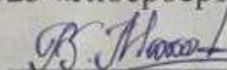


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект серверної інфраструктури автентифі-
кації, авторизації та обліку сервісів на основі протоколу
Diameter»

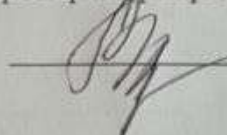
Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Богдан ГЕРАСИМЕНКО

Керівник старший викладач кафедри КІ та КБ

 Ігор ФАЛЬКОВСЬКИЙ

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

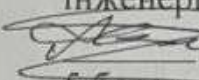
 Володимир ВОРОТНИКОВ

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Герасименко Богдан Миколайович

Тема роботи: Проект серверної інфраструктури автентифікації, авторизації та обліку сервісів на основі протоколу Diameter

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

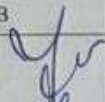
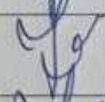
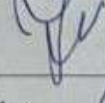
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

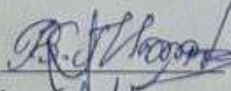
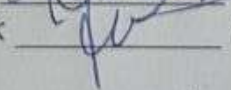
1. Побудова серверної інфраструктури AAA
2. Протокол Diameter

Обладнання та програмне забезпечення:

3. Операційні системи Windows 7, XP, Kali Linux, Ubuntu, Cisco IOS
4. Маршрутизатор Cisco ISR 1100 8P, комутатор Cisco CBS350-24P-4G.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор ФАЛЬКОВСЬКИЙ	12.03.2024 	12.03.2024
2	Ігор ФАЛЬКОВСЬКИЙ	16.04.2024 	16.04.2024
3	Ігор ФАЛЬКОВСЬКИЙ	17.05.2024 	17.05.2024

Студент  Богдан ГЕРАСИМЕНКО
Керівник  Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05 березня 2022	Виконано
2	Пошук інформації для реалізації серверної інфраструктури	12 березня 2024 – 17 березня 2024	Виконано
3	Аналіз технології	03 квітня 2024 – 15 квітня 2024	Виконано
4	Підбір та проектування топології мережі	18 квітня 2024 – 22 квітня 2024	Виконано
5	Розробка IP-адресації та вибір обладнання	28 квітня 2024 – 5 травня 2024	Виконано
6	Налаштування пристроїв мережі	15 травня 2024 – 21 травня 2024	Виконано
7	Тестування на проникнення	23 травня 2024 – 26 травня 2024	Виконано
8	Друк пояснювальної записки	27 травня 2024 – 2 черня 2024	Виконано
9	Підготовка додаткових матеріалів	4 червня 2024 – 6 червня 2024	Виконано
10	Отримання відгуку та рецензії на кваліфікаційну роботу	6 червня 2024 – 7 червня	Виконано
11	Захист кваліфікаційної роботи	9 червня 2024	Виконано

Студент Богдан ГЕРАСИМЕНКО

Керівник Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Кваліфікаційна робота містить опис та приклад реалізації проєкту серверної інфраструктури автентифікації, авторизації та обліку сервісів на основі протоколу Diameter. Пояснювальна записка складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 57 сторінках друкованого тексту. Пояснювальна записка має 8 сторінок додатків. В роботі наведено 50 рисунків та 4 таблиці. Загальний обсяг роботи – 70 сторінок

Метою роботи є розробка проєкту серверної інфраструктури автентифікації, авторизації та обліку сервісів на основі протоколу Diameter.

У ході роботи було спроектовано серверну інфраструктуру автентифікації, авторизації та обліку сервісів на основі протоколу Diameter. Також, досліджено особливості функціонування та захисту протоколів AAA. Описано роботу, функціонування протоколів AAA. Розглянуто основи, принцип роботи та побудови серверних інфраструктур.

Ключові слова: МЕРЕЖА, СЕРВЕР, ІНФРАСТРУКТУРА, ПРОТОКОЛ, АДМІНІСТРУВАННЯ, АУТЕНТИФІКАЦІЯ, АУТОРИЗАЦІЯ, ОБЛІК, КОРИСТУВАЧ, ЗАГРОЗА, МОНІТОРИНГ, DIAMETER, RADIUS, AAA.

ККІК.КР.Б – 125 – 02 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата
Розроб.		Герасименко Б. М.		28.08.2024
Керівник		Фальковський І. Г.		28.08.2024
Реценз.		Воротніков В. В.		28.08.2024
Н. контр.		Фальковський І. Г.		28.08.2024
Затверд.		Сфіменко А. А.		28.08.2024

Проект серверної інфраструктури автентифікації, авторизації та обліку сервісів на основі протоколу Diameter

Лім.	Арк.	Аркушів
	4	70

ФІКТ, Гр. КБ-20-1

ANNOTATION

The qualification of the robot describes the application of the implementation of the server infrastructure project for authentication, authorization and the scope of services based on the Diameter protocol. The explanatory note consists of an introduction, three sections, chapters, a list of references and supplements. The text part is published on 57 pages of the original text. The explanatory note contains 8 pages of supplements. The robot contains 50 drawings and 4 tables. Zagalny obsyag roboti – 70 pages

The method of work is the development of a server infrastructure project for authentication, authorization and a range of services based on the Diameter protocol.

During the work, a server infrastructure for authentication, authorization and a range of services based on the Diameter protocol was designed. Also, the peculiarities of the functioning and protection of AAA protocols were investigated. The robot and the functioning of the AAA protocols are described. The fundamentals and principles of operation and operation of server infrastructures are reviewed.

Keywords: MEREZHA, SERVER, INFRASTRUCTURE, PROTOCOL, ADMINISTRATION, AUTHENTICATION, AUTHORIZATION, OBLIK, KORI-STUVACH, THREAT, MONITORING, DIAMETER, RADIUS, AAA.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРИТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ СЕРВІСІВ НА ОСНОВІ ПРОТОКОЛУ DIAMETER	10
1.1 Принцип побудови та основи функціонування протоколів AAA	10
1.2 Зворотня сторона проблем протоколу.	11
1.3 AAA (Аутентифікація, Авторизація, Облік)	12
1.4 Принцип роботи серверної інфраструктури	14
1.5 Функціонал та застосування протоколу RADIUS у комп'ютерних мережах	15
1.6 Основи, принцип роботи та побудови протоколу DIAMETER.	18
1.7 Спільна робота серверів Diameter з серверами Radius та порівняння роботи серверів.	23
1.8 Нововведення у роботі протоколу Diameter	27
РОЗДІЛ 2. ПРОЄКТУВАННЯ МЕРЕЖІ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ СЕРВІСІВ НА ОСНОВІ ПРОТОКОЛУ DIAMETER.....	32
2.1 Проєктування мережі серверної інфраструктури	32
2.2 Аналіз інфраструктури системи моніторингу мережі	35
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПРОЄКТУ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ СЕРВІСІВ НА ОСНОВІ ПРОТОКОЛУ DIAMETER	36
3.1 Підбір мережного обладнання	36
3.2 Налаштування комп'ютерної мережі серверної інфраструктури.....	39
3.3 Встановлення та налаштування серверної інфраструктури Diameter.	47
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	57
ДОДАТКИ.....	58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

AAA – Authentication, Authorization, Accounting

IP – Internet Protocol

ПК – Персональний комп'ютер

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

Wi-Fi – Wireless Fidelity

PAP – Password Authentication Protocol

CHAP – Challenge Handshake Authentication Protocol

EAP – Extended Protocol Authentication

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

RADIUS – Remote Access Dial-In User Service

NAS – Network Attached Storage

IETF – Internet Engineering Task Force

RAP – Resource Allocation Protocol

WG – Work Group

HTTP – HyperText Transfer Protocol

ROAMOPS – Roaming Operations Task Force

SCTP – Stream-Control Transmission-Protocol

TLS – Transport Layer Security

IPsec – Internet Protocol Security

OCS – Open Conference System

PCRF – Policy and Charging Rules Function

IMS – Internet Protocol Multimedia Subsystem

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сучасні комп'ютерні мережі часто піддаються впливу зловмисників з метою отримання конфіденційної чи комерційної інформації, облікових даних користувачів, несанкціонованого доступу до обладнання. Багато компаній та постачальників послуг зв'язку для запобігання вищевказаних небезпек розгортають сервіси AAA (Authentication, Authorization, Accounting) на основі своєї мережевої інфраструктури.

Автентифікація – це процес визначення персони та співставлення інформації облікового запису у системі безпеки.

Авторизація – це процес співставлення визначеної персони з дозволеними повноваженнями (перевірка рівня доступу).

Облік – це процес журналювання дій користувача, що пройшов автентифікацію та авторизацію.

Для впровадження архітектури AAA існує декілька протоколів: TACACS, TACACS+, XTACACS, RADIUS та Diameter. На сьогодні, найпопулярнішим та найпоширенішим є протокол RADIUS (Remote Access Dial-In User Service). Але оскільки RADIUS має велику кількість системних недоліків, то як логічне продовження, що усуває частину проблем, було розроблено AAA протокол Diameter.

Метою кваліфікаційної роботи є проєктування серверної інфраструктури автентифікації, авторизації та обліку сервісів на основі протоколу Diameter

Визначена мета обумовлює наступні завдання:

- дослідження та порівняння технологій автентифікації, авторизації та обліку сервісів;
- розробка інфраструктури мережевої автентифікації, авторизації та обліку сервісів;
- тестування та налаштування віртуальної мережі;
- перевірка коректної працездатності та стійкості серверної інфраструктури.

Об'єктом дослідження є процес розробки серверної інфраструктури на основі протоколу Diameter.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Предметом дослідження є протокол серверної автентифікації, авторизації та обліку Diameter, порівняння протоколу Diameter з протоколом RADIUS, питання практичного застосування протоколу в локальних та глобальних мережах організацій, а також можливості застосування протоколу з метою проведення моніторингу користувачів мережі.

У процесі виконання кваліфікаційної роботи було розроблено проєкт серверної інфраструктури автентифікації, авторизації та обліку сервісів на основі протоколу Diameter, досліджено роботу протоколу на фізичному рівні, протестований функціонал та стійкість роботи.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРИТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ СЕРВІСІВ НА ОСНОВІ ПРОТОКОЛУ DIAMETER

1.1 Принцип побудови та основи функціонування протоколів AAA

Оскільки за останні роки кількість нових послуг в мережі Інтернет стрімко зросла маршрутизатори та сервери доступу до мережі (NAS) необхідно постійно оновлювати, щоб впоратися з великою кількістю даних, що проходять через мережеве обладнання. Більшість цих нових служб потребують контролю. Протокол автентифікації, авторизації та обліку (AAA) для полегшення політики навантаження на зовнішній сервер.

Оскільки інтернет-провайдери не хочуть брати на себе масштабний адміністративний тягар переналаштування всіх своїх користувачів кожного разу, коли обладнання NAS оновлюється. З метою уникнення проблем, інтернет-провайдери дуже успішно використовують різні протоколи AAA, наприклад Kerberos, TACACS і RADIUS (Remote Access Dial-In User Service), внаслідок цього протоколи AAA широко використовуються сьогодні на ринку.

Історично склалося так, що протокол RADIUS використовувався для надання послуг AAA для комутованого з'єднання PPP (протокол «точка-точка») і доступу до термінальних серверів. Згодом маршрутизатори і сервери доступу до мережі (NAS) зросли за складністю та щільністю. І деякі послуги протоколу RADIUS стають все більш непридатними для використання в сучасних мережах.

Послуги передачі голосових повідомлень через IP, факс через IP, мобільний IP і RAP втрачають свою актуальність в сучасній інфраструктурі комп'ютерних мереж.

Поточна тенденція стосується кожної робочої групи IETF (голос через IP, факс через IP, мобільний IP і RAP), щоб визначити власний протокол політики для конкретної служби, кожна зі своїми власні нюанси. Це вимагає від клієнтів розгортання кількох серверів політик, які збільшують витрати на адміністрування та ускладнює роботу мережі.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Останнім часом у рамках IETF значна увага приділяється необхідності покращення структурувати інформацію, яка передається в протоколах, що працюють в межах доступу до мережі. Перевагою структурованої інформації є послідовність у визначенні та повторне використання окремих елементів даних. Чітко визначені засоби для розширення існуючих структур для підтримки нових або власних функцій і можливостей.

Протокол Діаметр (Diameter) – це загальне рішення для зазначених вище сценаріїв і потреб визначення базового протоколу, який визначає формати заголовків, розширення безпеки та вимоги, а також невелика кількість обов'язкових команд і AVP. Всі нові служби мають можливість розширювати Diameter шляхом додавання програм розширення базового протоколу для підтримки нових функцій. Це дозволяє кожній робочій групі в рамках IETF для використання Diameter додавати свою нову необхідну, спеціальну функцію.

1.2 Зворотня сторона проблем протоколу.

Сьогодні протокол Radius є провідним протоколом AAA на ринку. Головна причина використання RADIUS полягає в тому, що протокол забезпечує автентифікацію, авторизацію та облік в середовищі розподіленої, комутованої мережі (PPP). Нові послуги та області використання, які можуть отримати користь від використання протоколу AAA, збільшилася майже експоненціально за останні роки. Зі збільшенням користувачів технології почали виникати проблеми та обмеження протоколів AAA. З деякими послугами доцільність від підтримки деяких протоколів AAA в сучасних реаліях стає марною.

Розробка нового відкритого стандарту під назвою Diameter для охоплення нових послуг і областей використання. Головною метою реалізації протоколу Diameter є його популяризація та поширення в компаніях по всьому світу. Сьогодні використання RADIUS або його конкурентних протоколів – це лише невелика частина доступних функціональних можливостей, що потребують удосконалення з адаптацією до нових послуг на ринку. Тож менеджери у великих компаніях бачать

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

недоліки сьогоденішніх протоколів і намагаються вирішити, чи хочуть вони оновити до наступних поколінь протоколи AAA або просто спробувати виправити недоліки.

Сьогодні все вказує на те, що ми рухаємося до бездротової спільноти з появою Mobile IP та широкого застосування безпроводних (Wi-Fi) мереж все більше провайдерів побачити переваги їхнього протоколу AAA, здатного взаємодіяти з протоколами бездротової передачі інформації.

1.3 AAA (Аутентифікація, Авторизація, Облік)

Інтернет – це небезпечне місце. Багато протоколів, які використовуються в мережі Інтернеті не завжди здатні забезпечити повноцінну безпеку своїх систем. Інструменти для несанкціонованого отримання паролів у мережі є базовими навичками зловмисників (хакерів). Таким чином, програми, які надсилають незашифрований пароль через мережу, є надзвичайно вразливими. Що ще гірше, клієнт, сервер, додатки покладаються на те, що клієнтська програма буде «чесною» щодо кінцевого користувача. Інші програми покладаються на те, що клієнт обмежує свою діяльність тими, що це дозволено при використанні продукту, без будь-яких інших примусових заходів з боку сервера. Ось чому необхідно підтвердити, що ви є особою або клієнтом. Після того, як автор запиту автентифікований певним способом, потрібно визначити, які дії дозволені кінцевому користувачу (запитувачу). З використанням рішень на основі політики безпеки запитувач можна авторизуватися для різних служб, оцінивши політику дозволів на доступні користувачу послуги. Щоб відстежувати всіх авторизованих користувачів, збирається облікова інформація для різних цілей, наприклад журналювання зловживань зловмисних користувачів. Або-забезпечити максимальне покриття зростаючої кількості абонентів роумінгу та мобільного зв'язку Інтернет-провайдери можуть об'єднують свої ресурси NAS для збереження контролю над доступом своїх абонентів до конфіденційної інформації (паролі, логіни, платіжна інформація тощо). Всі ці послуги вимагають координації між різними системами адміністрування, що підтримуються різними провайдерами.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Основою автентифікації, авторизації та обліку ААА є їх відповідність викликів у спрощений та масштабований спосіб. ААА – визначає структуру для координації окремих користувачів на багатьох мережевих технологіях і платформах. На практиці сервер ААА з базою даних профілів користувачів та даних конфігурації взаємодіє з клієнтами ААА, які знаходяться в мережевих компонентах, таких як NAS і маршрутизатори, щоб забезпечити розподіл ААА послуги.

Автентифікація (Authentication) – це акт перевірки заявленої особистості у формі попередньо існуючої мітки у відомому просторі імен, як джерело повідомлення (автентифікація повідомлення) або як кінцева точка каналу (автентифікація сутності). Автентифікація, перша літера «А» в ААА, передбачає попередню перевірку ідентифікації кінцевого користувача з метою дозволу йому доступу до мережі. Цей процес базується на понятті, що кінцевий користувач володіє унікальною інформацією, комбінацією імені користувача та пароля, секретного ключа або біометрією (відбитки пальців, рогівка ока), що служить ідентифікаційними даними. Сервер ААА порівнює дані надані користувачем з даними, що пов'язані з користувачем, які зберігаються в базі даних. І якщо облікові дані збігаються, користувачеві надається доступ до мережі. Різні дані призводить до помилки автентифікації та відмові доступу до мережі.

Авторизація (Authorization) – це акт визначення того, чи може бути надане право доступу до певного ресурсу. Авторизація, друга літера «А» в ААА, визначає, які права та послуги має кінцевий користувач після надання даних авторизації. Це може включати надання IP-адреси, викликаючи фільтр, щоб визначити, які програми чи протоколи підтримуються. Автентифікація та авторизація зазвичай виконуються разом у середовищі ААА.

Облік (Accounting) – це процес збору інформації про використання ресурсів з метою аналізу тенденцій, аудиту та фіксації подій. Облік, третя літера «А» в ААА, забезпечує методологію збору інформації про використання ресурсів кінцевим користувачем, яка потім може бути оброблена з метою аудиту, планування, а також для боротьби зі зловмисними діями в мережі.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

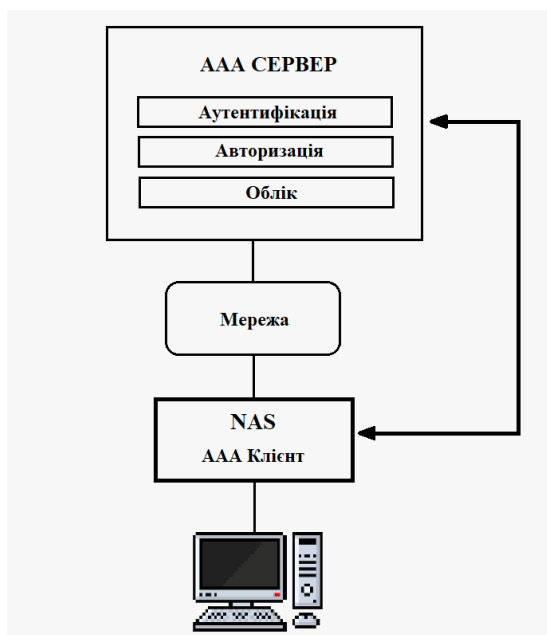
1.4 Принцип роботи серверної інфраструктури

На рисунку 1.1 нижче продемонстровано компоненти інфраструктури AAA. Сервер AAA або певна кількість серверів може використовуватись для забезпечення стійкості та контролю підключення до мережі та служити центральним місцем зберігання та поширення інформації AAA. Пристрій, що використовується як точка входу в мережу зазвичай є NAS (хоча це також може бути маршрутизатор або інший хост), який містить функцію клієнта AAA.

Обробку AAA можна підсумувати такими кроками:

1. Кінцевий користувач підключається до пристрою точки доступу та запитує доступ до мережі;
2. Клієнтська функція NAS AAA збирає та пересилає облікові дані кінцевого користувача на сервер AAA;
3. Сервер AAA обробляє дані та повертає відповідь щодо прийняття або відхилення;
4. Клієнт AAA на NAS повідомляє кінцевого користувача, що доступ надано або заборонено для вказаних ресурсів.

NAS також може надсилати облікове повідомлення на сервер AAA під час підключення, налаштування або завершення збору та зберігання записів.



		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок. 1.1 – Принцип роботи AAA архітектури. Клієнт AAA (NAS) у POP (Point-of-presence) мережі передає дані на сервер AAA для надання послуг.

Однією з переваг цієї архітектури є те, що сервер AAA можна розмістити в обчислювальній системі загального призначення, яка зазвичай доступна за хорошим співвідношенням ціни та продуктивності, пропонуючи дискове сховище великого обсягу та оптимізоване адміністрування бази даних. Це дає провайдерам комутованих послуг необхідну для обробки пакетів запитів AAA від багатьох пристроїв NAS, а також ємність пам'яті, необхідну для запису облікової інформації для кожного з багатьох з'єднань кінцевих користувачів.

Один сервер AAA може діяти як централізована адміністративна точка керування для кількох клієнтів AAA, які містяться в NAS і мережевих компонентах від різних постачальників. Таким чином, функції AAA можна додати до сервера та поступово до клієнта, не порушуючи існуючі функції попередньо створеної мережі.

1.5 Функціонал та застосування протоколу RADIUS у комп'ютерних мережах

RADIUS (Remote Access Dial-IN User Service) – сьогодні є найпоширенішим AAA протоколом у світі, конкуруючи з TACACS+ і Kerberos. Одна з речей, яка зробила RADIUS популярним серед існуючих протоколів AAA, це те, що він є незалежним від постачальника, тобто не контролюється одним постачальником, на відміну від TACACS+ (від компанії Cisco) і Kerberos (від компанії Merit).

RADIUS був розроблений у середині 90-х компанією Livingston Enterprises (пізніше куплена компанією Lucent Technologies), щоб забезпечити своє обладнання NAS аутентифікацією, авторизацією та обліком. Схематичний принцип роботи протоколу RADIUS зображено на рисунку 1.2. IETF формалізували роботу в 1996 році шляхом призначення RADIUS WG (work group - робоча група), яка призвела до того, що всі функції та формат стандартизовано в RFC 2138.

Функціональні можливості RADIUS можна підсумувати наступним чином:

- Операції на основі клієнт-сервера.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- Клієнт RADIUS знаходиться на NAS і комутується через мережу з сервером RADIUS, який працює на хості комп'ютера.
- Сервер RADIUS може служити проксі-клієнтом для RADIUS або інших серверів автентифікації.

Усі комунікації між клієнтом RADIUS і на сервері автентифікуються за допомогою спільного секретного ключа, який ніколи не надсилається через мережу. Крім того, паролі користувачів, що містяться в RADIUS повідомленнях шифруються, щоб запобігти їх читанню хакерами шляхом перехвату трафіку.

RADIUS може підтримувати багаторазову автентифікацію, включаючи PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) і EAP (Extended Protocol Authentication).

Повідомлення RADIUS містять інформацію AAA у кодованому вигляді. У полях, які називаються атрибутами (або пара атрибут/значення). Загальні приклади атрибутів включають: ім'я користувача, пароль користувача, Framed-Protocol (наприклад, PPP), Framed-IP-Address (IP-адреса для кінцевого користувача).

RFC 2138 і спеціальна документація постачальника містять більш повні списки атрибутів RADIUS, які підтримуються серверами та клієнтами.

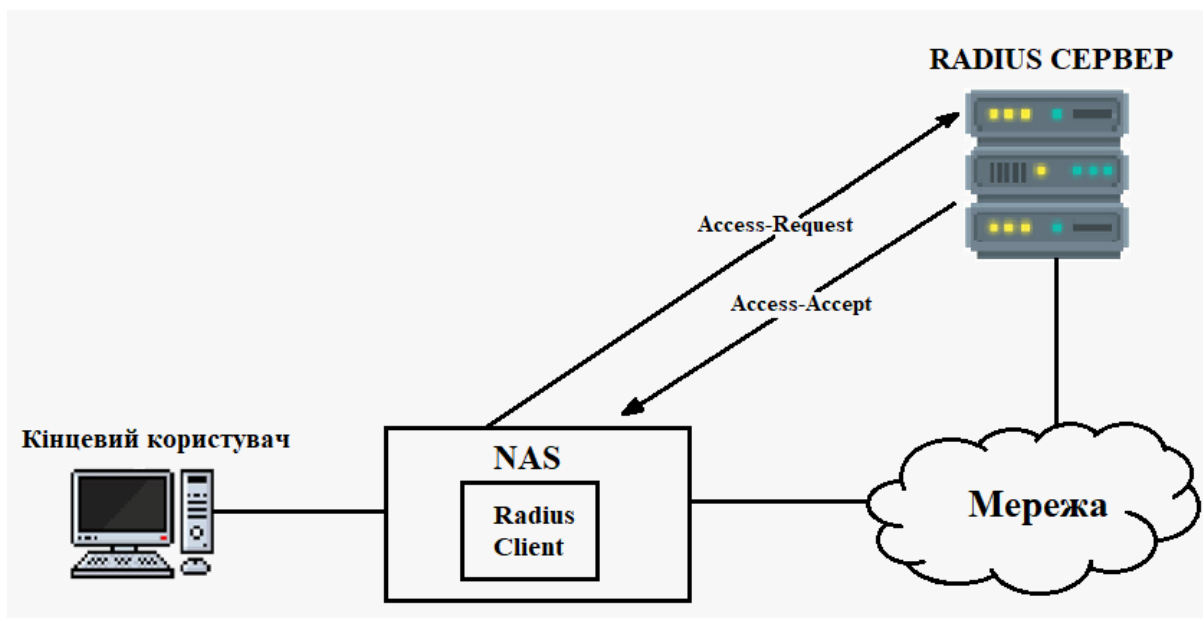


Рисунок 1.2 – Функціональний принцип роботи протоколу RADIUS.

Клієнт RADIUS на NAS пересилає облікові дані кінцевого користувача в запиті на доступ повідомлення до сервера RADIUS. Після перевірки облікових даних

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

кінцевого користувача RADIUS сервер повертає клієнту повідомлення Access-Асcept.

Кінцевий користувач підключається до NAS, який підтримує клієнт RADIUS. Далі NAS зберігає ім'я користувача та пароль від кінцевого користувача. Потім він використовує UDP/IP для пересилання зашифрованого повідомлення Access-Request через мережі до сервера RADIUS. Повідомлення також може містити такі атрибути, як ідентифікатор порту NAS та IP-адреса. Наступним кроком сервер RADIUS перевіряє атрибут User-Name на наявність збереженого відповідного запису у своїй базі даних. Якщо відповідності немає, то сервер повертає повідомлення (Access-Reject) до NAS разом із додатковим текстовим повідомленням та зазначенням причини збою. NAS, у свою чергу, повідомляє кінцевого користувача про збій автентифікації. Якщо збіг є знайдено і пароль правильний, тоді сервер RADIUS повертає Access-Асcept повідомлення до NAS разом із будь-якою необхідною додатковою конфігураційною інформацією завершення підключення. Наприклад, IP-адреса для кінцевого користувача, яка обмежує їх до певного типу протоколу, наприклад Telnet або HTTP. Схематичний вигляд пакета запиту та відповіді протокола RADIUS зображений на рис. 1.3.

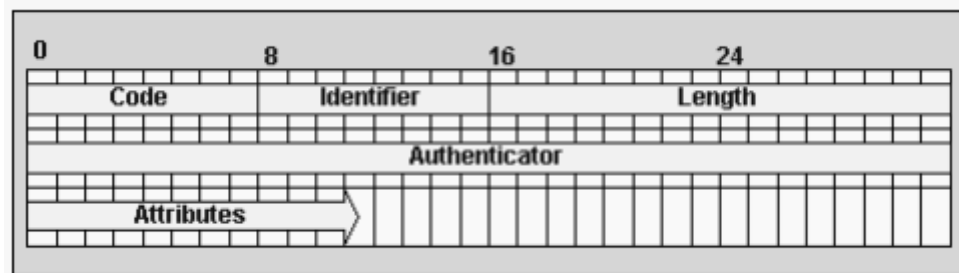


Рисунок 1.3 – Принцип передачі інформації в пакеті RADIUS.

Заголовок у пакеті RADIUS складається з чотирьох різних полів даних:

- Одне 8-бітне кодове поле (Код), яке визначає тип пакета.
- Одне 8-бітне поле ідентифікатора (Ідентифікатор), яке допомагає зіставляти запити відповіді.
- Одне 16-бітне поле довжини (Length), що містить довжину пакета, включаючи всі AVP.

- Одне 32-бітне поле автентифікації (Автентифікатор), яке використовується для автентифікації відповіді від сервера RADIUS, а також використовується як частина алгоритму для приховування пароля клієнта при запитах.

RADIUS AVP містить певну автентифікацію, авторизацію та облік інформації та деталі конфігурації щодо запитів/відповідей. AVP складається з трьох полів (див. рис. 1.4 нижче).

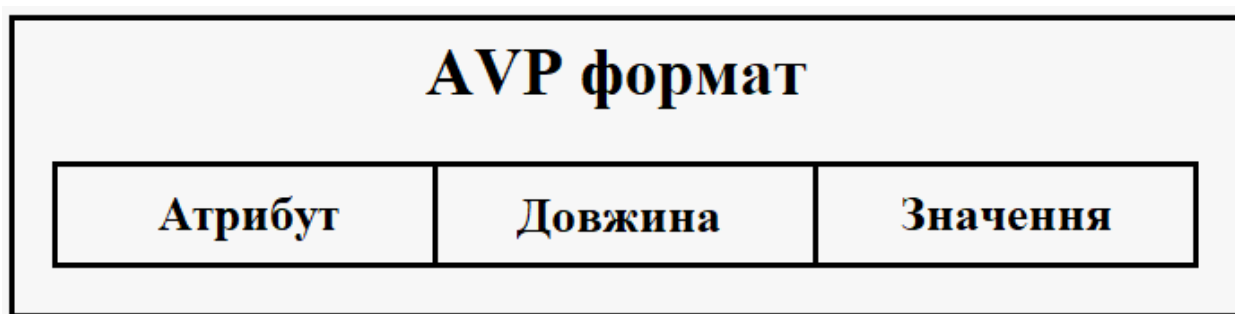


Рисунок 1.4 – AVP формат.

1.6 Основи, принцип роботи та побудови протоколу DIAMETER.

Протокол RADIUS використовувався з послугами AAA для телефонного підключення PPP (протокол точка-точка) і доступу до термінального сервера. Але з такою ж швидкістю, як маршрутизаторів і серверів доступу до мережі (NAS) збільшилася кількість і розмір запитів. Протокол RADIUS став менш корисним у таких великих мережах. Протокол Diameter не був створений на порожньому місці, але розробники скоріше зберегли основу формату RADIUS і спробували виправити всі відомі недоліки протоколу RADIUS.

Протокол Diameter не використовує той самий блок даних протоколу (PDU), що й RADIUS, але все ж достатньо запозичено з RADIUS, щоб бути зворотною сумісним.

Ідея Diameter полягає в тому, щоб створити базовий протокол, який можна легко розширити щоб дозволити нові методи доступу. На даний момент розробники обмежують область застосування протоколу Diameter для доступу в Інтернет, через загальний PPP і через критерії, визначені моделями ROAMOPS.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Архітектура протоколу Diameter складається з базового протоколу та різних розширень і програм, наприклад, CMS Security, NASREQ і Mobile-IP (див. мал. 1.5). Все базове в протоколі Diameter реалізовано спільні для всіх додатків і сервісів функціоналу протоколу, у той час як усі специфічні функції програми існують окремо. Базовий протокол також визначає певні правила, які застосовуються до всіх обмінів повідомленнями між Diameter вузлами. Базовий протокол Diameter призначений для забезпечення структури AAA для Mobile-IP, NASREQ (Вимоги до сервера доступу до мережі) і ROAMOPS. Базовий протокол також визначає формат повідомлення, маршрут, повідомлення про помилки та служби безпеки, які повинні використовуватися програмами та повинні підтримуватися всіма релізами протоколу Diameter. Для того, щоб використовувати протокол Diameter для різних служб, різні реалізації протоколу повинні підтримувати програми, що забезпечують функції, пов'язані з послугами.

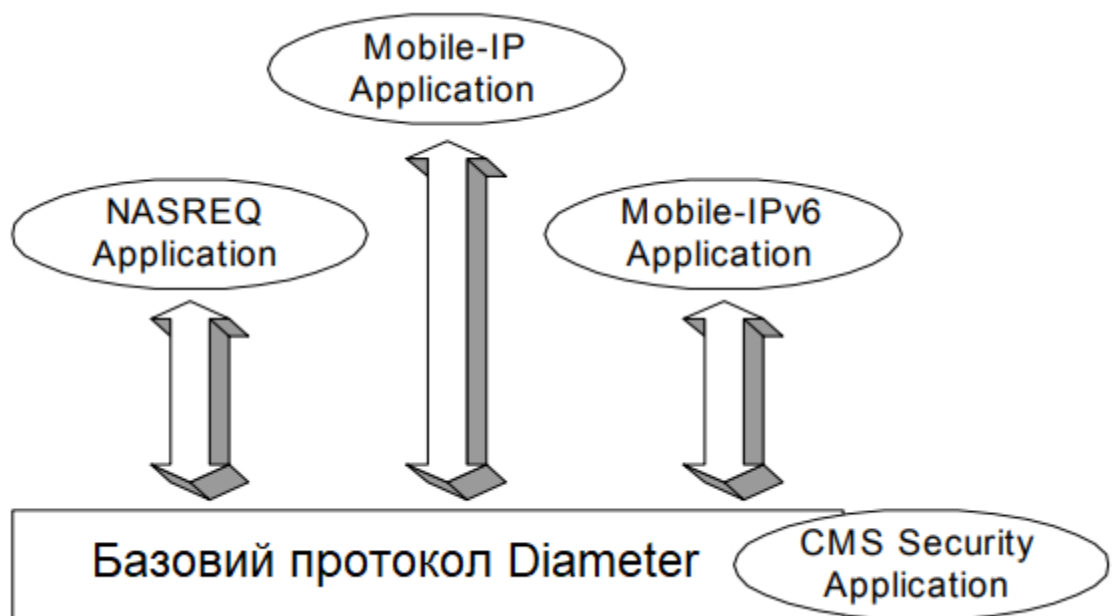


Рисунок 1.5 – Внутрішня архітектура протоколу Diameter.

На рис. 1.5 показано схематичне зображення архітектури протоколу Diameter, з базовим протоколом тісно пов'язаним з додатком безпеки CMS, щоб забезпечити безпеку для всіх програм. Але маючи різні функції, усі програмні продукти повинні підтримувати базовий протокол Diameter для коректної роботи.

Повідомлення Diameter, як і повідомлення RADIUS, складаються із заголовка (див. рис. 1.6), за яким слідує вибір AVP.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Version	Message Length
RPE	Command-Code
Vendor ID	
Hop-by-Hop Identifier	
End-to-End Identifier	
AVPs	

Рисунок 1.6 – Принцип побудови повідомлення протоколом Diameter.

AVP складаються із заголовка (див. рис. 1.7), за яким слідують дані, пов'язані з вибраним заголовком.

AVPs	
VMP	AVP length
Vendor ID	
Data	

Рисунок 1.7 – Структура та побудова AVP заголовку.

Як було зазначено раніше, базовий протокол має підтримуватися всіма реалізаціями Diameter, а також більшою частиною додатків. Базовий протокол визначає PDU (Protocol-Data Unit) формат для Diameter, а також кілька примітивів і базову безпеку в Diameter, яка розширена за допомогою тісного підключення до програми безпеки CMS.

На відміну від RADIUS, базовий протокол визначає Diameter для роботи через Stream-Control Transmission-Protocol (SCTP), який постачає Diameter з надійною та стабільною можливістю ретрансляції. Оскільки SCTP дозволяє використовувати “вікна”, сервери AAA можуть обмежувати кількість вхідних повідомлень пакетів, що дозволяє клієнтам Diameter розподіляти навантаження трафіку між різними серверами. Повторна передача та таймери очікування транспортного рівня

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

дозволяють клієнтам і серверам визначати стан доступності однорангових вузлів, дозволяючи швидкий перехід до резервних серверів.

Базовий протокол передбачає модель однорангового зв'язку, на відміну від моделі клієнт-серверної інфраструктури.

Головні цілі проектування протоколу Diameter:

- Легкість та простота реалізації;
- Великий простір AVP заголовків;
- Ефективне кодування атрибутів, подібне до RADIUS;
- Підтримка спеціальних AVP заголовків і команд постачальника;
- Підтримка великої кількості одночасних запитів, що очікують на розгляд;
- Надійність, що забезпечується базовим протоколом SCTP;
- Чітко визначена схема блокування;
- Можливість швидкого виявлення недоступних користувачів;
- Стабільність отримання та передачі повідомлень;
- Підтримка небажаних повідомлень кінцевим користувачам
- Цілісність і конфіденційність інформації;
- Безпека Нор-by-Нор;
- Один сеанс на один запит автентифікації та авторизації;
- Надання послуг перенаправлення (рефералів).

Базовий протокол Diameter призначений для забезпечення безпечного транспортування повідомлення, визначені в різних розширеннях для певних програм. Важливо, щоб основа була легкою та простою у використанні. В протоколі Diameter, об'єкти даних інкапсулюються в пару значень атрибутів (AVP). AVP складається з трьох частин: ідентифікатора, пам'яті та даних. Унікальний AVP ідентифікатор призначається всім об'єктам даних, щоб можна було розрізняти де дані містяться. Крім того, якщо адміністратори бажають додати «власні» розширення має бути дозвіл робити це за допомогою спеціального простору імен постачальника, керованого IANA.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Протягом багатьох років питання про те, чи повинен RADIUS працювати через UDP або TCP викликало бурхливу дискусію. Необхідно визначити, чи приносить користь UDP, чи надає складнощів реалізації та побудові функціональної мережі. Згодом, згідно RFC 2865, стало зрозуміло, що ці переваги цілком варті витрат. Питання з TCP полягає в тому, що протокол AAA вимагає швидкої повторної передачі даних, яку TCP не може забезпечити. Протокол Diameter повинен мати можливість працювати над маршрутизацією, яка має швидкий алгоритм повторної передачі для ефективного перемикання на альтернативний хост.

На відміну від RADIUS, протокол Diameter вимагає, щоб кожен вузол у ланцюжку підтвердив запит або відповідь на маршрутизацію. Оскільки Diameter працює через SCTP, що забезпечує надійність маршрутизації, кожен вузол у ланцюжку проксі відповідає за повторну передачу непідтверджених повідомлень. SCTP забезпечує виявлення повторної передачі, що значно спрощує серверу роботу і дозволяє даному серверу підтримувати набагато більшу кількість дій в секунду. SCTP також забезпечує вікна, що дозволяє потік пакетів до певного сервера, який потрібно контролювати. Тоді головний сервер може надіслати пакети на альтернативні сервери, які можуть впоратися з навантаженням.

За винятком кількох помилок, пов'язаних із безпекою, базовий протокол Diameter вимагає, щоб усі повідомлення були підтверджені, або отримали успішну відповідь. Там, де протокол RADIUS є клієнт-сервером, протокол Diameter є одноранговим, дозволяючи надсилати небажані повідомлення до NAS. Однорангові протоколи AAA мають багато переваг. Одним із прикладів є пошук облікових даних на вимогу.

Протокол Diameter забезпечує поетапну безпеку, подібну до схеми праці протоколу RADIUS. Однак протокол Diameter також передбачає захист від повторного відтворення через механізм часових позначок. Ця схема безпеки може використовувати ключ узгодження поза групою. Базовий протокол також дозволяє вимкнути вбудовані заходи безпеки, що корисно, якщо ви хочете використовувати IPSec для забезпечення цілісності та конфіденційності між користувачами Diameter.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Протокол Diameter є сеансово-орієнтованим протоколом, тобто для кожного автентифікованого користувача, існує сеанс між ініціалізацією запиту автентифікації/авторизації та сервером Diameter. Всі наступні транзакції протоколу Diameter (наприклад, облік) повинні містити ідентифікатор сеансу для посилання на сесію.

У реаліях сьогодення процесори працюють більш ефективно, адже використовуються 32-бітні межі, а протокол Diameter вимагає мінім 32-бітне (краще 64 біти) поле вирівнювання всіх заголовків і даних. На разі це стало загальною вимогою для багатьох нових протоколів IETF.

1.7 Спільна робота серверів Diameter з серверами Radius та порівняння роботи серверів.

Протокол Diameter розроблено з урахуванням сумісності з RADIUS. Протокол RADIUS визначає простір атрибутів в один октет, а протокол Diameter резервує перші 255 ідентифікаторів атрибутів як ті, що визначені в RADIUS. Це дозволяє серверам Diameter легко виконувати перетворення протоколів, оскільки для того, щоб зіставити атрибут RADIUS з Diameter AVP, додатковий пошук у словнику не потрібен. Сервер Diameter здатен розуміти профільні дані протоколу RADIUS без жодного додаткового перетворення шляхом повторного використання простору атрибутів RADIUS, що заперечує необхідність дублювати профілі користувачів для обох протоколів і робить конвертацію бази даних непотрібною.

Стандартизований API (інтерфейс програми) не є абсолютно необхідним для протоколу взаємодії, але це дуже допомагає сприяти використанню та розгортанню протоколу Diameter шляхом зменшення обсягу необхідної роботи розробки та утримання додатків, які використовують протокол.

Незважаючи на те, що всі реалізації протоколу Diameter мають підтримувати базу даних протокол ніколи не використовується сам по собі. Базовий протокол завжди розширено принаймні однією програмою для підтримки певної служби. Хоча Diameter можна використовувати для вирішення широкого кола проблем AAA, і це одна з причин, чому розроблено заміну/доповнення RADIUS.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Робоча група в IETF наразі обмежує сферу застосування протоколу до трьох додатків Diameter, які визначені в супровідних документах до базового протоколу: NASREQ, Mobile-IP і CMS Security, щоб гарантувати, що зусилля залишаються зосередженим на задоволенні вимог доступу до мережі. Інші робочі групи IETF, такі як робоча група Mobile-IP і NASREQ визначають набори специфікацій для протоколу Diameter, щоб підтримувати їх роботу, яка призвела до створення робочих груп.

Робоча група з питань роумінгу (ROAMOPS) опублікувала набір специфікації, які визначають, як користувач PPP може отримати доступ до Інтернету без підключення до пулу модемів свого домашнього постачальника послуг мережі Інтернет. Це досягається шляхом дозволу постачальником послуг здійснювати перехресну автентифікацію своїх користувачів.

Розширення Diameter NASREQ визначає набір команд автентифікації/авторизації, які можна використовувати для CHAP, PAP та EAP. Diameter підтримує властивості SCTP використовувати EAP, що дозволяє наскрізну автентифікацію користувача, що зменшує велику кількість атак з метою автентифікації. Додаток NASREQ у поєднанні з базовим протоколом, відповідає вимогам, визначеним у специфікації критеріїв NASREQ AAA та специфікація критеріїв ROAMOPS AAA. Додаток NASREQ містить два основні розділи. Перший розділ визначає командні коди Diameter і AVP, необхідні для підтримки застарілих RADIUS протоколів автентифікації. Другий розділ визначає коди команд і AVP необхідні для того, щоб вузол Diameter підтримував розширюваний протокол автентифікації PPP. Розширення NASREQ використовує атрибути, визначені в протоколі RADIUS для перенесення об'єктів даних. Це необхідно для полегшення перенесення існуючого функціоналу RADIUS на сервери Diameter, оскільки вони могли спільно використовувати один словник і профіль користувача. Крім того, це зменшує кількість дій необхідних для обробки інформації, необхідної для взаємодії систем RADIUS та Diameter.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Базовий протокол Diameter дозволяє серверам безпечно обмінюватися інформацією за допомогою покрокової автентифікації. Покрокова автентифікація означає, що запит серверу має безпечний зв'язок із проксі-сервером або сервером пере-направлення, а проксі має безпечний зв'язок з сервером в офісі. Безпека передачі інформації забезпечується тим фактом, що базовий протокол Diameter спирається на IPsec (IP Security) або TLS (Transport Layer Security) для цілісності та конфіденційності між двома Diameter вузлами.

Базовий протокол також визначає проксі-сервер Diameter, який пересилає запити на інші сервери, коли виявляє, що даний запит не може отримати відповідь локально. Робоча група ROAMOPS в рамках IETF визначила вимогу, що сервери Diameter, які спілкуються через проксі, повинні забезпечують наскрізну цілісність і конфіденційність AVP заголовків, що ускладнює роботу проксі агентам, з метою зміни та перегляду конфіденційної інформації в повідомленні.

Документ додатка CMS Security описує, наскільки надійна автентифікація та шифрування може бути забезпечена в протоколі Diameter шляхом інкапсуляції CMS (Синтаксис криптографічного повідомлення) в AVP.

Існує два основних способи захисту повідомлень, які надає CMS Security додаток. Цифрові підписи (разом із цифровими сертифікатами) забезпечують автентифікацію, цілісність і незаперечність. Шифрування забезпечує конфіденційність (використовуючи асиметричні методи шифрування ключа, який потім використовується для шифрування повідомлення). Обидва методи можна використовувати одночасно для забезпечення наскрізної автентифікації та конфіденційності, таким чином забезпечуючи наскрізну безпеку.

У випадку, зображеному на рис 1.9, ініціатор запиту та відповіді може додати цифровий підпис, який охоплює набір AVP заголовків у повідомленні. Тоді захищені AVP можуть бути зміненими проміжним проксі-сервером (DIA2, DIA3).

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

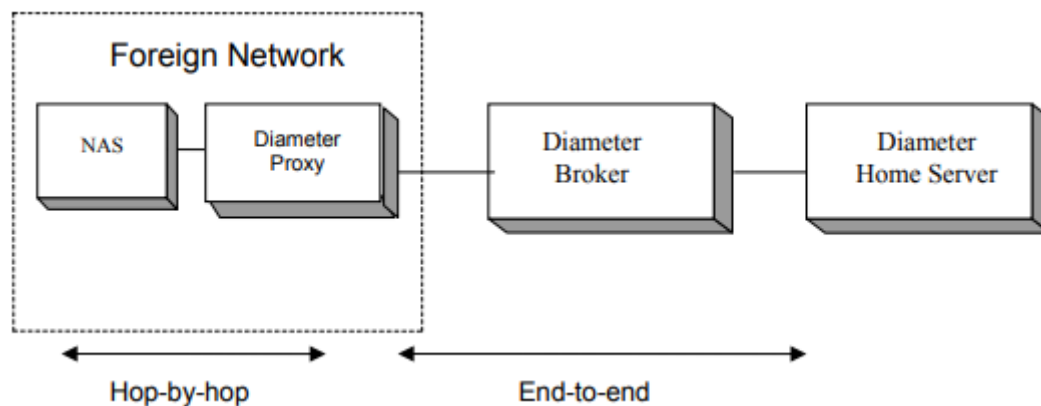


Рисунок 1.9 – Змішана схема захисту протоколу Diameter.

Коли використовуються служби перенаправлення, протокол безпеки мережевого рівня IPSec може використовуватися для захисту трафіку між двома серверами Diameter. Проте безпека на рівні програми все ще може знадобитися в цій мережній конфігурації, зокрема можливість автентифікації вибраного набору AVP.

З огляду на те, що операції асиметричного перетворення дорogi, сервери Diameter можуть використовувати лише під час роботи з міждоменними серверами.

Оскільки протокол Diameter ще не досяг стандартизації – жоден NAS не підтримує протокол Diameter. Але великі компанії підтримують розробку протоколу Diameter, фінансуючи розробку та вдосконалення протоколу.

Вивчаючи різні проекти Diameter можна ідентифікувати осіб і компанії, які працюють з протоколом.

Список компаній та людей, які займаються удосконаленням протоколу Diameter представлено нижче.

- Blackstorm Networks – Пет Калхун;
- Sun Microsystems – Ерік Гутман;
- Nortel Networks – Хейс Актар;
- LM Ericsson – Ярі Арко;
- Tut-systems – Аллан К. Рубенс;
- Системи Cisco – Глен Цорн та Джефф Хаг;
- Merit Network – Вільям Буллі;
- Дослідницький центр Nokia – Чарльз Е. Перкінс;
- Microsoft – Бернад Нейк.

Окрім цих компаній, зацікавленість у розробці протоколу Diameter викликає ще одна компанія під назвою Interlink Networks, що намагаються реалізувати спільну роботу протоколів Diameter та RADIUS.

1.8 Нововведення у роботі протоколу Diameter

Назви протоколів Diameter і RADIUS звучать як геометрія. Але, очевидно, ці терміни також використовуються в комп'ютерних мережах, системах та телекомунікаційних технологіях. Diameter — це протокол автентифікації, авторизації та обліку (AAA), який належить до прикладного рівня набору Інтернет-протоколів. Протокол Diameter розвинувся на основі свого попередника RADIUS (сервіс віддаленої автентифікації, авторизації, обліку користувачів віддаленого зв'язку). Термін Diameter також походить від RADIUS, оскільки Diameter – це подвоєний RADIUS.

На сьогодні різноманітні функції мереж використовують протокол Diameter. Оскільки критично важливі мережеві функції, такі як функції політик та правил стягнення плати (PCRF), домашній абонентський сервер (HSS) і онлайн-система стягнення плати (OCS) працюють спільно з протоколами AAA.

У цьому контексті протокол встановлює комплексну структуру для повідомлень AAA та команд відповіді разом із пов'язаними атрибутами. Це забезпечує системний підхід до зв'язку між компонентами мережі, підвищуючи ефективність роботи в сучасних телекомунікаційних мережах.

Відмінності протоколу Diameter від протоколу RADIUS наведені в систематизованій таблиці 1.1.

Таблиця 1.1 – Порівняння протоколів Diameter та RADIUS.

Протокол RADIUS	Протокол Diameter
Використовується для UDP зв'язку	Підтримує як TCP, так і SCTP, забезпечуючи більш надійні та безпечні функціональні можливості
Простий у використанні, але менш розширений функціонально	Комплексно розширений, але складний у використанні

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Підтримує PAP, CHAP, EAP методи	Підтримує широкий спектр методів автентифікації, включаючи EAP і більш безпечні механізми
Надає базові можливості авторизації	Пропонує більш розширені та гнучкі можливості авторизації
RADIUS не потребує з'єднання, не вимагає попереднього створення сеансу	Diameter - це протокол, орієнтований на підключення
Для автентифікації використовує порт UDP 1812 або 1645, а для обліку порт 1813 або 1646	Працює на портах TCP і SCTP 3868
Забезпечує безпеку Нор-by-Нор	Забезпечує автентифікацію Нор-by-Нор, а також може забезпечити наскрізну безпеку
Відсутня підтримка проксі, оскільки передбачає пряме підключення	Підтримка ретранслятора (Relay, Proxy, Redirect)
Обмежені коди помилок та обробка даних	Покращена обробка помилок завдяки розширеному журналу помилок
Сервер не може надсилати запити клієнту	Сервер може надсилати запити клієнту

RADIUS спочатку був розроблений для базової автентифікації в мережах віддаленого доступу. У типовому налаштуванні RADIUS користувач надає облікові дані для входу (наприклад, ідентифікатор користувача та пароль) серверу доступу. Потім сервер доступу перевіряє ці облікові дані на централізоване сховище політик LDAP. Однак модель RADIUS стикається з проблемами в мережах IMS, особливо з мобільними користувачами, які отримують доступ до динамічних програм і послуг у мережах різних постачальників послуг.

З іншого боку, Diameter втручається у вирішення цих проблем. Він підтримує розширений контроль політики, динамічні правила, якість обслуговування,

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

розподіл смуги пропускання та механізми стягнення плати, що є ключовими для сучасних мереж та систем. Крім того, Diameter пропонує більш надійну, безпечну та гнучку структуру для обміну повідомленнями автентифікації, авторизації та обліку (AAA).

Оскільки протокол RADIUS має об'єктивні недоліки (викладені у попередньому розділі), йому на зміну прийшов Diameter (RFC 3588 та 6733). Вже із назви стає зрозуміло, що це не цілком новий протокол для забезпечення архітектури AAA, а логічне продовження та покращення RADIUS, покликане в першу чергу для подолання деяких його обмежень. Diameter бере суть архітектури AAA із RADIUS і визначає набір досить узагальнених повідомлень, які служать його базовим ядром. Наразі, новий протокол широко використовується у архітектурі IMS (IP Multimedia Subsystem). У якості транспортного протоколу, Diameter використовує TCP (порт 3868) та підтримує TLS, DTLS або IPSec шифрування. Крім того, важливим удосконаленням, порівняно із RADIUS, є підтримка моделей зі збереженням та без збереження стану (stateful/stateless).

Diameter має однорангову архітектуру (Peer-To-Peer), і кожен хост, який реалізує даний протокол, може виступати або клієнтом, або сервером, у залежності від мережевої інфраструктури:

Diameter-клієнт – це мережевий пристрій, що безпосередньо обробляє трафік користувача. Зазвичай, це NAS.

Diameter-сервер – це вузол, що обробляє запити клієнта. Він виконує автентифікацію, на основі інформації, отриманої від клієнта (напр. логін та пароль). У випадку успішної автентифікації, сервер відправляє клієнту відповідь, що включає авторизацію (повноваження користувача). На перший погляд, описана вище структура має вигляд традиційної клієнт-серверної, проте, це не так. Іноді, вузол, може виступати у ролі клієнта. Крім того, у протоколі чітко визначено ще один тип вузла – Diameter-агент.

Види Diameter-агентів:

- **relay agent** (агент ретранслятор) – перенаправляє повідомлення відповідному адресату, в залежності від інформації у повідомленні.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Такий агент може бути корисним при об'єднуванні запитів із різних регіонів у певну область, що усуває необхідність кропіткого налаштування NAS при зміні Diameter-сервера;

- **proxy agent** (проксі агент) – також перенаправляє повідомлення, але може змінювати вміст повідомлення, надавати додаткові служби, застосовувати правила для різних повідомлень та виконувати функції адміністрування для різних областей;
- **redirect agent** (агент перенаправлення) – виступає у ролі централізованого «сховища» конфігурацій для інших Diameter-серверів. При отриманні повідомлення, переглядає власну таблицю маршрутизації та повертає відповідь разом із інформацією про перенаправлення відправнику. Такий функціонал корисний, оскільки усуває необхідність списку маршрутизації на інших Diameter-вузлах.

З огляду на те, що Diameter є удосконаленням RADIUS, існує ще один спеціальний агент – translation agent (агент трансляції), який реалізує сумісність із RADIUS шляхом перетворення повідомлення одного AAA-протоколу у інший. Такий агент корисний тоді, коли у компанії/провайдера фізичні пристрої не сумісні на рівні AAA-протоколів.

Висновки до першого розділу

У першому підрозділі було розглянуто основи побудови та принцип функціонування протоколів AAA, зокрема протоколу RADIUS та Diameter.

У другому підрозділі було розглянуто проблемні місця протоколів AAA.

У третьому підрозділі описано роботу, функціонування протоколів AAA. Встановлено, що при практичному використанні сервер AAA з базою даних профілів користувачів та даних конфігурації взаємодіє з клієнтами AAA, які знаходяться в мережевих компонентах, таких як NAS і маршрутизатори, щоб забезпечити розподіл AAA послуги.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

У четвертому підрозділі опрацьовано принцип роботи серверної інфраструктури. В ході опрацювання, встановлено, що один сервер AAA може діяти як централізована адміністративна точка керування для кількох клієнтів AAA, які містяться в NAS і мережевих компонентах від різних постачальників.

У п'ятому підрозділі проаналізовано функціонал та застосування протоколу RADIUS у комп'ютерних мережах. Результатом аналізу отримано висновок, що клієнт RADIUS знаходиться на NAS і комутується через мережу з сервером RADIUS, який працює на хості комп'ютера. А сервер RADIUS може служити проксі-клієнтом для RADIUS або інших серверів автентифікації.

У шостому підрозділі було розглянуто основи, принцип роботи та побудови серверної інфраструктури на основі протоколу DIAMETER. З'ясовано, що протокол Diameter є сеансово-орієнтованим протоколом, тобто для кожного автентифікованого користувача, існує сеанс між ініціалізацією запиту автентифікації/авторизації та сервером Diameter.

У сьомому підрозділі перевірена спільна робота серверів Diameter з серверами Radius та здійснено порівняння роботи серверів на теоретичному рівні.

У восьмому підрозділі було розглянуто нововведення у протоколі Diameter та порівняно функціональні можливості та особливості функціонування протоколів при проектуванні та побудові мережних систем. Було встановлено, що протокол Diameter є удосконаленням протоколу RADIUS.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЄКТУВАННЯ МЕРЕЖІ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ СЕРВІСІВ НА ОСНОВІ ПРОТОКОЛУ DIAMETER

2.1 Проєктування мережі серверної інфраструктури

Наразі протокол Diameter активно використовується в мережах організацій для доступу до віртуальних частних мереж (VPN), точок бездротового (Wi-Fi) доступу, до провідних комутаторів Ethernet, DSL та іншим типам мережного доступу.

Реалізація схеми топології мережі була здійснена в редакторі Draw.io. А загальну топологію мережі було наведено на рис 2.1. При побудові використано приєти (зображення) мережного обладнання, які використовує компанія Cisco для створення наочних схем мережі.

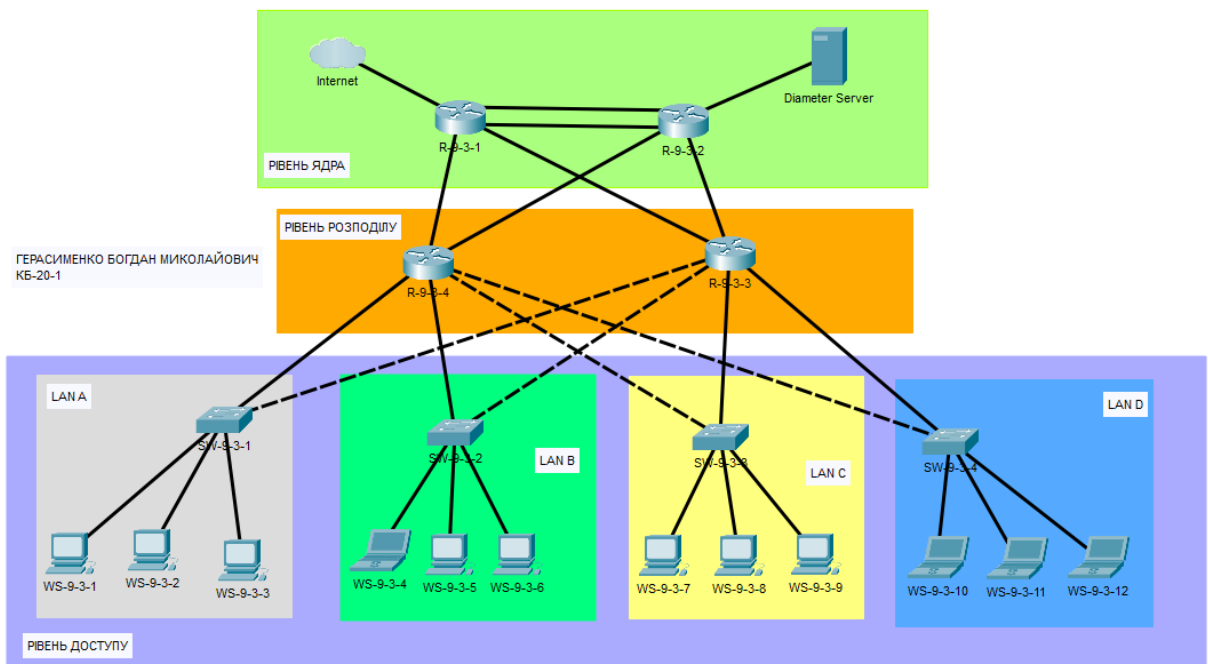


Рисунок 2.1 – Топологія мережі.

Для створення мережі було взято за основу трьохрівневу систему мережі, яку розробила компанія Cisco. Таким чином мережа стає ієрархічною та складається з трьох окремих рівнів. А саме рівня ядра, рівня розподілу та рівня доступу.

До рівня ядра входить 2 маршрутизатори з'єднаних між собою транковим каналом, сервер AAA, що працює за протоколом Diameter та надана можливість доступу до мережі WAN (Internet) за допомогою транляції адрес за допомогою протоколу NAT.

Рівень розподілу складається також з 2 маршрутизаторів, що з'єднані з ядром мережі та рівнем доступу (клієнтським).

На каналах передачі даних здійснена агрегація з метою підвищення продуктивності роботи мережі.

Зважаючи на те, що розподілення об'єктів мережі за рівнями відбувається відповідно до їх функціоналу, що виконує кожен об'єкт – це допомагає аналізувати кожен рівень незалежно від іншого. Тобто розподіл виконується не фізичними поняттями, а логічними.

Отже, базовий рівень (Core) на рівні ядра необхідний для швидкісної і відмовостійкої передачі великого обсягу трафіку без тривалих затримок. Необхідно враховувати, що ACL і оптимальна маршрутизація між компонентами мережі може знизити швидкість трафіку. Зазвичай при виникненні проблеми з рівнем швидкості виконання процесів маршрутизації ядром потрібно не розширювати, а модернізувати обладнання. Тому краще відразу використовувати максимально функціонально розширене мережне обладнання, не забувши про наявність швидкісного та стабільного підключення до WAN мережі. Якщо використовується декілька вузлів, то рекомендується об'єднати їх у кільце для забезпечення подальшого резервування. На базовому рівні застосовують маршрутизатори з налаштуванням VLAN (одна або декілька) на один рівень розподілу.

На рівні розподілу відбувається маршрутизація трафіку користувача між мережами VLAN і його фільтрація на основі ACL. На цьому рівні описується політика мережі для кінцевих користувачів, формуються широкомовні домени та багатоадресні розсилки. Велика кількість портів забезпечує можливість підключення безлічі вузлів рівня доступу, а інтерфейс SFP надає можливість у використанні електричних або оптичних каналів передачі інформації на нижчих рівнях. Також рекомендоване об'єднання декількох вузлів в кільце.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

До рівня доступу фізично приєднуються самі користувачі. На цьому рівні трафік з користувацьких портів маркується DSCP мітками. Тут застосовуються комутатори з можливістю активації та налагодження послуг VLAN на портах користувачів.

Таблиця 2.1 – Параметри ір адресації.

Мережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	ІР-адреса	Маска	Префікс
Підмережа А	-	193.9.3.0	255.255.255.0	/24
Підмережа В	-	194.9.3.0	255.255.255.0	/24
Маршрутизатор R-9-3-1	Інтерфейс Fa0/0	193.9.3.1	255.255.255.0	/24
	Інтерфейс Fa0/0	194.9.3.1	255.255.255.0	/24
Комутатор SW-9-3-1	Інтерфейс Vlan 1	193.9.3.2	255.255.255.0	/24
	Шлюз за замовчу- ванням	193.9.3.1	255.255.255.0	/24
Комутатор SW-9-3-2	Інтерфейс Vlan 1	194.9.3.2	255.255.255.0	/24
	Шлюз за замовчу- ванням	194.9.3.1	255.255.255.0	/24
Робоча станція WS-9-3-1	Мережний адаптор	DHCP		
	Шлюз за замовчув.			

На рисунку нижче продемонстровано

Дана мережа представлена 1 маршрутизатором та хмарним інтерфейсом, що являє Інтернет. Маршрутизатор в цьому відрізку мережі є частиною ядра, що дозволяє всім пристроям топології отримати доступ до глобальної мережі. Для подальшого надання доступу реалізовано динамічну маршрутизацію протоколом EIGRP (див. рис. 2.2).

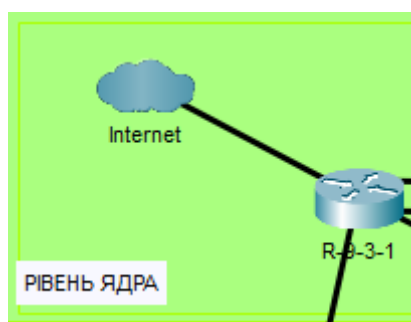


Рисунок 2.2 – Ділянка мережі, що дозволяє доступ до глобальної мережі Інтернет.

Від маршрутизатора R-9-3-1 виходить 1 мережа - MGM. Дана мережа потрібна для роботи сервера Diameter, моніторингу та тестування безпеки мережі. На комутаторах 10 портів є вільними, тобто виступають резервними. Підключення до маршрутизатора та між комутаторами виконане за допомогою витої пари технології Gigabit Ethernet та Fast Ethernet. Всі інші підключення даної мережі реалізовані за допомогою технології Fast Ethernet та витої пари.

2.2 Аналіз інфраструктури системи моніторингу мережі

Серверна інфраструктура – це об’єднаний комплекс обладнання та програмне забезпечення, яке надає можливість ефективної та зручної взаємодії співробітників компанії з інформаційним середовищем та подальшим обміном даними між пристроями.

Підключення до пристрою може здійснюватися або фізично, або шляхом підключення через консольний порт (рядок консолі 0), без введення команд команд, або через протокол TELNET. При чому в останньому випадку, навіть якщо задати IP-адресу на Cisco обладнанні не буде отримано доступ до пристрою (спосіб аутентифікації “line”). Якщо пароль на лінії vty заданий, то пристрій чекатиме тільки введення паролю, що істотно знижує безпеку підключення, так як для входу не потрібно вводити логі (хоча, складність пароля також відіграє важливу роль). При виконанні команди “login local” пристрою, встановивши з’єднання, потрібно буде ввести логін і пароль для входу.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПРОЄКТУ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ СЕРВІСІВ НА ОСНОВІ ПРОТОКОЛУ DIAMETER

3.1 Підбір мережного обладнання

Серверна інфраструктура – це об'єднане в один комплекс обладнання та програмне забезпечення, яке надає можливість ефективної та зручної взаємодії співробітників компанії з інформаційним середовищем та подальшого обміну даними між пристроями. Відмінно налагоджена серверна інфраструктура дозволяє користувачам отримувати своєчасний доступ до файлів та будь-яких даних. Найважливішими критеріями при побудові серверної інфраструктури можна відзначити швидкість відновлення даних, стійкість до відмов і віртуалізацію. Гнучка система дозволяє уникнути втрати інформації та своєчасно отримувати доступ до неї. Відмінно побудована система зберігання даних повинна спростити роботу і допомагати вирішувати багато завдань компанії, дотримуючись важливої деталі у вигляді мережної безпеки.

Правильна організація серверної інфраструктури є дуже важливою складовою ефективної роботи у будь-якій компанії, що має комп'ютерну мережу. При виборі архітектури слід приділити увагу трьом основним напрямкам:

Розподіл ролей. Залежно від навантаження та використовуваних серверних ролей, у компанії вони розподіляються між серверами. Декілька ролей можуть бути поєднані на одному сервері, також одна роль може розподілятися на кілька серверів або дублюватися (резервуватися).

Продуктивність. Важливо вибрати правильну кількість апаратних ресурсів, щоб їх вистачило для відповідних серверних ролей.

Вартість. При виборі комплектуючих потрібно не тільки орієнтуватися на те, щоб не було великих надлишків, оскільки це підвищує витрати.

У ході реалізації спроектованої інфраструктури (комп'ютерної мережі) було прийняте рішення використання мережного обладнання компанії Cisco Systems, inc.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Для реалізації рівня ядра потрібен маршрутизатор, що здатний підтримувати технологію Gigabit Ethernet, та протоколи EIGRP. Для побудови рівня ядра було використано відносно новий маршрутизатор Cisco C1111-8P (рис. 3.1).



Рисунок 3.1 – Cisco C1111-8P.

Маршрутизатор Cisco ISR 1100 8 Ports (C1111-8P) – це легкі і компактні маршрутизатори з можливістю уніфікованого управління різними типами мережі. C1111-8P можуть працювати умовах, де середовище, тепловиділення і низьке енергоспоживання є критичними факторами. Дана модель має підтримку PoE / PoE +

Cisco 1100 Ethernet Series ISR- це маршрутизатори під управлінням Cisco IOS XE, яке дозволяє об'єднати WAN, комплексну продуктивність, провідну та бездротову мережу в одну високопродуктивну платформу. Маршрутизатор відмінно підходить для використання малим і середнім бізнесом.

Базова комплектація Cisco P1111-8P налічує:

- Багатоядерний процесор, який підтримує високопродуктивні WAN мережі;
- Оперативна пам'ять: 4 Гб;
- 8 x 10/100/1000 Ethernet портів для WAN / LAN;
- 1 xGE / SFP комбо порт;
- 1 xGE порт;
- Можливість доступу до консолі через USB-порт;
- Підтримка PoE / PoE +;

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

- Присутній 4 Гб флеш пам'яті;
- Підтримка 3.0 micro-USB порту;

Також є комплектація з гарячою заміною мережевих модулів та резервних джерел живлення.

Широкі можливості керування досягаються з використанням програм CiscoWorks, CiscoView, і CiscoView Stack Management Interface.

При виборі мережного комутатора необхідно звернути увагу на кількість вільних портів Ethernet. Їх має бути достатня кількість. Також необхідно, щоб порти були здатні передавати дані на достатній швидкості і була можливість налаштування VLAN'ів, отже необхідно, щоб комутатор був керованим. Доцільним стане вибір комутатора Cisco CBS350-24P-4G (рис. 3.2).



Рисунок 3.2 – Комутатор Cisco CBS350-24P-4G.

Комутатор Cisco CBS350-24P-4G-EU – це керований комутатор серії Cisco Business 350, який є важливим елементом будь-якої мережі невеликого офісу. Комутатор має інтуїтивно зрозумілу панель, що полегшує конфігурацію мережі, а розширені функції безпеки здатний забезпечити якісну безпеку мережному трафіку. Комутатори Cisco Business 350 дозволяють легко підключати співробітників у невеликих офісах до всіх серверів, принтерів та інших пристроїв, створюючи більш продуктивне робоче місце.

Комутатор Cisco CBS350-24P-4G-EU має 24 порти Gigabit Ethernet, які додатково підтримують живлення PoE з максимальною потужності 195 Вт. Також комутатор має чотири порти SFP та забезпечує загальну пропускну здатність 56 Гбіт/с.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Попереднє налаштування комутатора може здійснюватись за допомогою Cisco Business Dashboard. Це графічний інтерфейс адміністратора від компанії Cisco, що дозволяє легко керувати комутаторами Business 350, а також маршрутизаторами і бездротовими точками доступу. Даний програмний продукт здатний забезпечити контроль над всією корпоративною мережею, що дозволяє контролювати параметри мережевих пристроїв. Інформаційна панель Cisco Business Dashboard автоматично виявляє всі мережі, надаючи повну видимість топології мережі (рис. 3.3).

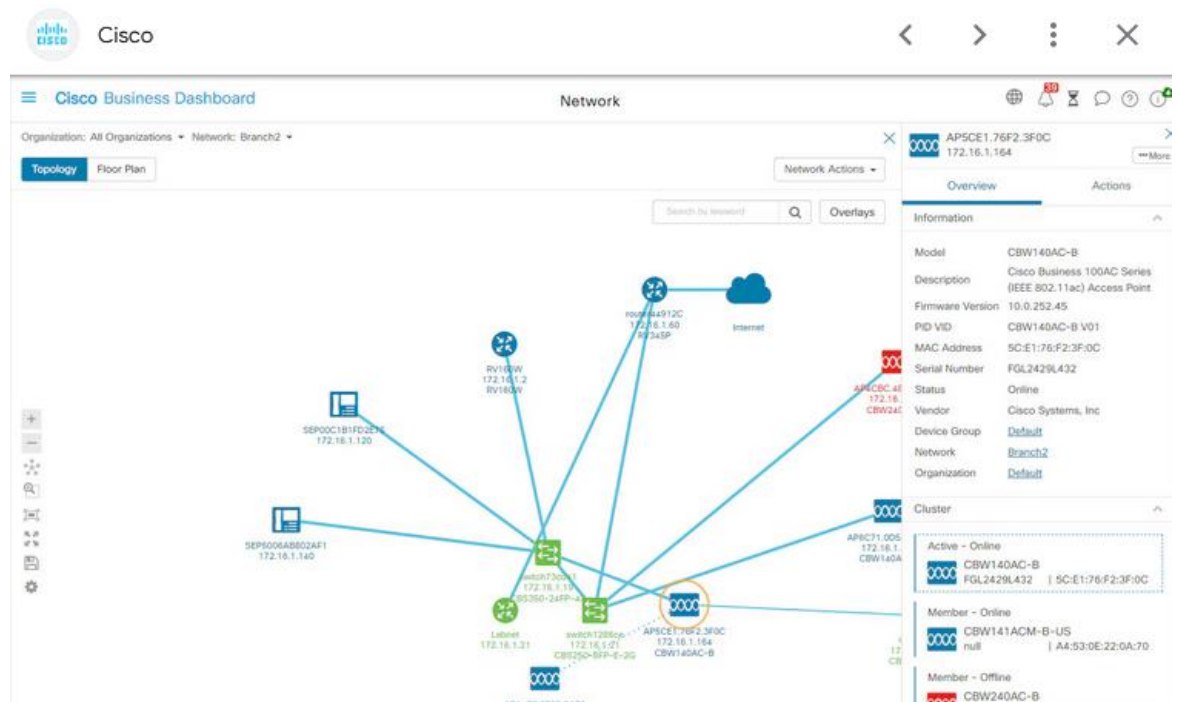


Рисунок 3.3 – Інформаційна панель Cisco Business Dashboard.

Комутатори Cisco CBS350-24P-4G-EU – підтримують високий рівень безпеки. Комутатор використовує інтегровані мережеві рішення, які знижують ризик порушення безпеки, таких як контроль доступу IEEE 802.1X та запобігання атакам DoS. Комутатор містить списки контролю доступу (ACL) для захисту конфіденційних мережевих даних від неавторизованих користувачів. Також підтримується безпечна гостьова мережа, ізолювана від критично важливого для бізнесу мережевого трафіку.

3.2 Налагодження комп'ютерної мережі серверної інфраструктури

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

З метою коректної роботи мережі було здійснено налаштування покрокове налаштування правильних параметрів мережних компонентів.

```
R-9-3-1#configure terminal
R-9-3-1(config)#interface fastEthernet0/0
R-9-3-1(config-if)#description link_to_R-9-2-2
R-9-3-1(config-if)#ip address 192.9.9.3 255.255.255.0
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
R-9-3-1(config)#int fastEthernet1/0
R-9-3-1(config-if)#description link_to_R-9-2-3
R-9-3-1(config-if)#ip address 196.9.3.3 255.255.255.0
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
R-9-3-1(config)#interface fastEthernet1/0
R-9-3-1(config-if)#description link_to_R-9-3-2
R-9-3-1(config-if)#ip address 193.9.2.3 255.255.255.0
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
R-9-3-1(config)#int fastEthernet1/1
R-9-3-1(config-if)#description link_to_R-9-2-3
R-9-3-1(config-if)#ip address 196.9.3.4 255.255.255.0
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
```

Наступним кроком було налаштовані DHCP-сервери для отримання автоматичного IP адресу. Приклад налаштування продемонстровано на R-9-2-3 (рис. 3.4).

```
R-9-2-3 (config) #
R-9-2-3 (config) #ip dhcp excluded-address 196.9.2.1 196.9.2.10
R-9-2-3 (config) #ip dhcp pool LAN-A-Herasymenko
R-9-2-3 (dhcp-config) #network 196.9.2.1 255.255.255.0
R-9-2-3 (dhcp-config) #default-router 196.9.2.1
R-9-2-3 (dhcp-config) #dns-server 8.8.8.8
R-9-2-3 (dhcp-config) #do
R-9-2-3 (dhcp-config) #domain-name herasymenkoA.com
R-9-2-3 (dhcp-config) #end
R-9-2-3 #
R-9-2-3 #
```

Рисунок 3.4 – Приклад налаштування DHCP-сервера.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Наступним кроком здійснюється перевірка отримання адресного простору імен робочими станціями організації (продемонстровано на рис. 3.5 – 3.8).

```
WS-9-3-1> dhcp -r
DDORA IP 195.9.3.102/24 GW 195.9.3.1
WS-9-3-1> █
```

Рисунок 3.5 – Процес отримання адреси від DHCP сервера.

```
WS-9-3-2> dhcp -r
DDORA IP 195.9.3.103/24 GW 195.9.3.1
WS-9-3-2> █
```

Рисунок 3.6– Процес отримання адреси від DHCP сервера.

```
WS-9-3-3> dhcp -r
DDORA IP 195.9.3.104/24 GW 195.9.3.1
WS-9-3-3> █
```

Рисунок 3.7 – Процес отримання адреси від DHCP сервера.

```
WS-9-3-4> dhcp -r
DDORA IP 195.9.3.105/24 GW 195.9.3.1
WS-9-3-4> █
```

Рисунок 3.8 – Процес отримання адреси від DHCP сервера.

Наступним кроком здійснюється перевірка маршрутизації між робочими станціями та компонентами мережі.

```
R-9-3-1#ping 195.9.3.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.9.3.102, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/12 ms
R-9-3-1#
```

Рисунок 3.9 – Перевірка зв'язку маршрутизації, виконання команди ping.

```
R-9-3-1#ping 195.9.3.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.9.3.103, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
R-9-3-1#
```

Рисунок 3.10 – Перевірка зв'язку маршрутизації, виконання команди ping.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

```

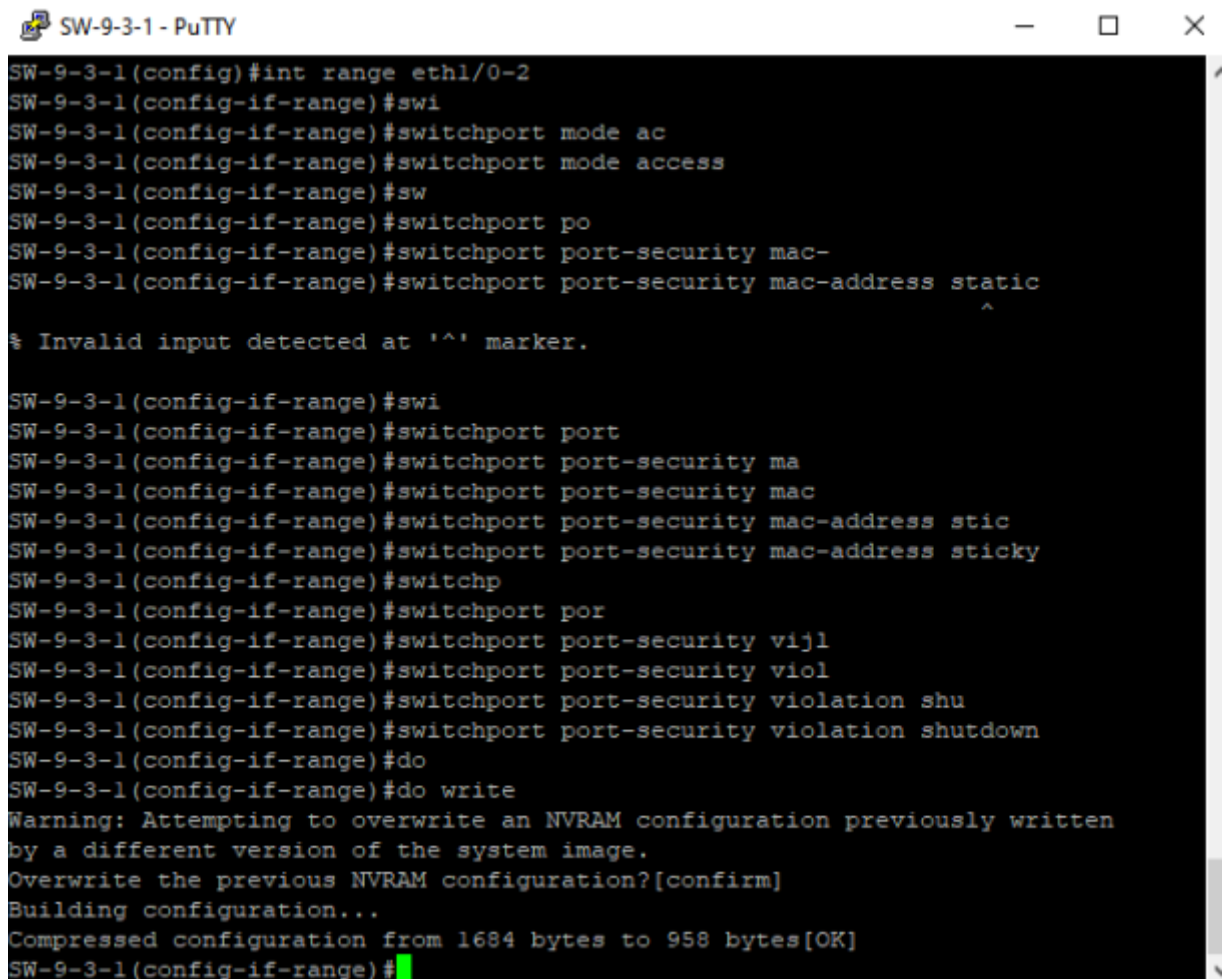
R-9-3-1#ping 195.9.3.104

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.9.3.104, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
R-9-3-1#

```

Рисунок 3.11 – Перевірка зв'язку маршрутизації, виконання команди ping.

Для захисту мережних портів комутаторів було виконано налаштування Port Security для портів до яких підключені робочі станції (рис. 3.12 – 3.15).



```

SW-9-3-1(config)#int range eth1/0-2
SW-9-3-1(config-if-range)#swi
SW-9-3-1(config-if-range)#switchport mode ac
SW-9-3-1(config-if-range)#switchport mode access
SW-9-3-1(config-if-range)#sw
SW-9-3-1(config-if-range)#switchport po
SW-9-3-1(config-if-range)#switchport port-security mac-
SW-9-3-1(config-if-range)#switchport port-security mac-address static
^
% Invalid input detected at '^' marker.

SW-9-3-1(config-if-range)#swi
SW-9-3-1(config-if-range)#switchport port
SW-9-3-1(config-if-range)#switchport port-security ma
SW-9-3-1(config-if-range)#switchport port-security mac
SW-9-3-1(config-if-range)#switchport port-security mac-address stic
SW-9-3-1(config-if-range)#switchport port-security mac-address sticky
SW-9-3-1(config-if-range)#switchp
SW-9-3-1(config-if-range)#switchport por
SW-9-3-1(config-if-range)#switchport port-security vijl
SW-9-3-1(config-if-range)#switchport port-security viol
SW-9-3-1(config-if-range)#switchport port-security violation shu
SW-9-3-1(config-if-range)#switchport port-security violation shutdown
SW-9-3-1(config-if-range)#do
SW-9-3-1(config-if-range)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1684 bytes to 958 bytes[OK]
SW-9-3-1(config-if-range)#

```

Рисунок 3.12 – Налаштування функції безпеки Port Security для портів, до яких підключені робочі станції на комутаторі SW-9-3-1.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

SW-9-3-2#
SW-9-3-2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-9-3-2(config)#int ra
SW-9-3-2(config)#int range eth1/0-2
SW-9-3-2(config-if-range)#swit
SW-9-3-2(config-if-range)#switchport mod
SW-9-3-2(config-if-range)#switchport mode acc
SW-9-3-2(config-if-range)#switchport mode access
SW-9-3-2(config-if-range)#switch
SW-9-3-2(config-if-range)#switchport por
SW-9-3-2(config-if-range)#switchport port-security
SW-9-3-2(config-if-range)#swit
SW-9-3-2(config-if-range)#switchport por
SW-9-3-2(config-if-range)#switchport port-security ma
SW-9-3-2(config-if-range)#switchport port-security mac
SW-9-3-2(config-if-range)#switchport port-security mac-address st
SW-9-3-2(config-if-range)#switchport port-security mac-address sticky
SW-9-3-2(config-if-range)#switch
SW-9-3-2(config-if-range)#switchport por
SW-9-3-2(config-if-range)#switchport port-security vio
SW-9-3-2(config-if-range)#switchport port-security violation shu
SW-9-3-2(config-if-range)#switchport port-security violation shutdown
SW-9-3-2(config-if-range)#do wr
% Ambiguous command: "do wr"
SW-9-3-2(config-if-range)#do write
% Ambiguous command: "do write"
SW-9-3-2(config-if-range)#do write
Building configuration...
Compressed configuration from 1823 bytes to 1029 bytes[OK]
SW-9-3-2(config-if-range)#

```

Рисунок 3.13 – Налаштування функції безпеки Port Security для портів, до яких підключені робочі станції на комутаторі SW-9-3-2.

Інші наявні в мережні комутати налаштовані за аналогічним принципом.

```

SW-9-3-3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-9-3-3(config)#int eth0/1
SW-9-3-3(config-if)#sw
SW-9-3-3(config-if)#switchport mod
SW-9-3-3(config-if)#switchport mode access
SW-9-3-3(config-if)#sw
SW-9-3-3(config-if)#switchport po
SW-9-3-3(config-if)#switchport port-security
SW-9-3-3(config-if)#swi
SW-9-3-3(config-if)#switchport po
SW-9-3-3(config-if)#switchport port-security max
SW-9-3-3(config-if)#switchport port-security maximum 12
SW-9-3-3(config-if)#swi
SW-9-3-3(config-if)#swi
SW-9-3-3(config-if)#switchport po
SW-9-3-3(config-if)#switchport port-security aging time 12
SW-9-3-3(config-if)#swi
SW-9-3-3(config-if)#switchport port-s
SW-9-3-3(config-if)#switchport port-security violation re
SW-9-3-3(config-if)#switchport port-security violation restrict
SW-9-3-3(config-if)#swi
SW-9-3-3(config-if)#switchport po
SW-9-3-3(config-if)#switchport port-security agi
SW-9-3-3(config-if)#switchport port-security aging type ina
SW-9-3-3(config-if)#switchport port-security aging type inactivity
SW-9-3-3(config-if)#ex
SW-9-3-3(config)#err
SW-9-3-3(config)#errdisable re
SW-9-3-3(config)#errdisable recovery ca
SW-9-3-3(config)#errdisable recovery cause pse
SW-9-3-3(config)#errdisable recovery cause psecure-violation
SW-9-3-3(config)#err
SW-9-3-3(config)#errdisable rec
SW-9-3-3(config)#errdisable recovery in
SW-9-3-3(config)#errdisable recovery interval 360
SW-9-3-3(config)#do w

```

Рисунок 3.14 – Налаштування функції безпеки Port Security для портів.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-9-3-3 - PuTTY
SW-9-3-3#QQ^@
Translating "QQ"

Translating "QQ"
% Unknown command or computer name, or unable to find computer address
SW-9-3-3#Q
SW-9-3-3#sh
SW-9-3-3#show po
SW-9-3-3#show por
SW-9-3-3#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Et0/1          12              2              0              Restrict
Et1/0          1              1              0              Shutdown
Et1/1          1              1              0              Shutdown
Et1/2          1              1              0              Shutdown
Et1/3          1              1              0              Shutdown
Et2/0          1              1              0              Shutdown
Et2/1          12              0              0              Restrict
-----
Total Addresses in System (excluding one mac per port)    : 1
Max Addresses limit in System (excluding one mac per port) : 4096

```

Рисунок 3.15 – Таблиця захищених портів.

Наступним кроком здійснена перевірка роботи Port Security. Для цього була додана робоча станція з емуляцією Kali Linux для перевірки роботи Port Security. Візуальна схема підключення словмисної робочої станції продемонстровано на рис. 3.16.

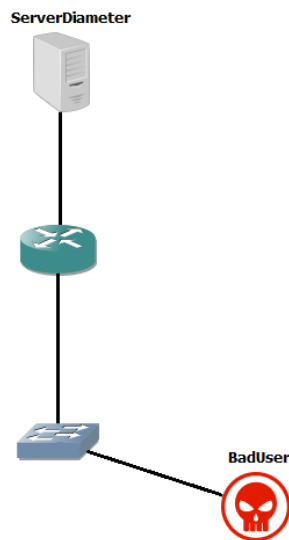


Рисунок 3.16 – Візуальна схема підключення хакерської робочої станції.

Для реалізації атаки було змінено MAC-адресу та здійснено перевірку на маршрутизаторі (рис. 3.17 – 3.19).

```

root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# sudo ip link set dev eth0 down

(root@kali)-[/home/kali]
# macchanger --mac=00:50:79:66:68:08 eth0
Current MAC: 08:00:27:f4:6a:54 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:f4:6a:54 (CADMUS COMPUTER SYSTEMS)
New MAC: 00:50:79:66:68:08 (PRIVATE)

(root@kali)-[/home/kali]
# sudo ip link set dev eth0 up

(root@kali)-[/home/kali]
#

```

Рисунок 3.17 – Змінена MAC-адреса на станції зловмисника.

```

SW-9-3-3#sh po
SW-9-3-3#sh por
SW-9-3-3#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Et0/1         12                2                0                Restrict
Et1/0          1                1                1                Shutdown
Et1/1          1                1                0                Shutdown
Et1/2          1                1                0                Shutdown
Et1/3          1                1                0                Shutdown
Et2/0          1                1                0                Shutdown
Et2/1         12                1                0                Restrict
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 4096
SW-9-3-3#

```

Рисунок 3.18 – В результаті підключення лічильник порушень безпеки збільшився на 1 для інтерфейсу, до якого було під'єднано сторонню робочу станцію.

```

SW-9-3-3#show port-security int eth1/0
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0050.7966.6828:1
Security Violation Count : 1

```

Рисунок 3.19 – Інформація про користувача, який тільки що підключився до маршрутизатора.

Наступними кроками була спроба реалізувати атаку MAC-Flooding та дослідити роботу засобів захисту комутатора від цієї атаки (рис. 3.20 – 3.22).

```
(root@kali)-[/home/kali]
# ping 195.9.3.3
PING 195.9.3.3 (195.9.3.3) 56(84) bytes of data.
64 bytes from 195.9.3.3: icmp_seq=1 ttl=255 time=4.39 ms
64 bytes from 195.9.3.3: icmp_seq=2 ttl=255 time=1.10 ms
64 bytes from 195.9.3.3: icmp_seq=3 ttl=255 time=0.960 ms
64 bytes from 195.9.3.3: icmp_seq=4 ttl=255 time=1.03 ms
64 bytes from 195.9.3.3: icmp_seq=5 ttl=255 time=0.897 ms
64 bytes from 195.9.3.3: icmp_seq=6 ttl=255 time=1.12 ms
64 bytes from 195.9.3.3: icmp_seq=7 ttl=255 time=0.944 ms
64 bytes from 195.9.3.3: icmp_seq=8 ttl=255 time=1.19 ms
64 bytes from 195.9.3.3: icmp_seq=9 ttl=255 time=1.40 ms
64 bytes from 195.9.3.3: icmp_seq=10 ttl=255 time=0.978 ms
64 bytes from 195.9.3.3: icmp_seq=11 ttl=255 time=1.22 ms
^C
— 195.9.3.3 ping statistics —
11 packets transmitted, 11 received, 0% packet loss, time 10059ms
rtt min/avg/max/mdev = 0.897/1.383/4.388/0.960 ms

(root@kali)-[/home/kali]
#
```

Рисунок 3.20 – Перевірка підключення.

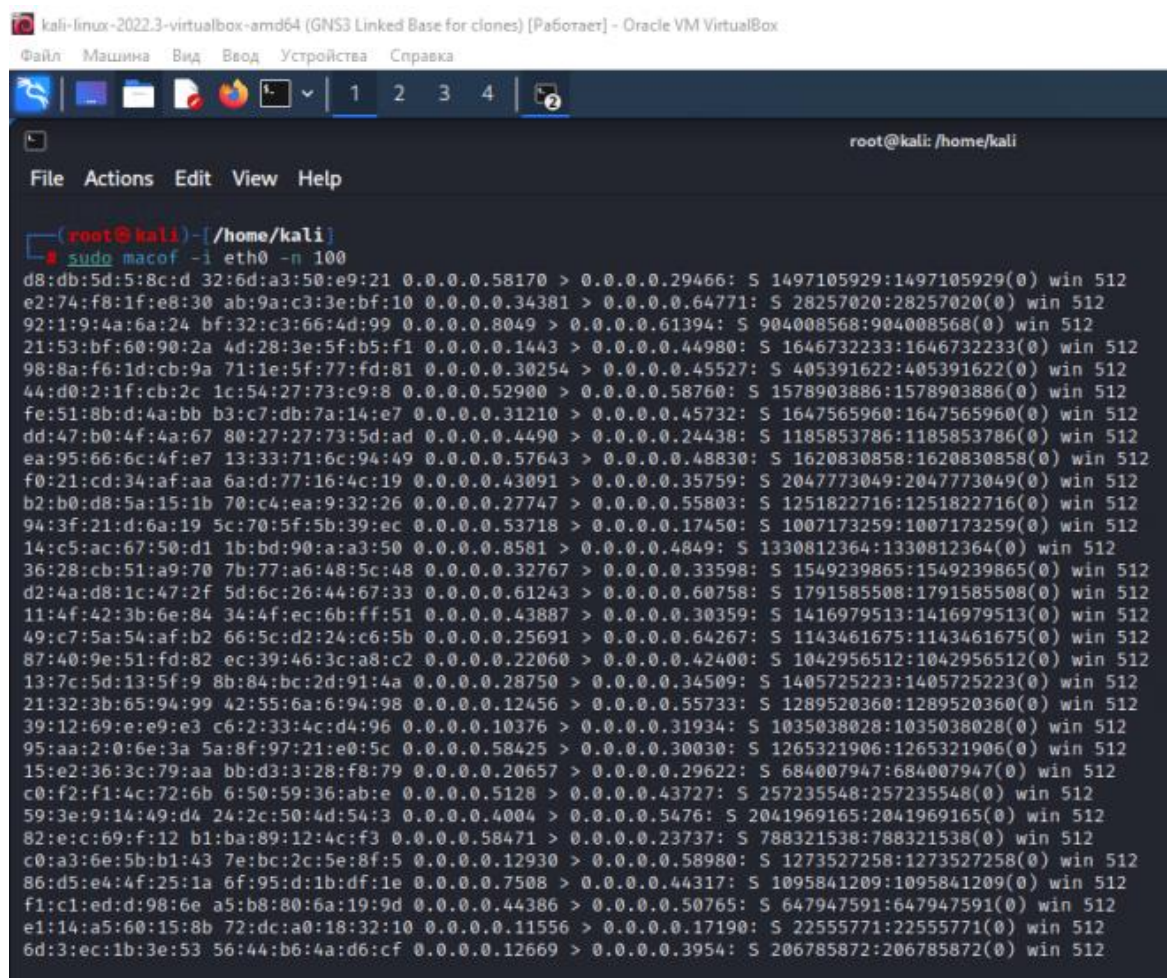


Рисунок 3.21 – Приведення атаки Mac-Flooding.

```
SW-9-3-3#
*Jan 9 15:12:47.155: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 3628.cb51.a970 on port Ethernet2/1.
SW-9-3-3#
```

Рисунок 3.22 – В результаті проведення атаки комутатор відключив потр до якого під’єднався злочинець.

3.3 Встановлення та налаштування серверної інфраструктури Diameter.

Встановлення та налаштування freeDiameter та MySQL модулів продемонстровано на рисунках рис. 3.23 – 3.40.

```
Herasymentko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
root@Server-Diameter: /
root@Server-Diameter:/# sudo apt-get install libdate-time-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans linux-image-6.5.0-18-generic
  linux-modules-6.5.0-18-generic linux-modules-extra-6.5.0-18-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libalgorithm-c3-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl
  libclass-c3-perl libclass-c3-xs-perl libclass-data-inheritable-perl
  libclass-inspector-perl libclass-method-modifiers-perl
  libclass-singleton-perl libclass-xsaccessor-perl libdata-optlist-perl
  libdate-time-locale-perl libdate-time-timezone-perl libdevel-callchecker-perl
  libdevel-caller-perl libdevel-lexalias-perl libdevel-stacktrace-perl
  libdynamloader-functions-perl libeval-closure-perl libexception-class-perl
  libfile-sharedir-perl libmodule-implementation-perl libmodule-runtime-perl
  libmro-compat-perl libnamespace-autoclean-perl libnamespace-clean-perl
  libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl
  libparams-classify-perl libparams-util-perl
  libparams-validationcompiler-perl libreadonly-perl libref-util-perl
  libref-util-xs-perl librole-tiny-perl libspecio-perl libsub-exporter-perl
  libsub-exporter-progressive-perl libsub-identify-perl libsub-install-perl
  libsub-name-perl libsub-quote-perl libvariable-magic-perl libxstring-perl
```

Рисунок 3.23 – Встановлення пакунку libdate-time-perl.

```
Herasymentko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
root@Server-Diameter: /
E: Unable to locate package libdbd-mysql-perl
root@Server-Diameter:/# sudo apt-get install libdbd-mysql-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans linux-image-6.5.0-18-generic
  linux-modules-6.5.0-18-generic linux-modules-extra-6.5.0-18-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libmysqlclient21 mysql-common
The following NEW packages will be installed:
  libdbd-mysql-perl libmysqlclient21 mysql-common
0 upgraded, 3 newly installed, 0 to remove and 132 not upgraded.
Need to get 1 397 kB of archives.
After this operation, 7 178 kB of additional disk space will be used.
Do you want to continue? [Y/n] yes
Get:1 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 mysql-common all 5.8+
  1.0.8 [7 212 B]
Get:2 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libmysqlclien
  t21 amd64 8.0.37-0ubuntu0.22.04.3 [1 302 kB]
Get:3 http://ua.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libdbd-my
  sql-perl amd64 4.050-5ubuntu0.22.04.1 [87,6 kB]
Fetched 1 397 kB in 1s (2 016 kB/s)
```

Рисунок 3.24 – Встановлення пакунку libdbd-mysql-perl з метою коректної роботи SQL бази даних в середовищі linux.

```

Herasymenko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 20 Jun
root@Server-Diametr: /
root@Server-Diametr:/#
root@Server-Diametr:/# sudo apt-get install libdigest-hmac-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans linux-image-6.5.0-18-generic
  linux-modules-6.5.0-18-generic linux-modules-extra-6.5.0-18-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  libdigest-hmac-perl
0 upgraded, 1 newly installed, 0 to remove and 132 not upgraded.
Need to get 10,8 kB of archives.
After this operation, 28,7 kB of additional disk space will be used
Get:1 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 libdigest-hmac-perl 1.04+dfsg-1 [10,8 kB]
Fetched 10,8 kB in 0s (106 kB/s)
Selecting previously unselected package libdigest-hmac-perl.
(Reading database ... 257358 files and directories currently installed.)
Preparing to unpack .../libdigest-hmac-perl_1.04+dfsg-1_all.deb ...
Unpacking libdigest-hmac-perl (1.04+dfsg-1) ...
Setting up libdigest-hmac-perl (1.04+dfsg-1) ...
Processing triggers for man-db (2.10.2-1) ...
root@Server-Diametr:/#

```

Рисунок 3.25 – Встановлення пакунку libdigest-hmac-perl.

```

Herasymenko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 20 Jun 18:45
root@Server-Diametr: /
root@Server-Diametr:/# sudo apt-get install libdatetime-format-rfc3339-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans linux-image-6.5.0-18-generic
  linux-modules-6.5.0-18-generic linux-modules-extra-6.5.0-18-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  libdatetime-format-rfc3339-perl
0 upgraded, 1 newly installed, 0 to remove and 132 not upgraded.

```

Рисунок 3.26 – Встановлення пакунку.

```

Herasymenko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 20 Jun 18:45
root@Server-Diametr: /
root@Server-Diametr:/# sudo apt-get install eapoltest
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans linux-image-6.5.0-18-generic
  linux-modules-6.5.0-18-generic linux-modules-extra-6.5.0-18-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  eapoltest
0 upgraded, 1 newly installed, 0 to remove and 132 not upgraded.

```

Рисунок 3.27 – Встановлення пакунку.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

```
Herasyenko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal

root@Server-Diametr:~# sudo apt -y install libfreediameter-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbfdcore6 libfdproto6 libgcrpt20-dev libgmp-dev libgmpxx4ldbl
  libgnutls-dane0 libgnutls-openssl27 libgnutls28-dev libgnutls30
  libgnutlsxx28 libgpg-error-dev libidn-dev libidn11-dev libidn2-dev
  libp11-kit-dev libsctp-dev libsctp1 libtasn1-6-dev libtasn1-doc libunbound8
  nettle-dev pkg-config
Suggested packages:
  libgcrpt20-doc gmp-doc libgmp10-doc libmpfr-dev gnutls-bin gnutls-doc idn
  p11-kit-doc lksctp-tools
The following NEW packages will be installed:
  libbfdcore6 libfdproto6 libfreediameter-dev libgcrpt20-dev libgmp-dev
  libgmpxx4ldbl libgnutls-dane0 libgnutls-openssl27 libgnutls28-dev
  libgnutlsxx28 libgpg-error-dev libidn-dev libidn11-dev libidn2-dev
  libp11-kit-dev libsctp-dev libsctp1 libtasn1-6-dev libtasn1-doc libunbound8
  nettle-dev pkg-config
The following packages will be upgraded:
  libgnutls30
1 upgraded, 22 newly installed, 0 to remove and 190 not upgraded.
Need to get 4 733 kB/5 700 kB of archives.
After this operation, 16,3 MB of additional disk space will be used.
Get:1 http://ua.archive.ubuntu.com/ubuntu jammy/universe amd64 libfdproto6 amd64
1.2.1-8build1 [75,5 kB]
Get:2 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 libsctp1 amd64 1.0.19
+dfsg-1build1 [9 370 B]
Get:3 http://ua.archive.ubuntu.com/ubuntu jammy/universe amd64 libbfdcore6 amd64
1.2.1-8build1 [143 kB]
Get:4 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libunbound8 a
md64 1.13.1-1ubuntu5.5 [399 kB]
Get:5 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgnutls-dan
e0 amd64 3.7.3-4ubuntu1.5 [22,6 kB]
Get:6 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgnutls-ope
nssl27 amd64 3.7.3-4ubuntu1.5 [22,8 kB]
Get:7 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgnutlsxx28
amd64 3.7.3-4ubuntu1.5 [16,3 kB]
Get:8 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 libidn2-dev amd64 2.3
```

Рисунок 3.28 – Встановлення пакунку.

```
Herasyenko-KB-20-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal

root@Server-Diametr:~#
Get:21 http://ua.archive.ubuntu.com/ubuntu jammy/universe amd64 libfreediameter-
dev amd64 1.2.1-8build1 [48,2 kB]
Get:22 http://ua.archive.ubuntu.com/ubuntu jammy/main amd64 libtasn1-doc all 4.1
8.0-4build1 [305 kB]
Fetched 4 733 kB in 1s (6 311 kB/s)
(Reading database ... 206345 files and directories currently installed.)
Preparing to unpack .../libgnutls30_3.7.3-4ubuntu1.5_amd64.deb ...
Unpacking libgnutls30:amd64 (3.7.3-4ubuntu1.5) over (3.7.3-4ubuntu1.4) ...
Setting up libgnutls30:amd64 (3.7.3-4ubuntu1.5) ...
Selecting previously unselected package libfdproto6:amd64.
(Reading database ... 206345 files and directories currently installed.)
Preparing to unpack .../00-libfdproto6_1.2.1-8build1_amd64.deb ...
Unpacking libfdproto6:amd64 (1.2.1-8build1) ...
Selecting previously unselected package libsctp1:amd64.
Preparing to unpack .../01-libsctp1_1.0.19+dfsg-1build1_amd64.deb ...
Unpacking libsctp1:amd64 (1.0.19+dfsg-1build1) ...
Selecting previously unselected package libbfdcore6:amd64.
Preparing to unpack .../02-libbfdcore6_1.2.1-8build1_amd64.deb ...
Unpacking libbfdcore6:amd64 (1.2.1-8build1) ...
Selecting previously unselected package libunbound8:amd64.
Preparing to unpack .../03-libunbound8_1.13.1-1ubuntu5.5_amd64.deb ...
Unpacking libunbound8:amd64 (1.13.1-1ubuntu5.5) ...
Selecting previously unselected package libgnutls-dane0:amd64.
Preparing to unpack .../04-libgnutls-dane0_3.7.3-4ubuntu1.5_amd64.deb ...
Unpacking libgnutls-dane0:amd64 (3.7.3-4ubuntu1.5) ...
Selecting previously unselected package libgnutls-openssl27:amd64.
Preparing to unpack .../05-libgnutls-openssl27_3.7.3-4ubuntu1.5_amd64.deb ...
Unpacking libgnutls-openssl27:amd64 (3.7.3-4ubuntu1.5) ...
Selecting previously unselected package libgnutlsxx28:amd64.
Preparing to unpack .../06-libgnutlsxx28_3.7.3-4ubuntu1.5_amd64.deb ...
Unpacking libgnutlsxx28:amd64 (3.7.3-4ubuntu1.5) ...
Selecting previously unselected package libidn2-dev:amd64.
Preparing to unpack .../07-libidn2-dev_2.3.2-2build1_amd64.deb ...
Unpacking libidn2-dev:amd64 (2.3.2-2build1) ...
Selecting previously unselected package libp11-kit-dev:amd64.
Preparing to unpack .../08-libp11-kit-dev_0.24.0-6build1_amd64.deb ...
Unpacking libp11-kit-dev:amd64 (0.24.0-6build1) ...
Selecting previously unselected package libtasn1-6-dev:amd64.
Preparing to unpack .../09-libtasn1-6-dev_4.18.0-4build1_amd64.deb ...
```

Рисунок 3.29 – Встановлення пакунку.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Preparing to unpack .../18-libidn11-dev_1.38-4ubuntu1_amd64.deb ...
Unpacking libidn11-dev:amd64 (1.38-4ubuntu1) ...
Selecting previously unselected package libscpt-dev:amd64.
Preparing to unpack .../19-libscpt-dev_1.0.19+dfsg-1build1_amd64.deb ...
Unpacking libscpt-dev:amd64 (1.0.19+dfsg-1build1) ...
Selecting previously unselected package libfreediameter-dev.
Preparing to unpack .../20-libfreediameter-dev_1.2.1-8build1_amd64.deb ...
Unpacking libfreediameter-dev (1.2.1-8build1) ...
Selecting previously unselected package libtasn1-doc.
Preparing to unpack .../21-libtasn1-doc_4.18.0-4build1_all.deb ...
Unpacking libtasn1-doc (4.18.0-4build1) ...
Setting up libgnutls-openssl27:amd64 (3.7.3-4ubuntu1.5) ...
Setting up libtasn1-doc (4.18.0-4build1) ...
Setting up libunbound8:amd64 (1.13.1-1ubuntu5.5) ...
Setting up libgmpxx4ldbl:amd64 (2:6.2.1+dfsg-3ubuntu1) ...
Setting up libgpg-error-dev (1.43-3) ...
Setting up libfdproto6:amd64 (1.2.1-8build1) ...
Setting up pkg-config (0.29.2-1ubuntu3) ...
Setting up libgnutlsxx28:amd64 (3.7.3-4ubuntu1.5) ...
Setting up libidn2-dev:amd64 (2.3.2-2build1) ...
Setting up libscpt1:amd64 (1.0.19+dfsg-1build1) ...
Setting up libtasn1-6-dev:amd64 (4.18.0-4build1) ...
Setting up libidn-dev:amd64 (1.38-4ubuntu1) ...
Setting up libp11-kit-dev:amd64 (0.24.0-6build1) ...
Setting up libgnutls-dane0:amd64 (3.7.3-4ubuntu1.5) ...
Setting up libidn11-dev:amd64 (1.38-4ubuntu1) ...
Setting up libgmp-dev:amd64 (2:6.2.1+dfsg-3ubuntu1) ...
Setting up nettle-dev:amd64 (3.7.3-1build2) ...
Setting up libfdcore6:amd64 (1.2.1-8build1) ...
Setting up libgcrypt20-dev (1.9.4-3ubuntu3) ...
Setting up libscpt-dev:amd64 (1.0.19+dfsg-1build1) ...
Setting up libgnutls28-dev:amd64 (3.7.3-4ubuntu1.5) ...
Setting up libfreediameter-dev (1.2.1-8build1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for install-info (6.8-4build1) ...
root@Server-Diametr:~#

```

Рисунок 3.30 – Налаштування бібліотек freeDiameter. Цей посібник було написано для Xubuntu 22.04 LTS, який постачається з пакетами бібліотеки freeDiameter v1.2.1. Відомо, що інші дистрибутиви, такі як Debian 10, також пропонують стандартну підтримку freeDiameter v1.2.1 на основі пакетів, тому очікується, що вони будуть так само сумісні.

```

root@Server-Diametr:~#
root@Server-Diametr:~#
root@Server-Diametr:~# sudo apt -y install opensips-diameter-module
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

```

Рисунок 3.31 – Встановлення модуля OpenSIPS "aaa_diameter".

OpenSIPS — це багатофункціональний, багатоцільовий SIP-сервер сигналізації, який використовується операторами, телекомунікаційними компаніями та ITSP для таких рішень, як житлові платформи класу 4/5, транкінгові/оптові, корпорати-

вні/віртуальні RBX-рішення, граничні контролери сеансів, сервери додатків, переднє завантаження Балансери, платформи IMS, кол-центри та багато інших – перегляньте повний набір функцій.

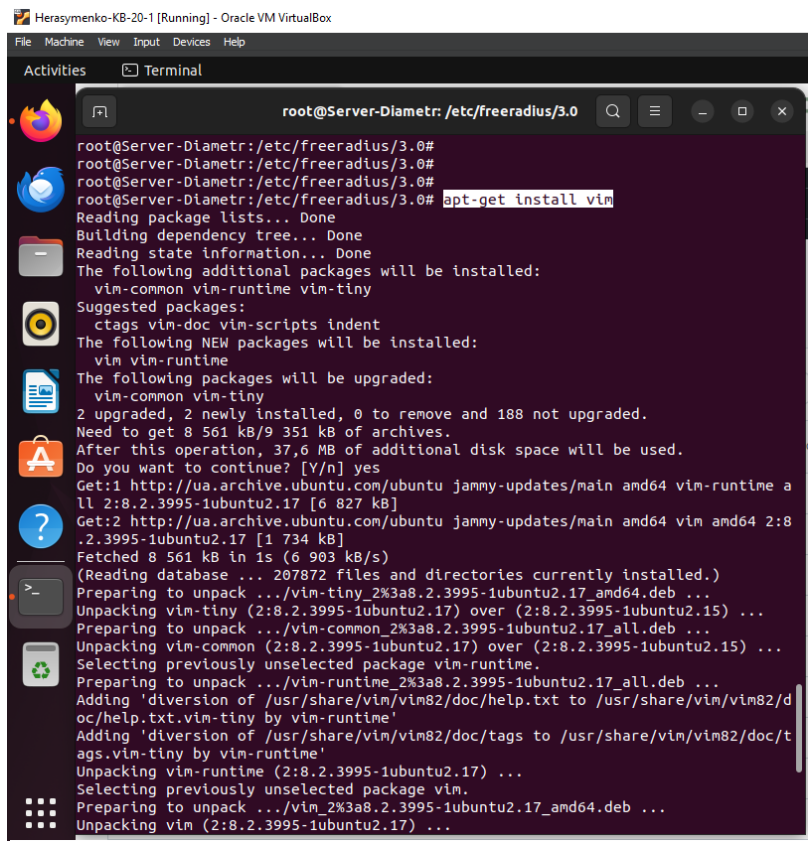


Рисунок 3.32 – apt-get install vim.

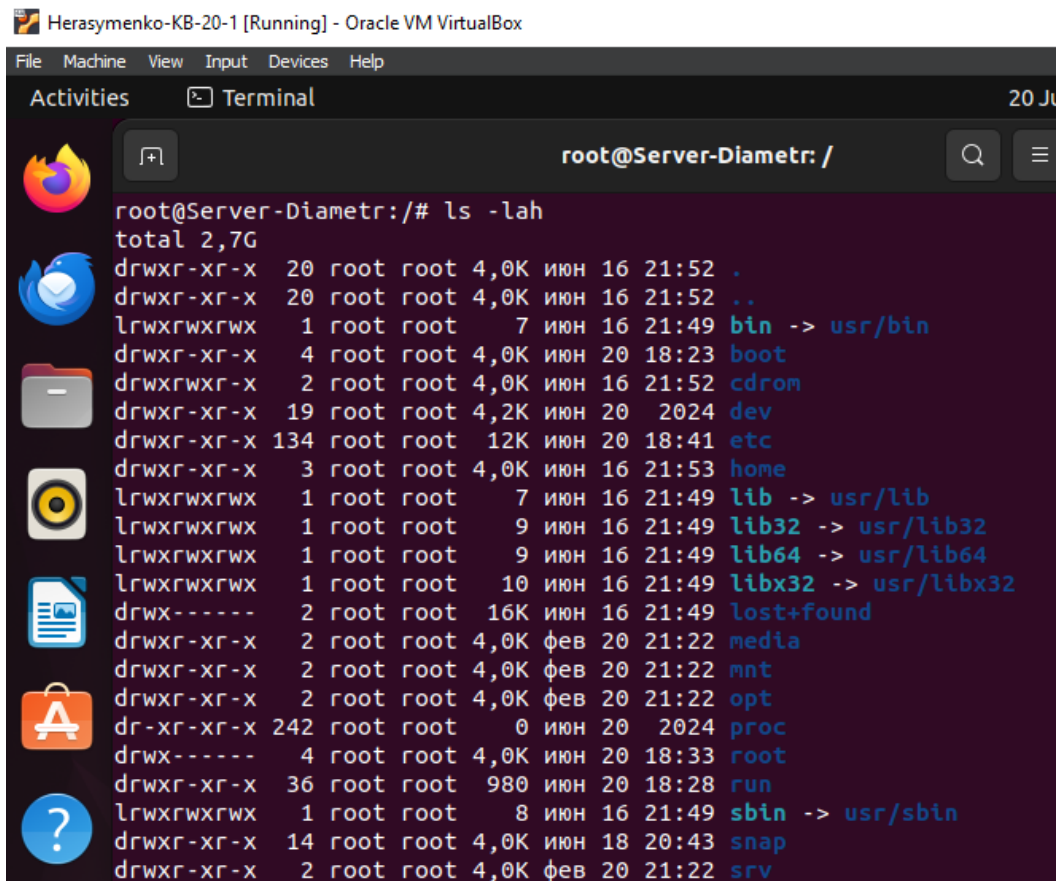


Рисунок 3.33 – Перевірка встановлених пакунків.

Активация та старт протоколу Diameter

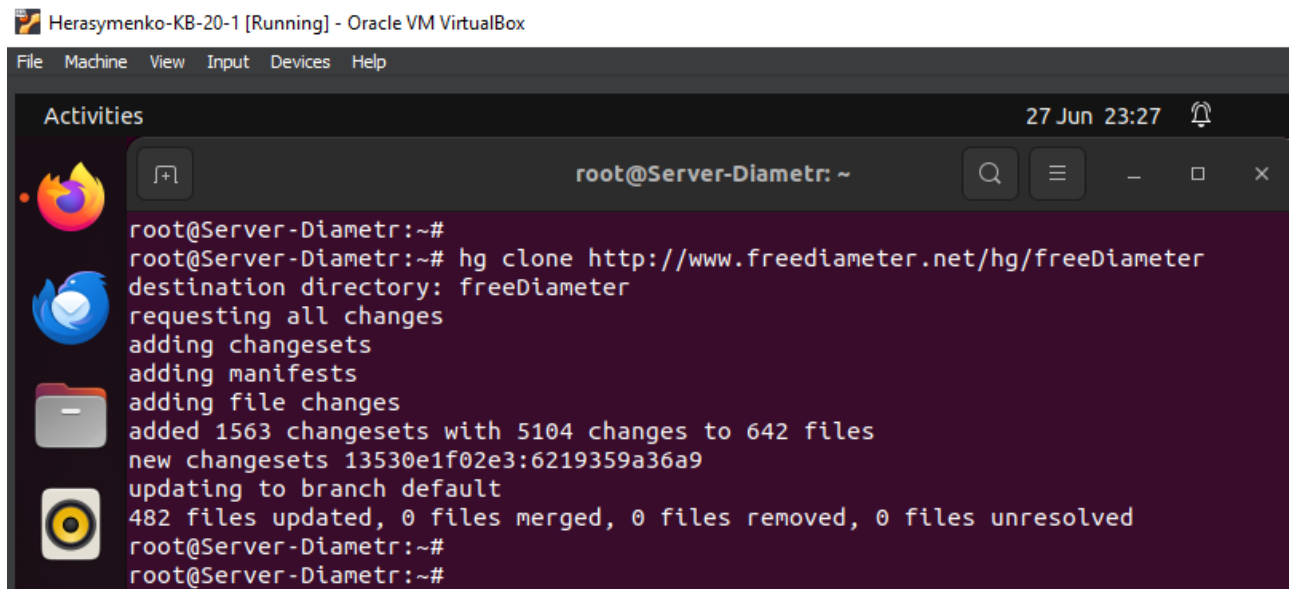
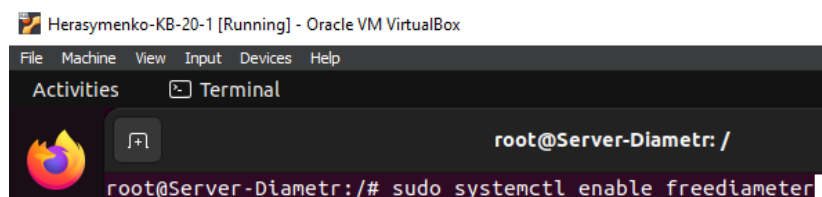


Рисунок 3.34 – Процес копіювання необхідних пакетів.



		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Рисунок 3.35 – Перезапуск протоколу.

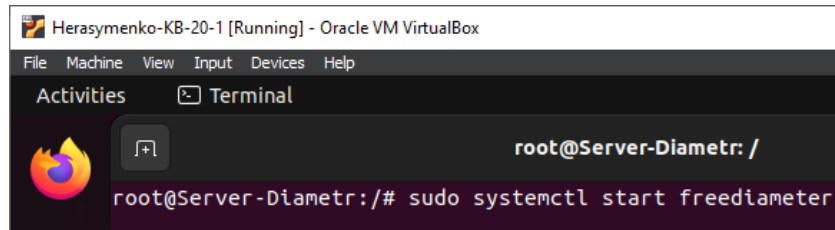


Рисунок 3.36 – Запуск сервера.

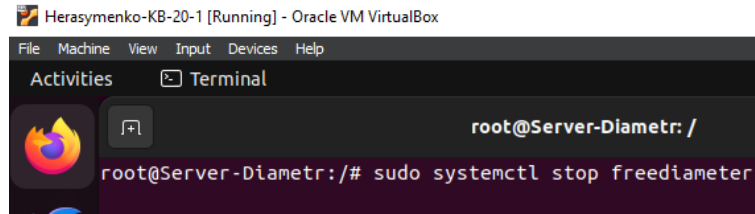


Рисунок 3.37 – Зупинка сервера.

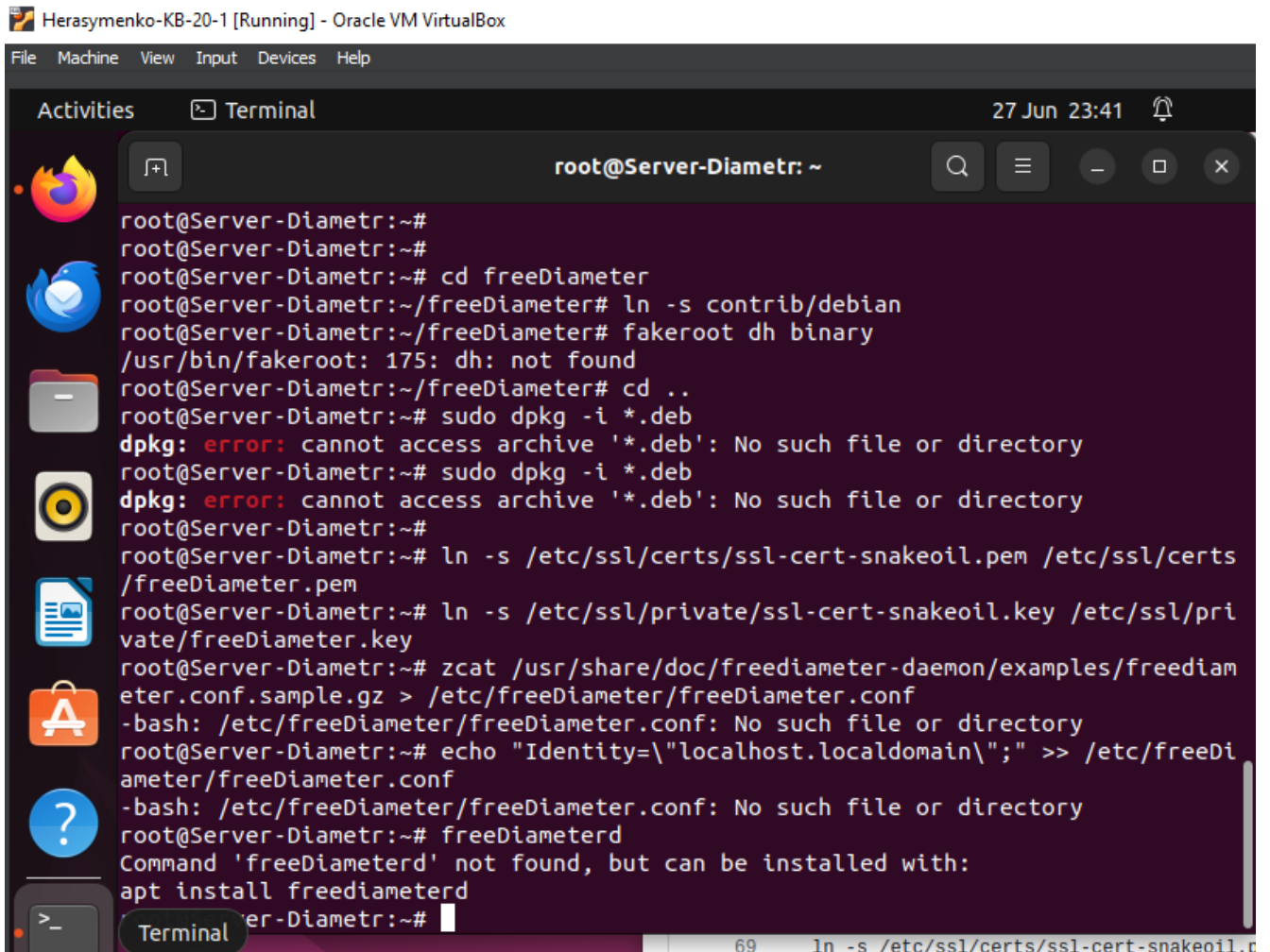


Рисунок 3.38 – Інсталяція пакетів.

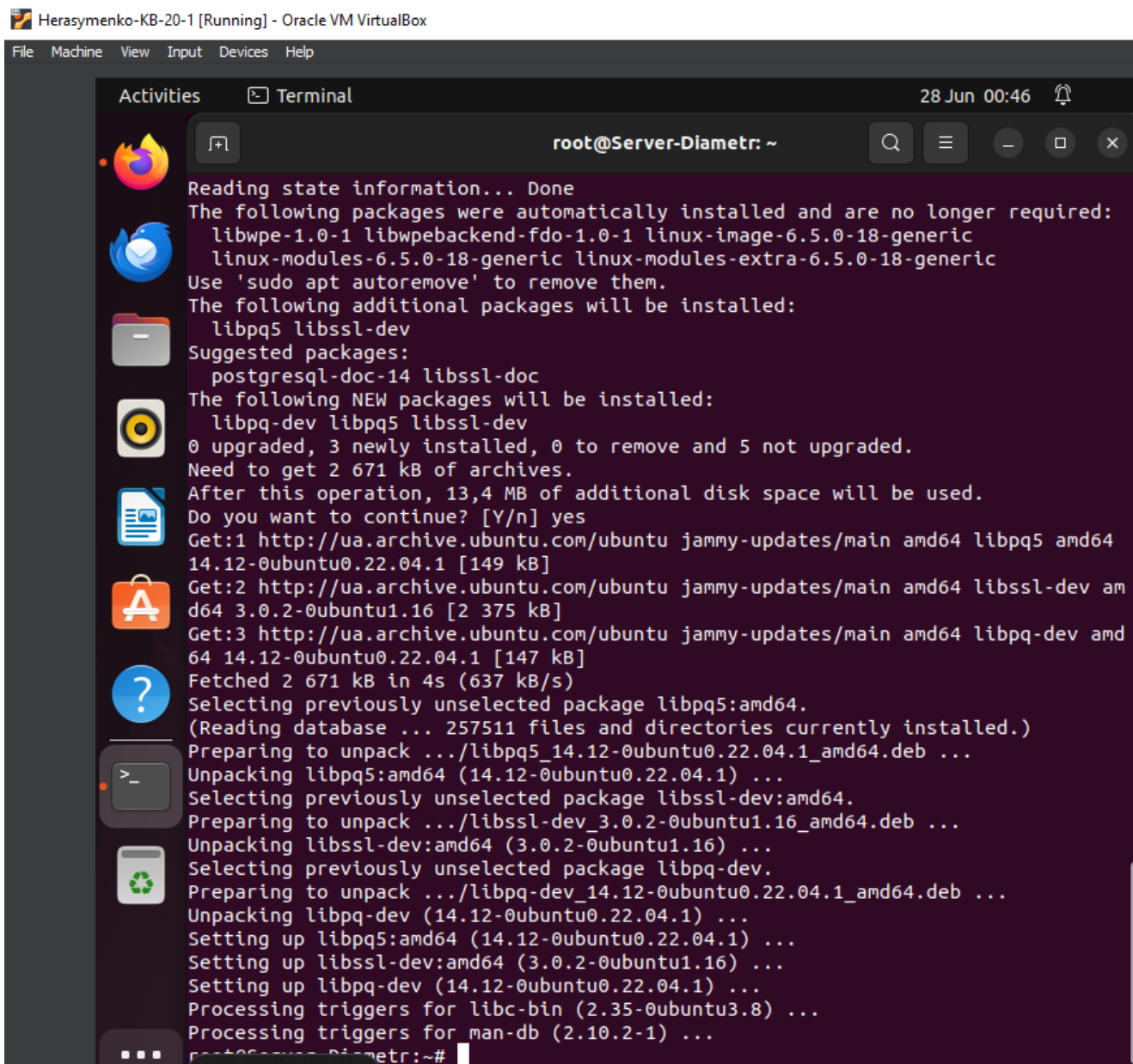


Рисунок 3.39 – Встановлення пакетів, що допоможуть коректно працювати мережі.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

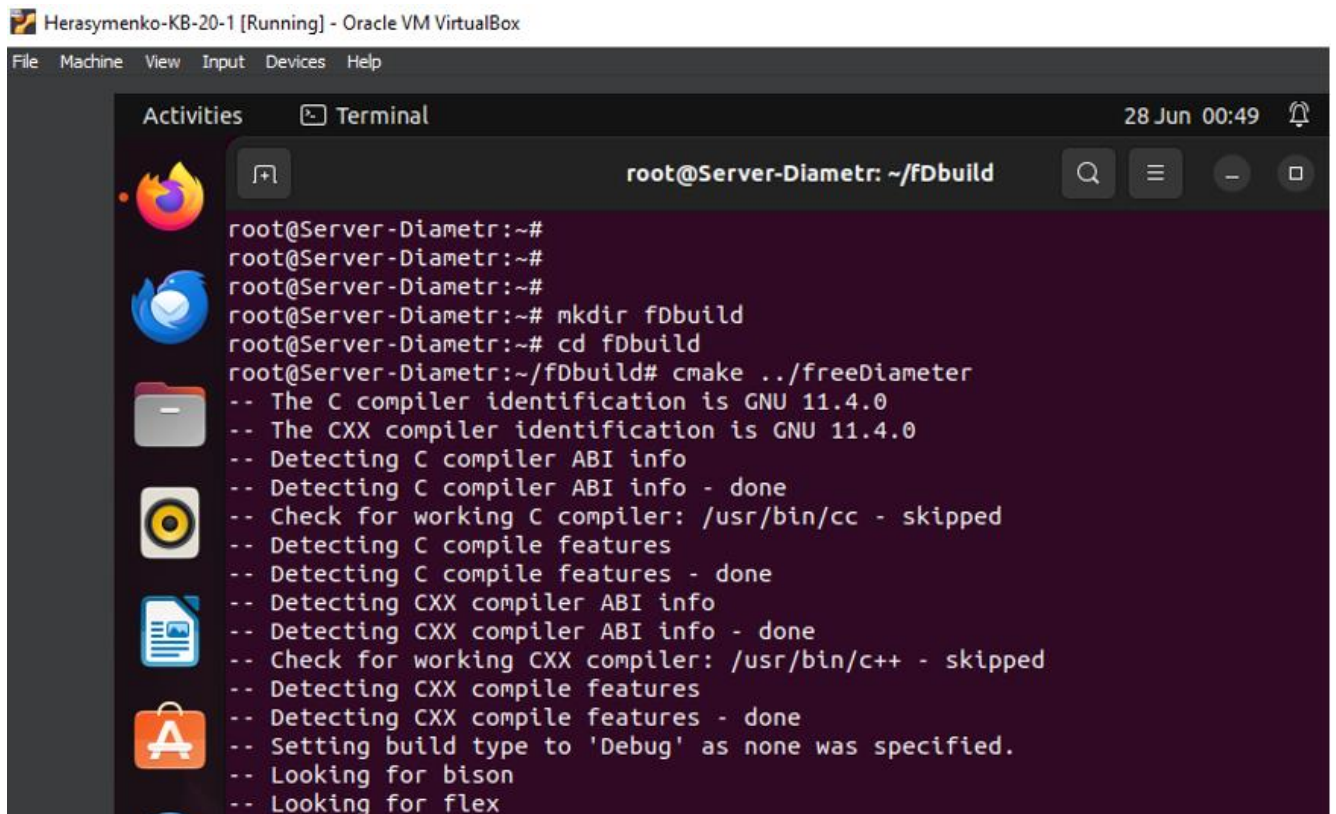


Рисунок 3.40 – Створення директорії Diameter.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В ході виконання випускної кваліфікаційної роботи було спроектовано серверну інфраструктуру автентифікації, авторизації та обліку сервісів на основі протоколу Diameter. Серверну інфраструктуру реалізовано за допомогою емулятора GNS3. Досліджено особливості функціонування та захисту протоколу Port Security. Також було проаналізовано та вирішено проблеми безпеки та вразливості під час побудови мережі.

У першому розділі було опрацьовано теоретичні відомості щодо протоколу RADIUS, який в подальшому перетворився в протокол Diameter. У першому підрозділі було розглянуто основи побудови та принцип функціонування протоколів AAA, зокрема протоколу RADIUS та Diameter. Було розглянуто проблемні місця протоколів AAA. Описано роботу, функціонування протоколів AAA. Встановлено, що при практичному використанні сервер AAA з базою даних профілів користувачів та даних конфігурації взаємодіє з клієнтами AAA, які знаходяться в мережових компонентах, таких як NAS і маршрутизатори, щоб забезпечити розподіл AAA послуги. Попередньо опрацьовано принцип роботи серверної інфраструктури. В ході опрацювання, встановлено, що один сервер AAA може діяти як централізована адміністративна точка керування для кількох клієнтів AAA, які містяться в NAS і мережових компонентах від різних постачальників. Проаналізовано функціонал та застосування протоколу RADIUS у комп'ютерних мережах. Результатом аналізу отримано висновок, що клієнт RADIUS знаходиться на NAS і комується через мережу з сервером RADIUS, який працює на хості комп'ютера. А сервер RADIUS може служити проксі-клієнтом для RADIUS або інших серверів автентифікації. Розглянуто основи, принцип роботи та побудови серверної інфраструктури на основі протоколу DIAMETER. З'ясовано, що протокол Diameter є сеансово-орієнтованим протоколом, тобто для кожного автентифікованого користувача, існує сеанс між ініціалізацією запиту автентифікації/авторизації та сервером Diameter. Перевірена спільна робота серверів Diameter з серверами Radius та здійснено порівняння роботи серверів на теоретичному рівні.

Також було розглянуто нововведення у протоколі Diameter та порівняно функціональні можливості та особливості функціонування протоколів при проектуванні та побудові мережних систем. Було встановлено, що протокол Diameter є удосконаленням протоколу RADIUS.

У другому розділі було спроектовано загальну топологію мережі та проекти локальних ділянок, розроблено схему адресації з урахуванням. Проведено аналіз можливих загроз мережі відповідно до протоколів, які будуть функціонувати у спроектованій мережі.

У третьому розділі здійснено вибір відповідного програмного продукту серверної інфраструктури обладнання мережі. Було налаштовано мережу у відповідності до проекту та перевірено правильність функціонування налаштованого протоколу.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)" [Електронний ресурс] – <https://datatracker.ietf.org/doc/html/rfc2865>
2. C. Rigney, W. Willats, P. Calhoun, "RADIUS Extensions" [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ietf.org/rfc/rfc2869.txt>
3. Pat R. Calhoun, Glen Zorn, Ping Pan, Haseeb Akhtar, "Diameter Framework Document" [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ietf.org/proceedings/50/I-D/1id-abstracts.txt>
4. Pat R. Calhoun, Haseeb Akhtar, Jari Arkko, Erik Guttman, Allan C. Rubens, Glen Zorn, "Diameter Base Protocol" [Електронний ресурс] –
5. Pat R. Calhoun, Stephen Farrell, William Bulley, "Diameter CMS Security Application" [Електронний ресурс] – <https://www.ietf.org/archive/id/draft-ietf-aaa-diameter-cms-sec-02.txt>
6. Pat R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application" [Електронний ресурс] – <https://datatracker.ietf.org/doc/rfc4004/>
7. C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)" [Електронний ресурс] – <https://www.scirp.org/reference/referencespapers?referenceid=1631785>
8. J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)" [Електронний ресурс] – <https://datatracker.ietf.org/doc/html/rfc1510>
9. M. Beadles, D. Mitton, "Criteria for Evaluating Network Access Server Protocols" [Електронний ресурс] – <https://ftp.ripe.net/rfc/rfc2989.html>
10. D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service) Protocol" [Електронний ресурс] – <https://www.rfc-editor.org/rfc/rfc2749.html>
11. Glass, S., Hiller, T., Jacobs, S. and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements" [Електронний ресурс] – <http://www.ietf.org/rfc/rfc2977.txt>
12. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч.1 / підг. А. А. Єфіменко. – Житомир: ЖДТУ, 2018. – 112 с.
13. Коренівський Д. Г. Дестабілізуючий ефект параметричного білого шуму в неперервних та дискретних динамічних системах : монографія / Д. Г. Коренівський. — 2-ге вид., доп. — Київ : Сузір'я, 2006. — 111 с.
14. Одом Уенделл. Офіційне керівництво Cisco з підготовки до сертифікаційних екзаменів CCNA ICND2 200-101: маршрутизація і комутація, акад. вид. / пер. з англ.

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігурації та лістинги пристроїв мережі

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-9-3-1
SW-9-3-1(config)#no ip domain-lookup
SW-9-3-1(config)#interface FastEthernet 0/3
SW-9-3-1(config-if)#description LINK-TO-SW-9-3-2
SW-9-3-1(config-if)#duplex half
SW-9-3-1(config-if)#speed 100
SW-9-3-1(config-if)#exit
SW-9-3-1(config)#exit
```

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-9-3-2
SW-9-3-2(config)#no ip domain-lookup
SW-9-3-2(config)#interface FastEthernet 0/24
SW-9-3-1(config-if)#description LINK-TO-SW-9-20-1
SW-9-3-1(config-if)#duplex half
SW-9-3-1(config-if)#speed 100
SW-9-3-1(config-if)#exit
SW-9-3-1(config)#exit
```

```
SW-9-3-2>enable
SW-9-3-2#configure terminal
SW-9-3-2(config)#interface FastEthernet 0/21
SW-9-3-2(config-if)#description LINK-TO-R-9-3-1
SW-9-3-2(config-if)#duplex full
SW-9-3-2(config-if)#speed 100
SW-9-3-2(config-if)#exit
SW-9-3-2(config)#exit
```

```
Router#enable
Router#configure terminal
Router(config)#hostname R-9-3-1
R-9-3-1(config)#interface FastEthernet 0/0
R-9-3-1(config-if)#description LINK-T0-SW-9-3-2
R-9-3-1(config-if)#duplex full
R-9-3-1(config-if)#speed 100
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
```

```
SW-9-3-1>enable
```

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-9-3-1#clock set 11:06:10 may 05 2024
SW-9-3-1#configure terminal
SW-9-3-1 (config)#clock timezone EET 2
SW-9-3-1 (config)#clock summertime EET reccuring last Monday may 3:00 last monday
march 3:00
SW-9-3-1 (config)#banner motd
# Connection to SW-9-3-1#

```

```

SW-9-3-1>enable
SW-9-3-1#configure terminal
SW-9-3-1 (config)#service password-encryption
SW-9-3-1(config)#enable secret adminpass9
SW-9-3-1 (config)#line vty 0 4
SW-9-3-1 (config-line)#password adminpass1
SW-9-3-1 (config-line)#login
SW-9-3-1 (config-line)#transport input telnet
SW-9-3-1 (config-line)#logout-warning 30
SW-9-3-1 (config-line)#absolute-timeout 10
SW-9-3-1 (config-line)#logging synchronous
SW-9-3-1 (config-line)#exit
SW-9-3-1 (config)#exit

```

```

SW-9-3-2>enable
SW-9-3-2#clock set 10:50:30 may 03 2024
SW-9-3-2#configure terminal
SW-9-3-2(config)#clock timezone EET 2
SW-9-20-2(config)#clock summertime EET reccuring last Monday may 3:00 last mon-
day march 3:00
SW-9-3-2(config)#banner motd # Connection to SW-9-3-2#

```

```

SW-9-3-2>enable
SW-9-3-2#configure terminal
SW-9-3-2(config)#username admin20 privilege 15 secret adminpass20
SW-9-3-2(config)#username technic20 privilege 1 secret technicpass20
SW-9-3-2(config)#enable secret adminpass9
SW-9-3-2(config)#ip domain-name mynet.net
SW-9-3-2(config)#crypto key generate rsa general-keys modulus 1344
SW-9-3-2(config)#ip ssh version 1
SW-9-3-2(config)#line vty 0 4
SW-9-3-2(config-line)#login local
SW-9-3-2(config-line)#transport input ssh
SW-9-3-2(config-line)#transport output ssh
SW-9-3-2(config-line)#logout-warning 30

```

		Герасименко Б. М.			ККИКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

```
SW-9-3-2(config-line)#absolute-timeout 10
SW-9-3-2(config-line)#logging synchronous
SW-9-3-2(config-line)#exit
SW-9-3-2(config)#exit
```

```
SW-9-3-2>enable
SW-9-3-2#configure terminal
SW-9-3-2 (config)#login block-for 150 attempts 5 within 5
SW-9-3-2(config)#login delay 10
SW-9-3-2(config)#login on-failure log
SW-9-3-2(config)#login on-success log
SW-9-3-2(config)#ip ssh time-out 20
SW-9-3-2(config)#ip ssh authentication-retries 5
SW-9-3-2 (config)#ip ssh maxstartups 5
SW-9-3-2(config)#ip ssh logging events
SW-9-3-2(config)#exit
SW-9-3-2 #exit
```

```
R-9-3-1>enable
R-9-3-1#clock set 11:13:10 may 25 2024
R-9-3-1#configure terminal
R-9-3-1(config)#clock timezone EET 2
R-9-3-1 (config)#clock summertime EET reccuring last Monday may 3:00 last monday
march 3:00
R-9-3-1 (config)#banner motd
# Connection to R-9-3-1#
```

```
R-9-3-1>enable
R-9-3-1#configure terminal
R-9-3-1(config)#username admin20 privilege 15 secret adminpass20
R-9-3-1(config)#username technic20 privilege 1 secret technicpass20
R-9-3-1(config)#enable secret adminpass9
R-9-3-1(config)#ip domain-name mynet.net
R-9-3-1(config)#crypto key generate rsa general-keys modulus 1344
R-9-3-1(config)#ip ssh version 2
R-9-3-1 (config)#line vty 0 4
R-9-3-1 (config-line)#login local
R-9-3-1 (config-line)#transport input ssh
R-9-3-1 (config-line)#transport output ssh
R-9-3-1(config-line)#logout-warning 30
R-9-3-1 (config-line)#absolute-timeout 10
R-9-3-1 (config-line)#logging synchronous
R-9-3-1 (config-line)#exit
R-9-3-1 (config)#exit
R-9-3-1#exit
```

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-9-3-2
SW-9-3-2(config)#no ip domain-lookup
SW-9-3-2 (config)#banner motd
# Connection to SW-9-3-2#
SW-9-3-2(config)#interface FastEthernet 0/1
SW-9-3-2 (config-if)#description LINK-TO-R-9-3-1
SW-9-3-2 (config-if)#duplex full
SW-9-3-2 (config-if)#speed 100
SW-9-3-2 (config-if)#exit
SW-9-3-2 (config)#exit

```

```

R-9-3-1>enable
R-9-3-1#configure terminal
R-9-3-1 (config)#login block-for 150 attempts 5 within 5
R-9-3-1(config)#login delay 10
R-9-3-1(config)#login on-failure log
R-9-3-1(config)#login on-success log
R-9-3-1(config)#ip ssh time-out 20
R-9-3-1(config)#ip ssh authentication-retries 5
R-9-3-1 (config)#ip ssh maxstartups 5
R-9-3-1(config)#ip ssh logging events
R-9-3-1 (config)#exit
R-9-3-1 #exit

```

```

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-9-3-1
SW-9-3-1(config)#no ip domain-lookup
SW-9-3-1 (config)#banner motd
# Connection to SW-9-3-1#
SW-9-3-1(config)#interface FastEthernet 0/1
SW-9-3-1 (config-if)#description LINK-TO-R-9-3-1
SW-9-3-1 (config-if)#duplex full
SW-9-3-1 (config-if)#speed 100
SW-9-3-1 (config-if)#exit
SW-9-3-1 (config)#exit

```

```

Router#enable
Router#configure terminal
Router(config)#hostname R-9-3-2
R-9-3-2(config)#banner motd

```

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```
#Connection to R-9-3-3#
R-9-3-2(config)#interface FastEthernet 0/1
R-9-3-2(config-if)#description LINK-T0-SW-9-3-2
R-9-3-2(config-if)#duplex full
R-9-3-2(config-if)#speed 100
R-9-3-2(config-if)#no shutdown
R-9-3-2(config-if)#exit
```

```
Router#enable
Router#configure terminal
R-9-3-1(config)#interface FastEthernet 0/0
R-9-3-1(config-if)#description LINK-T0-SW-9-20-2
R-9-3-1(config-if)#duplex full
R-9-3-1(config-if)#speed 100
R-9-3-1(config-if)#no shutdown
R-9-3-1(config-if)#exit
```

```
R-9-3-1>enable
R-9-3-1#configure terminal
R-9-3-1 (config)#interface fa2/1
R-9-3-1 (config-if)#description LINK-TO- R-9-3-2
R-9-3-1 (config-if)# bandwidth 1280
R-9-3-1 (config-if)#no shutdown
R-9-3-1 (config-if)#exit
R-9-3-1 (config)#exit
```

```
R-9-3-2>enable
R-9-3-2#configure terminal
R-9-3-2(config)#banner motd
# Connection to R-9-3-2#
R-9-3-2 (config)#interface fa2/1
R-9-3-2 (config-if)#description LINK-TO- R-9-20-1
R-9-3-2 (config-if)#clock rate 19200
R-9-3-2 (config-if)# bandwidth 1280
R-9-3-2 (config-if)#no shutdown
R-9-3-2 (config-if)#exit
R-9-3-2 (config)#exit
```

```
R-9-3-3>enable
R-9-3-3#configure terminal
Router(config)#hostname R-9-3-3
R-9-3-3(config)#banner motd
# Connection to R-9-3-3#
R-9-3-3(config)#interface fa2/0
R-9-3-3(config-if)#description LINK-TO- R-9-3-1
```

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

R-9-3-3(config-if)#clock rate 64000
R-9-3-3 (config-if)# bandwidth 320
R-9-3-3 (config-if)#no shutdown
R-9-3-3 (config-if)#exit
R-9-3-3 (config)#exit

Маршрутизатор R-9-3-1 (Інтерфейс Fa0/1)

MAC-адреса: 001b.d5f0.3EBF

MAC-адресу інтерфейсу розбиваємо на дві однакові частини: : 00-1b-d5 та f0-3e-bf

Значення біту G/L змінюємо на 1: 00000010

Старший байт після зміни у шістнадцятковому форматі: 00000010₂ → 02₁₆

Формуємо номер вузла: 021b:d5ff:fef0:3ebf

Номер мережі: FE80:0000:0000:0000::

Відповідно IP-адреса версії 6 має вигляд:

у основному форматі: FE80:0000:0000:0000:021b:D5FF:FEF0:3EBF/64

у скороченому форматі: FE80::21B:D5FF:FEF0: 3EBF/64

Комутатор SW-9-3-1 (Інтерфейс vlan1)

MAC-адреса: 0019.AADB.56C0

Значення біту G/L змінюємо на 1: 00000010

Старший байт після зміни у шістнадцятковому форматі: 02₁₆

Формуємо номер вузла: 0219:AAFF:FEDB:56C0

Номер мережі: FE80:0000:0000:0000::

Відповідно IP-адреса версії 6 має вигляд:

у основному форматі: FE80:0000:0000:0000:0219:AAFF:FEDB:56C0/64

у скороченому форматі: FE80::219:AAFF:FEDB:56C0/64

Підмережа R-9-3-1 – R-9-3-2 (Підмережа С):

Маршрутизатор R-9-3-1(Інтерфейс Se0/3/0)

Відповідно IP-адреса версії 6 має вигляд: FE80::1

Маршрутизатор R-9-3-2(Інтерфейс Se0/1/0)

Відповідно IP-адреса версії 6 має вигляд: FE80::2

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Підмережа R-9-3-2 – R-9-3-3 (Підмережа D):

Маршрутизатор R-9-3-2(Інтерфейс fa2/1)

Відповідно IP-адреса версії 6 має вигляд: FE80::3

Маршрутизатор R-9-3-3(Інтерфейс fa2/2)

Відповідно IP-адреса версії 6 має вигляд: FE80::4

SW-9-3-1>enable

SW-9-3-1 (config)#interface Vlan1

SW-9-3-1(config-if)#ipv6 address 2001:9:20:A::2/64

SW-9-3-1(config-if)#ipv6 address FE80::219:AAFF:FEDB:56C0 link-local

SW-9-3-1 (config-if)#no shutdown

SW-9-3-1 (config-if)#exit

SW-9-3-1(config-if)#ipv6 route ::/0 2001:9:20:A::1

R-9-3-1>enable

R-9-3-1#configure terminal

R-9-3-1(config)#interface FastEthernet 0/1

R-9-3-1(config-if)#description LAN_A

R-9-3-1(config-if)# ipv6 address 2001:9:20:A::1/64

R-9-3-1(config-if)# ipv6 address FE80::21B:D5FF:FEF0:3EBF link-local

R-1(config-if)#no shutdown

R-1(config-if)#exit

SW-9-3-2>enable

SW-9-3-2 (config)#interface Vlan 1

SW-9-3-2(config-if)#ipv6 address 2001:9:20:B::2/64

SW-9-3-2(config-if)#ipv6 address FE80::9E4E:20FF:FE23:7540 link-local

SW-9-3-2 (config-if)#no shutdown

SW-9-3-2 (config-if)#exit

SW-9-3-2(config-if)#ipv6 route ::/0 2001:9:20:B::1

R-9-3-1>enable

R-9-3-1#configure terminal

R-9-3-1(config)#interface FastEthernet 0/0

R-9-3-1(config-if)#description LAN_B

R-9-3-1(config-if)# ipv6 address 2001:9:20:B::1/64

R-9-3-1(config-if)# ipv6 address FE80::21B:D5FF:FEF0:3EBE link-local

R-1(config-if)#no shutdown

R-1(config-if)#exit

R-9-2-1>enable

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

R-9-2-1#configure terminal
R-9-2-1 (config)#ipv6 unicast-routing
R-9-2-1 (config)#interface fa1/1
R-9-2-1 (config-if)#ipv6 address 2001:9:20:C::1/64
R-9-2-1 (config-if)#ipv6 address fe80::1 link-local
R-9-2-1 (config-if)#exit
R-9-2-1 (config)#exit

```

```

R-9-3-2>enable
R-9-3-2#configure terminal
R-9-3-2 (config)#ipv6 unicast-routing
R-9-3-2 (config)#interface f0/1
R-9-3-2(config-if)#ipv6 address 2001:9:20:C::2/64
R-9-3-2(config-if)#ipv6 address fe80::2 link-local
R-9-3-2(config-if)#exit
R-9-3-2(config)#ipv6 route ::/0
R-9-3-2 (config)#exit

```

```

R-9-3-1>enable
R-9-3-1#configure terminal
R-9-3-1 (config)#ipv6 unicast-routing
R-9-3-1 (config)#interface fa0/0
R-9-3-1 (config-if)#ipv6 address 2001:9:20:D::1/64
R-9-3-1 (config-if)#ipv6 address fe80::3 link-local
R-9-3-1 (config-if)#exit
R-9-3-1 (config)#exit

```

```

R-9-3-3>enable
R-9-3-3#configure terminal
R-9-3-3 (config)#ipv6 unicast-routing
R-9-3-3 (config)#interface fa0/1
R-9-3-3(config-if)#ipv6 address 2001:9:20:D::2/64
R-9-3-3(config-if)#ipv6 address fe80::4 link-local
R-9-3-3(config-if)#exit
R-9-3-3(config)#ipv6 route ::/0
R-9-3-3 (config)#exit

```

		Герасименко Б. М.			ККІКБ.КР.Б – 125 – 02 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		66