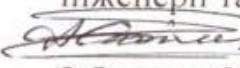
Житомир – 2025

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

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Сердійчук Іван Сергійович

Тема роботи: «Проект захищеної гетерогенної мережі організації з використанням технологій VPN»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 20 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

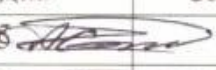
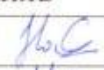
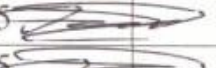
Предмет дослідження: методи, засоби та технології для побудови захищеної мережевої інфраструктури

Об'єкт дослідження: процес забезпечення інформаційної безпеки в гетерогенних корпоративних мережах.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 4321 (с4000)
2. Маршрутизатор MikroTik CCR2216-1G-12XS-2XQ
3. Комутатор Cisco WS-C2960-24TT-L
4. ОС Windows
5. ОС Linux

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А	12.03.2025 	12.03.2025 
2	Єфіменко А.А	21.04.2025 	21.04.2025 
3	Єфіменко А.А	29.05.2025 	29.05.2025 

Студент  Іван СЕРДІЙЧУК

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	20.03.2025	Виконано
2	Аналіз літературних джерел	31.03.2025	Виконано
3	Аналіз об'єкта дослідження	16.04.2025	Виконано
4	Розробка структурної моделі	19.04.2025	Виконано
5	Розрахунок параметрів адресації	23.04.2025	Виконано
6	Вибір технології для реалізації	29.04.2025	Виконано
7	Налаштування мережі	03.05.2025	Виконано
8	Налагодження IPsec VPN	19.05.2025	Виконано
9	Адміністрування мережі	25.05.2025	Виконано
10	Проведення тестування на працездатність	30.05.2025	Виконано
11	Оформлення пояснювальної записки	06.06.2025	Виконано
12	Оформлення презентації	14.06.2025	Виконано
13	Захист	20.06.2025	Виконано

Студент  Іван СЕРДІЙЧУК

Керівник  Олександра ПОКОТИЛО

АНОТАЦІЯ

Кваліфікаційна робота присвячена проектуванню, налаштуванню та тестуванню захищеної гетерогенної мережі з використанням технологій VPN.

Загальний обсяг пояснювальної записки – 83 сторінки. Робота містить 74 рисунки, 18 таблиць. Список використаних джерел налічує 29 найменувань та розміщений на 3 сторінках.

Метою кваліфікаційної роботи є розробка та налаштування проекту захищеної гетерогенної корпоративної мережі з використанням технології VPN для забезпечення конфіденційності, цілісності та доступності даних.

У роботі представлено комплексне рішення для створення захищеної гетерогенної мережі організації. Проведено аналіз переваг та недоліків гетерогенних середовищ. Розглянуто теоретичні основи технології VPN, її типи та протоколи, на основі чого обґрунтовано вибір IPsec як основного механізму захисту. Досліджено принципи динамічної маршрутизації та переваги протоколу OSPF, такі як швидка конвергенція та підтримка ієрархічної структури, для використання в проєкті.

Апаратною базою слугує обладнання Cisco та MikroTik. Практична частина включає розробку топології комп'ютерної мережі на основі трирівневої ієрархічної моделі Cisco, розроблено детальну систему IP-адресації для 19 підмереж та виконано послідовне налаштування мережевих сервісів: DHCP, протоколу OSPF, IPsec VPN, SSH та Syslog.

Фінальне тестування підтвердило повну працездатність, зв'язність усіх сегментів мережі та коректну роботу механізмів захисту.

Ключові слова: ГЕТЕРОГЕННА МЕРЕЖА, VPN, IPSEC, OSPF, CISCO, MIKROTIK, МЕРЕЖЕВА БЕЗПЕКА, МАРШРУТИЗАЦІЯ, DHCP, SYSLOG.

					ККІК.КР.Б – 125 – 17 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної гетерогенної мережі організації з використанням технологій VPN	Літ.	Арк.	Аркушів
Розроб.		Сердійчук І.С.		18.06.25				
Керівник		Покотило О.А.		18.06.25			4	104
Реценз.		Воротніков В.В.		18.06.25		ФІКТ, Гр. КБ-21-1		
Н. контр.		Борисенко М.А.		18.06.25				
Затверд.		Сфіменко А.А.		18.06.25				

ANNOTATION

The qualification work is devoted to the design, configuration, and testing of a secure heterogeneous network using VPN technologies.

The total volume of the explanatory note is 83 pages. The work contains 74 figures and 18 tables. The list of references contains 29 items and is located on 3 pages.

The purpose of the thesis is to develop and configure a secure heterogeneous corporate network using VPN technology to ensure data confidentiality, integrity, and availability.

The work presents a comprehensive solution for creating a secure heterogeneous network for an organization. An analysis of the advantages and disadvantages of heterogeneous environments is conducted. The theoretical foundations of VPN technology, its types and protocols are considered, on the basis of which the choice of IPsec as the main protection mechanism is justified. The principles of dynamic routing and the advantages of the OSPF protocol, such as fast convergence and support for a hierarchical structure, are investigated for use in the project.

Cisco and MikroTik equipment serves as the hardware base. The practical part includes the development of a computer network topology based on Cisco's three-level hierarchical model, the development of a detailed IP addressing system for 19 subnets, and the sequential configuration of network services: DHCP, OSPF protocol, IPsec VPN, SSH, and Syslog.

Final testing confirmed the full operability and connectivity of all network segments and the correct operation of security mechanisms.

Keywords: HETEROGENEOUS NETWORK, VPN, IPSEC, OSPF, CISCO, MIKROTIK, NETWORK SECURITY, ROUTING, DHCP, SYSLOG.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНОЇ ГЕТЕРОГЕННОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN.....	10
1.1 Поняття гетерогенних мереж	10
1.1.1. Визначення та особливості гетерогенних мереж	10
1.1.2 Типи гетерогенних мереж	12
1.1.3 Переваги та недоліки гетерогенних мереж	15
1.2 Технології VPN.....	17
1.2.1 Історія та визначення VPN.....	17
1.2.2 Типи та принципи роботи VPN	19
1.2.3 Протоколи VPN.....	24
1.3 Протокол маршрутизації OSPF.....	29
1.3.1 Маршрутизація.....	29
1.3.2 Визначення та історія створення OSPF.....	30
1.3.3 Огляд роботи OSPF.....	31
1.3.4 Переваги та недоліки OSPF	33
РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	36
2.1 Розробка топології комп'ютерної мережі	36
2.2 Розробка системи IP-адресації	43
2.3 Проектування служб та сервісів прикладного рівня.....	49
2.4 Проектування підсистеми мережного захисту	54
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЕКТОВАНОЇ МЕРЕЖІ.....	58
3.1 Вибір обладнання та ОС пристроїв для розробленого проекту мережі.....	58
3.2. Побудова та налагодження мережі	62
3.3 Тестування роботи мережі	71
ВИСНОВКИ.....	79
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	81
ДОДАТКИ.....	84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

VPN – Virtual Private Network

IPsec – Internet Protocol Security

OSPF – Open Shortest Path First

DHCP – Dynamic Host Configuration Protocol

SSH – Secure Shell

LAN – Local Area Network

WAN – Wide Area Network

WLAN – Wireless Local Area Network

HetNet – Heterogeneous Network

IoT – Internet of Things

TCP/IP – Transmission Control Protocol/Internet Protocol

UDP – User Datagram Protocol

DNS – Domain Name System

Syslog – System Logging Protocol

PPTP – Point-to-Point Tunneling Protocol

QoS – Quality of Service

NIM – Network Interface Module

ISR – Integrated Services Routers

SFP – Small Form-factor Pluggable

DoS – Denial-of-Service

LSA – Link-State Advertisement

IETF – Internet Engineering Task Force

SPF – Shortest Path First

VLSM – Variable Length Subnet Mask

CIDR – Classless Inter-Domain Routing

HTTP – Hypertext Transfer Protocol

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. В умовах стрімкої цифровізації та зростання кіберзагроз, забезпечення надійного захисту корпоративних мереж є критично важливим завданням для будь-якої організації. Гетерогенні мережі, що поєднують обладнання від різних виробників, стали поширеним явищем через гнучкість та економічну ефективність. Однак така різноманітність створює додаткові виклики у питаннях сумісності та централізованого керування безпекою. Використання технологій віртуальних приватних мереж дозволяє вирішити ці проблеми, створюючи захищені канали для передачі конфіденційних даних через публічні мережі, що є особливо актуальним для компаній з віддаленими працівниками та філіями.

Метою кваліфікаційної роботи є розробка та налаштування проекту захищеної гетерогенної корпоративної мережі з використанням технології VPN для забезпечення конфіденційності, цілісності та доступності даних.

Визначена мета обумовлює наступні завдання:

- Аналіз сучасних методів безпеки гетерогенних мереж.
- Обґрунтування вибору мережевого обладнання та технологій захисту.
- Розробка топології гетерогенної мережі на базі обладнання Cisco та MikroTik.
- Налаштування основних мережевих сервісів та протоколів: DHCP для автоматичного призначення IP-адрес та динамічної маршрутизації OSPF.
- Конфігурування захищеного VPN-тунелю за допомогою протоколу IPsec для безпечної передачі даних між філіями.
- Впровадження системи моніторингу та збору логів за допомогою Syslog.
- Проведення тестування працездатності та надійності мережі.

Об'єктом дослідження є процес забезпечення інформаційної безпеки в гетерогенних корпоративних мережах. Цей процес розглядається як комплексна діяльність, що охоплює кілька ключових етапів: від аналізу потенційних вразливостей та загроз до впровадження й підтримки цілісної системи захисту.

Предметом дослідження є методи, засоби та технології для побудови захищеної мережевої інфраструктури, зокрема конфігурування маршрутизаторів Cisco

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

та MikroTik, вони розглядаються як апаратна основа мережі; налаштування протоколу маршрутизації OSPF, він досліджується як інструмент для автоматизації обміну маршрутною інформацією між різними сегментами мережі; механізму безпеки IPsec VPN, який є центральним елементом захисту, охоплюється архітектура протоколу IPsec, механізми автентифікації, шифрування та перевірки цілісності даних; механізму Syslog, він вивчається як засіб для централізованого збору, моніторингу та аналізу системних повідомлень з мережевих пристроїв.

У процесі виконання кваліфікаційної роботи було розроблено проект захищеної гетерогенної мережі, що об'єднує обладнання Cisco та MikroTik. Проект демонструє створення безпечного каналу зв'язку між підмережами за допомогою IPsec VPN та забезпечує динамічний обмін маршрутною інформацією через протокол OSPF.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНОЇ ГЕТЕРОГЕННОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

1.1 Поняття гетерогенних мереж

1.1.1. Визначення та особливості гетерогенних мереж.

Гетерогенна комп'ютерна мережа – комп'ютерна мережа, що з'єднує персональні комп'ютери та інші пристрої з різними операційними системами або протоколами передавання даних. Наприклад, локальна мережа, яка з'єднує комп'ютери під управлінням операційних систем Microsoft Windows, Linux і MacOS, є гетерогенною. Термін «гетерогенні мережі» також вживають у бездротових мережах, які використовують різні технології для підключення. Наприклад, бездротова мережа, яка забезпечує доступ через бездротову локальну мережу і здатна забезпечувати доступ, перемикаючись на стільниковий зв'язок, також називається гетерогенною мережею[1].

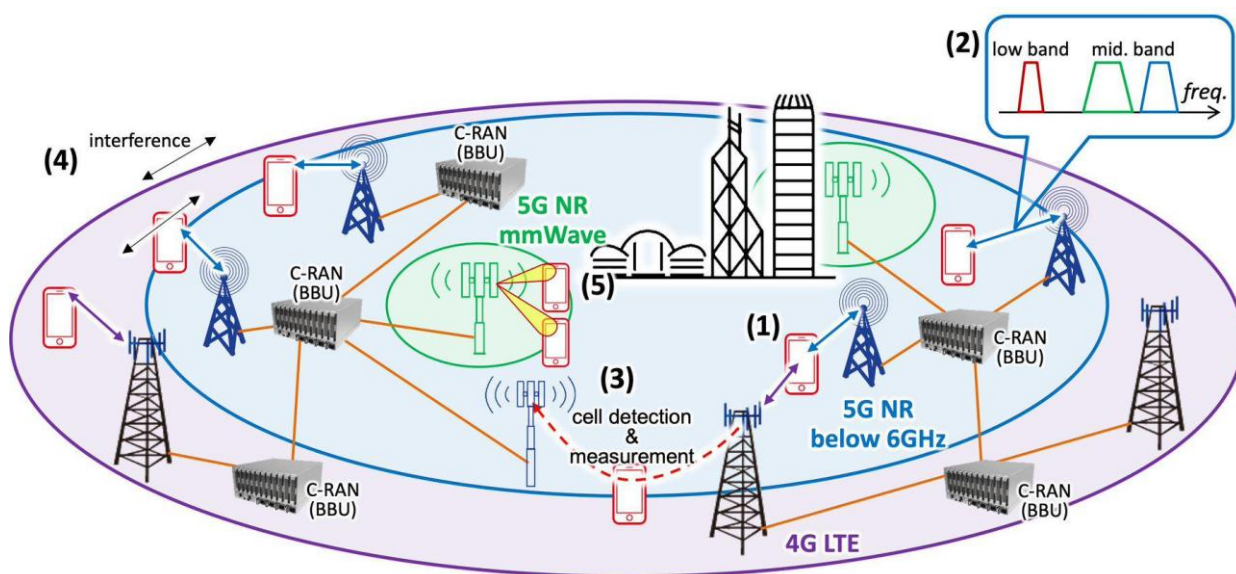


Рисунок 1.1 – Демонстрація роботи гетерогенної мережі

Ключовими елементами гетерогенних мереж є провідні та безпроводні технології, такі як – Ethernet, який забезпечує високу швидкість передачі даних на локальному рівні, Wi-Fi або 4G/5G, вони дозволяють підключення мобільних пристроїв у великих масштабах. В межах однієї мережі можуть співіснувати пристрої з Windows, macOS, Linux та іншими ОС, забезпечуючи взаємодію між різними

платформами. Також використовуються різні протоколи, наприклад, TCP/IP для передачі даних, UDP для швидкої передачі чи специфічні протоколи для IoT.

Однією з ключових задач гетерогенних мереж є забезпечення взаємодії різних компонентів. Це вимагає сумісності між системами, програмних та апаратних рішень, які підтримують загальні стандарти, наприклад, IEEE 802 для локальних мереж. Для зв'язку між різними протоколами чи форматами даних використовуються мережеві шлюзи, проксі-сервери та адаптери. Інтеграція локальних та глобальних мереж дозволяє об'єднати офісні мережі з інтернетом чи хмарними рішеннями.

Гетерогенні мережі дуже легко адаптуються до змін та дозволяють додавати нові пристрої чи сегменти. Наприклад, при відкритті нового офісу достатньо інтегрувати його локальну мережу з центральною. Адміністратор може налаштувати пріоритети трафіку чи маршрутизацію без повного перезапуску мережі. Мережа може масштабуватися як вертикально, так і горизонтально.

Віртуалізація також відіграє ключову роль у гетерогенних мережах. Наприклад віртуальні приватні мережі забезпечують безпечне з'єднання між віддаленими сегментами мережі, навіть через інтернет. Хмарні платформи, такі як Microsoft Azure або Amazon AWS, інтегруються з локальними системами для розширення функціоналу. Використання віртуалізації серверів дозволяє запускати кілька віртуальних серверів на одному фізичному.

Через складність та різноманітність гетерогенні мережі вимагають посиленого захисту. Основними механізмами є шифрування даних, багаторівневий контроль доступу та моніторинг і виявлення загроз. Інтеграція систем Security Information and Event Management дозволяє аналізувати мережеву активність. Адміністрування гетерогенних мереж є складним процесом. ІТ-спеціалісти повинні знати особливості кожної технології та протоколу, а всі налаштування та зміни в мережі мають бути задокументовані для швидкого розв'язання проблем.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

1.1.2 Типи гетерогенних мереж

Гетерогенні мережі поділяються на кілька основних типів залежно від їхньої архітектури, технологій зв'язку та сфер застосування. Далі ми детальніше пройдемо по кожному із цих типів.

Гетерогенні локальні мережі (LAN) використовуються для з'єднання різних типів пристроїв в одному просторі, наприклад, в офісі або будинку. Вони можуть спільно використовувати такі ресурси, як файли, принтери та інтернет. Пристрої, що працюють на різних операційних системах, наприклад Windows, Linux, macOS взаємодіють через мережеві адаптери та драйвери. Основними стандартами є Ethernet для дротових з'єднань і Wi-Fi для бездротових. Такі мережі мають високу швидкість передачі даних і використовуються в домашньому та офісному середовищі. Наприклад, в офісних мережах комп'ютери з різними операційними системами можуть спільно використовувати мережне сховище.



Рисунок 1.2 – Приклад локальної мережі

Гетерогенні глобальні мережі (WAN) з'єднують пристрої та системи на великій відстані за допомогою різних технологій передачі даних, таких як оптоволоконні лінії, супутниковий зв'язок і підводні кабелі. WAN інтегрують протоколи TCP/IP і PPP для передачі даних через різні мережі. Ці мережі охоплюють великі географічні території, включаючи багато країн і континентів. Вони використовую-

ються міжнародними компаніями, банківськими системами та державними установами. Наприклад, банківські системи дозволяють клієнтам отримувати доступ до своїх рахунків у різних країнах через одну мережу[21].

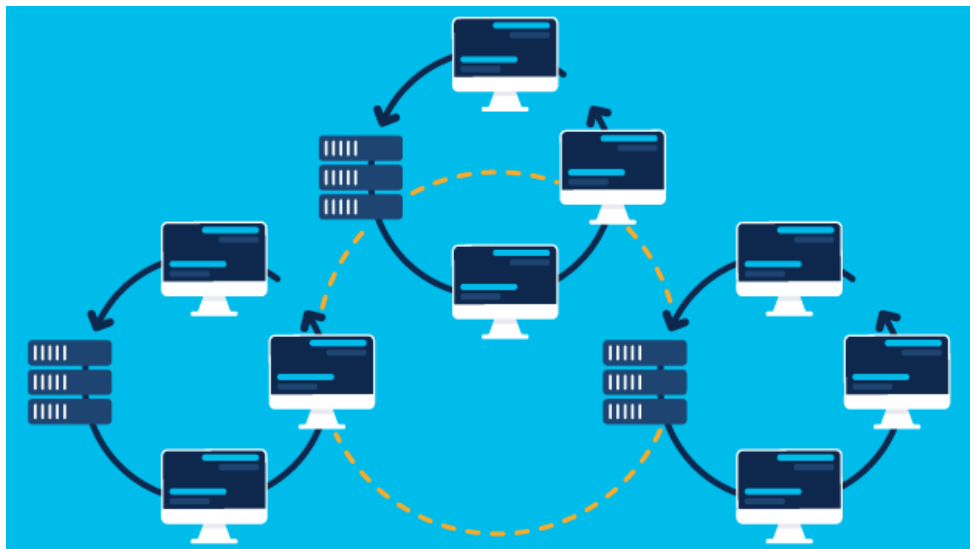


Рисунок 1.3 – Приклад глобальної мережі

Гетерогенні бездротові мережі (HetNet) інтегрують різні технології зв'язку, такі як Wi-Fi, LTE, 5G і Bluetooth, щоб забезпечити безперебійне з'єднання між пристроями і мережами. HetNet використовує макростільники для великих територій і покриття всередині приміщень, а малі стільники для покращеного покриття всередині приміщень. Перемикання між технологіями відбувається автоматично, залежно від якості сигналу[22].

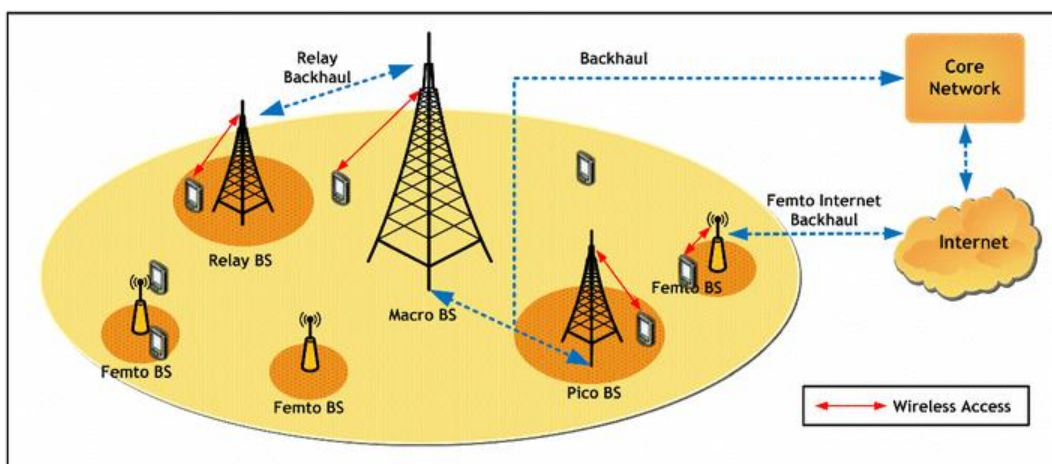


Рисунок 1.4 – Приклад бездротової мережі

Гетерогенні мережі центрів обробки даних (DataCenters) об'єднують сервери, системи зберігання даних і мережеві пристрої з різними апаратними платформами та програмним забезпеченням. Віртуалізація та програмно-визначені мережі

забезпечують масштабованість і високу продуктивність. Такі мережі широко використовуються у хмарних сервісах, обчислювальних кластерах та корпоративних системах[23].

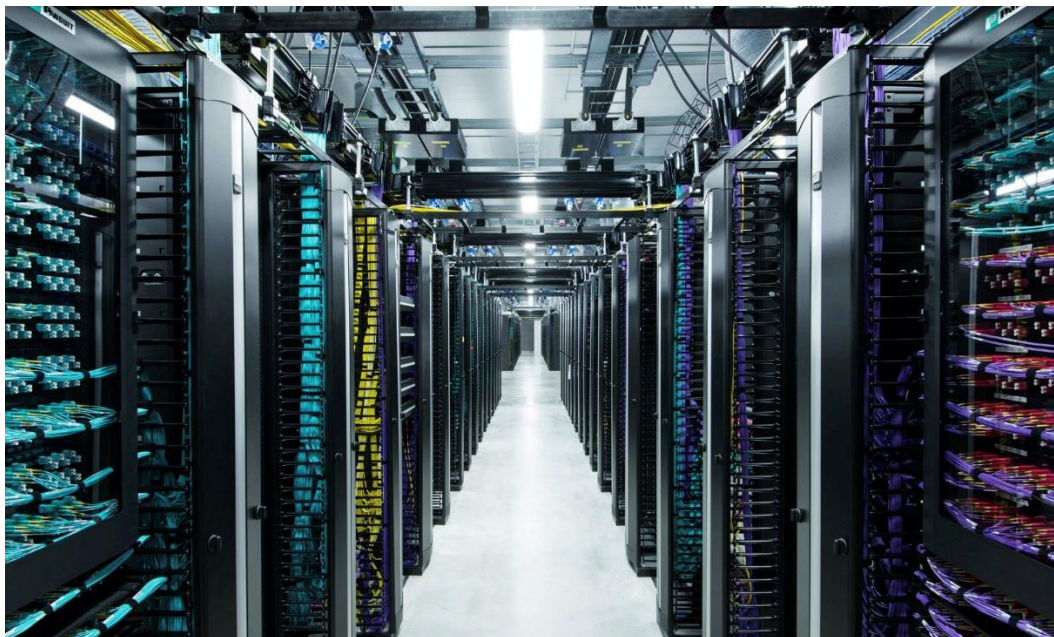


Рисунок 1.5 – Приклад мережі центрів обробки даних

Гетерогенні мережі Інтернету речей (IoT) об'єднують різні пристрої, такі як датчики, смарт-пристрої та промислове обладнання. Вони використовують шлюзи для перетворення даних між різними протоколами, такими як ZigBee, Z-Wave, LoRaWAN і Wi-Fi. Ці мережі оптимізовані для енергоефективності та дозволяють централізовано керувати пристроями. Вони використовуються в розумних будинках, промисловості та сільському господарстві. Наприклад, системи розумного будинку об'єднують датчики руху, термостати і розумні камери в єдину мережу[24].



Рисунок 1.6 – Приклад мережі Інтернету речей

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

1.1.3 Переваги та недоліки гетерогенних мереж

Як і будь-яка технологія, гетерогенні мережі мають свої переваги та недоліки, які необхідно враховувати при їх розробці та впровадженні. Далі ми розглянемо та детально проаналізуємо сильні та слабкі сторони гетерогенних мереж з метою визначення їхньої ефективності в різних умовах використання.

Переваги:

- Гнучкість інтеграції
- Масштабованість та адаптивність
- Економія ресурсів
- Стійкість до відмов
- Інтеграція з існуючими системами

Тепер давайте розглянемо кожен із переваг більш детально.

Гнучкість інтеграції: Гетерогенні мережі об'єднують апаратне та програмне забезпечення від різних виробників і забезпечують сумісність за допомогою стандартів передачі даних і спеціалізованого проміжного програмного забезпечення. Це гарантує, що різні операційні системи, такі як Windows, macOS і Linux, можуть працювати, а стандарти, такі як TCP/IP і REST API, можуть використовуватися для зв'язку між пристроями. Також різні периферійні пристрої можуть підтримуватися незалежно від специфікації.

Масштабованість та адаптивність: Гетерогенні мережі мають високу масштабованість і легко адаптуються до нових технологій, дозволяючи додавати нові пристрої без зміни базової архітектури. Наприклад, сервери, робочі станції та датчики Інтернету речей можна динамічно підключати без переривання роботи мережі. Це особливо корисно для великих підприємств, які можуть додавати нові точки доступу Wi-Fi і комутатори для підтримки тисяч користувачів.

Економія ресурсів: Мережі дозволяють ефективно поєднувати старе обладнання з новими компонентами, щоб продовжити термін їхньої експлуатації. Наприклад, старі комп'ютери можна використовувати як термінальні клієнти, тоді як сер-

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

вісна інфраструктура може залишатися на старих серверах, якщо є достатньо ресурсів. Крім того, віртуалізація може заощадити витрати за рахунок оптимізації використання апаратних ресурсів.

Стійкість до відмов: Різноманітність компонентів забезпечує гнучкість мережі. Наприклад, можна створити резервні шляхи передачі даних через різні маршрутизатори або використовувати сервери з різними операційними системами, щоб уникнути залежності від однієї платформи. Якщо один сервер виходить з ладу, інший може взяти на себе основні функції.

Інтеграція з існуючими системами: У гетерогенних мережах інфраструктуру можна модернізувати поступово, без необхідності повної заміни застарілих систем. Це зменшує витрати на міграцію та захищає існуючі інвестиції в обладнання. Наприклад, організації можуть інтегрувати хмарні сервіси, такі як Office 365, у свою локальну мережу без необхідності відмовлятися від серверів Exchange.

Гетерогенні мережі, попри свої тотальні переваги, мають декілька недоліків:

- Складність управління
- Висока вартість обслуговування
- Уразливість безпеки
- Зниження продуктивності

Далі пройдемося по кожному із недоліків більш детально

Складність управління: Гетерогенні мережі вимагають спеціальних знань і використання різних інструментів управління. Оновлення програмного забезпечення та прошивки вимагають окремого підходу для кожного пристрою, що вимагає залучення фахівців з різними компетенціями для ефективного управління та збільшує витрати на обслуговування. Наприклад, мережі серверів Linux, робочих станцій Windows і пристроїв різних виробників вимагають інтегрованого підходу до управління.

Висока вартість обслуговування: Для кожного компонента можуть знадобитися окремі ліцензії на програмне забезпечення, а регулярне оновлення для забезпечення відповідності існуючим стандартам збільшить витрати. Персонал потребує

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

ватиме постійного навчання, щоб адаптуватися до змін, спричинених впровадженням нових технологій. Наприклад, компаніям з серверами Linux, настільними комп'ютерами Windows та мобільними пристроями потрібно буде купувати різні ліцензії, що збільшить витрати на обслуговування.

Уразливість безпеки: Це пов'язано з тим, що різноманітність компонентів ускладнює впровадження централізованої політики безпеки. Пристрої можуть бути різними у рівні шифрування, а старі моделі, які більше не будуть отримувати оновлення, є точками атак. Наприклад, маршрутизатор, який підтримує лише WPA2, може бути вразливим елементом, в мережі з іншими компонентами, які використовують WPA3.

Зниження продуктивності: Це пов'язано з різницею у швидкості роботи мережевих компонентів. Застарілі комутатори та маршрутизатори можуть стати вузькими місцями, сповільнюючи роботу сучасних сегментів мережі та викликаючи конфлікти між локальними та хмарними рішеннями через низьку пропускну здатність застарілих протоколів. Наприклад, маршрутизатори у віддалених офісах не можуть ефективно обробляти VoIP-трафік, що призводить до затримок і низької якості дзвінків.

Проаналізувавши всі переваги та недоліки можна зробити висновок, хоч недоліки і присутні, проте вони не значні та переваг більше. Отож гетерогенна мережа є оптимальним вибором для ефективної та надійної роботи.

1.2 Технології VPN

1.2.1 Історія та визначення VPN

Virtual private network, або ж просто VPN – це узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачу бути повноцінним учасником віддаленої мережі і користуватись її сервісами, такими як внутрішні сайти, бази, принтери, політики виходу в інтернет. Безпеку передавання інформації через загальнодоступні мережі реалізовано за допомогою шифрування, внаслідок чого створюється закритий для

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

сторонніх канал обміну інформацією. Технологія дозволяє об'єднати декілька географічно віддалених мереж у єдину мережу з використанням для зв'язку між ними непідконтрольних каналів[4].

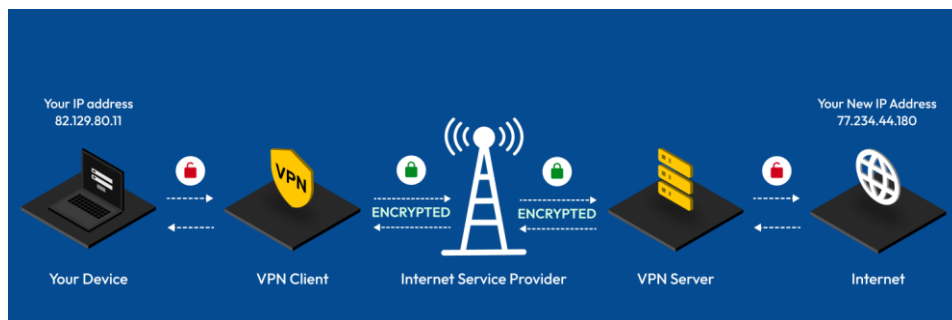


Рисунок 1.7 – Принцип роботи VPN

Історія створення та розвитку VPN

З часів розробки унікального протоколу передачі даних TCP/IP. Ще в 70-х роках минулого століття підрозділи військової розвідки США намагалися створити систему швидкого електронного обміну даними. Результатом таких зусиль стала мережа комутації пакетів Advanced Research Projects Agency Network (ARPANET). Саме в ній вперше була використана цифрова модель передачі даних TCP/IP.

Як тільки протокол TCP/IP з'явився на ринку у вільному доступі, різні компанії активно почали брати його на озброєння. Особливу увагу він привернув з боку великих корпорацій, які шукали оптимальне рішення для об'єднання декількох власних представництв в єдину мережу. Водночас багато представників бізнесу також почали замислюватися про забезпечення безпеки комунікацій.

Так, у 1993 році з'явилася перша програма, здатна шифрувати дані під час їх передачі по IP-протоколу - Software IP Encryption Protocol (swIPe). Ця розробка фахівців Колумбійського університету стала основою для розвитку віртуальних приватних мереж.

Ключовий переломний момент у розвитку технології VPN стався в 1996 році. Йдеться про створення протоколу Peer to Peer Tunneling Protocol (PPTP). З його допомогою в незахищеній мережі Microsoft формувалася окремий закритий тунель, через який передавалися дані. Ця технологія була сертифікована Microsoft, а клієнт PPTP автоматично встановлювався в усіх версіях операційної системи Windows,

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

починаючи з 95-ї. Свого часу багато інших операційних систем також працювали на цьому протоколі: Linux, Mac OS, iOS, FreeBSD.

PPTP пройшов величезну кількість тестувань і перевірок на безпеку. На жаль, в ньому було виявлено досить багато вразливостей, в результаті чого багато експертів почали говорити про те, що IPsec все ж буде надійніше. Поступово ця технологія була витіснена з ринку. Але все ж багато експертів сходяться на думці, що саме ця технологія стала предтечею сучасних віртуальних приватних мереж.

Завдання, яке поставили перед собою розробники VPN, полягало в управлінні віддаленими співробітниками компанії. Важливо було надати кожному співробітнику доступ до свого комп'ютера, незалежно від того, знаходиться він в офісі, вдома чи у відрядженні. Але при цьому з'єднання повинно було здійснюватися виключно по захищеному і безпечному каналу. Так з'явилися перші VPN-клієнти на комп'ютерах співробітників. Якщо якомусь зловмиснику все ж вдавалося перехопити інформацію, що передавалася по захищеному з'єднанню, то єдине, що він бачив - це повністю захищений трафік. Тобто ніякої корисної і важливої інформації зловмисник не міг звідси отримати.

Але, незважаючи на те, що технології VPN були створені досить давно, масового поширення на практиці вони отримали приблизно в 2010 році. Тоді, коли інтерес до захисту персональних даних став масовим. Це призвело до появи цілої індустрії всілякого програмного забезпечення для персональних комп'ютерів і мобільних пристроїв, середовища для забезпечення безпечного перегляду в інтернеті, а згодом і для обходу всіляких обмежень, в тому числі і на регіональному рівні.[6]

1.2.2 Типи та принципи роботи VPN

Типи VPN відрізняються за методами створення тунелів, використанням протоколів і призначенням. Далі більш детально пройдемося по кожному із типів та розглянемо їх принципи роботи.

Site-to-Site VPN – це з'єднання між двома або більше мережами, наприклад, корпоративною мережею та мережею філії. Організації використовують VPN як

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

альтернативу виділеним MPLS-з'єднанням, щоб використовувати інтернет-з'єднання для приватного трафіку.

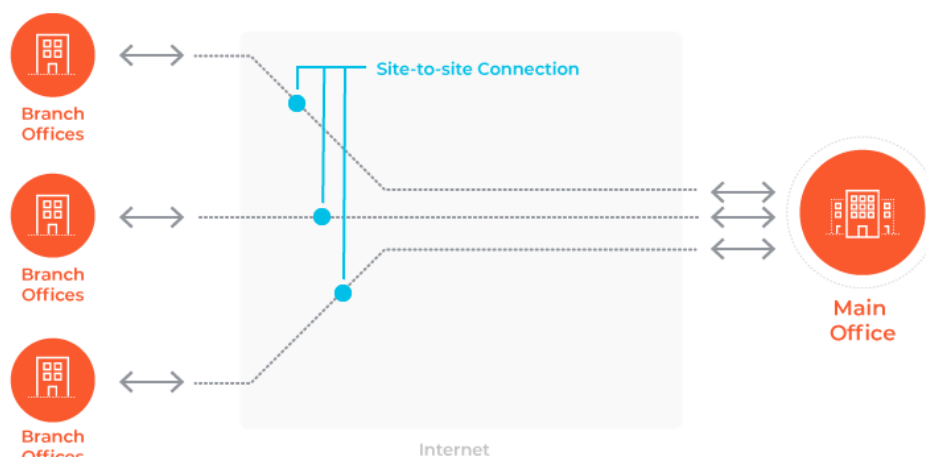


Рисунок 1.8 – Демонстрація роботи Site-to-site VPN

Site-to-site VPN часто використовуються компаніями з декількома офісами в різних географічних точках, яким потрібен доступ до корпоративної мережі. Site-to-site VPN дозволяє компаніям безпечно з'єднувати свої корпоративні мережі з віддаленими офісами, спілкуватися і спільно використовувати ресурси як єдину мережу. Також він забезпечує доступ з однієї мережі до іншої через Інтернет. Site-to-site VPN працює шляхом створення безпечного, зашифрованого тунелю між двома мережами, розташованими в різних місцях. Тунель діє як пряме з'єднання, через яке можна безпечно передавати дані.

VPN використовує таблиці маршрутизації, щоб направляти пакети даних по правильному шляху в тунелі. Тунелі між сайтами покладаються на протоколи шифрування, щоб гарантувати, що дані не можуть бути перехоплені або прочитані несанкціонованими сторонами.

Процес передбачає розміщення шлюзів на обох кінцях мережі, ефективно з'єднуючи всю мережу з VPN-сервером. Шлюз VPN керує шифруванням і дешифруванням даних, що входять і виходять з тунелю. Дані проходять через загальнодоступний Інтернет у цьому тунелі.

Завдяки шифруванню дані є непрозорими для сторонніх і виглядають як незрозуміла тарабарщина. Після досягнення шлюзу призначення дані розшифрову-

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

ються і надсилаються у внутрішню мережу одержувача. Цей захищений міст забезпечує безперебійний і безпечний потік інформації між мережами. Ресурси можна використовувати так, ніби вони знаходяться в одній локальній мережі[9].

Remote Access VPN дозволяє користувачам, які працюють віддалено, отримати безпечний доступ до додатків і даних, що знаходяться в корпоративному центрі обробки даних і головному офісі, шифруючи весь трафік, який користувачі надсилають і отримують

Безпечні VPN для віддаленого доступу створюють практично приватний тунель між мережею і віддаленим користувачем. Трафік шифрується і не може бути прочитаний підслуховуючими пристроями. Віддалені користувачі можуть безпечно підключатися до мережі та користуватися нею так, ніби вони знаходяться в офісі. Використання VPN для віддаленого доступу гарантує, що дані можуть передаватися без ризику перехоплення або фальсифікації.

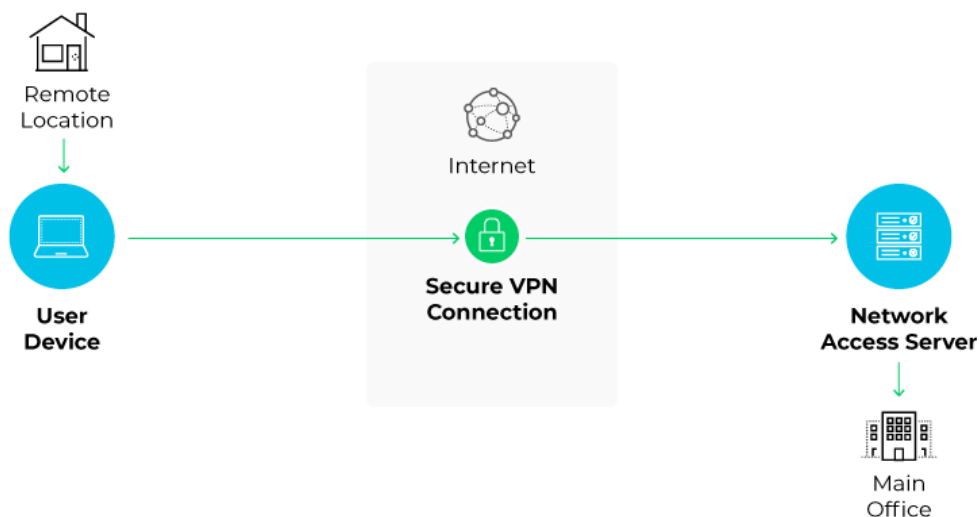


Рисунок 1.9 – Демонстрація роботи Remote Access VPN

Remote Access VPN працює шляхом встановлення безпечного, зашифрованого з'єднання між пристроєм користувача та корпоративною мережею. Цей процес починається з VPN-клієнта, який керує початковим процесом автентифікації, підтверджуючи, що тільки авторизовані користувачі можуть встановити з'єднання. Після автентифікації програмне забезпечення VPN-клієнта створює зашифрований тунель до VPN-шлюзу. Шлюз діє як VPN-сервер, забезпечуючи безпечний шлях для передачі даних.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Навіть у загальнодоступних інтернет-мережах усі дані, що передаються через тунель, шифруються для захисту конфіденційності та цілісності. Захищені тунелі розширюють периметр мережі до віддалених користувачів, фактично розміщуючи їх всередині корпоративної мережі. Це забезпечує безпечний доступ до внутрішніх ресурсів, таких як програми, файлові сервери та бази даних. Remote Access VPN зазвичай включає такі функції безпеки, як багатофакторна автентифікація та передові стандарти шифрування. Додаткові рівні безпеки гарантують, що з'єднання залишається приватним і захищає корпоративну мережу від потенційних загроз з боку віддалених пристроїв[8].

Cloud VPN – це мережевий сервіс, який забезпечує безпечні та зашифровані з'єднання через Інтернет між віддаленими користувачами та корпоративними ресурсами, розміщеними в хмарі.

Cloud VPN дозволяє віддаленим користувачам безпечно підключатися до мережі компанії, гарантуючи, що конфіденційні дані, які передаються через загальнодоступні мережі, зашифровані та захищені від несанкціонованого доступу. Цей тип VPN вигідний для організацій з мобільними працівниками та активними користувачами хмарних сервісів. Він швидко налаштовується та управляється постачальником корпоративних VPN-рішень, що робить його економічно вигідним та ефективним рішенням для сучасних організацій.

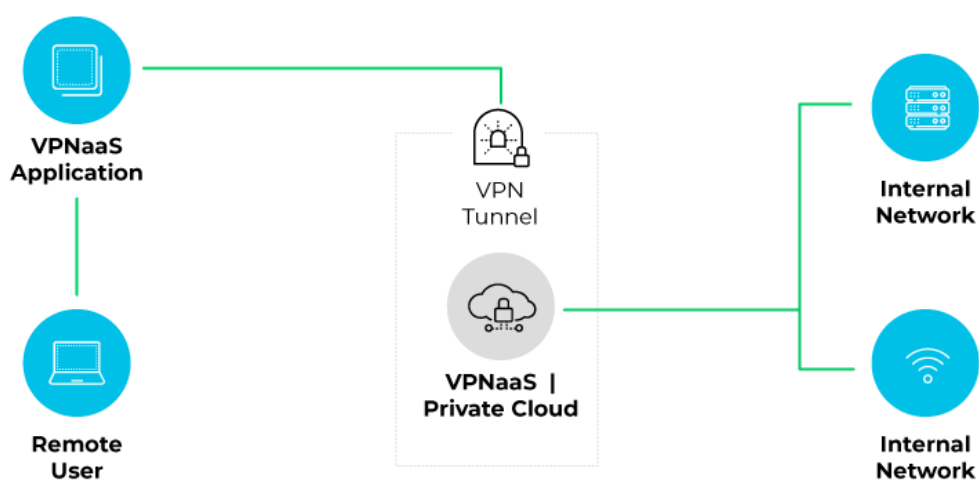


Рисунок 1.10 – Демонстрація роботи Cloud VPN

Cloud VPN також відомий як VPNaaS (VPN як послуга) або хмарна VPN для віддаленого доступу. Він працює шляхом встановлення зашифрованого VPN-з'єднання через Інтернет між користувачем і мережевою інфраструктурою хмарної компанії. Зашифроване з'єднання зазвичай забезпечується VPN-шлюзом, який виступає в ролі посередника для шифрування і розшифрування даних, що надсилаються до хмарних ресурсів.

Процес починається з підключення користувача до хмарного VPN-сервісу. Сервіс автентифікує користувача та його пристрій, зазвичай використовуючи багатофакторну автентифікацію для посилення безпеки. Після успішної автентифікації Cloud VPN створює зашифрований тунель за допомогою встановленого протоколу VPN, такого як IPsec або SSL/TLS. Цей тунель захищає дані, що передаються між користувачем і хмарию, і не може бути прочитаний несанкціонованими організаціями, які перехоплюють трафік.

В межах хмари, VPN-шлюз шифрує вихідні дані, перш ніж вони потрапляють в інтернет, і розшифровує вхідні дані для пристрою-одержувача. Таке шифрування має вирішальне значення для захисту конфіденційної інформації, оскільки вона проходить через потенційно небезпечні мережі. Цей процес підтримує тунель шифрування, адаптуючись за необхідності до змін у мережі. Це особливо важливо для віддалених працівників, які можуть переключатися між різними інтернет-з'єднаннями.

Cloud VPN часто включає розширені заходи безпеки, що виходять за рамки зашифрованих тунелів. Які в свою чергу включають сегментацію мережі, яка контролює доступ на рівні додатків і гарантує, що користувачі можуть отримати доступ лише до тих ресурсів, на використання яких вони мають дозвіл. Хмарні VPN-сервіси підвищують безпеку хмарних мереж, захищаючи від шкідливого програмного забезпечення, фішингу та інших кіберзагроз[10].

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

1.2.3 Протоколи VPN

Протоколи VPN визначають правила і процедури, які використовуються для створення захищеного тунелю між пристроями. Вибір протоколу залежить від вимог до безпеки, швидкості та сумісності. Далі розглянемо протоколи більш детально.

Point-to-Point Tunneling Protocol (PPTP) – це мережевий протокол, який використовується для встановлення безпечного VPN-з'єднання через Інтернет.

Протокол тунелювання «точка-точка» полегшує приватну передачу даних від віддаленого клієнта до сервера шляхом інкапсуляції пакетів на рівні TCP/IP. Незважаючи на свою роль у ранньому розвитку VPN, PPTP був значною мірою витіснений більш безпечними протоколами через його відомі вразливості та слабкі стандарти шифрування.

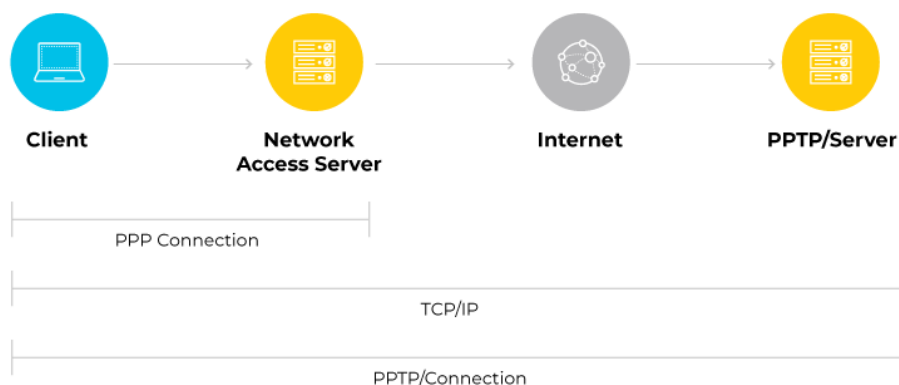


Рисунок 1.11 – Демонстрація роботи Point-to-Point Tunneling Protocol

Протокол PPTP встановлює VPN-з'єднання шляхом інкапсуляції кадрів в IP-пакети для передачі через Інтернет. Він працює за допомогою каналу управління TCP і тунелю загальної інкапсуляції маршрутизації. Ця комбінація дозволяє протоколу інкапсулювати PPP-пакети, що робить можливим використання VPN в різних мережах.

Протокол використовує архітектуру клієнт-сервер, де клієнт ініціює з'єднання з сервером для встановлення тунелю. Протокол використовує TCP-порт 1723 для налаштування каналу управління і GRE для тунелювання PPP-кадрів. Ця двокомпонентна структура полегшує управління сеансами VPN і безпечну передачу пакетів даних між клієнтом і сервером.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Протокол має два режими тунелювання VPN: добровільний і примусовий. Добровільне тунелювання ініціюється клієнтом і відбувається після встановлення мережевого з'єднання. Примусове тунелювання ініціюється сервером і зазвичай відбувається на рівні інтернет-провайдера. Ці режими визначають точку ініціації та управління процесом тунелювання.

Хоча протокол тунелювання PPTP був революційною технологією для свого часу, зараз він вважається застарілим. Далі більш детально розберемо чому ж це сталося.

Point-to-Point Tunneling Protocol застарів у світі корпоративної безпеки через значні проблеми з безпекою. Спочатку прийнятий за свою простоту і швидкість, протокол втратив популярність після того, як стали очевидними його вразливості. Метод шифрування, який він використовує, а саме Microsoft Point-to-Point Encryption, пропонує лише 128-розрядні ключі, що було визнано недостатнім для захисту від сучасних загроз.

Підприємства перейшли на більш безпечні протоколи через нездатність Point-to-Point Tunneling Protocol забезпечити надійний захист в умовах мінливого ландшафту кіберзагроз. Структура протоколу вразлива до декількох типів атак, включаючи добре задокументовані атаки на перекидання бітів. Такі вразливості потенційно можуть дозволити зловмисникам розшифровувати потоки даних або видавати себе за авторизованих користувачів. Обмежена сумісність з брандмауерами NAT сприяє його застаріванню, оскільки він погано підтримує сучасні мережеві конфігурації.

Перехід від цього протоколу до більш безпечних VPN-рішень відображає еволюцію заходів кібербезпеки. Оскільки компанії надають пріоритет захисту даних і систем, використовувати протоколи з більш надійними методами автентифікації та більш досконалим шифруванням стає все більш важливо.[11]

IPsec (Internet Protocol Security) – це набір протоколів і технологій для захисту мережевих IP-комунікацій шляхом автентифікації та шифрування кожного IP-пакету під час сеансу зв'язку.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Він включає в себе протокол для встановлення взаємної автентифікації між агентами на початку сеансу і узгодження криптографічного ключа, який буде використовуватися під час сеансу. Зазвичай використовується у віртуальних приватних мережах для забезпечення безпечної передачі даних через незахищені мережі шляхом створення зашифрованого тунелю між пристроями.

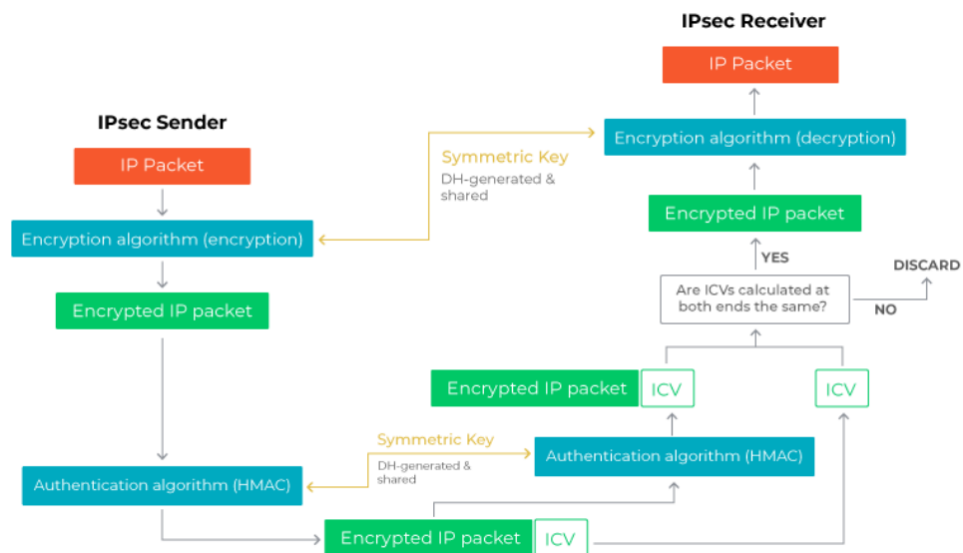


Рисунок 1.12 – Демонстрація роботи IPsec

Давайте більш детально розберемо як він працює.

Безпека інтернет-протоколу починає безпечно з'єднання зі створення асоціації безпеки між пристроями. Сама асоціація безпеки це, по суті, договір, який визначає криптографічні ключі та протоколи, що застосовуються для шифрування та автентифікації. Створення SA (Security Association) є важливим початковим кроком, який підтверджує, що обидві сторони згодні з заходами безпеки для своєї комунікації. Це включає використання агресивного режиму, коли попередньо надані спільні ключі прискорюють встановлення асоціації безпеки.

Після цього відбувається залучення протоколу. Асоціації безпеки використовує два основні протоколи: автентифікаційний заголовок (Authentication Header) та інкапсуляційне корисне навантаження безпеки (Encapsulating Security Payload). АН відповідає за цілісність і автентифікацію пакетів даних, підтверджуючи, що вони не були підроблені під час передачі. А ESP в свою чергу шифрує корисне навантаження пакета, приховуючи дані від потенційних перехоплювачів.

Наступним кроком є передача даних. Під час неї служба Internet Protocol Security інкапсулює оригінальний IP-пакет у заголовок ESP або AH, ефективно захищаючи дані всередині. Процес інкапсуляції є основою роботи IPsec, гарантуючи, що корисне навантаження даних залишається конфіденційним і цілісним від точки відправлення до точки призначення.

Останнім етапом є керування ключами та припинення дії асоціації безпеки. Безпека IPsec є динамічною. Постійне управління ключами та періодичне переукладання угод є необхідним для запобігання порушенням безпеки. Коли безпечне з'єднання більше не потрібне, угода розривається, а захищений тунель фактично закривається. Припинення дії угоди знижує ризик несанкціонованого доступу, гарантуючи, що захищений канал не залишається активним довше необхідного часу.

IPsec має два режими роботи: транспортний і тунельний. Транспортний режим використовується для захисту даних між двома кінцевими точками (наприклад, між двома серверами або між клієнтом і сервером). У цьому режимі захищається лише корисне навантаження IP-пакета, а IP-заголовок не змінюється. Іншими словами, IP-адреси відправника і одержувача залишаються незмінними. В свою чергу, режим тунелю використовується для створення захищеного тунелю між двома мережами або між двома пристроями, що діють як шлюзи (наприклад, між двома маршрутизаторами або між шлюзом і кінцевою точкою). Цей режим захищає весь IP-пакет, включно із заголовком, інкапсулюючи його в новий IP-пакет з новим заголовком[12].

OpenVPN - це протокол VPN з відкритим вихідним кодом, призначений для захисту інтернет-трафіку шляхом створення зашифрованого з'єднання між пристроями. Він забезпечує високий рівень безпеки завдяки надійному шифруванню, автентифікації та підтримці різних мережових конфігурацій. Розроблений для гнучкості, він дозволяє різні налаштування VPN, включаючи з'єднання між сайтами та віддалений клієнтський доступ.

OpenVPN - це програмний проект з відкритим вихідним кодом, протоколом тунелювання VPN, а також назвою компанії, що стоїть за протоколом. Він встановлює безпечні мережові з'єднання через Інтернет. *OpenVPN* функціонує шляхом

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

створення зашифрованих тунелів для пакетів даних, забезпечуючи безпечну передачу між клієнтом і сервером.

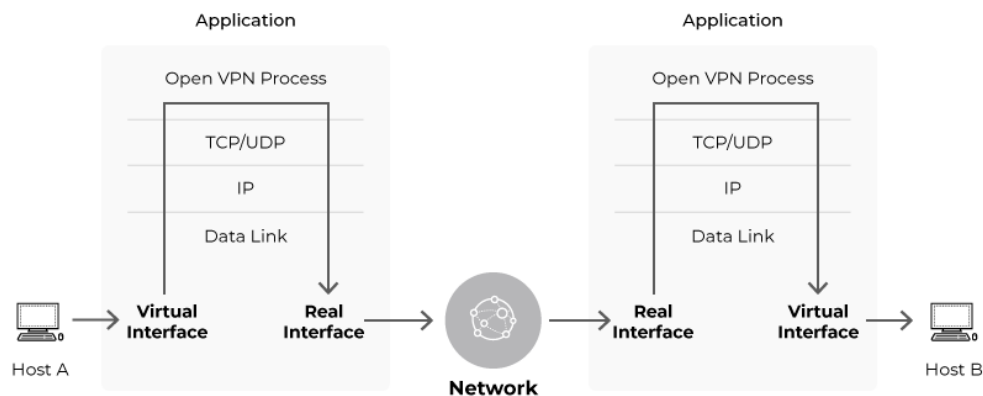


Рисунок 1.13 – Демонстрація роботи OpenVPN

Протокол працює в двох режимах: Transmission Control Protocol (протокол управління передачею) і User Datagram Protocol (протокол користувацьких дейтаграм). Режим TCP забезпечує доставку пакетів даних у правильному порядку і повторно передає будь-які втрачені пакети. Режим TCP забезпечує надійність, хоча і за рахунок швидкості. В свою ж чергу, режим UDP зазвичай використовується за замовчуванням. UDP швидший, але не гарантує порядок пакетів, що робить його менш надійним, але більш ефективним для потокового передавання даних і зв'язку в реальному часі.

OpenVPN використовує бібліотеку OpenSSL для шифрування і дешифрування, забезпечуючи безпечний канал для передачі даних. Для обміну ключами використовується протокол SSL/TLS, що дозволяє використовувати надійні механізми шифрування, які включають 256-бітове шифрування за допомогою сучасних наборів шифрів. Це гарантує, що навіть якщо пакети даних будуть перехоплені, без відповідних ключів розшифрувати їх буде неможливо.

Як програмне забезпечення для VPN, OpenVPN дозволяє конфігурувати та керувати VPN-з'єднаннями. Воно надає інструменти, необхідні підприємствам для створення VPN-серверів, управління доступом користувачів і контролю потоку трафіку. Веб-інтерфейс адміністратора OpenVPN спрощує управління VPN-серверами та доступом користувачів. Також він надає адміністраторам зручний інтерфейс для керування мережевими налаштуваннями та моніторингу продуктивності

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

системи. Програмне забезпечення легко адаптується і підтримує цілий ряд операційних систем. Воно пропонує такі функції, як мережеве з'єднання, повне тунелювання та розділене тунелювання, які мають вирішальне значення для складних конфігурацій мереж.

Гнучкість програмного забезпечення поширюється і на методи автентифікації, де воно підтримує взаємну автентифікацію між клієнтами і серверами VPN за допомогою різних методів. Ці методи включають попередньо надані ключі, автентифікацію на основі сертифікатів та автентифікацію за допомогою імені користувача та пароля. Гнучкість гарантує, що підприємства можуть впроваджувати політики безпеки, не обмежуючись програмним забезпеченням VPN[13].

1.3 Протокол маршрутизації OSPF

1.3.1 Маршрутизація

Маршрутизація – це процес визначення маршруту прямування інформації між мережами. Маршрутизатор приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж.

В основному існує два типи маршрутизації: статична та динамічна. Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. [15]

Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Але і у великих мережах часто конфігуруються статичні маршрути для спеціальних цілей у комбінації з протоколами динамічної маршрутизації, оскільки статична маршрутизація є стабільнішою і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Динамічні маршрути виставляються іншим чином. Після того, як адміністратор активізував і налаштував динамічну маршрутизацію за одним з протоколів, інформація про маршрути оновлюється автоматично в процесі маршрутизації після кожного отримання з мережі нової інформації про маршрути. Маршрутизатори обмінюються повідомленнями про зміни у топології мережі в процесі динамічної маршрутизації.

Протокол маршрутизації – мережевий протокол, який використовується маршрутизаторами для визначення можливих маршрутів прямування даних в комп'ютерній мережі. Застосування протоколу маршрутизації дозволяє уникнути ручного введення всіх допустимих маршрутів, що, у свою чергу, знижує кількість помилок, забезпечує узгодженість дій усіх маршрутизаторів в мережі і полегшує працю адміністраторів. Вони не переміщують інформацію від джерела до пункту призначення, а лише оновлюють таблицю маршрутизації, яка містить інформацію. Протоколи мережевого маршрутизатора допомагають визначити спосіб обміну даними між маршрутизаторами. Це дозволяє мережі вибирати маршрути між будь-якими двома вузлами комп'ютерної мережі[18].

1.3.2 Визачення та історія створення OSPF

Open Shortest Path First, або ж OSPF - це протокол IP-маршрутизації, який використовує математичний алгоритм для обчислення найефективнішого шляху для спрямування трафіку в IP-мережах. OSPF є відкритим стандартом і визначений Робочою групою з розробки інтернету (IETF) як один з декількох протоколів внутрішнього шлюзу в сімействі протоколів TCP/IP

OSPF розподіляє інформацію про маршрутизацію між маршрутизаторами в єдиній автономній системі (AS) на основі технології переадресації за станом з'єднання або найкоротшим шляхом (SPF). Ця особливість відрізняє OSPF від застарілих протоколів маршрутизації TCP/IP. Використовуючи алгоритм найкоротшого шляху Дейкстри, OSPF обчислює найкоротший шлях для всіх маршрутизаторів в області AS, ефективно використовуючи пропускну здатність мережі і забезпечує

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

ючи масштабованість. Автономна система, як і глобальні мережі, можуть бути розділені на кілька взаємопов'язаних мереж. Топологія видима лише для маршрутизаторів в одній області[16][19].

Історія створення протоколу маршрутизації OSPF розпочалась із того, що у 1988 році, IETF (Internet Engineering Task Force) сформували робочу групу для розробки нового протоколу маршрутизації, заснованого на більш ефективному алгоритмі з'єднання який також називають найкоротшим шляхом (SPF). Дослідження цього типу протоколів розпочалися ще в 1970-х роках, частина з них проводилася в мережі ARPAnet, попередниці Інтернету, на основі якої була розроблена значна частина протоколу TCP/IP.

Цей новий протокол отримав назву Open Shortest Path First, або OSPF, і його назва відображає дві його найважливіші характеристики. Перше слово вказує на те, що протокол, як і всі стандарти TCP/IP, був розроблений за допомогою відкритого і публічного процесу RFC, тому він не є пропрієтарним і для його використання не потрібна ліцензія. Частина назви SPF вказує на тип алгоритму, який він використовує, і який призначений для того, щоб дозволити маршрутизаторам динамічно визначати найкоротший шлях між будь-якими двома мережами[20].

1.3.3 Огляд роботи OSPF

Фундаментальною концепцією OSPF є структура даних, яка називається базою даних стану з'єднання. Кожен маршрутизатор в автономній системі підтримує копію цієї бази даних, яка містить інформацію у вигляді орієнтованого графа, що описує поточний стан автономної системи. Кожне з'єднання з мережею або іншим маршрутизатором представлено записом у базі даних, і кожне з них має відповідну вартість (або метрику). Метрика може включати в себе багато різних аспектів продуктивності маршруту, а не тільки простий підрахунок хопів, як це використовується в RIP.

Інформація про автономну систему рухається по автономній системі у вигляді оголошень про стан з'єднання (LSA), повідомлень, які дозволяють кожному маршрутизатору повідомити іншим, що він знає про стан автономної системи на даний момент. З часом інформація, яку кожен маршрутизатор має про автономну

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

систему, збігається з інформацією інших, і всі вони мають однакові дані. Коли в мережі відбуваються зміни, маршрутизатори надсилають оновлення, щоб гарантувати, що всі маршрутизатори мають актуальну інформацію.

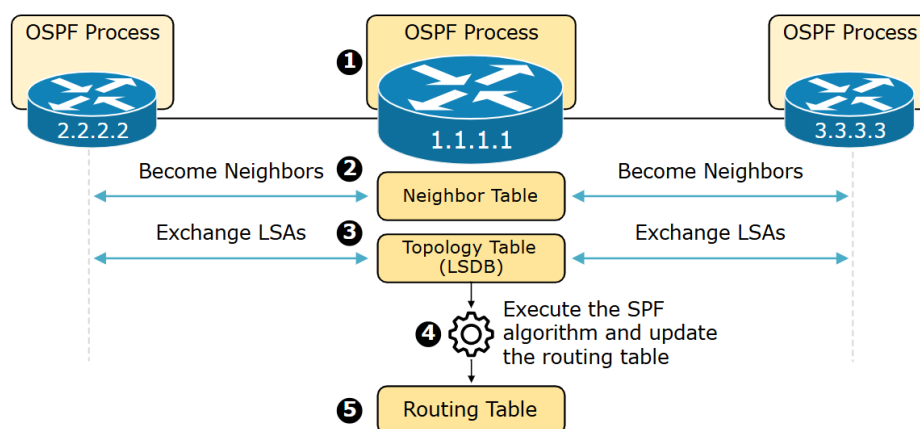


Рисунок 1.14 – Демонстрація роботи OSPF

Для визначення фактичних маршрутів кожен маршрутизатор використовує свою базу даних стану з'єднань для побудови дерева найкоротшого шляху. Це дерево показує зв'язки маршрутизатора з іншими маршрутизаторами та мережею і дозволяє визначити найдешевший маршрут до будь-якого місця. При надходженні нової інформації про стан мережі це дерево може бути перераховане, тому найкращий маршрут динамічно коригується залежно від стану мережі. Якщо існує більше одного маршруту з однаковою вартістю, трафік може бути розподілений між ними.

Далі давайте більш детально розберемо типи пакетів OSPF

OSPF використовує пакети стану каналу для установки та збереження відносин суміжності, а також для обміну оновленнями маршрутизації. Кожен тип пакета виконує певне завдання у процесі маршрутизації OSPF:

Тип 1: пакет привітання (hello) – використовується для встановлення та підтримання відносин суміжності з маршрутизаторами OSPF.

Тип 2: пакет опису бази даних або дескриптор бази даних (DBD) – містить скорочений список баз даних станів каналів відправляючого маршрутизатора. Використовується приймаючими маршрутизаторами для звірки з локальною базою даних стану каналу. Для створення точного дерева найкоротших шляхів SPF маршрутизатори, які використовують протоколи маршрутизації за станом каналу в межах області, повинні використовувати однакову базу даних стану каналу.

Тип 3: пакет запиту стану каналу (LSR) – маршрутизатори, які отримують дані, можуть запитати додаткову інформацію про будь-який запис у пакеті опису бази даних (DBD), використовуючи пакет запиту стану каналу (LSR).

Тип 4: Пакет оновлення стану зв'язку (LSU) - використовується для надси- лання відповіді на запит стану зв'язку (LSR) та оголошення нових даних. Пакети Link State Update (LSU) містять сім різних записів LSA.

Тип 5: Пакет підтвердження стану каналу (LSAck) - при отриманні пакета Link State Update (LSU) маршрутизатор надсилає підтвердження отримання у ви- гляді пакета Link State Confirmation (LSAck) і залишає поле даних в LSAck порож- нім.

1.3.4 Переваги та недоліки OSPF

Переваги:

Використання алгоритму SPF (Dijkstra): OSPF використовує алгоритм SPF для визначення найкоротшого шляху між вузлами мережі. Це мінімізує затримки та підвищує ефективність передачі даних.

Швидка конвергенція: Коли топологія мережі змінюється, OSPF швидко ада- птується до нових умов. Ця функція особливо важлива у великих мережах для за- безпечення безперервності обміну даними.

Підтримка VLSM і CIDR Завдяки використанню масок підмереж змінної до- вжини (VLSM) і безкласової маршрутизації (CIDR), протокол сприяє кращому ви- користанню простору IP-адрес і підвищує гнучкість конфігурації мережі.

Ієрархічна структура: Поділяючи мережу на області, OSPF зменшує обсяг об- числень, необхідних маршрутизаторам, і дозволяє ефективно управляти інформа- цією про маршрутизацію. Наприклад, у великих корпоративних мережах можна ви- ділити магістральну область і кілька підобластей.

Багатоадресний зв'язок: OSPF уникає непотрібного широкомовного трафіку і зменшує навантаження на мережу, використовуючи багатоадресну розсилку для обміну інформацією про маршрутизацію.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Підтримка аутентифікації: OSPF знижує ризик несанкціонованого втручання в роботу протоколу, забезпечуючи автентифікацію повідомлень різними методами, такими як прості паролі або ж HMAC.

Незалежність від постачальника: OSPF підтримується багатьма виробниками мережевого обладнання (Cisco, Juniper, MikroTik) як відкритий стандарт, що забезпечує його універсальність та сумісність.

Гнучкість і масштабованість: OSPF працює в мережах різного розміру, від невеликих локальних мереж до глобальних мереж підприємств. Його ієрархічна структура дозволяє легко розширювати мережу без необхідності вносити значні зміни в конфігурацію.

Недоліки:

Складність налаштування та управління: OSPF вимагає детального розуміння топології мережі для правильного налаштування. Наприклад, адміністратору необхідно визначати області, межі маршрутизаторів (Area Border Routers) і конфігурацію суміжностей.

Високі вимоги до ресурсів: Протокол потребує значних обчислювальних потужностей для обробки алгоритму SPF та підтримки бази даних стану каналів. У великих мережах це може створювати навантаження на процесори маршрутизаторів та пам'ять.

Проблеми зі масштабованістю в надвеликих мережах: Незважаючи на підтримку ієрархічної структури, у дуже великих мережах управління областями стає складним, а кількість маршрутів може перевищувати можливості обробки маршрутизаторами.

Чутливість до помилок конфігурації: Помилки під час налаштування OSPF (наприклад, неправильно налаштовані фільтри чи метрики) можуть призвести до некоректної маршрутизації або повного збою мережі.

Навантаження на мережу при великих змінах: У разі значних змін у топології мережі OSPF може створювати значне навантаження через необхідність перерахунку маршрутів та оновлення LSAs.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Неоптимально для малих мереж: У невеликих мережах простіші протоколи, такі як RIP, можуть бути більш доцільними через менші вимоги до ресурсів і простоту налаштування.

Проаналізувавши всі переваги та недоліки ми можемо дійти висновку, що OSPF є потужним та універсальним протоколом маршрутизації, що ідеально підходить для великих мереж із високими вимогами до швидкості, гнучкості та безпеки маршрутизації. Проте його складність у налаштуванні та управлінні може створювати виклики, особливо для адміністраторів із недостатнім досвідом. Так як у нашому проекті представлена гетерогенна мережа, із вимогами до безпеки, та швидкості. Було прийняте рішення у використанні даного протоколу маршрутизації

Висновки до першого розділу:

У першому розділі було закладено теоретичне підґрунтя для проектування захищеної гетерогенної мережі. Було досліджено концепцію гетерогенних мереж, які визначаються як інфраструктури, що поєднують пристрої з різними операційними системами та протоколами передавання даних.

Для вирішення проблем безпеки було проаналізовано технології VPN. Порівняльний аналіз протоколів VPN виявив, що PPTP є застарілим, тоді як IPsec та OpenVPN пропонують високий рівень захисту. IPsec, як набір протоколів для шифрування та автентифікації на мережевому рівні ідеально підходить для створення захищених тунелів між шлюзами, що є ключовою вимогою для даного проекту.

Також було розглянуто принципи маршрутизації та обґрунтовано вибір протоколу OSPF. Порівняно з іншими протоколами, перевагами OSPF є відкритий стандарт, він забезпечує швидку конвергенцію, підтримує ієрархічну структуру для кращої масштабованості та автентифікацію для підвищення безпеки.

Таким чином, проведений теоретичний аналіз дозволив визначити, що поєднання гнучкості гетерогенних мереж з безпекою технології IPsec VPN та ефективністю динамічної маршрутизації OSPF є оптимальною стратегією для досягнення мети кваліфікаційної роботи.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Розробка топології комп'ютерної мережі

Розробляючи томологію комп'ютерної мережі, нами було прийняте рішення використати трирівневу ієрархічну модель Cisco. Мережа дуже легко може бути розширена додаванням нових сегментів та пристроїв без істотного впливу на вже існуючу структуру завдяки масштабованості. Це робить її ідеальним рішенням для організацій, які планують розширювати свою мережу в довгостроковій перспективі.

Також, чіткий розподіл функцій ядра, розподільчого рівня і рівня доступу забезпечує оптимізовану маршрутизацію і передачу даних, а ще надзвичайно високу продуктивність. Це гарантує швидку передачі даних і мінімальну затримку, які відіграють важливу роль в ефективній роботі мережевих сервісів.

Крім того, трирівнева ієрархічна модель підвищує безпеку мережі. Це пов'язано з тим, що розподіл мережевих функцій між рівнями уможливорює багаторівневі заходи безпеки. Наприклад, рівень розподілу може реалізовувати контроль доступу та фільтрацію трафіку для захисту від несанкціонованого доступу та кіберзагроз. Нарешті, гнучкість моделі дозволяє легко інтегрувати нові технології та послуги, такі як відеоконференції та бездротові мережі, без значного впливу на основну мережу.

Чіткий розподіл функцій ядра, розподільчого рівня і рівня доступу дозволяє ефективно управляти мережею, швидко виявляти і вирішувати проблеми, а також забезпечувати швидкість і надійність передачі даних.

Рівень ядра, або ж базовий рівень – формує ядро мережі. На самому верху ієрархії цей рівень відповідає за швидке і надійне пересилання великих об'ємів трафіку. Єдиним призначенням базового рівня є швидка комутація трафіку. Трафік передається на базовому рівні спільно для кількох користувачів. Однак на рівні розподілу обробляються призначені для користувача дані, що може привести до додаткових запитів в базовий рівень.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арх.
		Покотило О.А.				
Змн.	Арх.	№ докум.	Підпис	Дата		36

Якщо відбувається помилка на базовому рівні, то вона впливає на всіх користувачів. Отже, вельми важливо забезпечити високу надійність на цьому рівні. На рівні ядра обробляються великі обсяги трафіку, тому не менш важливо враховувати швидкість і затримки.

Рівень розподілу, або ж рівень робочих груп – розташований між базовим рівнем та рівнем доступу. Основні функції рівня розподілу складаються в маршрутизації, фільтрації і доступі до регіональних мереж, а також (якщо необхідно) у визначенні правил доступу пакетів до базового рівня. Рівень розподілу зобов'язаний встановлювати найбільш швидкий спосіб обробки запитів до служб (наприклад, метод файлового звернення до сервера).

Після визначення на рівні поширення найкращого шляху доступу, запит може бути переданий на базовий рівень, де реалізований швидкісний транспорт запиту до потрібної служби. На рівні розподілу встановлюється політика мережі, а також забезпечуються можливості гнучкого опису мережевих операцій.

Рівень доступу, або ж рівень робочих станцій – утворює собою основу мережі. Цей рівень з'єднує кінцеві пристрої, такі як комп'ютери, принтери та IP-телефони, з мережею через комутатори доступу. Основне призначення рівня доступу - забезпечити фізичне і логічне підключення до кінцевих пристроїв, а також контроль доступу і безпеки. Рівень доступу реалізує політики безпеки, такі як аутентифікація користувачів і фільтрація трафіку для захисту мережі від несанкціонованого доступу.

Помилки на рівні доступу можуть вплинути на підключення кінцевих пристроїв. Рівень доступу необхідний для забезпечення надійного підключення та безпеки кінцевих пристроїв і ефективної роботи мережевої інфраструктури[26].

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

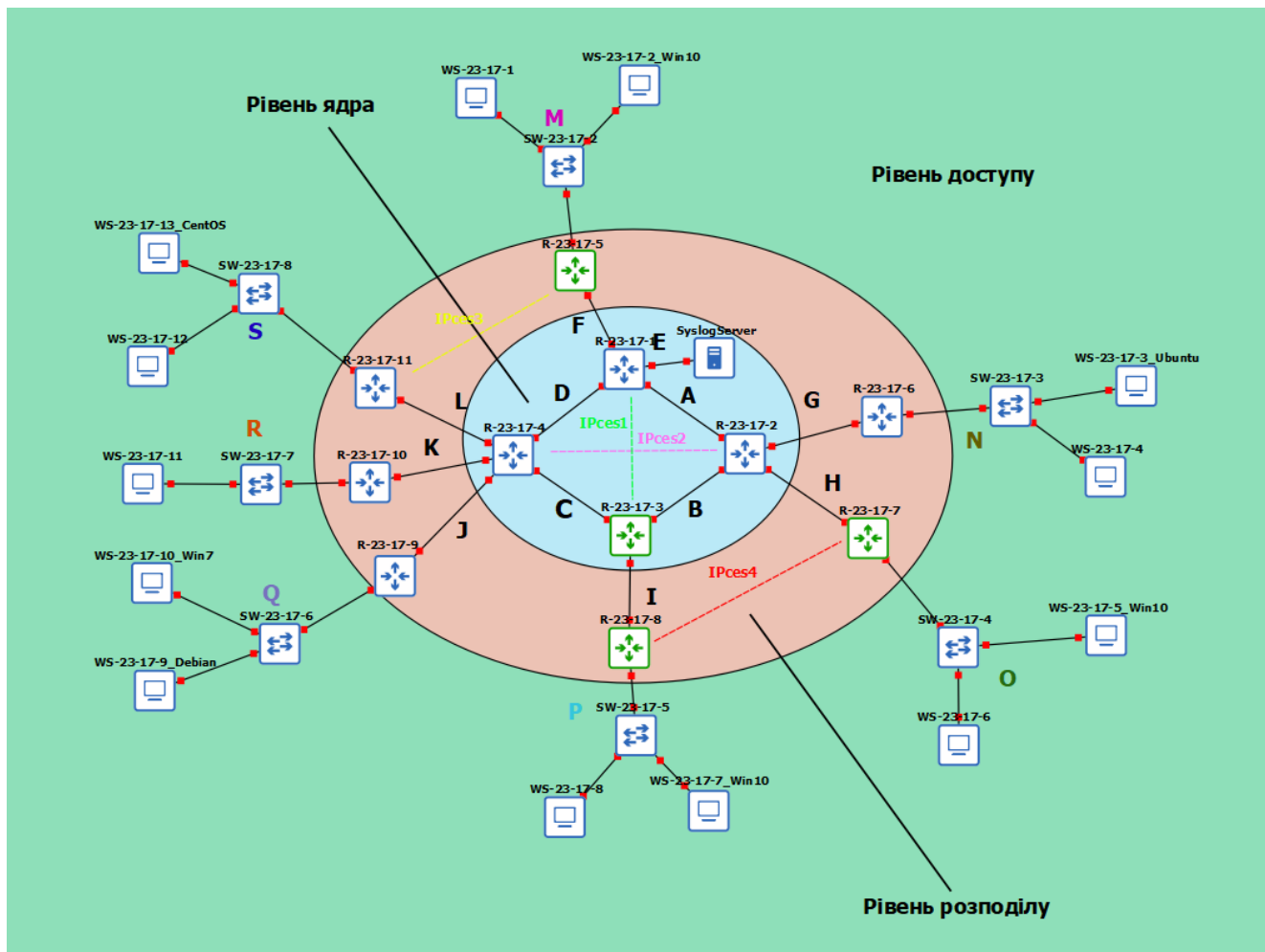


Рисунок 2.1 – Схема загальної топології

Під час виконання кваліфікаційної роботи для зв'язку між пристроями використовувались технології FastEthernet та Ethernet. Середовище передачі даних – вита пара.

Далі давайте пройдемося більш детально по мережі. Вона складається з 19 підмереж. Для створення гетерогенної мережі організації було використано одинадцять маршрутизаторів різних виробників, а саме Cisco та MikroTik, сім комутаторів Cisco, тринадцять робочих станцій із різними операційними системами, такими як Windows, Linux та 1 сервер.

Розглянемо докладніше кожен підмережу:

Підмережі A, B, C, D та E являють собою рівень ядра мережі. Вони складається із трьох маршрутизаторів Cisco: R-23-17-1, R-23-17-2, R-23-17-4, одного маршрутизатора MikroTik: R-23-17-3, а також Syslog сервера. Пристрої між собою з'єднані за допомогою виті пари FastEthernet та Ethernet.

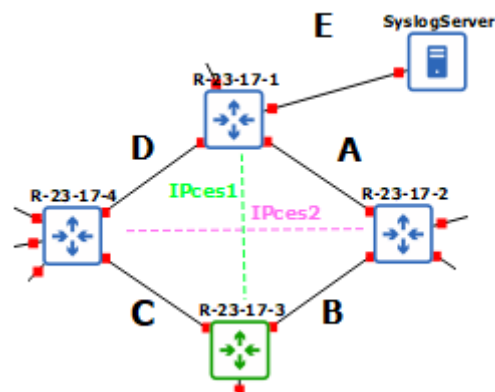


Рисунок 2.2 – Підмережі A, B, C, D та E

Також між маршрутизаторами рівня ядра було налаштовано IPsec VPN для покращення обміну даними та захисту пакетів.

У підмережах F, G, H, I, J, K та L знаходяться по 2 маршрутизатори. Дані підмережі слугують перехідним етапом від рівня ядра до рівня розподілу. Чотири маршрутизатори Cisco: R-23-17-6, R-23-17-9, R-23-17-10, R-23-17-6 та три маршрутизатори MikroTik: R-23-17-5, R-23-17-7, R-23-17-8 і утворюють собою рівень робочих груп. Підключення даних робочих станцій відбувається за допомогою витої пари FastEthernet.

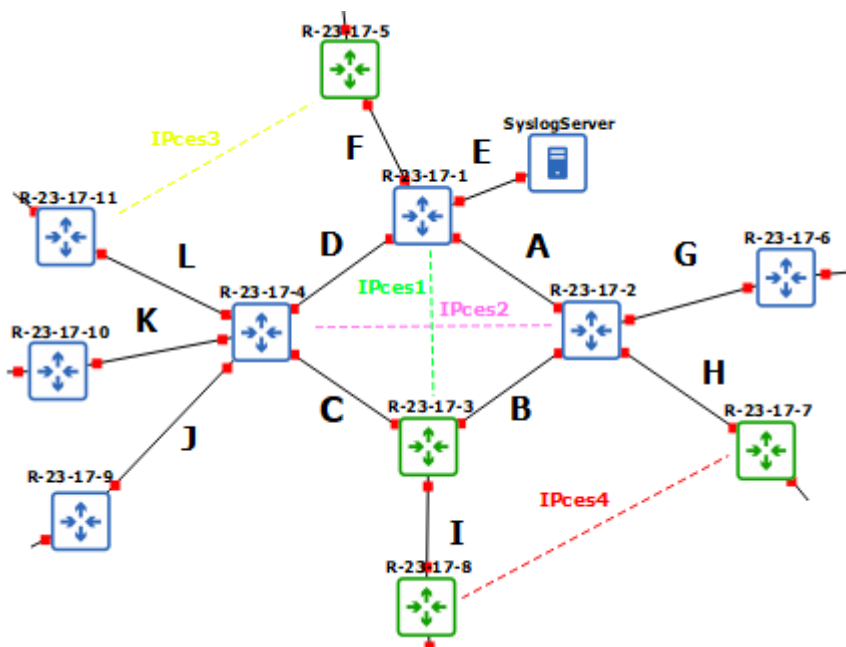


Рисунок 2.3 – Підмережі F, G, H, I, K та L

Також між маршрутизаторами R-23-17-7 та R-23-17-8 підмереж I та H відповідно, а також маршрутизаторами R-23-17-11 та R-23-17-5 підмереж L та F, аналогічно до рівня ядра було налаштовано IPsec VPN. Як і в першому випадку його

роллю є забезпечення більш швидкої передачі даних, а також покращення їх захи-
сту.

Підмережа М складається із маршрутизатора R-23-17-5, комутатора на 24 пор-
ти SW-23-17-1, а також із кінцевих робочих станцій WS-23-17-1 та WS-23-17-
2_Win10, на другій робочій станції використовується операційна система Windows
10. З'єднання виконані за допомогою витої пари FastEthernet та Ethernet

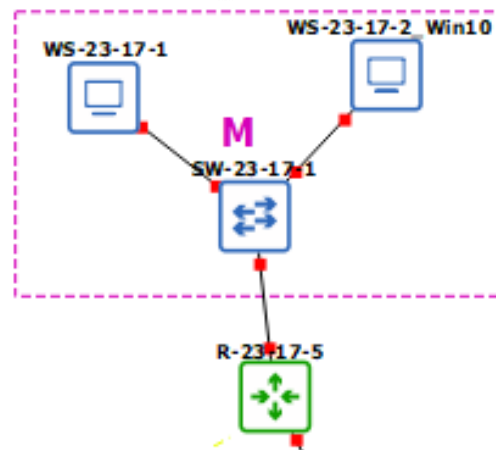


Рисунок 2.4 – Підмережа М

Підмережа N складається із маршрутизатора R-23-17-6, комутатора на 24 пор-
ти SW-23-17-2 а також із двох робочих станцій WS-23-17-3_Ubuntu, із викорис-
танням операційної системи Linux та WS-23-17-4. З'єднання між пристроями вико-
нані за допомогою витої пари Ethernet та FastEthernet.

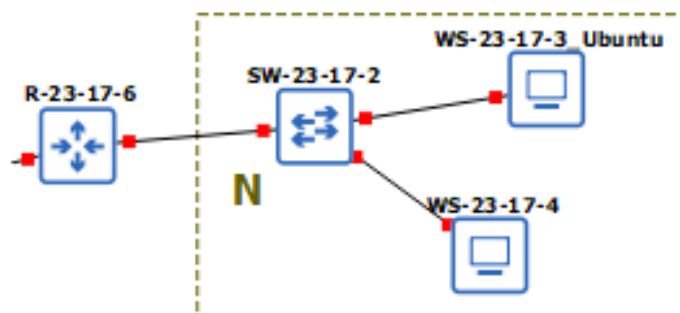


Рисунок 2.5 – Підмережа N

Підмережа О включає у себе маршрутизатор R-23-17-7, комутатор із 24 пор-
тами SW-23-17-3 та дві робочі станції WS-23-17-6 та WS-23-17-5_Win10, на якій
використовується операційна система Windows 10. Для з'єднання пристроїв вико-
ристовується вита пара FastEthernet та Ethernet

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

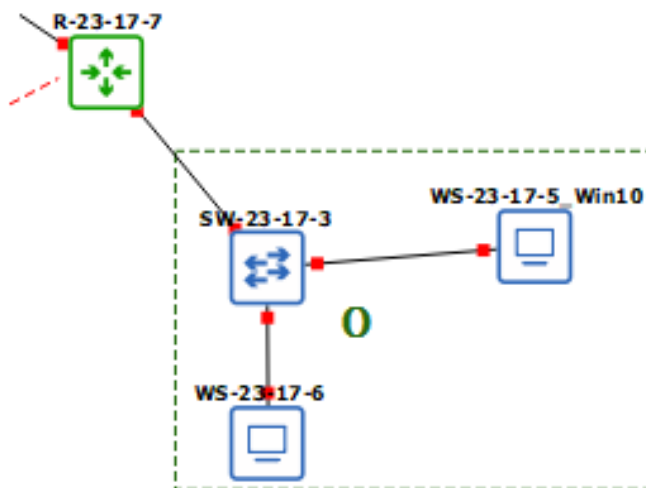


Рисунок 2.6 – Підмережа О

Підмережа Р складається із маршрутизатора R-23-17-8, комутатора на 24 порти SW-23-17-5, а також із кінцевих робочої станцій WS-23-17-8 та WS-23-17-7_Ubun. На останній використовується операційна система Ubuntu. З'єднання пристроїв відбувається за допомогою витої пари FastEthernet та Ethernet

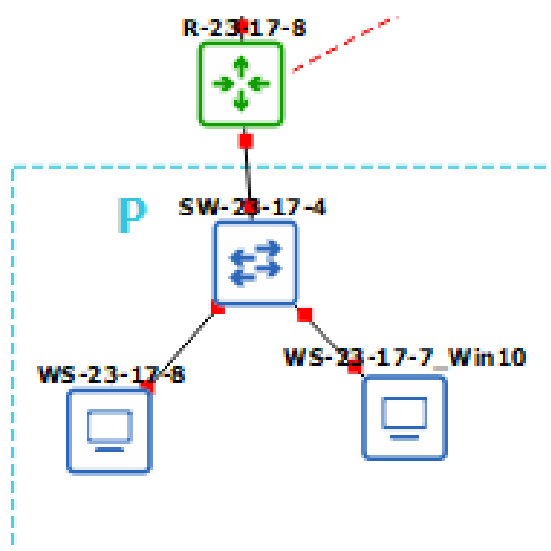


Рисунок 2.7 – Підмережа Р

Підмережа Q складається із маршрутизатора R-23-17-9, комутатору SW-23-17-5 на 24 порти та кінцевими робочими станціями: WS-23-17-9_Debian, на операційній системі Ubuntu та WS-23-17-10_Win7 на якій використовується операційна система Windows7. Пристрої між собою з'єднані за допомогою витої пари FastEthernet, а також Ethernet.

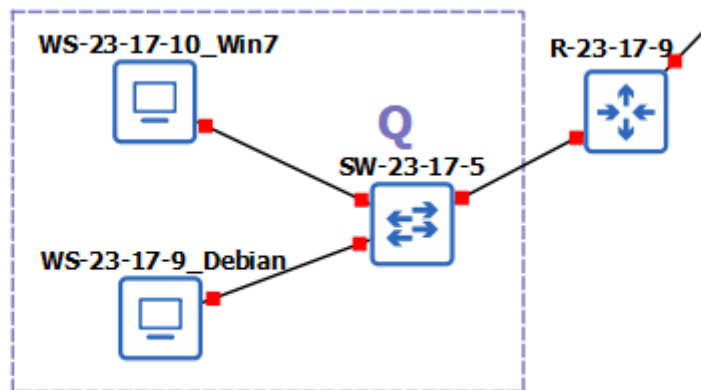


Рисунок 2.8 – Підмережа Q

До складу підмережі R входять: маршрутизатор R-23-17-10, комутатор SW-23-17-6 на 24 порти та робоча станція WS-23-17-11. Пристрої між собою з'єднані за допомогою витії пари FastEthernet, а також Ethernet.

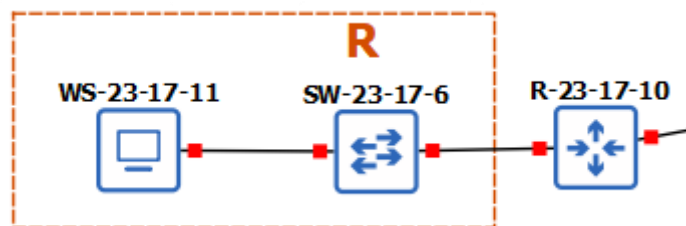


Рисунок 2.9 – Підмережа R

Останньою підмережею нашої мережі є підмережа S. Вона складається із маршрутизатора R-23-17-11, комутатора SW-23-17-7 та двох робочих станцій WS-23-17-13 та WS-23-17-12_CentOS. На останній використовується операційна система Linux. Пристрої між собою з'єднані за допомогою витії пари FastEthernet, а також Ethernet.

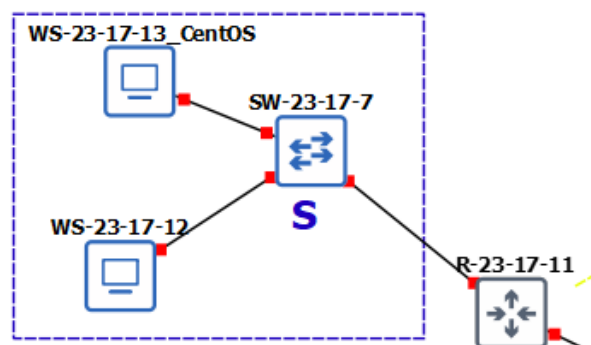


Рисунок 2.10 – Підмережа S

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Для забезпечення зв'язку між усіма підмережами було використано протокол динамічної маршрутизації OSPF.

2.2 Розробка системи IP-адресації

Спочатку розробимо ір-адресу кожної підмережі

Таблиця 2.1 IP-адресація

IP-адресація

Підмережа	IP-адреса підмережі	Префікс
Підмережа А	193.23.17.0	/30
Підмережа В	193.23.17.4	/30
Підмережа С	193.23.17.8	/30
Підмережа D	193.23.17.12	/30
Підмережа Е	193.23.17.64	/26
Підмережа F	194.23.17.0	/26
Підмережа G	195.23.17.0	/26
Підмережа Н	195.23.17.64	/26
Підмережа I	196.23.17.0	/26
Підмережа J	196.23.17.64	/26
Підмережа K	197.23.17.0	/26
Підмережа L	197.23.17.64	/26
Підмережа M	198.23.17.0	/25
Підмережа N	199.23.17.0	/25
Підмережа O	199.23.17.128	/25
Підмережа P	200.23.17.0	/25
Підмережа Q	200.23.17.128	/25
Підмережа R	201.23.17.0	/25
Підмережа S	201.23.17.128	/25

Далі проведемо повний розрахунок ір-адресації для кожної із підмереж

Таблиця 2.2 IP-адресація

Розрахунок ір-адресації для підмереж А, В:

Призначення	IP-адреси	
	Підмережа А	Підмережа В
Адреса мережі	193.23.17.0	193.23.17.4
Маска мережі	255.255.255.252 /30	255.255.255.252 /30
Інвертована маска	0.0.0.3	0.0.0.3
Мінімальна адреса	193.23.17.1	193.23.17.5
Максимальна адреса	193.23.17.2	193.23.17.6
Широкомовна адреса	193.23.17.3	193.23.17.7

Таблиця 2.3 IP-адресація

Розрахунок ір-адресації для підмереж С, D:

Призначення	ІР-адреси	
	Підмережа С	Підмережа D
Адреса мережі	193.23.17.8	193.23.17.12
Маска мережі	255.255.255.252 /30	255.255.255.252 /30
Інвертована маска	0.0.0.3	0.0.0.3
Мінімальна адреса	193.23.17.9	193.23.17.13
Максимальна адреса	193.23.17.10	193.23.17.14
Широкомовна адреса	193.23.17.11	193.23.17.15

Таблиця 2.4 IP-адресація

Розрахунок ір-адресації для підмережі E:

Призначення	ІР-адреси
Адреса мережі	193.23.17.64
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	193.23.17.65
Максимальна адреса	193.23.17.126
Широкомовна адреса	193.23.17.127
Шлюз по замовчуванням	193.23.17.65
Діапазон адрес майбутніх ПК	193.23.17.70 - 193.23.17.119
Діапазон вільних адрес	193.23.17.120 - 193.23.17.126

Таблиця 2.5 IP-адресація

Розрахунок ір-адресації для підмережі F:

Призначення	ІР-адреси
Адреса мережі	194.23.17.0
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	194.23.17.1
Максимальна адреса	194.23.17.62
Широкомовна адреса	194.23.17.63
Шлюз по замовчуванням	194.23.17.1
Діапазон адрес майбутніх ПК	194.23.17.10 - 194.23.17.55
Діапазон вільних адрес	194.23.17.56 - 194.23.17.62

Таблиця 2.6 IP-адресація

Розрахунок ір-адресації для підмережі G:

Призначення	ІР-адреси
Адреса мережі	195.23.17.0
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	195.23.17.1
Максимальна адреса	195.23.17.62
Широкомовна адреса	195.23.17.63
Шлюз по замовчуванням	195.23.17.1
Діапазон адрес майбутніх ПК	195.23.17.10 - 195.23.17.55
Діапазон вільних адрес	195.23.17.56 - 195.23.17.62

Таблиця 2.7 IP-адресація

Розрахунок ір-адресації для підмережі H:

Призначення	ІР-адреси
Адреса мережі	195.23.17.64
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	195.23.17.65
Максимальна адреса	195.23.17.126
Широкомовна адреса	195.23.17.127
Шлюз по замовчуванням	195.23.17.65
Діапазон адрес майбутніх ПК	195.23.17.73 - 195.23.17.119
Діапазон вільних адрес	195.23.17.120 - 195.23.17.126

Таблиця 2.8 IP-адресація

Розрахунок ір-адресації для підмережі I:

Призначення	ІР-адреси
Адреса мережі	196.23.17.0
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	196.23.17.1
Максимальна адреса	196.23.17.62
Широкомовна адреса	196.23.17.63
Шлюз по замовчуванням	196.23.17.1
Діапазон адрес майбутніх ПК	196.23.17.10 - 196.23.17.55
Діапазон вільних адрес	196.23.17.56 - 196.23.17.62

Таблиця 2.9 IP-адресація

Розрахунок ір-адресації для підмережі J:

Призначення	ІР-адреси
Адреса мережі	196.23.17.64
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	196.23.17.65
Максимальна адреса	196.23.17.126
Широкомовна адреса	196.23.17.127
Шлюз по замовчуванням	196.23.17.65
Діапазон адрес майбутніх ПК	196.23.17.73 - 196.23.17.119
Діапазон вільних адрес	196.23.17.120 - 196.23.17.126

Таблиця 2.10 IP-адресація

Розрахунок ір-адресації для підмережі K:

Призначення	ІР-адреси
Адреса мережі	197.23.17.0
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	197.23.17.1
Максимальна адреса	197.23.17.62
Широкомовна адреса	197.23.17.63
Шлюз по замовчуванням	197.23.17.1
Діапазон адрес майбутніх ПК	197.23.17.10 - 197.23.17.55
Діапазон вільних адрес	197.23.17.56 - 197.23.17.62

Таблиця 2.11 IP-адресація

Розрахунок ір-адресації для підмережі L:

Призначення	ІР-адреси
Адреса мережі	197.23.17.64
Маска мережі	255.255.255.192 /26
Інвертована маска	0.0.0.63
Мінімальна адреса	197.23.17.65
Максимальна адреса	197.23.17.126
Широкомовна адреса	197.23.17.127
Шлюз по замовчуванням	197.23.17.65
Діапазон адрес майбутніх ПК	197.23.17.73 - 197.23.17.119
Діапазон вільних адрес	197.23.17.120 - 197.23.17.126

Таблиця 2.12 IP-адресація

Розрахунок ір-адресації для підмережі М:

Призначення	ІР-адреси
Адреса мережі	198.23.17.0
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	198.23.17.1
Максимальна адреса	198.23.17.126
Широкомовна адреса	198.23.17.127
Шлюз по замовчуванням	198.23.17.1
Діапазон адрес майбутніх ПК	198.23.17.12 - 198.23.17.112
Діапазон вільних адрес	198.23.17.113 - 198.23.17.126

Таблиця 2.13 IP-адресація

Розрахунок ір-адресації для підмережі N:

Призначення	ІР-адреси
Адреса мережі	199.23.17.0
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	199.23.17.1
Максимальна адреса	199.23.17.126
Широкомовна адреса	199.23.17.127
Шлюз по замовчуванням	199.23.17.1
Діапазон адрес майбутніх ПК	199.23.17.2 - 199.23.17.11
Діапазон вільних адрес	199.23.17.12 - 199.23.17.112

Таблиця 2.14 IP-адресація

Розрахунок ір-адресації для підмережі О:

Призначення	ІР-адреси
Адреса мережі	199.23.17.128
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	199.23.17.129
Максимальна адреса	199.23.17.254
Широкомовна адреса	199.23.17.255
Шлюз по замовчуванням	199.23.17.129
Діапазон адрес майбутніх ПК	199.23.17.130 - 199.23.17.139
Діапазон вільних адрес	199.23.17.140 - 199.23.17.240

Таблиця 2.15 IP-адресація

Розрахунок ір-адресації для підмережі Р:

Призначення	ІР-адреси
Адреса мережі	200.23.17.0
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	200.23.17.1
Максимальна адреса	200.23.17.126
Широкомовна адреса	200.23.17.127
Шлюз по замовчуванням	200.23.17.1
Діапазон адрес майбутніх ПК	200.23.17.2 - 200.23.17.11
Діапазон вільних адрес	200.23.17.12 - 200.23.17.112

Таблиця 2.16 IP-адресація

Розрахунок ір-адресації для підмережі Q:

Призначення	ІР-адреси
Адреса мережі	200.23.17.128
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	200.23.17.129
Максимальна адреса	200.23.17.254
Широкомовна адреса	200.23.17.255
Шлюз по замовчуванням	200.23.17.129
Діапазон адрес майбутніх ПК	200.23.17.130 - 200.23.17.139
Діапазон вільних адрес	200.23.17.140 - 200.23.17.240

Таблиця 2.17 IP-адресація

Розрахунок ір-адресації для підмережі R:

Призначення	ІР-адреси
Адреса мережі	201.23.17.0
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	201.23.17.1
Максимальна адреса	201.23.17.126
Широкомовна адреса	201.23.17.127
Шлюз по замовчуванням	201.23.17.1
Діапазон адрес майбутніх ПК	201.23.17.2 - 201.23.17.11
Діапазон вільних адрес	201.23.17.12 - 201.23.17.112

Таблиця 2.18 IP-адресація

Розрахунок ір-адресації для підмережі S:

Призначення	ІР-адреси
Адреса мережі	201.23.17.128
Маска мережі	255.255.255.128 /25
Інвертована маска	0.0.0.127
Мінімальна адреса	201.23.17.129
Максимальна адреса	201.23.17.254
Широкомовна адреса	201.23.17.255
Шлюз по замовчуванням	201.23.17.129
Діапазон адрес майбутніх ПК	201.23.17.130 - 201.23.17.139
Діапазон вільних адрес	201.23.17.140 - 201.23.17.240

2.3 Проектування служб та сервісів прикладного рівня

Під час налаштування мережі було використано призначення ір-адрес за допомогою DHCP.

DHCP (Dynamic Host Configuration Protocol) - це протокол мережевого керування, який використовується для динамічного призначення IP-адреси будь-якому пристрою в мережі, щоб він міг взаємодіяти. DHCP автоматизує і централізовано керує цими конфігураціями, не вимагаючи від мережевих адміністраторів призначати IP-адреси вручну всім мережевим пристроям. DHCP можна використовувати як у малих локальних мережах, так і у великих корпоративних мережах.

DHCP є розширенням протоколу BOOTP (Bootstrap Protocol) 1985 року, протоколу керування IP-адресами в мережі. DHCP є більш досконалим; його сервери можуть обробляти запити клієнтів BOOTP, якщо в сегменті мережі існують клієнти BOOTP.

Використовуючи один центральний сервер BOOTP для обслуговування хостів у багатьох IP-підмережах, BOOTP запровадив концепцію агента-ретранслятора, який уможливив пересилання пакетів BOOTP через мережі. Однак BOOTP вимагав ручного процесу додавання інформації про конфігурацію для кожного клієнта, не надаючи механізму для відновлення IP-адрес, які більше не використовуються.

DHCP призначає нові IP-адреси в кожному місці, коли пристрої переміщуються в нове місце в мережі. Це означає, що мережевим адміністраторам не потрібно вручну налаштовувати кожен пристрій з дійсною IP-адресою або переналаштовувати пристрій з новою IP-адресою, якщо він переміщується на нове місце. Версії DHCP доступні як для IPv4 так і для IPv6.

DHCP працює на прикладному рівні стека TCP/IP. Він динамічно призначає IP-адреси та розподіляє інформацію про конфігурацію TCP/IP серед клієнтів DHCP. Інформація про конфігурацію включає наступне:

- IP-адреси шлюзу за замовчуванням.
- Інформація про маску підмережі.
- Адреси системи доменних імен (DNS).

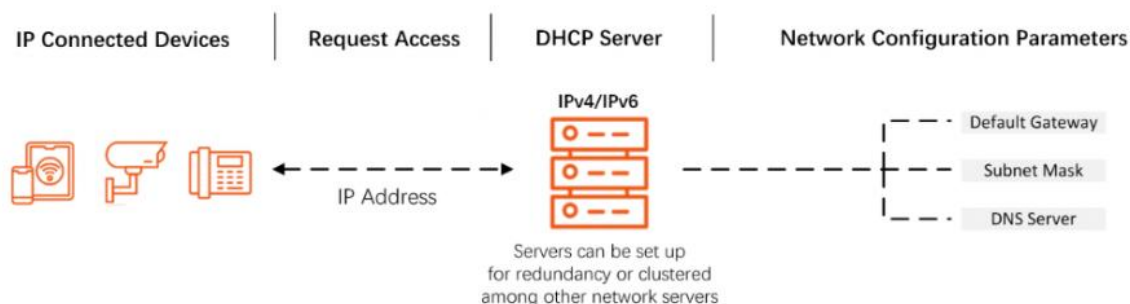


Рисунок 2.11 – Приклад роботи DHCP

DHCP - це протокол клієнт-сервер. Сервери керують пулом унікальних IP-адрес та інформацією про параметри конфігурації клієнта. Сервери призначають адреси з цих пулів адрес. Клієнти з підтримкою DHCP надсилають запити на сервер DHCP під час підключення до мережі.

Клієнти, налаштовані за допомогою DHCP, можуть надсилати запити на інформацію про конфігурацію своєї локальної мережі на сервер DHCP. Зазвичай клієнт надсилає цей запит одразу після завантаження. DHCP-сервер відповідає на запит клієнта, надаючи інформацію про конфігурацію IP, попередньо визначену мережевим адміністратором. Сюди входить конкретна IP-адреса і термін оренди - час, протягом якого розподіл дійсний.

Клієнт DHCP запитує ті самі параметри, коли оновлює своє призначення адреси. Однак сервер DHCP може призначити нову IP-адресу на основі політик, встановлених адміністратором. Також можна налаштувати клієнтів DHCP на інтерфейсі Ethernet.

Сервер DHCP керує записом усіх IP-адрес, які він призначає вузлам мережі. Сервер ідентифікує переміщений вузол за допомогою його адреси керування доступом до медіа. Це запобігає випадковому налаштуванню декількох пристроїв з однаковою IP-адресою. Налаштування DHCP-сервера також вимагає створення конфігураційного файлу, в якому зберігається мережева інформація для клієнтів.

DHCP не є маршрутизованим протоколом. Він обмежений конкретною локальною мережею, а це означає, що достатньо одного DHCP-сервера на локальну мережу. Однак, може бути корисно використовувати два сервери на випадок обходу відмови. Більші мережі можуть мати глобальну мережу (WAN), яка містить кілька окремих точок. Залежно від зв'язків між цими точками і кількості клієнтів у кожній точці, команди можуть налаштувати кілька серверів DHCP для керування розподілом адрес. Користувачі можуть працювати з командним рядком, керуючи численними DHCP-серверами або DHCP-серверами у глобальній мережі. Користувачі повинні розуміти, що запуск, зупинка і перезапуск можуть вплинути на роботу демона.

Якщо мережеві адміністратори хочуть, щоб сервер DHCP забезпечував адресацію до декількох підмереж у мережі, вони повинні налаштувати служби ретрансляції DHCP, розташовані на з'єднувальних маршрутизаторах, через які повинні проходити запити DHCP. Ці агенти пересилають повідомлення між клієнтами і серверами DHCP, розташованими у різних підмережах.

Статичні пристрої, такі як веб-сервери та комутатори, мають постійні IP-адреси. За допомогою динамічного DHCP клієнт не володіє призначеною йому IP-адресою, а орендує її на певний період часу. Щоразу, коли пристрій з динамічною IP-адресою вмикається, він повинен зв'язатися з DHCP-сервером, щоб орендувати нову IP-адресу. Бездротові пристрої є прикладами клієнтів, яким присвоюються динамічні IP-адреси під час підключення до мережі.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

У разі динамічного налаштування DHCP клієнтові, можливо, доведеться припинити дію своєї IP-адреси, перш ніж він зможе знову підключитися до мережі з іншою. Час оренди DHCP варіюється залежно від того, як довго користувачеві потрібне підключення до Інтернету в конкретному місці. Пристрої звільняють свої IP-адреси, коли закінчується термін оренди. Потім, якщо вони залишаються в мережі, вони запитують поновлення. Сервер DHCP може призначити нову адресу, а не поновити стару.

Типовий цикл динамічної оренди DHCP виглядає наступним чином:

1. Клієнт отримує орендовану IP-адресу, запитуючи її у DHCP-сервера.
2. Якщо клієнт вже має IP-адресу з існуючого договору оренди, він повинен оновити свою IP-адресу під час перезавантаження після вимкнення і звернутися до DHCP-сервера для перерозподілу IP-адреси.
3. Коли договір оренди активний, клієнт прив'язаний до договору оренди та адреси.
4. Коли термін оренди закінчується, клієнт звертається до сервера, який спочатку надав оренду, щоб поновити її, щоб продовжити використання IP-адреси.
5. Якщо клієнт переходить в іншу мережу, його динамічна IP-адреса припиняє свою дію, і він запитує нову IP-адресу у DHCP-сервера нової мережі.

Переваги використання DHCP:

- зниження витрат на управління мережею
- зменшення ймовірності зіткнення IP-адрес
- спрощення масштабування мережі
- автоматичне налаштування нових пристроїв

Недоліком DHCP є те, що він не є безпечним за своєю суттю. Якщо злоумисники отримають доступ до сервера DHCP, вони можуть завдати шкоди. DHCP не має вбудованого механізму, який би дозволяв клієнтам і серверам автентифікувати один одного. Обидві сторони вразливі до обману та атак, коли недобросовісні клієнти можуть вичерпати пул IP-адрес DHCP-сервера.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Однією з ключових вразливостей DHCP є атаки типу man-in-the-middle (зловмисник посередині). Під час MitM-атаки зловмисник таємно перехоплює і передає повідомлення між двома сторонами, які вважають, що спілкуються безпосередньо одна з одною. Крім того, якщо DHCP-сервер не має резервної копії і сервер виходить з ладу, то з ладу виходять і пристрої, які він обслуговує.

Безпека DHCP може бути досягнута за допомогою таких методів, як DHCP snooping, для запобігання підробки DHCP-повідомлень, фільтрація MAC-адрес для контролю доступу до мережі та використання VLAN для розділення мережевого трафіку[25][27].

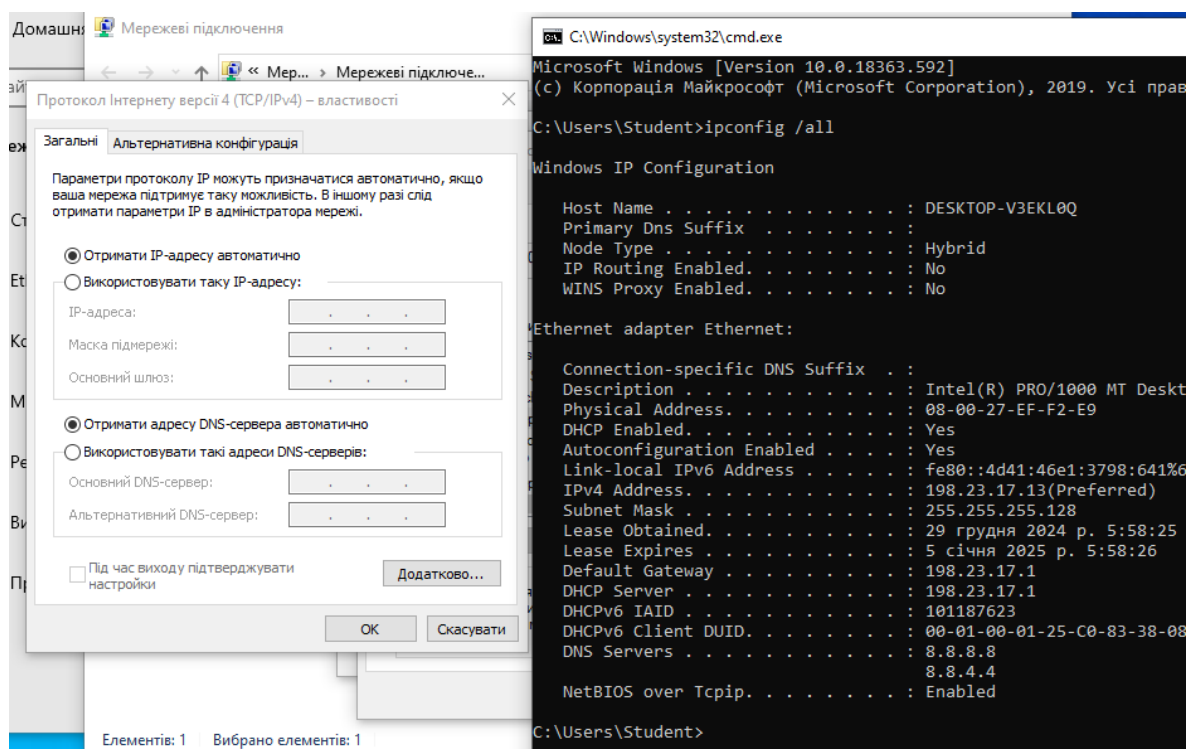


Рисунок 2.12 – Приклад використання DHCP

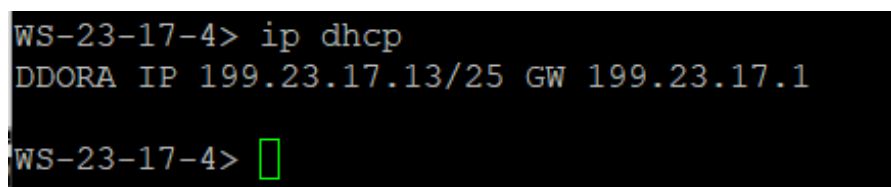


Рисунок 2.13 – Приклад використання DHCP

2.4 Проектування підсистеми мережного захисту

Для забезпечення захисту комунікаційних пристроїв та для можливості віддаленого доступу під час виконання кваліфікаційної роботи було використано протокол SSH.

SSH - це мережевий протокол, який надає користувачам, зокрема системним адміністраторам, безпечний спосіб доступу до комп'ютера через незахищену мережу.

SSH також відноситься до набору утиліт, які реалізують протокол SSH. Secure Shell забезпечує надійну автентифікацію за допомогою пароля і відкритого ключа, а також зашифровану передачу даних між двома комп'ютерами, з'єднаними через відкриту мережу, таку як Інтернет. SSH важливий для підтримки безпеки систем, оскільки протокол діє як безпечний спосіб надання доступу та управління мережевими системами.

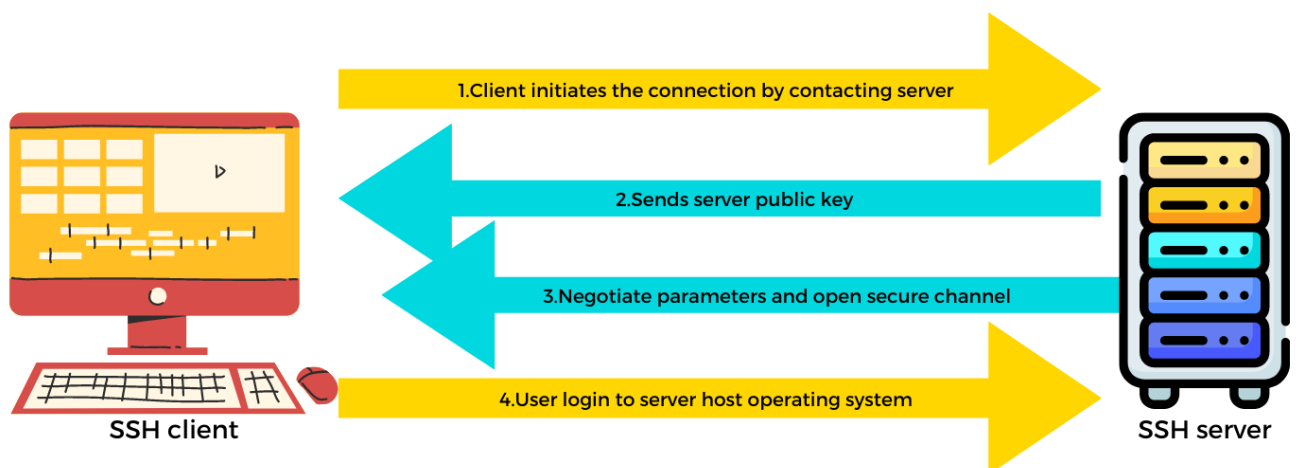


Рисунок 2.14 – Приклад роботи SSH

Окрім забезпечення надійного шифрування, SSH широко використовується мережевими адміністраторами для віддаленого керування системами та програмами, дозволяючи їм входити в систему на іншому комп'ютері через мережу, виконувати команди та переміщувати файли з одного комп'ютера на інший.

SSH відноситься як до криптографічного мережевого протоколу, так і до набору утиліт, які реалізують цей протокол. SSH використовує модель клієнт-сервер, з'єднуючи клієнтську програму Secure Shell, яка є кінцем, де відображається сеанс,

з SSH-сервером, який є кінцем, де виконується сеанс. Реалізації SSH часто включають підтримку прикладних протоколів, що використовуються для емуляції терміналів або передачі файлів.

SSH також можна використовувати для створення безпечних тунелів для інших прикладних протоколів - наприклад, для безпечного віддаленого запуску графічних сеансів X Window System. За замовчуванням для роботи протоколу використовується TCP-22 порт: на ньому сервер (хост) очікує вхідне підключення і після отримання команди і проведення аутентифікації організує запуск клієнта, відкриваючи обрану користувачем оболонку. При необхідності користувач може змінювати порт, що використовується. Для створення SSH підключення клієнт повинен ініціювати з'єднання з сервером, забезпечивши захищене з'єднання і підтвердивши свій ідентифікатор.

Присутній у всіх дата-центрах, SSH постачається за замовчуванням з кожним сервером Unix, Linux і Mac. SSH-з'єднання використовуються для захисту різних типів зв'язку між локальною машиною і віддаленим хостом, включаючи безпечний віддалений доступ до ресурсів, віддалене виконання команд, доставку виправлень і оновлень програмного забезпечення та інші адміністративні або управлінські завдання.

Крім створення захищеного каналу між локальними і віддаленими комп'ютерами, SSH використовується для управління маршрутизаторами, серверним обладнанням, платформами віртуалізації і операційними системами, а також внутрішніми програмами управління системами і передачі файлів.

Secure Shell використовується для підключення до серверів, внесення змін, завантаження та виходу за допомогою інструментів або безпосередньо через термінал. SSH-ключі можуть бути використані для автоматизації доступу до серверів і часто застосовуються в скриптах, системах резервного копіювання та інструментах управління конфігурацією.

Розроблені для зручності та роботи поза межами організації, ключі SSH забезпечують єдиний вхід (SSO), щоб користувачі могли переходити між своїми обліковими записами без необхідності кожного разу вводити пароль.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

SSH також можна використовувати для створення захищених тунелів для інших прикладних протоколів. Наприклад, безпечні тунелі можна використовувати для локального, віддаленого і динамічного перенаправлення портів. Відіграючи ключову роль в управлінні ідентифікацією і доступом, SSH робить більше, ніж просто аутентифікація через зашифроване з'єднання. Весь трафік SSH шифрується. Незалежно від того, передають користувачі файл, переглядають веб-сторінки або запускають команди, їх дії є приватними.

Хоча можна використовувати SSH зі звичайним ідентифікатором користувача і паролем в якості облікових даних, SSH частіше покладається на автентифікацію на основі ключів, використовуючи пари відкритих ключів для автентифікації хостів один з одним.

Окремі користувачі все одно повинні використовувати свій ідентифікатор користувача і пароль - або інші методи автентифікації користувача - для підключення до віддаленого хоста, але локальний і віддалений комп'ютери автентифікуються окремо один від одного. Це досягається шляхом генерації унікальної пари відкритих ключів для кожного хоста в комунікації. Для одного сеансу потрібні дві пари відкритих ключів: одна пара відкритих ключів для автентифікації віддаленого комп'ютера на локальному комп'ютері, а друга пара відкритих ключів для автентифікації локального комп'ютера на віддаленому комп'ютері.

SSH також використовується для керування та налаштування брандмауерів та інших програм безпеки, забезпечуючи безпечні адміністративні зміни конфігурації та доступ[28][29].

```
Username: admin
Password:
R-23-17-5#ssh -l admin 196.23.17.66
Password:

R-23-17-9#en
R-23-17-9#conf t
```

Рисунок 2.15 – Приклад використання SSH

```
R-23-17-5#ssh -l user 193.23.17.13
Password:

R-23-17-1>en
Password:
R-23-17-1#conf t
```

Рисунок 2.16 – Приклад використання SSH

Висновки до другого розділу:

У другому розділі було спроектовано топологію комп'ютерної мережі та зроблено систему IP-адресації. В якості основи для топології була обрана трирівнева ієрархічна модель Cisco, що забезпечує високу продуктивність, масштабованість та безпеку. Чіткий розподіл функцій між рівнем ядра, розподілу та доступу дозволяє ефективно керувати мережею та оптимізувати передачу даних.

Далі було визначено програмні рішення та сервіси, необхідні для забезпечення функціональності мережі, з акцентом на розробку сервісів та послуг прикладного рівня. На останньому етапі цього розділу розглядалось проектування підсистеми мережевої безпеки та визначались механізми і протоколи для забезпечення безпеки мережі та захисту від небажаних загроз.

Таким чином, у рамках розділу було створено комплексну, масштабовану та захищену архітектуру гетерогенної мережі, що готова до подальшого налаштування та експлуатації.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЕКТОВАНОЇ МЕРЕЖІ

3.1 Вибір обладнання та ОС пристроїв для розробленого проекту мережі

Вибір обладнання - важливий крок у побудові надійної та ефективної комп'ютерної мережі. На цьому етапі враховуються потреби користувачів, очікувані обсяги трафіку, вимоги до безпеки та масштабованості мережі.

Вибір маршрутизатора є невід'ємною частиною конфігурації мережі. Маршрутизатори передають дані і маршрутизують трафік між різними сегментами мережі. Для проекту кваліфікаційної роботи було обрано два маршрутизатори різних компаній: Cisco 4321 та MikroTik



Рисунок 3.1 – Маршрутизатор Cisco 4321 (с4000)

Маршрутизатор Cisco 4321 це маршрутизатор із серії Cisco 4000 ISR, розроблений для забезпечення гнучкості, масштабованості та інтеграції сучасних мережевих сервісів. Ця модель ідеально підходить для невеликих і середніх офісів, а також для філій великих організацій, які потребують високої надійності та продуктивності. Вона забезпечує підтримку як традиційних, так і сучасних мережевих протоколів і технологій, таких як VPN, IPsec, QoS, голосовий трафік і хмарні інтеграції.

Cisco ISR 4321 оснащений двома вбудованими портами Gigabit Ethernet RJ-45, які можна використовувати як для WAN, так і для LAN-з'єднань, а також одним портом SFP для підключення оптичних ліній зв'язку. Маршрутизатор має два слоти

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

для модулів NIM (Network Interface Module), що дозволяють додавати додаткові мережеві інтерфейси, такі як серійні порти або додаткові Ethernet-порти. Він оснащений процесором Intel x86 з тактовою частотою 1.4 GHz, оперативною пам'яттю 4 ГБ (розширюється до 8 ГБ) і флеш-пам'яттю 4 ГБ (розширюється до 16 ГБ). Базова пропускна здатність маршрутизації становить 50 Мбіт/с із можливістю збільшення до 100 Мбіт/с за допомогою ліцензії. Пристрій підтримує до 50 одночасних IPsec VPN-з'єднань і працює під управлінням операційної системи Cisco IOS-XE, яка забезпечує підтримку сучасних протоколів маршрутизації (BGP, OSPF, EIGRP) та можливість масштабування функцій.

Станом на 2025 рік Cisco ISR 4321 залишається актуальним, але поступається новішим моделям, таким як Cisco Catalyst 8000, які пропонують кращу продуктивність, підтримку SD-WAN і інші сучасні функції. Для компаній, які потребують великої пропускної здатності, цей маршрутизатор є оптимальним вибором завдяки його надійності, компактності та функціональності.



Рисунок 3.2 – Маршрутизатор MikroTik CCR2216-1G-12XS-2XQ

MikroTik CCR2216-1G-12XS-2XQ – це потужний маршрутизатор флагманського класу, розроблений для високопродуктивних оптоволоконних мереж, яким потрібна висока пропускна здатність і надійність. Він є ідеальним рішенням для інтернет-провайдерів, великих підприємств, центрів обробки даних та будь-яких організацій, що потребують маршрутизації великих обсягів трафіку зі швидкістю до 100 Гбіт/с.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Однією з ключових особливостей цього маршрутизатора є наявність унікального комутаційного чіпа Marvell Prestera Aldrin2 з апаратною розвантаженням L3, що дозволяє досягти максимальної продуктивності мережі. Пристрій виконаний у металевому корпусі форм-фактора 1U для встановлення в серверну шафу або стійку, і поставляється з усіма необхідними кріпленнями. Він також оснащений двома резервними блоками живлення з можливістю гарячої заміни, що забезпечує високу відмовостійкість.

Ця модель є значним оновленням і потенційною заміною для попереднього флагмана MikroTik CCR1072, при цьому зберігаючи сумісність з існуючими SFP-модулями та блоками живлення.

На момент 2025 року, MikroTik CCR2216-1G-12XS-2XQ залишається дуже актуальним пристроєм, особливо для вимогливих мережевих інфраструктур. Завдяки 16-ядерному процесору, великому обсягу RAM та апаратному розвантаженню L3, він легко справляється з великими навантаженнями та забезпечує високу пропускну здатність, що є критично важливим для сучасних мереж з постійно зростаючими потребами в даних.

Наявність портів QSFP28 (100 Гбіт/с) робить його готовим до майбутніх потреб і дозволяє будувати високошвидкісні магістралі та агрегацію трафіку. Комбінація 100-гігабітних та 25-гігабітних портів забезпечує гнучкість у побудові мережі та дозволяє підключати різноманітне обладнання. Два резервні блоки живлення та чотири вентилятори з можливістю гарячої заміни забезпечують високий рівень надійності та безперебійної роботи, що є обов'язковим для критично важливих мереж. Ця модель позиціонується як наступник CCR1072, що підкреслює її лідерство в сегменті маршрутизаторів MikroTik і відповідність сучасним вимогам.

Він є відмінним вибором для організацій, що модернізують свою мережеву інфраструктуру, маршрутизатор забезпечує чудове співвідношення ціни до потужності та функціональності,

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Вибір комутатора також важливий при налаштуванні мережі. Комутатори використовуються для підключення пристроїв до локальної мережі (LAN). Вибір комутатора залежить від вимог до швидкості передачі даних та кількості підключених пристроїв. Для кваліфікаційної роботи було вирішено використовувати комутатор Cisco WS-C2960-24TT-L.



Рисунок 3.3 – Комутатор Cisco WS-C2960-24TT-L

Комутатор Cisco WS-C2960-24TT-L це керований комутатор початкового рівня із серії Cisco Catalyst 2960. Цей пристрій забезпечує високий рівень продуктивності, надійності та простоти в управлінні, що робить його популярним вибором для організацій, які потребують базових функцій комутації без складних налаштувань.

Основні характеристики комутатора Cisco WS-C2960-24TT-L:

- *Порти та підключення:* Комутатор має 24 порти для підключення пристроїв до мережі, які працюють на швидкості 10/100 Мбіт/с. Це стандартні порти Fast Ethernet, які підходять для більшості офісних пристроїв, таких як комп'ютери та принтери. Крім того, комутатор має 2 порти Gigabit Ethernet, які забезпечують більшу швидкість передачі даних — 10/100/1000 Мбіт/с. Один із цих портів має стандартний роз'єм RJ-45, а інший підтримує SFP-модулі для підключення до оптоволоконних ліній, що дозволяє використовувати даліші з'єднання з іншими мережами або пристроями.

- *Продуктивність:* Цей комутатор має досить високу продуктивність для свого класу. Його пропускна здатність становить 16 Гбіт/с, що означає, що комутатор може обробляти значну кількість даних одночасно. Крім того, він здатний пересилати до 6.5 мільйонів пакетів за секунду, що дозволяє ефективно працювати з

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

великим потоком даних. Ще одна важлива характеристика — це таблиця MAC-адрес, яка може зберігати до 8,000 записів. Це дає змогу комутатору обробляти трафік для значної кількості пристроїв, підключених до нього.

- *Фізичні параметри:* Цей комутатор має компактні розміри і може бути встановлений у стандартну стійку 19 дюймів, займаючи лише 1U висоти. Його розміри становлять 4.5 см у висоту, 44.5 см у ширину та 23.6 см у глибину. Вага пристрою — 3.6 кг. Що стосується енергоспоживання, комутатор використовує до 40 Вт енергії, що робить його енергоефективним для таких пристроїв.

- *Безпека:* комутатор підтримує технології безпеки, такі як IEEE 802.1x, яка дозволяє контролювати доступ до мережі, забезпечуючи автентифікацію пристроїв перед підключенням. Також є можливість налаштовувати списки контролю доступу, що дозволяє обмежити доступ до певних частин мережі. Крім того, комутатор захищений від атак типу DoS (Denial-of-Service), які можуть спричинити перевантаження мережі.

Як правило, комутатори Cisco WS-C2960-24TT-L є надійними і функціональними пристроями, які можуть використовуватися для створення мереж і забезпечують швидку передачу даних і можливості управління нею.

3.2. Побудова та налагодження мережі

Налаштування будь-якої мережі, звісно ж починається із ір-адресації. Тому спочатку проводимо налаштування статичної ір-адресації інтерфейсів на пристроях мережі:

```

R-23-17-10#
R-23-17-10#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-17-10(config)#int f0/0
R-23-17-10(config-if)#ip address 197.23.17.2 255.255.255.192
R-23-17-10(config-if)#no sh
R-23-17-10(config-if)#
*Dec 27 05:46:56.863: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec 27 05:46:57.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R-23-17-10(config-if)#ex
R-23-17-10(config)#int f1/0
R-23-17-10(config-if)#ip address 201.23.17.1 255.255.255.128
R-23-17-10(config-if)#no sh
  
```

Рисунок 3.4 – Налаштування IP-адресації

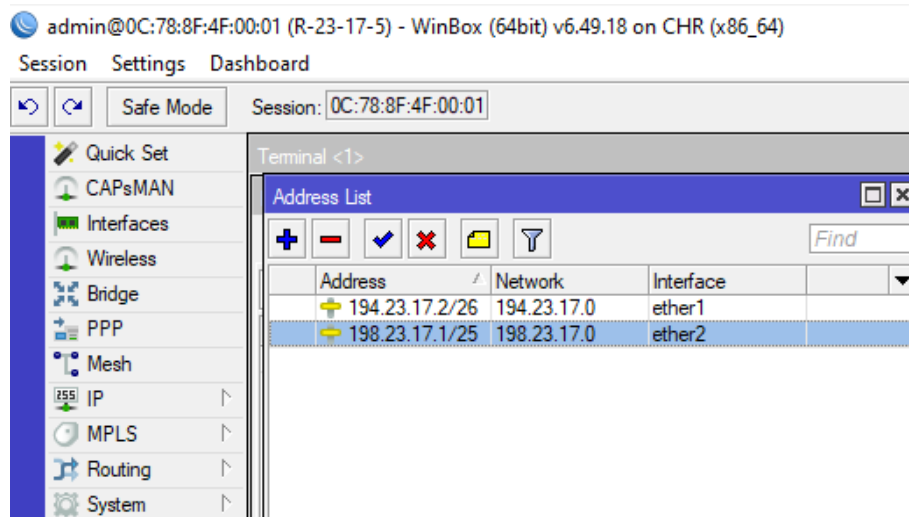


Рисунок 3.5 – Налаштування IP-адресації

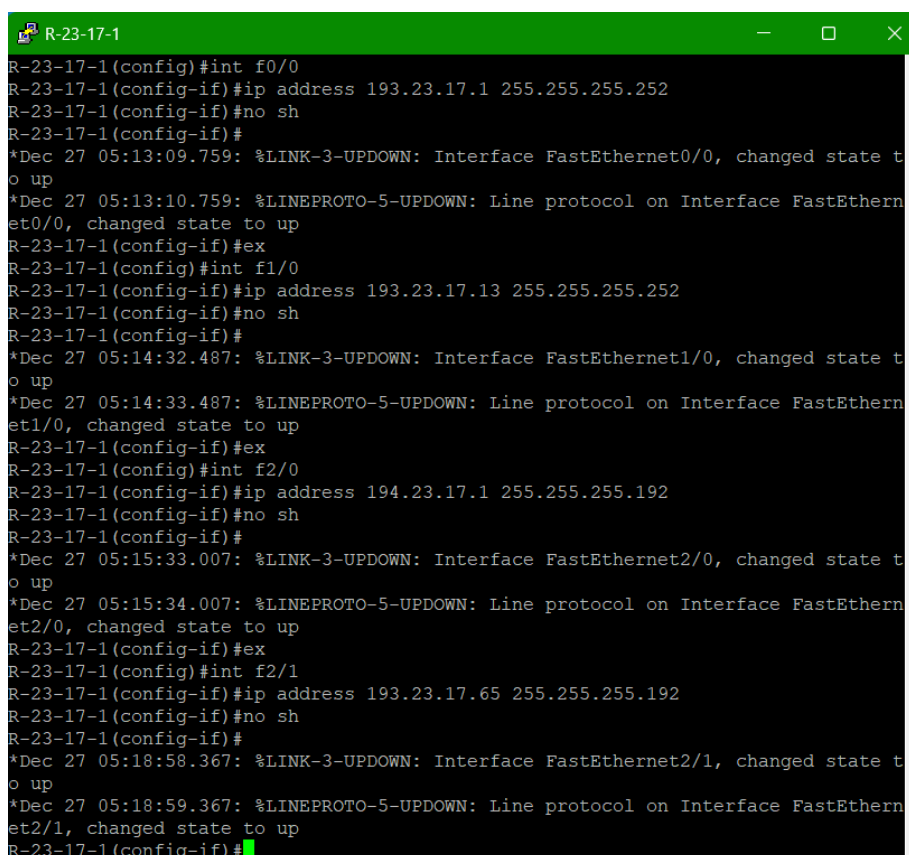


Рисунок 3.6 – Налаштування IP-адресації

На інших пристроях мережі проводимо аналогічні налаштування.

Нам також потрібно надати IP-адреси кінцевим пристроям у мережі. Найраціональніше отримувати IP-адреси динамічно. Тому налаштовуємо DHCP-сервер. В нашій мережі цими серверами будуть виступати маршрутизатори рівня розподілу: R-23-17-5, R-23-17-6, R-23-17-7, R-23-17-8, R-23-17-9, R-23-17-10 та R-23-17-11.

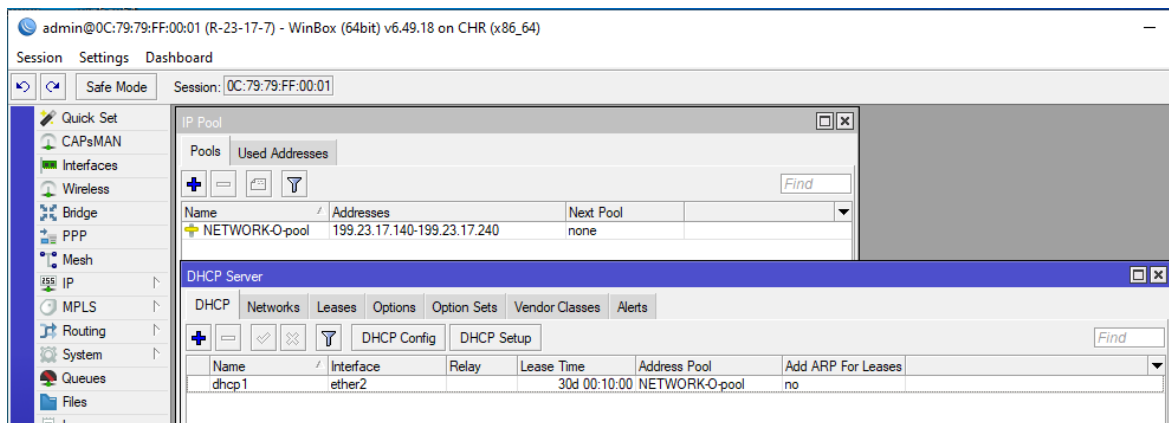


Рисунок 3.7 – Налаштування DHCP

```
R-23-17-11(config)#ip dhcp pool NETWORK-S
R-23-17-11(dhcp-config)#network 201.23.17.128 255.255.255.128
R-23-17-11(dhcp-config)#default-router 201.23.17.129
R-23-17-11(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
R-23-17-11(dhcp-config)#lease 7
R-23-17-11(dhcp-config)#ex
R-23-17-11(config)#ip dhcp exclu
R-23-17-11(config)#ip dhcp excluded-address 201.23.17.129 201.23.17.139
R-23-17-11(config)#ip dhcp excluded-address 201.23.17.241 201.23.17.254
```

Рисунок 3.8 – Налаштування DHCP

На інших маршрутизаторах рівня розподілу проводимо аналогічні налаштування.

Після налаштування IP-адресації необхідно перевірити зв'язок між сусідніми пристроями в підмережі. Після перевірки переходимо до налаштування динамічної маршрутизації для зв'язку між усіма пристроями в мережі. Протоколом маршрутизації є Open Shortest Path First (OSPF).

Маршрутизацію налаштовуємо на усіх маршрутизаторах мережі.

```
R-23-17-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-17-1(config)#int range f2/1, f2/0, f0/0, f1/0
R-23-17-1(config-if-range)#ip ospf message-digest-key 17 md5 cisco123
R-23-17-1(config-if-range)#ip ospf authentication message-digest
R-23-17-1(config-if-range)#ex
R-23-17-1(config)#router ospf 23171
R-23-17-1(config-router)#network 193.23.17.0 0.0.0.3 area 0
R-23-17-1(config-router)#network 193.23.17.12 0.0.0.3 area 0
R-23-17-1(config-router)#network 193.23.17.64 0.0.0.63 area 0
R-23-17-1(config-router)#network 194.23.17.0 0.0.0.63 area 0
R-23-17-1(config-router)#area 0 authentication message-digest
R-23-17-1(config-router)#ex
```

Рисунок 3.9 – Налаштування маршрутизації OSPF

```

R-23-17-4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-17-4(config)#int range f1/0, f2/0, f2/1, f1/1, f0/0
R-23-17-4(config-if-range)#ip ospf message-digest-key 17 md5 cisco123
R-23-17-4(config-if-range)#ip ospf authentication message-digest
R-23-17-4(config-if-range)#ex
R-23-17-4(config)#router ospf 23174
R-23-17-4(config-router)#network 193.23.17.12 0.0.0.3 area 0
R-23-17-4(config-router)#network 193.23.17.12 0.0.0.3 area 0
*Dec 28 02:11:49.079: %OSPF-5-ADJCHG: Process 23174, Nbr 194.23.17.1 on FastEthernet1/0 from
LOADING to FULL, Loading Done
R-23-17-4(config-router)#network 193.23.17.12 0.0.0.8 area 0
% OSPF: Invalid address/mask combination (discontiguous mask)
R-23-17-4(config-router)#network 193.23.17.8 0.0.0.3 area 0
R-23-17-4(config-router)#network 193.23.17.8 0.0.0.63 area 0
*Dec 28 02:12:11.619: %OSPF-5-ADJCHG: Process 23174, Nbr 196.23.17.1 on FastEthernet2/0 from
LOADING to FULL, Loading Done
R-23-17-4(config-router)#network 196.23.17.64 0.0.0.63 area 0
R-23-17-4(config-router)#network 197.23.17.0 0.0.0.63 area 0
R-23-17-4(config-router)#network 197.23.17.64 0.0.0.63 area 0
R-23-17-4(config-router)#area 0 authentication message-digest
R-23-17-4(config-router)#end

```

Рисунок 3.10 – Налаштування маршрутизації OSPF

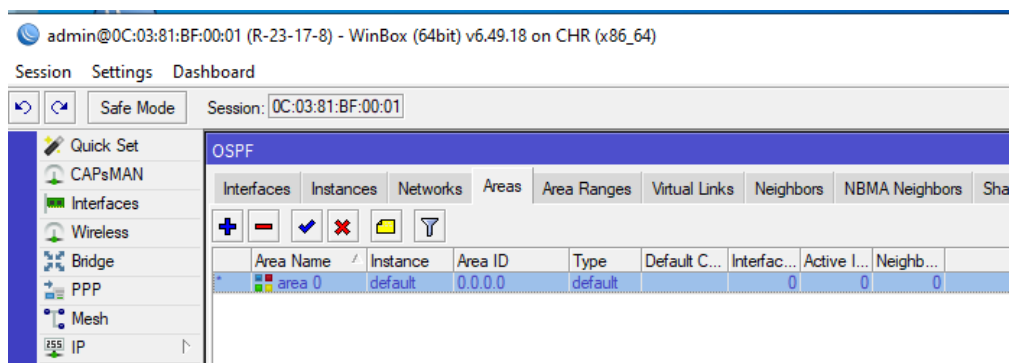


Рисунок 3.11 – Налаштування маршрутизації OSPF

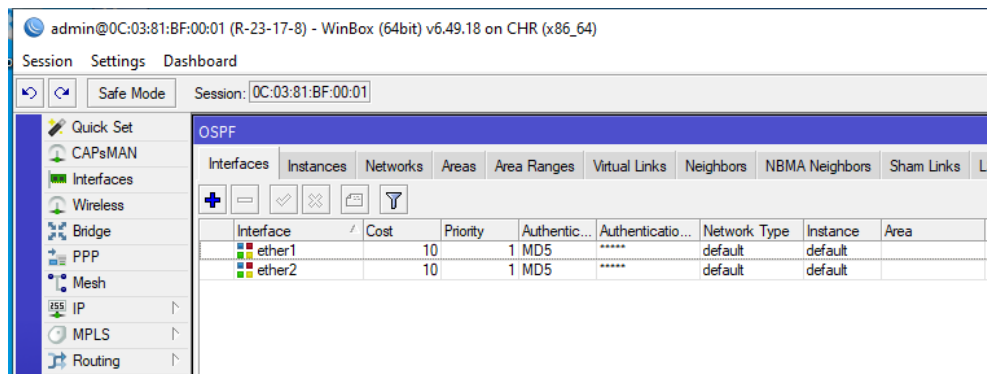


Рисунок 3.12 – Налаштування маршрутизації OSPF

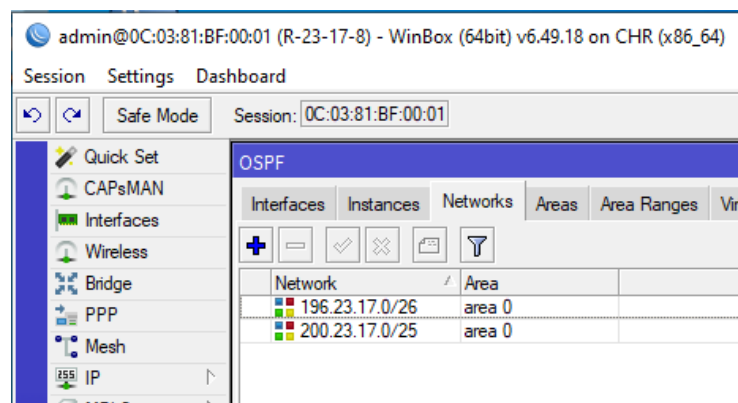


Рисунок 3.13 – Налаштування маршрутизації OSPF

Спочатку налаштовуємо діапазон інтерфейсів для OSPF автентифікації повідомлення-дайджесту і після цього безпосередньо налаштовуємо мережі OSPF

На інших маршрутизаторах мережі проводимо аналогічні налаштування але відповідно із дамини підмереж до яких вони входять.

Після налагодження маршрутизації, зв'язок повинен бути абсолютно між усіма пристроями мережі

Далі переходимо до налаштування IPsec VPN. Для прикладу маршрутизатора Cisco розберемо налаштування безпосередньо на маршрутизаторі R-23-17-4.

```
R-23-17-4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-17-4(config)#security password min-length 10
R-23-17-4(config)#enable secret cisco123456
R-23-17-4(config)#username admin privilege 15 secret adminpass1234
R-23-17-4(config)#line console 0
R-23-17-4(config-line)#login local
R-23-17-4(config-line)#exit
R-23-17-4(config)#crypto isakmp enable
R-23-17-4(config)#crypto isakmp policy 2317
R-23-17-4(config-isakmp)#hash sha
R-23-17-4(config-isakmp)#authentication pre-share
R-23-17-4(config-isakmp)#group 14
R-23-17-4(config-isakmp)#lifetime 7200
R-23-17-4(config-isakmp)#encryption aes 256
R-23-17-4(config-isakmp)#ex
R-23-17-4(config)#crypto isakmp key cisco222222 address 193.23.17.2
R-23-17-4(config)#crypto isakmp key cisco222222 address 193.23.17.5
R-23-17-4(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R-23-17-4(cfg-crypto-trans)#ex
R-23-17-4(config)#$ 101 permit ip 197.23.17.64 0.0.0.63 195.23.17.0 0.0.0.63
R-23-17-4(config)#$ 101 permit ip 197.23.17.64 0.0.0.63 195.23.17.64 0.0.0.63
R-23-17-4(config)#$ 101 permit ip 197.23.17.0 0.0.0.63 195.23.17.0 0.0.0.63
R-23-17-4(config)#$ 101 permit ip 197.23.17.0 0.0.0.63 195.23.17.64 0.0.0.63
R-23-17-4(config)#$ 101 permit ip 196.23.17.64 0.0.0.63 195.23.17.0 0.0.0.63
R-23-17-4(config)#$ 101 permit ip 196.23.17.64 0.0.0.63 195.23.17.64 0.0.0.63
R-23-17-4(config)#crypto map CAMP 2317 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R-23-17-4(config-crypto-map)#match address 101
R-23-17-4(config-crypto-map)#set peer 193.23.17.2
R-23-17-4(config-crypto-map)#set peer 193.23.17.5
R-23-17-4(config-crypto-map)#set peer 193.23.17.13
R-23-17-4(config-crypto-map)#set peer 193.23.17.1
R-23-17-4(config-crypto-map)#set pfs group14
R-23-17-4(config-crypto-map)#set transform-set 50
R-23-17-4(config-crypto-map)#set security-association lifetime seconds 900
R-23-17-4(config-crypto-map)#ex
R-23-17-4(config)#int range f1/0, f2/0
R-23-17-4(config-if-range)#crypto map CAMP
R-23-17-4(config-if-range)#ex
R-23-17-4(config)#
*Dec 28 07:07:40.299: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

Рисунок 3.14 – Налаштування IPsec VPN

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

Спочатку необхідно створити користувача із максимальним рівнем привілеїв. Після цього налаштовуємо політику isakmp. Наступним кроком є створення спільного ключа та визначення шифрування і хешування. Вкінці-кінців нам необхідно створити crypto map, провести в ній відповідні налагодження та додати її до інтерфейсу маршрутизатора.

На інших маршрутизаторах компанії Cisco: R-23-17-1, R-23-17-2, R-23-17-11, було виконано аналогічні налаштування, але відповідно із їх даними.

Налаштування маршрутизаторів MikroTik розберемо на прикладі R-23-17-8

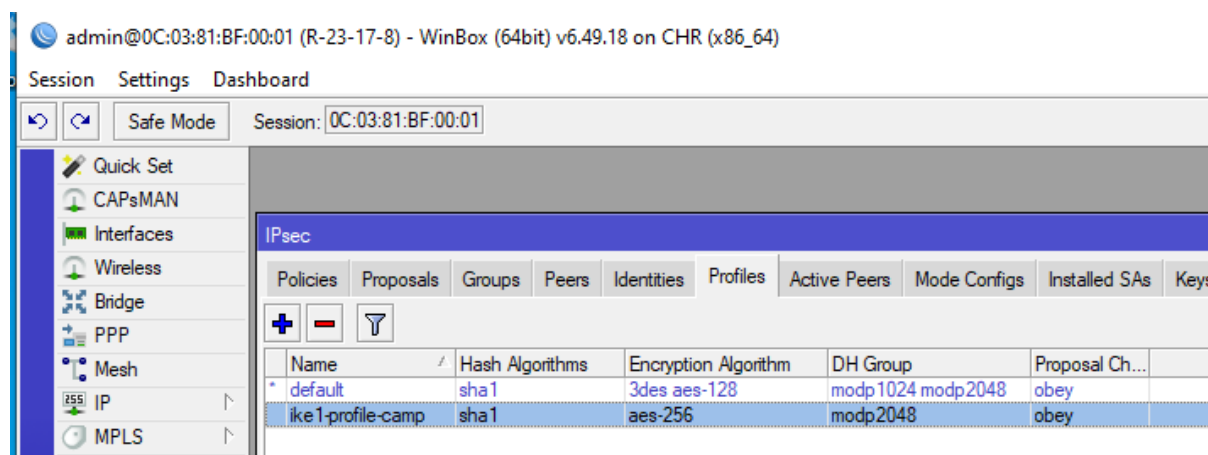


Рисунок 3.15 – Налаштування IPsec VPN

Перш за все, налаштовуємо профілі IKE фази 1. Визначаємо параметри для обміну ключами, такі як алгоритми хешування, шифрування та групу Діффі-Хеллмана для профілю "ike1-profile-camp"

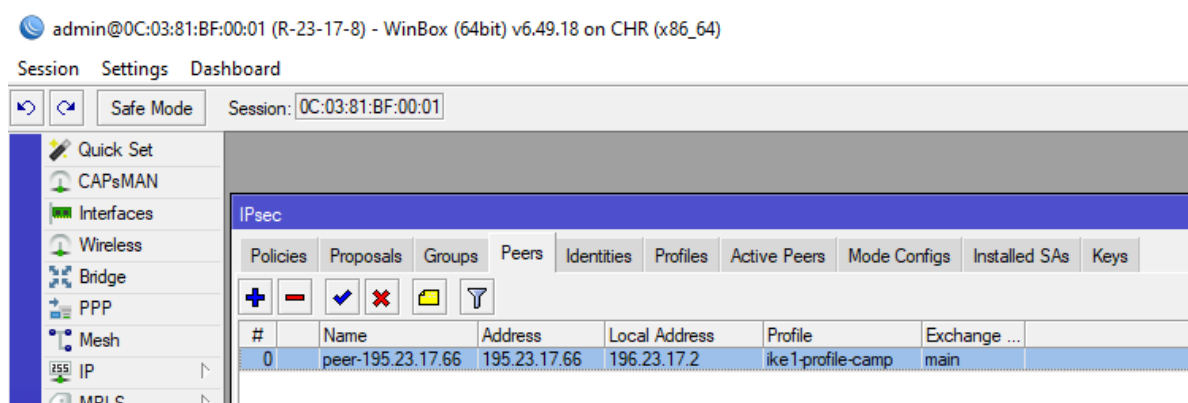


Рисунок 3.16 – Налаштування IPsec VPN

Далі налаштовуємо IPsec Peer. Вказуємо IP-адресу віддаленого пристрою, локальну адресу та прив'язуємо до раніше створеного профілю "ike1-profile-camp"

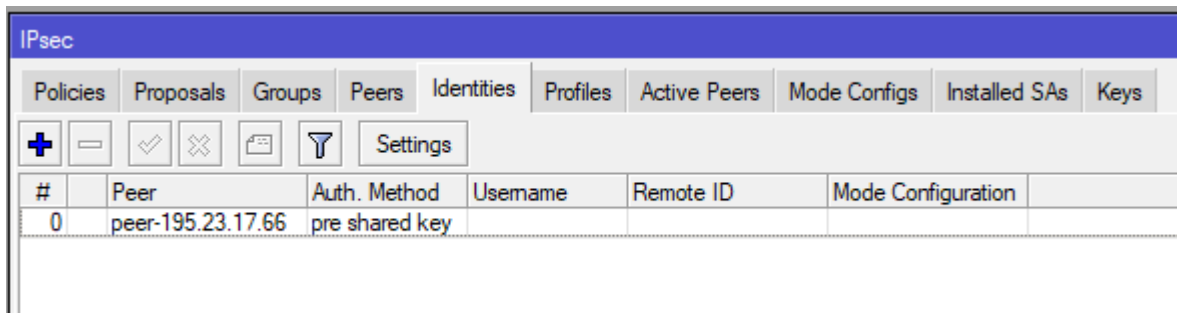


Рисунок 3.17 – Налаштування IPsec VPN

Після цього ми визначаємо метод автентифікації для піра. Встановлюємо, що використовуватиметься метод "pre shared key" для автентифікації з віддаленим піром та вказуємо цей ключ.

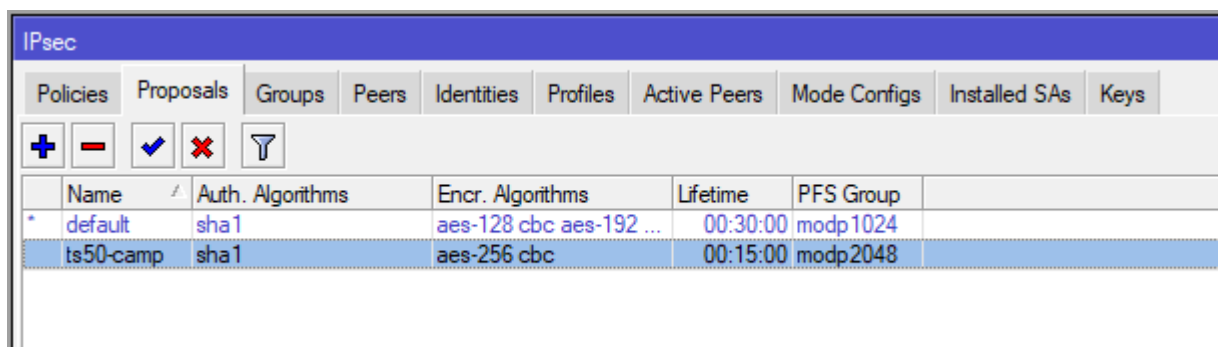


Рисунок 3.18 – Налаштування IPsec VPN

Далі налаштовуємо пропозиції IPsec для фази 2. Визначаємо алгоритми автентифікації, шифрування, час роботи та групу Perfect Forward Secrecy для пропозиції "ts50-camp"

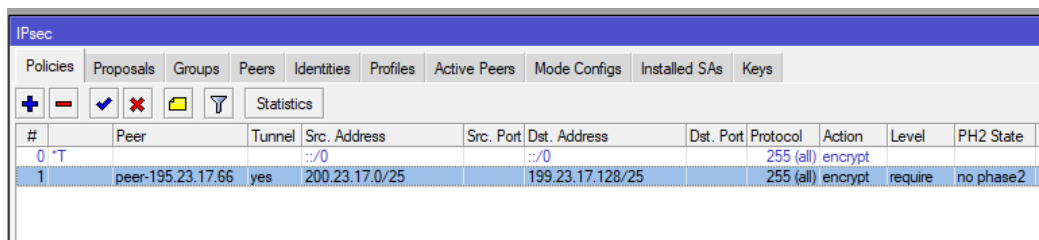


Рисунок 3.19 – Налаштування IPsec VPN

Вкінці-кінців створюємо політику IPsec, яка визначає, який трафік буде шифруватися. Вона вказує на шифрування трафіку між локальною підмережею та віддаленою за допомогою піра.

На інших маршрутизаторах компанії Mikrotik: R-23-17-3, R-23-17-5, R-23-17-7, було виконано аналогічні налаштування, але відповідно із їх даними.

Наступним кроком, для забезпечення захисту інформації в мережі було обрано налаштувати протокол віддаленого доступу SSH version 2.

Так як на маршрутизаторах де ми налаштовували IPsec VPN користувача admin із найвищим рівнем привілеїв уже створено, тому на них створюємо лише користувача user із рівнем привілеїв 1, а також налаштовуємо доменне ім'я.

```
R-23-17-4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-17-4(config)#ip domain-name serdiichuk.net
R-23-17-4(config)#username user privilege 1 secret userpass123
R-23-17-4(config)#
```

Рисунок 3.20 – Створення користувачів

А на інших маршрутизаторах створюємо двох користувачів: admin із рівнем привілеїв 15 та user рівень привілеїв 1, налаштовуємо доменне ім'я та задаємо пароль для входу в привілейований режим

```
R-23-17-10#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-23-17-10(config)#security password min-length 10
R-23-17-10(config)#ip domain-name serdiichuk.net
R-23-17-10(config)#username user privilege 1 secret userpass1234
R-23-17-10(config)#username admin privilege 15 secret adminpass1234
R-23-17-10(config)#enable secret cisco12345
R-23-17-10(config)#end
R-23-17-10#
```

Рисунок 3.21 – Створення користувачів

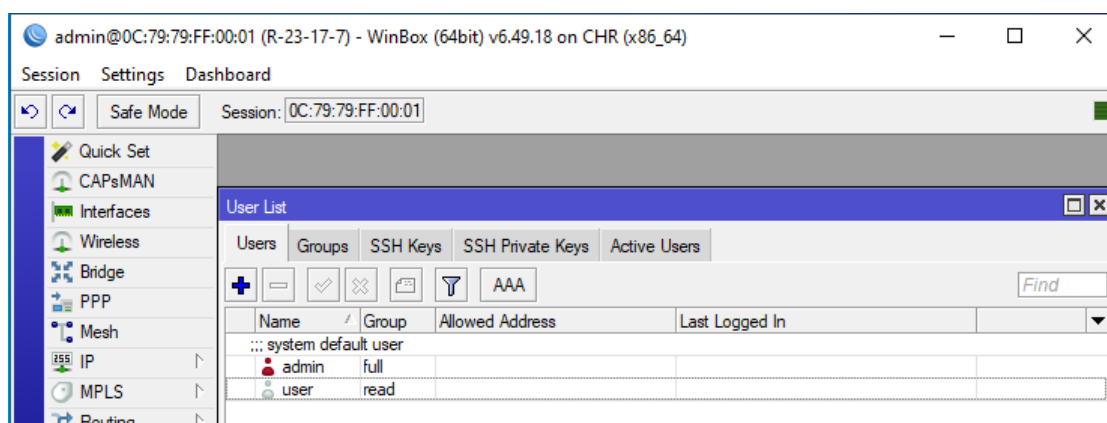


Рисунок 3.22 – Створення користувачів

Наступним кроком є налаштування шифрування та самого SSH version 2. Так як на маршрутизаторах MikroTik SSH вже є вбудованою функцією та окремого налаштування не потребує, тому ці налаштування виконуємо тільки на маршрутизаторах Cisco

```

R-23-17-2(config)#crypto key generate rsa
The name for the keys will be: R-23-17-2.serdiichuk.net
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 0 seconds)

R-23-17-2(config)#
*Dec 28 19:06:22.983: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-23-17-2(config)#ip ssh version 2
R-23-17-2(config)#ip ssh time-out 120
R-23-17-2(config)#ip ssh authentication-retries 3
R-23-17-2(config)#line vty 0 4
R-23-17-2(config-line)#transport input ssh
R-23-17-2(config-line)#transport output ssh
R-23-17-2(config-line)#login local

```

Рисунок 3.23 – Налаштування SSHv2

Дані налаштування проводимо на усіх Cisco маршрутизаторах мережі.

Для інформування адміністраторів про системні та мережеві події, обладнання здатне генерувати та надсилати відповідні сповіщення. Протокол Syslog є галузевим стандартом, що забезпечує централізований збір, зберігання та аналіз таких повідомлень з різних пристроїв.

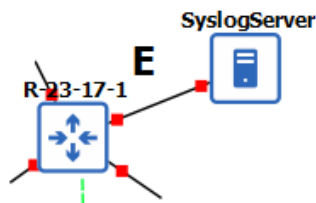


Рисунок 3.24 – Підключений SyslogServer до мережі

Для комфортної роботи було вирішено використати програмне забезпечення tftpd. Тому завантажуюмо та встановлюємо його

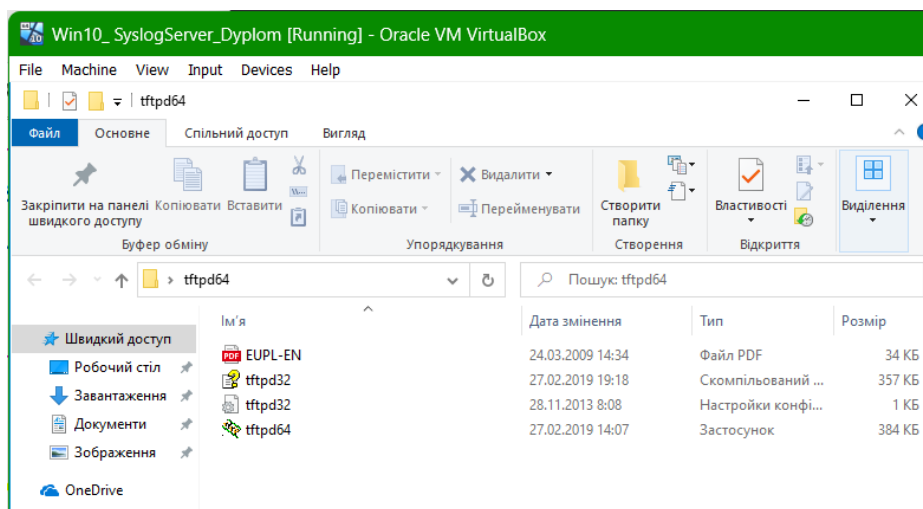


Рисунок 3.25 – Перелік завантажених файлів

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі для коректної роботи необхідно провести дані налаштування Syslog безпосередньо на всіх маршрутизаторах мережі:

```
R-23-17-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-23-17-2(config)#logging host 193.23.17.70
R-23-17-2(config)#
*Dec 29 00:13:07.419: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to I
port 514 started - CLI initiated
R-23-17-2(config)#logging trap informational
R-23-17-2(config)#service timestamps log datetime msec
R-23-17-2(config)#logging console informational
R-23-17-2(config)#logging buffered informational
```

Рисунок 3.26 – Налаштування Syslog

3.3 Тестування роботи мережі

По завершенню усіх налаштувань необхідно провести тестування мережі на роботоздатність. Після виконання певних команд ми зможемо переконатись у правильності налаштування мережі.

Спочатку перевіримо налаштування DHCP:

```
WS-23-17-4> ip dhcp
DDORA IP 199.23.17.13/25 GW 199.23.17.1

WS-23-17-4> show ip

NAME           : WS-23-17-4[1]
IP/MASK         : 199.23.17.13/25
GATEWAY         : 199.23.17.1
DNS             : 8.8.8.8 8.8.4.4
DHCP SERVER     : 199.23.17.1
DHCP LEASE      : 604704, 604800/302400/529200
MAC             : 00:50:79:66:68:05
LPORT          : 10016
RHOST:PORT      : 127.0.0.1:10017
MTU:            : 1500

WS-23-17-4>
```

Рисунок 3.27 – Перевірка налаштування

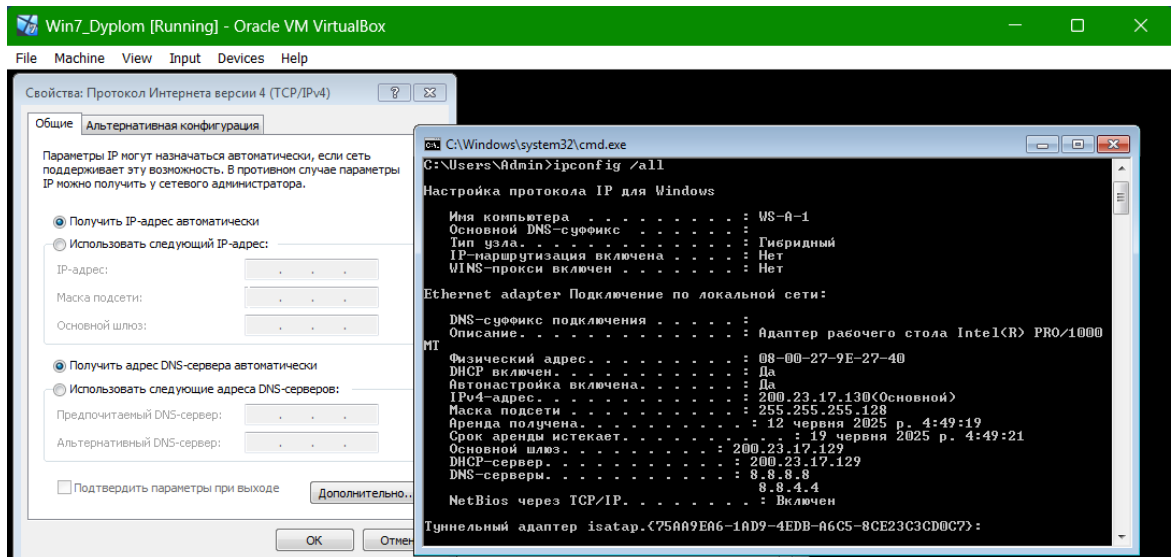


Рисунок 3.28 – Перевірка налаштування

Також на маршрутизаторах від MikroTik можна в режимі реального часу спостерігати за виданими IP-адресами.

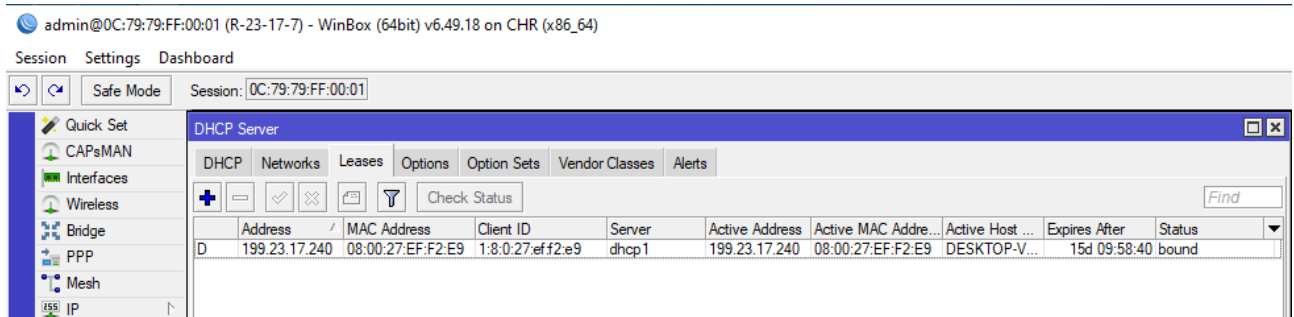


Рисунок 3.29 – Перевірка налаштування

Після цього, так як IP-адресація та маршрутизація налаштована протестуємо зв'язок між кінцевими пристроями різних підмереж

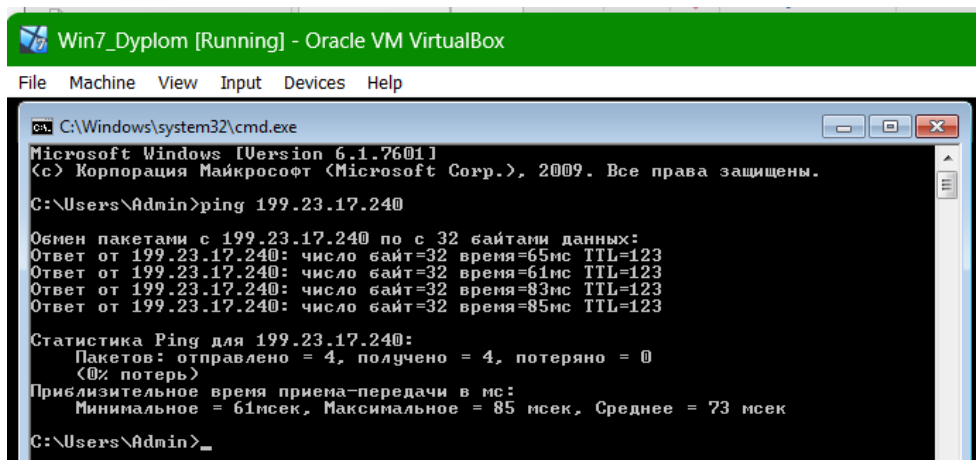


Рисунок 3.30 – Перевірка зв'язку

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

w10_dip [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.592]
(c) Корпорація Майкрософт (Microsoft Corporation), 2019. Усі права захищено.

C:\Users\Student>ping 201.23.17.140

Pinging 201.23.17.140 with 32 bytes of data:
Reply from 201.23.17.140: bytes=32 time=3092ms TTL=59
Reply from 201.23.17.140: bytes=32 time=80ms TTL=59
Reply from 201.23.17.140: bytes=32 time=86ms TTL=59
Reply from 201.23.17.140: bytes=32 time=89ms TTL=59

Ping statistics for 201.23.17.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 80ms, Maximum = 3092ms, Average = 836ms

C:\Users\Student>

```

Рисунок 3.31 – Перевірка зв'язку

На маршрутизаторі, ми можемо побачити усі маршрути, що отримав даний маршрутизатор, задля цього необхідно переглянути таблицю маршрутизації

Як приклад візьмемо таблицю маршрутизації із маршрутизатора R-23-17-4

```

R-23-17-4
R-23-17-4#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

    193.23.17.0/24 is variably subnetted, 7 subnets, 3 masks
O       193.23.17.0/30 [110/2] via 193.23.17.13, 00:22:38, FastEthernet1/0
O       193.23.17.4/30 [110/3] via 193.23.17.13, 00:22:38, FastEthernet1/0
O       193.23.17.64/26 [110/2] via 193.23.17.13, 00:22:38, FastEthernet1/0
    194.23.17.0/26 is subnetted, 1 subnets
O       194.23.17.0 [110/2] via 193.23.17.13, 00:22:38, FastEthernet1/0
    195.23.17.0/26 is subnetted, 2 subnets
O       195.23.17.0 [110/3] via 193.23.17.13, 00:22:38, FastEthernet1/0
O       195.23.17.64 [110/3] via 193.23.17.13, 00:22:38, FastEthernet1/0
    199.23.17.0/25 is subnetted, 1 subnets
O       199.23.17.128 [110/13] via 193.23.17.13, 00:22:05, FastEthernet1/0
    201.23.17.0/25 is subnetted, 1 subnets
O       201.23.17.128 [110/2] via 197.23.17.66, 00:12:35, FastEthernet0/0
R-23-17-4#

```

Рисунок 3.32 – Таблиця маршрутизації R-23-17-4

Після цього перевіримо правильність налаштування IPsec VPN. На маршрутизаторах Cisco це можна зробити, скориставшись діагностичною командою *show crypto ipsec sa*, спочатку вона нам виведе кількість запитів що була оброблена до перевірки зв'язку.

```

R-23-17-11#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: CAMP, local addr 197.23.17.66

protected vrf: (none)
local ident (addr/mask/prot/port): (201.23.17.0/255.255.255.128/0/0)
remote ident (addr/mask/prot/port): (198.23.17.0/255.255.255.128/0/0)
current_peer 194.23.17.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 197.23.17.66, remote crypto endpt.: 194.23.17.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x2C35BD5(46357461)
PFS (Y/N): Y, DH group: group14

inbound esp sas:
  spi: 0xAB09397A(2869508474)
  transform: esp-256-aes esp-sha-hmac ,

```

Рисунок 3.33 – Виконання команди *show crypto ipsec sa*

Далі виконуємо команду *ping* між робочими станціями WS-23-17-12 та WS-23-17-1 для перевірки з'єднання

```

WS-23-17-12> ping 198.23.17.109
84 bytes from 198.23.17.109 icmp_seq=1 ttl=60 time=62.967 ms
84 bytes from 198.23.17.109 icmp_seq=2 ttl=60 time=58.064 ms
84 bytes from 198.23.17.109 icmp_seq=3 ttl=60 time=60.681 ms
84 bytes from 198.23.17.109 icmp_seq=4 ttl=60 time=57.056 ms
84 bytes from 198.23.17.109 icmp_seq=5 ttl=60 time=61.494 ms

```

Рисунок 3.34 – Перевірка зв'язку

Тепер ще раз виконуємо діагностичну команду *show crypto ipsec sa*, тепер ми можемо побачити кількість запитів що була оброблена.

```

R-23-17-11#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: CAMP, local addr 197.23.17.66

protected vrf: (none)
local ident (addr/mask/prot/port): (201.23.17.0/255.255.255.128/0/0)
remote ident (addr/mask/prot/port): (198.23.17.0/255.255.255.128/0/0)
current_peer 194.23.17.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps:19, #pkts encrypt:19, #pkts digest: 19
  #pkts decaps:11, #pkts decrypt:11, #pkts verify: 11
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 197.23.17.66, remote crypto endpt.: 194.23.17.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x2C35BD5(46357461)
PFS (Y/N): Y, DH group: group14

inbound esp sas:
  spi: 0xAB09397A(2869508474)
  transform: esp-256-aes esp-sha-hmac ,
  in use settings = {Tunnel, }

```

Рисунок 3.35 – Виконання команди *show crypto ipsec sa*

Для більшої демонстрації на прикладі маршрутизатора R-23-17-4, за допомогою двох діагностичних команд *show crypto map* та *show crypto ipsec transform-set*, ми можемо побачити інформацію про налаштовані криптографічні карти, які

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

відповідають за шифрування даних у VPN та список налаштованих наборів трансформацій для IPsec відповідно.

```
R-23-17-4#show crypto map
Crypto Map IPv4 "CAMP" 2317 ipsec-isakmp
  Peer = 193.23.17.2
  Peer = 193.23.17.5
  Extended IP access list 101
    access-list 101 permit ip 197.23.17.64 0.0.0.63 195.23.17.0 0.0.0.63
    access-list 101 permit ip 197.23.17.64 0.0.0.63 195.23.17.64 0.0.0.63
    access-list 101 permit ip 197.23.17.0 0.0.0.63 195.23.17.0 0.0.0.63
    access-list 101 permit ip 197.23.17.0 0.0.0.63 195.23.17.64 0.0.0.63
    access-list 101 permit ip 196.23.17.64 0.0.0.63 195.23.17.0 0.0.0.63
    access-list 101 permit ip 196.23.17.64 0.0.0.63 195.23.17.64 0.0.0.63
  Current peer: 193.23.17.2
  Security association lifetime: 4608000 kilobytes/900 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): Y
  DH group: group14
  Transform sets={
    50: { esp-256-aes esp-sha-hmac },
  }
  Interfaces using crypto map CAMP:
    FastEthernet1/0
    FastEthernet2/0

R-23-17-4#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac }
  will negotiate = { Transport, },

Transform set 50: { esp-256-aes esp-sha-hmac }
  will negotiate = { Tunnel, },
```

Рисунок 3.36 – Виконання команд *show crypto map* та *show crypto ipsec transform-set* на R-23-17-4

Тепер перевіримо все те саме, але вже на маршрутизаторі від MikroTik. Для цього заходимо на вкладку *Active Peers* та можемо бачити що кількість запитів, яка була оброблена до перевірки зв'язку, дорівнюють нулю.

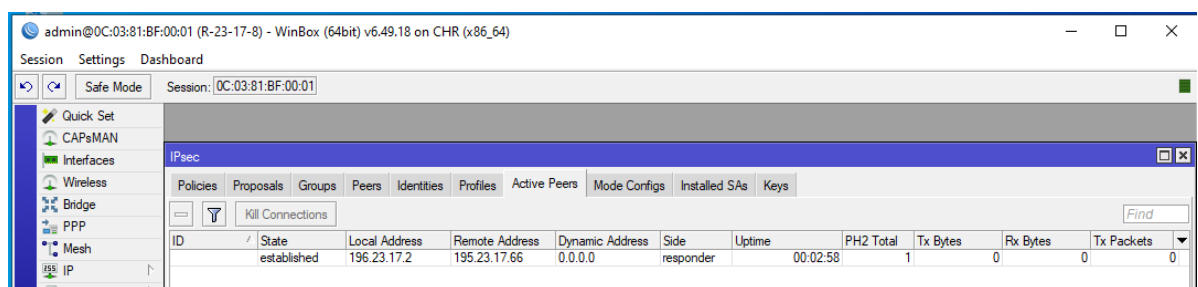


Рисунок 3.37 – Список активних пірів

Для перевірки зв'язку між робочими станціями WS-23-17-8 та WS-23-17-5_Win10 виконуємо команду *trace*.

```
WS-23-17-8> trace 199.23.17.240
trace to 199.23.17.240, 8 hops max, press Ctrl+C to stop
 1 200.23.17.1 1.003 ms 1.030 ms 1.826 ms
 2 195.23.17.66 15.886 ms 22.422 ms 20.544 ms
 3 *199.23.17.240 20.075 ms (ICMP type:3, code:3, Destination port unreachable)
WS-23-17-8>
```

Рисунок 3.38 – Виконання команди *trace*

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

Результат показує, що пакети успішно маршрутизуються від початкової до кінцевої мережі за допомогою IPsec.

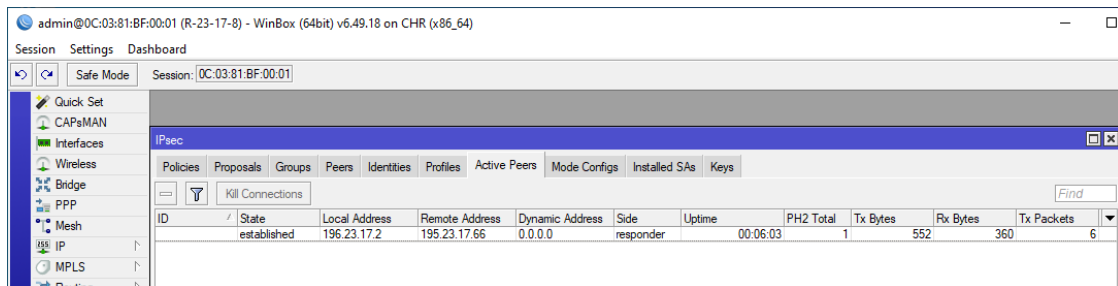


Рисунок 3.39 – Список активних пірів

Також ми можемо бачити зміни в кількості оброблених запитів, а отже IPsec налаштовано правильно та він працює.

Було реалізовано додаткову перевірку на проходження HTTP трафіку з використанням IPsec тунелю. Спочатку на маршрутизаторі R-23-17-8 було піднято HTTP сервер. Після цього, із кінцевої робочої станції на іншій стороні тунелю відбулась спроба підключення до цього серверу.

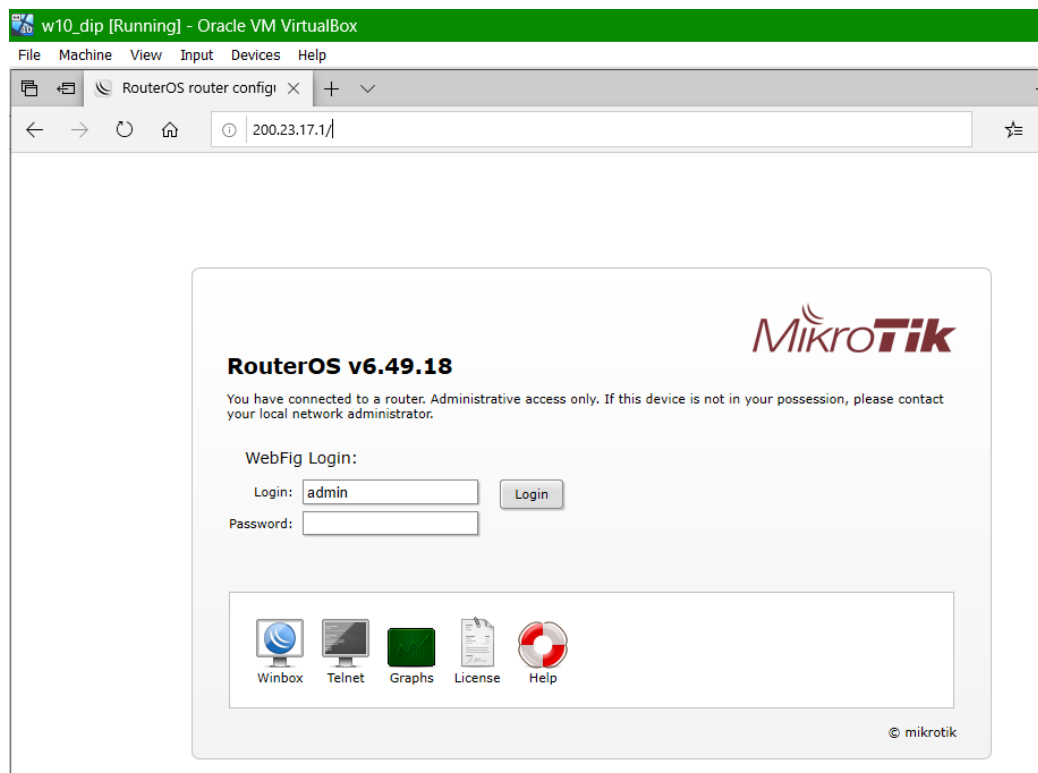


Рисунок 3.40 – Сторінка входу до веб-інтерфейсу маршрутизатора R-23-17-8

Спроба підключення є успішною, а отже HTTP сервер працює. Тепер давайте перевіримо чи змінилась кількість файлів з минулого тестування.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Також, необхідно перевірити систему отримання повідомлень Syslog Server

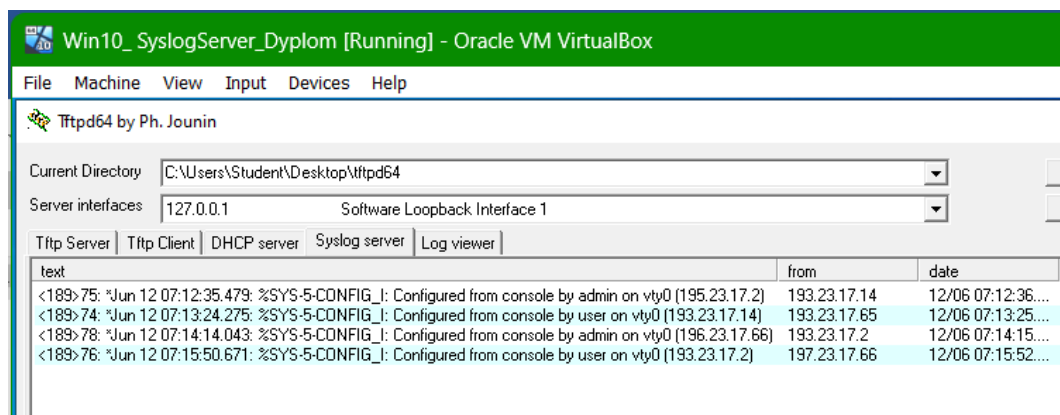


Рисунок 3.44 – Список повідомлень на Syslog Server

На даному рисунку ми можемо побачити по два входи на користувачів admin та user, що були виконані на рисунках вище, отож Syslog Server працює.

Висновки до третього розділу:

У третьому розділі було виконано практичну реалізацію спроектованої мережі, що охоплювало обґрунтований вибір обладнання, його послідовне налаштування та комплексне тестування. Процес побудови мережі розпочався зі статичної IP-адресації інтерфейсів мережевих пристроїв. Для автоматизації конфігурації кінцевих вузлів на маршрутизаторах рівня розподілу було налаштовано сервери DHCP. Повну зв'язність між усіма підмережами забезпечено шляхом впровадження протоколу динамічної маршрутизації OSPF на всіх маршрутизаторах проекту.

Для захисту трафіку між ключовими вузлами було налаштовано IPsec VPN тунелі. Безпечне віддалене адміністрування реалізовано за допомогою протоколу SSHv2. А централізований моніторинг та аналіз подій став можливим завдяки розгортанню Syslog-серверу. На завершальному етапі було проведено тестування, яке підтвердило повну працездатність мережі. Таким чином, усі завдання розділу були виконані, а створена мережа продемонструвала свою працездатність та відповідність вимогам безпеки

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було досягнуто поставленої мети – розроблено та налаштовано проект захищеної гетерогенної мережі з використанням технології VPN. Для досягнення цієї мети було послідовно вирішено наступні завдання, за якими отримано конкретні результати.

Було проведено аналіз сучасних методів безпеки, технологій та протоколів. В результаті було виявлено, що гетерогенні мережі є гнучкими та економічно ефективними. Аналіз технологій VPN показав, що протокол IPsec є надійним та стандартизованим рішенням для шифрування трафіку між мережевими шлюзами, а протокол динамічної маршрутизації OSPF є оптимальним для гетерогенних середовищ завдяки його вендорній незалежності, масштабованості та підтримці автентифікації.

Обґрунтовано вибір мережевого обладнання та технологій захисту. На основі теоретичного аналізу було обрано маршрутизатори Cisco 4321 та MikroTik CCR2216-1G-12XS-2XQ для збалансування продуктивності, надійності та функціональності на різних рівнях мережі, а також комутатори Cisco WS-C2960-24TT-L для рівня доступу. Основними технологіями для побудови мережі були обрані IPsec VPN для захисту даних, OSPF для маршрутизації, DHCP для автоматизації IP-адресації, SSH для безпечного управління та Syslog для моніторингу.

Було розроблено топологію гетерогенної мережі. За основу була взята трирівнева ієрархічна модель Cisco, що забезпечує високу масштабованість, продуктивність та безпеку. Спроектована мережа складається з 19 підмереж, на базі 11 маршрутизаторів та 7 комутаторів. Була розроблена детальна схема IP-адресації для всіх підмереж.

Налаштовано основні мережеві сервіси та протоколи. Було успішно впроваджено сервери DHCP на маршрутизаторах рівня розподілу для автоматичного надання IP-адрес кінцевим пристроям. На всіх маршрутизаторах мережі було налаштовано протокол динамічної маршрутизації OSPF, що забезпечило повну зв'язність між усіма 19 підмережами.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

Сконфігуровано захищений VPN-тунель за допомогою протоколу IPsec. Було створено безпечні Site-to-Site VPN-тунелі між ключовими маршрутизаторами на рівнях ядра та розподілу, що забезпечило шифрування трафіку, який передається між філіями організації, на обладнанні обох виробників — Cisco та MikroTik.

Також було проведено систему моніторингу та збору логів за допомогою Syslog. Було розгорнуто централізований Syslog-сервер та налаштовано всі маршрутизатори мережі на відправку системних повідомлень на цей сервер, що дозволяє здійснювати централізований моніторинг подій та аналізувати стан мережі.

Проведено тестування працездатності та надійності мережі. Результати тестування підтвердили коректну роботу всіх впроваджених сервісів та протоколів. Перевірка показала, що кінцеві пристрої успішно отримують IP-адреси від DHCP, маршрутизація OSPF забезпечує повну зв'язність, IPsec-тунелі коректно шифрують трафік, доступ по SSH є безпечним, а Syslog-сервер отримує повідомлення від усіх пристроїв.

Таким чином, у кваліфікаційній роботі було повністю виконано всі поставлені завдання. В результаті було створено комплексний, функціональний та перевірений на практиці проект захищеної гетерогенної мережі, що поєднує гнучкість, масштабованість та високий рівень безпеки.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вікіпедія Гетерогенні комп'ютерні мережі [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Гетерогенні_комп%27ютерні_ме-режі (Дата звернення 06.06.2025)
2. Максимов М.В. Комп'ютерні мережі : навчальний посібник для студентів закладів середньої професійної освіти / М.В. Максимов, І. І. Попов. - 6-те вид., перераб. і доп. - М.: ФОРУМ :ІНФРАМ, 016. - 464 с. : іл. - (Професійна освіта)
3. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с
4. Що таке VPN? [Електронний ресурс] – Режим доступу: <https://nordvpn.com/uk/what-is-a-vpn/> (Дата звернення 06.06.2025)
5. Вікіпедія VPN [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/VPN> (Дата звернення 06.06.2025)
6. History of the development of VPN [Електронний ресурс] – Режим доступу: <https://mobileproxy.space/en/pages/the-history-of-the-development-of-vpn-services-from-the-beginning-to-the-present-day.html> (Дата звернення 07.06.2025)
7. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. — 256 с
8. Cyberpedia What Is a Remote Access VPN? [Електронний ресурс] – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn> (Дата звернення 07.06.2025)
9. Cyberpedia What Is a Site-to-Site VPN? [Електронний ресурс] – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn> (Дата звернення 07.06.2025)
10. Cyberpedia What Is a Cloud VPN? [Електронний ресурс] – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-vpn> (Дата звернення 08.06.2025)

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

11. Cyberpedia What Is PPTP (Point-to-Point Tunneling Protocol)? [Електронний ресурс] – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-pptp> (Дата звернення 07.06.2025)
12. Cyberpedia What Is IPsec? [Електронний ресурс] – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-ipsec> (Дата звернення 07.06.2025)
13. Cyberpedia What Is OpenVPN? [Електронний ресурс] – Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-openvpn> (Дата звернення 09.06.2025)
14. Вікіпедія OSPF [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/OSPF> (Дата звернення 09.06.2025)
15. Вікіпедія Протокол маршрутизації [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Протокол_маршрутизації (Дата звернення 09.06.2025)
16. Вікіпедія DHCP – Режим доступу: <https://uk.wikipedia.org/wiki/DHCP> (Дата звернення 09.06.2025)
17. Онлайновий навчальний курс NSv1.00: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com (Дата звернення 10.06.2025)
18. Типи протоколів маршрутизації [Електронний ресурс] – Режим доступу: <https://www.guru99.com/uk/routing-protocol-types.html> (Дата звернення 10.06.2025)
19. Open Shortest Path First [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchnetworking/definition/OSPF-Open-Shortest-Path-First> (Дата звернення 10.06.2025)
20. OSPF Overview, History [Електронний ресурс] – Режим доступу: http://www.tcpipguide.com/free/t_OSPFOverviewHistoryStandardsandVersions.htm (Дата звернення 10.06.2025)

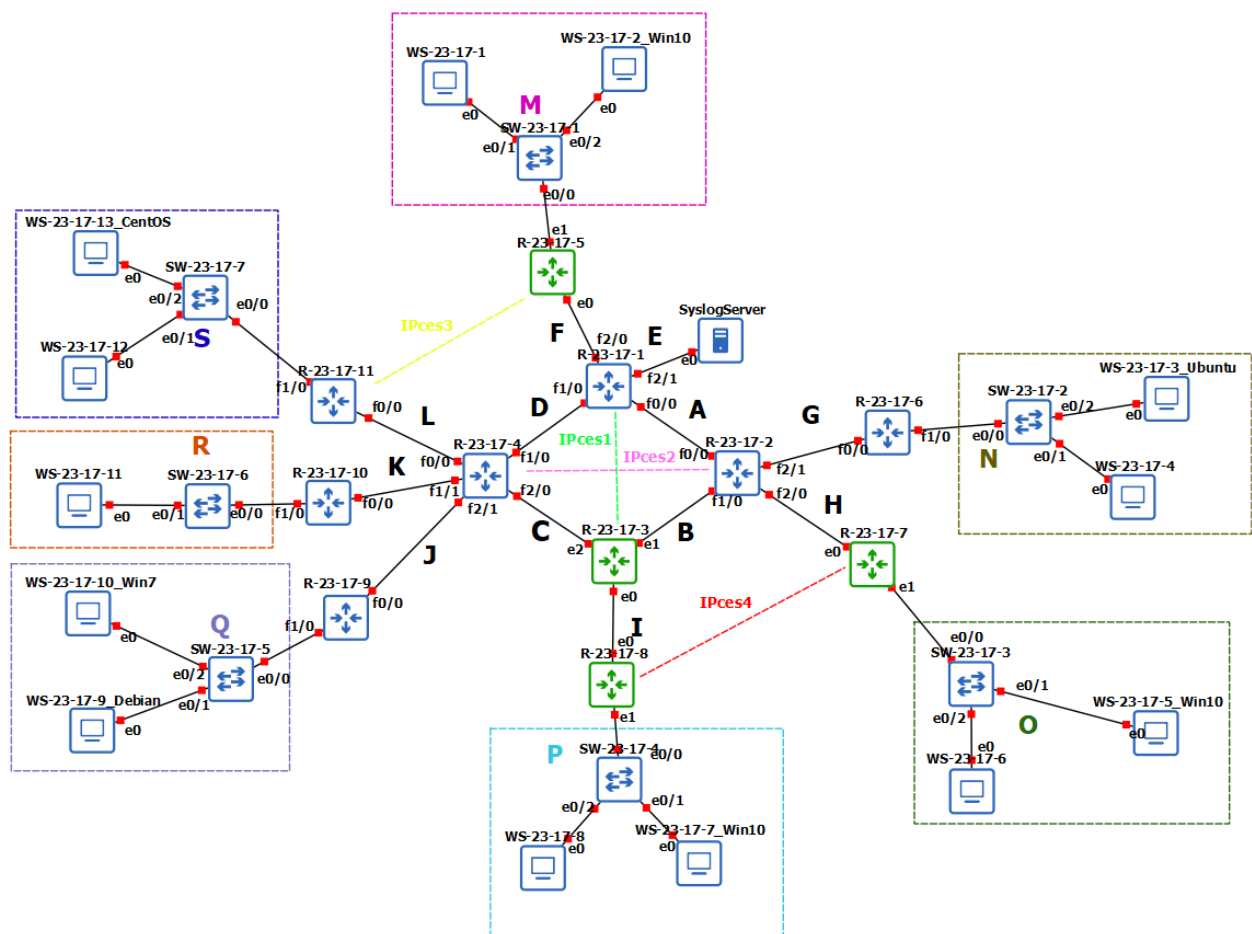
		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

21. What Is a WAN? Wide-Area Network [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html> (Дата звернення 11.06.2025)
22. Illustration of a four-tier HetNet architecture [Електронний ресурс] – Режим доступу: https://www.researchgate.net/figure/Illustration-of-a-four-tier-Het-Net-architecture_fig1_312542790 (Дата звернення 11.06.2025)
23. Introducing data center fabric the next-generation Facebook data center network [Електронний ресурс] – Режим доступу: <https://engineering.fb.com/2014/11/14/production-engineering/introducing-data-center-fabric-the-next-generation-facebook-data-center-network/> (Дата звернення 11.06.2025)
24. Інтернет речей: перспективи розвитку та можливості використання [Електронний ресурс] – Режим доступу: <https://duikt.edu.ua/ua/news-1-0-11324-internet-rechey-perspektivi-rozvitku-ta-mozhливosti-vikoristannya> (Дата звернення 11.06.2025)
25. What is DHCP (Dynamic Host Configuration Protocol)? [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchnetworking/definition/DHCP> (Дата звернення 12.06.2025)
26. Ієрархічна модель мережі [Електронний ресурс] – Режим доступу: <https://old.rci-c.com/technology/yerarkhycheskaia-model-sety/> (Дата звернення 12.06.2025)
27. Що таке DHCP? Простий посібник із розуміння призначення IP-адрес [Електронний ресурс] – Режим доступу: <https://fiberroad.com/uk/resources/glossary/what-is-dhcp/> (Дата звернення 12.06.2025)
28. What is SSH (Secure Shell) and How Does It Work? [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchsecurity/definition/Secure-Shell> (Дата звернення 12.06.2025)
29. What is SSH? [Електронний ресурс] – Режим доступу: <https://www.cloudns.net/blog/what-is-ssh/> (Дата звернення 12.06.2025)

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

ДОДАТКИ

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				84
Змн.	Арк.	№ докум.	Підпис	Дата		



Характеристики маршрутизатора Cisco 4321 ISR

Модель: Cisco 4321 ISR (Integrated Services Router)

Процесор: Модернізований процесор з архітектурою x86

- Ревізія А
- Підтримка до 4 ядер

Пам'ять:

- Оперативна пам'ять: 4096 MB (4 GB), розширюється до 8192 MB (8 GB).
- Пам'ять для програм: 16 GB (розширюється до 32 GB).

Інтерфейси:

- 2 x Gigabit Ethernet (вбудовані).
- Опціонально до 8 портів через модулі NIM.

Слоти для модулів:

- 2 слоти для вставки NIM (Network Interface Modules).
- 1 слот для SM-X (Service Modules).

Пам'ять Flash: 4 GB внутрішня, розширюється до 16 GB.

Підтримувані платформи:

- Cisco ISR 4321

Операційна система:

- Cisco IOS XE Software, версія залежить від ліцензії (наприклад, Cisco IOS XE 17.x).

Версія Bootstrap: Оновлюється залежно від прошивки.

Підтримка криптографічних функцій:

- Захищені протоколи (SSL, IPSec).
- Підтримка VPN з шифруванням AES-256.

Функціональні можливості:

- Високопродуктивна маршрутизація.
- Підтримка VPN (Virtual Private Network).
- Підтримка QoS (Quality of Service) для управління трафіком.
- Підтримка MPLS (Multiprotocol Label Switching).
- Підтримка IPSec (Internet Protocol Security).
- Інтеграція хмарних сервісів.
- Віртуалізація мережевих функцій через Cisco NFV.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

Характеристики маршрутизатора MikroTik CCR2216-1G-12XS-2XQ

Модель: MikroTik CCR2216-1G-12XS-2XQ (Cloud Core Router)

Процесор:

- Модель: AL73400
- Архітектура: ARM 64bit
- Кількість ядер: 16
- Номінальна частота: 2.0 GHz

Пам'ять:

- Оперативна пам'ять: 16 GB DDR4
- Пам'ять для програм (сховище): 128 MB NAND

Інтерфейси:

- 1 x Gigabit Ethernet
- 12 x 25G SFP28
- 2 x 100G QSFP28

Слоти для модулів:

- 2 слоти для M.2 SATA для розширення сховища.

Пам'ять Flash: 128 MB вбудована (тип NAND)

Підтримувані платформи:

- MikroTik Cloud Core Router Series

Операційна система:

- RouterOS v7 (Ліцензія рівня 6)

Версія Bootstrap: Залежить від версії RouterOS та прошивки RouterBOOT.

Підтримка криптографічних функцій:

- Апаратне прискорення IPsec
- Підтримка VPN з шифруванням AES, SHA1, SHA256 та іншими сучасними алгоритмами

Функціональні можливості:

- Високопродуктивна маршрутизація з апаратним розвантаженням L3.
- Підтримка VPN (IPsec, OpenVPN, L2TP, PPTP та ін.).
- Розширені можливості комутації (Switching) з чіпом Marvell Prestera Aldrin2.
- Підтримка QoS для управління пріоритетами трафіку.
- Підтримка MPLS.
- Підтримка BGP, OSPF та інших протоколів динамічної маршрутизації.
- Централізоване управління (CAPsMAN).
- Розширений функціонал брандмауера та фільтрації трафіку.

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

Характеристики комутатора Cisco WS-C2960-24TT-L

Модель: Cisco WS-C2960-24TT-L

Тип: Ethernet комутатор (Switch)

Кількість портів: 24 x 10/100 Mbps Fast Ethernet ports

Порти:

- 24 x 10/100 Mbps RJ-45 Ethernet ports
- x Fixed 10/100/1000BASE-T uplinks (опціонально)

Архітектура комутатора: Non-blocking

Максимальна пропускна здатність: 8.8 Gbps

Пропускна здатність на один порт: до 100 Mbps

Підтримка VLAN: до 255 VLANs одночасно

Пам'ять:

- Динамічна пам'ять для пакетів: 64 MB
- Пам'ять Flash: 32 MB

Розмір таблиці MAC-адрес: 8K

Фізичні характеристики:

- Розмір (Ш x Г x В): 445 x 272 x 44 мм
- Вага: 2.8 кг

Підтримка стандартів:

- IEEE 802.1p CoS (Class of Service)
- IEEE 802.1Q VLAN tagging
- IEEE 802.3af and Cisco prestandard PoE (Power over Ethernet) support

Максимальне витримуване навантаження: до 64 байт пакетів - 6.6 Mpps (мільйонів пакетів в секунду)

Інтерфейси керування:

- Консольний порт RJ-45
- Мережевий порт для керування (Management Port)

Системне програмне забезпечення: Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 15.0(2)SE5

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

R-23-17-1

Current configuration : 3549 bytes

!

upgrade fpd auto

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R-23-17-1

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

logging buffered informational

logging console informational

enable secret 5

\$1\$w/SY\$87Oow7YY5TORVx5fHS7a91

!

no aaa new-model

no ip icmp rate-limit unreachable

!

no ip domain lookup

ip domain name serdiichuk.net

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

username admin privilege 15 secret 5

\$1\$ePsG\$tSPuSf0paeF5O7m4f19n60

username user secret 5

\$1\$olhE\$eo6hn5nR4voXQ8vpPabpZ0

!

redundancy

!

ip tcp synwait-time 5

ip ssh version 2

!

crypto isakmp policy 2317

encr aes 256

authentication pre-share

group 14

lifetime 7200

crypto isakmp key cisco111111 address 193.23.17.6

crypto isakmp key cisco111111 address 193.23.17.9

!

crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac

mode tunnel

!

crypto map CAMP 2317 ipsec-isakmp

set peer 193.23.17.6

set peer 193.23.17.9

set security-association lifetime seconds 900

set transform-set 50

set pfs group14

match address 101

!

interface FastEthernet0/0

ip address 193.23.17.1 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 17 md5 cisco123

duplex half

crypto map CAMP

!

interface FastEthernet1/0

ip address 193.23.17.13 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 17 md5 cisco123

duplex half

speed auto

crypto map CAMP

!

interface FastEthernet1/1

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet2/0

ip address 194.23.17.1 255.255.255.192

ip ospf authentication message-digest

ip ospf message-digest-key 17 md5 cisco123

duplex auto

speed auto

!

interface FastEthernet2/1

ip address 193.23.17.65 255.255.255.192

ip ospf authentication message-digest

ip ospf message-digest-key 17 md5 cisco123

duplex auto

speed auto

!

interface FastEthernet3/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet3/1

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet4/0

no ip address

shutdown

duplex auto

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

```

speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address
shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23171
area 0 authentication message-digest

```

R-23-17-2

```

Current configuration : 3788 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-17-2
!
boot-start-marker
boot-end-marker
!

```

```

network 193.23.17.0 0.0.0.3 area 0
network 193.23.17.12 0.0.0.3 area 0
network 193.23.17.16 0.0.0.3 area 0
network 193.23.17.64 0.0.0.63 area 0
network 194.23.17.0 0.0.0.63 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
access-list 101 permit ip 194.23.17.0 0.0.0.63
196.23.17.0 0.0.0.63
access-list 101 permit ip 193.23.17.64 0.0.0.63
196.23.17.0 0.0.0.63
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
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
transport output ssh
!
end

```

```

!
security passwords min-length 10
logging buffered informational
logging console informational
enable secret 5
$1$JkW3$WEBCMFjqo9S0RLu.XNg/1.
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip domain name serdiichuk.net
ip cef

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		90

```

no ipv6 cef
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 5
$1$zdXq$q1OYgsjexIYbR8C.sBkks1
username user secret 5
$1$mLuJ$uIyhPWLNx4bgdA/dd7U7D.
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
crypto isakmp policy 2317
encr aes 256
authentication pre-share
group 14
lifetime 7200
crypto isakmp key cisco222222 address
193.23.17.14
crypto isakmp key cisco222222 address
193.23.17.10
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-
hmac
mode tunnel
!
crypto map CAMP 2317 ipsec-isakmp
set peer 193.23.17.14
set peer 193.23.17.10
set security-association lifetime seconds 900
set transform-set 50
set pfs group14
match address 101
!
interface FastEthernet0/0
ip address 193.23.17.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
crypto map CAMP
!
interface FastEthernet1/0
ip address 193.23.17.5 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
speed auto
crypto map CAMP
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!

```

```

interface FastEthernet2/0
ip address 195.23.17.65 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex auto
speed auto
!
interface FastEthernet2/1
ip address 195.23.17.1 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		91

```

shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23172
area 0 authentication message-digest
network 193.23.17.0 0.0.0.3 area 0
network 193.23.17.4 0.0.0.3 area 0
network 195.23.17.0 0.0.0.3 area 0
network 195.23.17.64 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
access-list 101 permit ip 195.23.17.0 0.0.0.63
197.23.17.64 0.0.0.63
access-list 101 permit ip 195.23.17.64 0.0.0.63
197.23.17.64 0.0.0.63
access-list 101 permit ip 195.23.17.0 0.0.0.63
197.23.17.0 0.0.0.63

```

```

access-list 101 permit ip 195.23.17.64 0.0.0.63
197.23.17.0 0.0.0.63
access-list 101 permit ip 195.23.17.0 0.0.0.63
196.23.17.64 0.0.0.63
access-list 101 permit ip 195.23.17.64 0.0.0.63
196.23.17.64 0.0.0.63
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
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
transport output ssh
!
end

```

R-23-17-3

```

# jun/12/2025 03:32:36 by RouterOS 6.49.18
# software id =
#
#
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 lifetime=4w2d name=\
ike1-profile-camp
/ip ipsec peer
add address=193.23.17.13/32 local-address=193.23.17.9 name=peer-193.23.17.13 \
profile=ike1-profile-camp
add address=193.23.17.1/32 local-address=193.23.17.6 name=peer-193.23.17.1 \
profile=ike1-profile-camp
/ip ipsec proposal
add enc-algorithms=aes-256-cbc lifetime=15m name=ts50-camp pfs-group=modp2048
/routing ospf area
set [ find default=yes ] name="area 0"
/routing ospf instance
set [ find default=yes ] router-id=196.23.17.1
/system logging action
add name=remoteloghost remote=193.23.17.70 target=remote

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

```

/ip address
add address=196.23.17.1/26 interface=ether1 network=196.23.17.0
add address=193.23.17.6/30 interface=ether2 network=193.23.17.4
add address=193.23.17.9/30 interface=ether3 network=193.23.17.8
/ip dhcp-client
add disabled=no interface=ether1
/ip dns
set servers=8.8.8.8
/ip ipsec identity
add peer=peer-193.23.17.13 secret=cisco111111
add peer=peer-193.23.17.1 secret=cisco111111
/ip ipsec policy
add dst-address=194.23.17.0/26 peer=peer-193.23.17.13 proposal=ts50-camp \
src-address=196.23.17.0/26 tunnel=yes
add dst-address=193.23.17.64/26 peer=peer-193.23.17.1 proposal=ts50-camp \
src-address=196.23.17.0/26 tunnel=yes
/ip service
set telnet disabled=yes
set www disabled=yes
/routing ospf interface
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
interface=ether1
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
interface=ether2
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
interface=ether3
/routing ospf network
add area="area 0" network=196.23.17.0/26
add area="area 0" network=193.23.17.4/30
add area="area 0" network=193.23.17.8/30
/system identity
set name=R-23-17-3
/system logging
add action=remoteloghost topics=info

```

R-23-17-4

Current configuration : 3976 bytes	!
!	no ip domain lookup
upgrade fpd auto	ip domain name serdiichuk.net
version 15.2	ip cef
service timestamps debug datetime msec	no ipv6 cef
service timestamps log datetime msec	!
no service password-encryption	multilink bundle-name authenticated
!	!
hostname R-23-17-4	username admin privilege 15 secret 5
!	\$1\$vVkh\$wLtVHIViGkYN1TL8LIxLf1
boot-start-marker	username user secret 5
boot-end-marker	\$1\$GGWP\$4sotf54EsQLCFIcwMxFWl/
!	!
security passwords min-length 10	redundancy
logging buffered informational	!
logging console informational	ip tcp synwait-time 5
enable secret 5	ip ssh version 2
\$1\$KELk\$X1TmPvBuhqcOvhkKWyStA1	!
!	crypto isakmp policy 2317
no aaa new-model	encr aes 256
no ip icmp rate-limit unreachable	authentication pre-share

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

```

group 14
lifetime 7200
crypto isakmp key cisco222222 address 193.23.17.2
crypto isakmp key cisco222222 address 193.23.17.5
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-
hmac
mode tunnel
!
crypto map CAMP 2317 ipsec-isakmp
set peer 193.23.17.2
set peer 193.23.17.5
set security-association lifetime seconds 900
set transform-set 50
set pfs group14
match address 101
!
interface FastEthernet0/0
ip address 197.23.17.65 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
!
interface FastEthernet1/0
ip address 193.23.17.14 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex auto
speed auto
crypto map CAMP
!
interface FastEthernet1/1
ip address 197.23.17.1 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 193.23.17.10 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex auto
speed auto
crypto map CAMP
!
interface FastEthernet2/1
ip address 196.23.17.65 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto

```

```

speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address
shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23174
area 0 authentication message-digest
network 193.23.17.8 0.0.0.3 area 0
network 193.23.17.12 0.0.0.3 area 0
network 196.23.17.64 0.0.0.63 area 0

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

```

network 197.23.17.0 0.0.0.63 area 0
network 197.23.17.64 0.0.0.63 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
access-list 101 permit ip 197.23.17.64 0.0.0.63
195.23.17.0 0.0.0.63
access-list 101 permit ip 197.23.17.64 0.0.0.63
195.23.17.64 0.0.0.63
access-list 101 permit ip 197.23.17.0 0.0.0.63
195.23.17.0 0.0.0.63
access-list 101 permit ip 197.23.17.0 0.0.0.63
195.23.17.64 0.0.0.63
access-list 101 permit ip 196.23.17.64 0.0.0.63
195.23.17.0 0.0.0.63
access-list 101 permit ip 196.23.17.64 0.0.0.63
195.23.17.64 0.0.0.63
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
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
transport output ssh
line vty 5 15
login local
transport input all
!
end

```

R-23-17-5

```

# jun/12/2025 03:42:55 by RouterOS 6.49.18
# software id =
#
#
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 lifetime=2h name=\
ike1-profile-camp
/ip ipsec peer
add address=197.23.17.66/32 local-address=194.23.17.2 name=peer-197.23.17.66 \
profile=ike1-profile-camp
/ip ipsec proposal
add enc-algorithms=aes-256-cbc lifetime=15m name=proposal-camp pfs-group=\
modp2048
/ip pool
add name=network-m-pool ranges=198.23.17.12-198.23.17.112
/ip dhcp-server
add address-pool=network-m-pool disabled=no interface=ether2 lease-time=4w2d \
name=dhcp1
/routing ospf area
set [ find default=yes ] name=area0
/system logging action
add name=remotelog remote=193.23.17.70 target=remote
/ip address
add address=194.23.17.2/26 interface=ether1 network=194.23.17.0
add address=198.23.17.1/25 interface=ether2 network=198.23.17.0
/ip dhcp-client
add disabled=no interface=ether1

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

```

/ip dhcp-server network
add address=198.23.17.0/25 gateway=198.23.17.1
/ip dns
set servers=8.8.8.8,8.8.4.4
/ip ipsec identity
add comment="Key for peer 197.23.17.66" peer=peer-197.23.17.66 secret=\
    cisco333333
/ip ipsec policy
add dst-address=201.23.17.0/25 peer=peer-197.23.17.66 proposal=proposal-camp \
    src-address=198.23.17.0/25 tunnel=yes
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
/ip ssh
set host-key-size=1024 strong-crypto=yes
/routing ospf interface
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
    interface=ether1
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
    interface=ether2
/routing ospf network
add area=area0 network=194.23.17.0/26
add area=area0 network=198.23.17.0/25
/system identity
set name=R-23-17-5
/system logging
add topics=info
add action=remotelog topics=info

```

R-23-17-6

```

Current configuration : 2830 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-17-6
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging buffered informational
logging console informational
enable secret 5
$1$p9Ao$qGlsP8F7/ZvVLbDPN3fRE1
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 199.23.17.1 199.23.17.11
ip dhcp excluded-address 199.23.17.113
199.23.17.126

```

```

!
ip dhcp pool NETWORK-N
network 199.23.17.0 255.255.255.128
default-router 199.23.17.1
dns-server 8.8.8.8 8.8.4.4
lease 7
!
no ip domain lookup
ip domain name serdiichuk.net
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
username user secret 5
$1$hbs4$xwFP8dUUUCubgGuTpyr.Y0
username admin privilege 15 secret 5
$1$PuZI$tyoS9fsJniTqw958bxZlp/
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
interface FastEthernet0/0

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

```

ip address 195.23.17.2 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
!
interface FastEthernet1/0
ip address 199.23.17.1 255.255.255.128
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown

```

```

duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address
shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23172
area 0 authentication message-digest
network 195.23.17.0 0.0.0.63 area 0
network 199.23.17.0 0.0.0.127 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

```

stopbits 1
line vty 0 4
login local
transport input ssh

transport output ssh
!
end

```

R-23-17-7

```

# jun/12/2025 03:26:40 by RouterOS 6.49.18
# software id =
#
#
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 lifetime=2h name=\
ike1-profile-camp
/ip ipsec peer
add address=196.23.17.2/32 local-address=195.23.17.66 name=peer-196.23.17.2 \
profile=ike1-profile-camp
/ip ipsec proposal
add enc-algorithms=aes-256-cbc,aes-128-cbc lifetime=15m name=ts50-camp \
pfs-group=modp2048
/ip pool
add name=NETWORK-O-pool ranges=199.23.17.140-199.23.17.240
/ip dhcp-server
add address-pool=NETWORK-O-pool disabled=no interface=ether2 lease-time=\
2w1d10h10m name=dhcp1
/routing ospf area
set [ find default=yes ] name="area 0"
/routing ospf instance
set [ find default=yes ] router-id=195.23.17.66
/system logging action
add name=remoteloghost remote=193.23.17.70 target=remote
/ip address
add address=195.23.17.66/26 interface=ether1 network=195.23.17.64
add address=199.23.17.129/25 interface=ether2 network=199.23.17.128
/ip dhcp-client
add disabled=no interface=ether1
/ip dhcp-server network
add address=199.23.17.128/25 dns-server=8.8.8.8,8.8.4.4 gateway=199.23.17.129
/ip dns
set servers=8.8.8.8
/ip ipsec identity
add peer=peer-196.23.17.2 secret=cisco444444
/ip ipsec policy
add dst-address=200.23.17.0/25 peer=peer-196.23.17.2 proposal=ts50-camp \
src-address=199.23.17.128/25 tunnel=yes
/ip service
set telnet disabled=yes
set www disabled=yes
/routing ospf interface
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
interface=ether1
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
interface=ether2
/routing ospf network

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		98

```
add area="area 0" network=195.23.17.64/26
add area="area 0" network=199.23.17.128/25
/system identity
set name=R-23-17-7
/system logging
add action=remoteloghost topics=info
```

R-23-17-8

```
# jun/12/2025 03:27:02 by RouterOS 6.49.18
# software id =
#
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 name=ike1-profile-camp
/ip ipsec peer
add address=195.23.17.66/32 local-address=196.23.17.2 name=peer-195.23.17.66 \
    profile=ike1-profile-camp
/ip ipsec proposal
add enc-algorithms=aes-256-cbc lifetime=15m name=ts50-camp pfs-group=modp2048
/ip pool
add name=NETWORK-P-pool ranges=200.23.17.12-200.23.17.112
/ip dhcp-server
add address-pool=NETWORK-P-pool disabled=no interface=ether2 lease-time=\
    2w1d10h10m name=dhcp1
/routing ospf area
set [ find default=yes ] name="area 0"
/routing ospf instance
set [ find default=yes ] router-id=196.23.17.2
/system logging action
add name=remoteloghost remote=193.23.17.70 target=remote
/ip address
add address=196.23.17.2/26 interface=ether1 network=196.23.17.0
add address=200.23.17.1/25 interface=ether2 network=200.23.17.0
/ip dhcp-client
add disabled=no interface=ether1
/ip dhcp-server network
add address=200.23.17.0/25 dns-server=8.8.8.8,8.8.4.4 gateway=200.23.17.1
/ip ipsec identity
add peer=peer-195.23.17.66 secret=cisco444444
/ip ipsec policy
add dst-address=199.23.17.128/25 peer=peer-195.23.17.66 proposal=ts50-camp \
    src-address=200.23.17.0/25 tunnel=yes
/ip service
set telnet disabled=yes
set www disabled=yes
/routing ospf interface
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
    interface=ether1
add authentication=md5 authentication-key=cisco123 authentication-key-id=17 \
    interface=ether2
/routing ospf network
add area="area 0" network=196.23.17.0/26
add area="area 0" network=200.23.17.0/25
/system identity
```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		99

```

set name=R-23-17-8
/system logging
add action=remoteloghost topics=info

```

R-23-17-9

```

Current configuration : 2829 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-17-9
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging buffered informational
logging console informational
enable secret 5 $1$dnwP$Dki9NA-
HAdJTKUVv54UZuC/
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 200.23.17.129
ip dhcp excluded-address 200.23.17.241
200.23.17.254
!
ip dhcp pool NETWORK-Q
network 200.23.17.128 255.255.255.128
default-router 200.23.17.129
dns-server 8.8.8.8 8.8.4.4
lease 7
!
no ip domain lookup
ip domain name serdiichuk.net
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
username user secret 5 $1$2vSy$lpBwkfsL-
tONsCvh64HUod.
username admin privilege 15 secret 5
$1$1gNi$SkC3nxqS2tmdN.rQCRpaHk0
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
interface FastEthernet0/0
ip address 196.23.17.66 255.255.255.192
ip ospf authentication message-digest

```

```

ip ospf message-digest-key 17 md5 cisco123
duplex full
!
interface FastEthernet1/0
ip address 200.23.17.129 255.255.255.128
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex full
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		100

```

interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address
shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23174
area 0 authentication message-digest

```

R-23-17-10

```

Current configuration : 2831 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-17-10
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging buffered informational
logging console informational
enable secret 5 $1$TaHK$wJAe-
nAhHj2jYnPzPgL2h2/
!
no aaa new-model
no ip icmp rate-limit unreachable

```

```

network 196.23.17.64 0.0.0.63 area 0
network 200.23.17.128 0.0.0.127 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
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
transport output ssh
!
end

```

```

!
ip dhcp excluded-address 201.23.17.1 201.23.17.11
ip dhcp excluded-address 201.23.17.113
201.23.17.126
!
ip dhcp pool NETWORK-R
network 201.23.17.0 255.255.255.128
default-router 201.23.17.1
dns-server 8.8.8.8 8.8.4.4
lease 7
!
no ip domain lookup
ip domain name serdiichuk.net
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
username user secret 5
$1$7Mab$qR0bVH9LiEmvwg0e/nQ6v/

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		101

```

username admin privilege 15 secret 5
$1$rWS4$y82bQ3XUZ6BZRelgflM/C/
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
interface FastEthernet0/0
ip address 197.23.17.2 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
!
interface FastEthernet1/0
ip address 201.23.17.1 255.255.255.128
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!

```

```

interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address
shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23174
area 0 authentication message-digest
network 197.23.17.0 0.0.0.63 area 0
network 201.23.17.0 0.0.0.127 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
shutdown
!

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		102

```

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15

```

R-23-17-11

```

Current configuration : 3327 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-23-17-11
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging buffered informational
logging console informational
enable secret 5
$1$VOJV$IVflfWbR.WviQYN826NYT1
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 201.23.17.129
201.23.17.139
ip dhcp excluded-address 201.23.17.241
201.23.17.254
!
ip dhcp pool NETWORK-S
network 201.23.17.128 255.255.255.128
default-router 201.23.17.129
dns-server 8.8.8.8 8.8.4.4
lease 7
!
no ip domain lookup
ip domain name serdiichuk.net
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 5
$1$5GLA$CkVqy6ZEoYmCcP1v3WqFX1
username user secret 5 $1$15Kx$ejHmj4gjA-
OUoDLIK77KAh1
!
redundancy
!

```

```

logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
transport output ssh
!
end

```

```

ip tcp synwait-time 5
ip ssh version 2
!
crypto isakmp policy 2317
encr aes 256
authentication pre-share
group 14
lifetime 7200
crypto isakmp key cisco333333 address 194.23.17.2
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-
hmac
mode tunnel
!
crypto map CAMP 2317 ipsec-isakmp
set peer 194.23.17.2
set security-association lifetime seconds 900
set transform-set 50
set pfs group14
match address 101
!
interface FastEthernet0/0
ip address 197.23.17.66 255.255.255.192
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
crypto map CAMP
!
interface FastEthernet1/0
ip address 201.23.17.129 255.255.255.128
ip ospf authentication message-digest
ip ospf message-digest-key 17 md5 cisco123
duplex half
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		103

```

interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Ethernet6/0
no ip address
shutdown
duplex half
!
interface Ethernet6/1
no ip address
shutdown
duplex half
!
interface Ethernet6/2
no ip address
shutdown
duplex half
!
interface Ethernet6/3
no ip address
shutdown
duplex half
!
router ospf 23174
area 0 authentication message-digest
network 197.23.17.64 0.0.0.63 area 0
network 201.23.17.128 0.0.0.127 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging host 193.23.17.70
access-list 101 permit ip 201.23.17.0 0.0.0.127
198.23.17.0 0.0.0.127
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
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
transport output ssh
!
!
end

```

		Сердійчук І.С.			ККІКБ.КР.Б – 125 – 17 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		104